



Guía para desarrolladores

Amazon Route 53



Versión de API 2013-04-01

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Route 53: Guía para desarrolladores

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es Amazon Route 53?	1
Cómo funciona el registro de dominios	3
se dirige el tráfico de Internet a su sitio web o aplicación web	4
Información general de cómo configurar Amazon Route 53 para dirigir el tráfico de Internet de su dominio	5
Cómo dirige Amazon Route 53 el tráfico de su dominio	6
Cómo verifica Amazon Route 53 el estado de los recursos	8
Conceptos de Amazon Route 53	10
Conceptos de registro de dominios	11
Conceptos del sistema de nombres de dominio (DNS)	12
Conceptos de plano de datos y control	18
Conceptos de comprobación de estado	19
Primeros pasos con Amazon Route 53	20
Acceso a Amazon Route 53	21
AWS Identity and Access Management	21
Precios y facturación de Amazon Route 53	22
Trabajando con AWS SDKs	22
Introducción	24
Configuración	24
Inscríbase en una Cuenta de AWS	25
Creación de un usuario con acceso administrativo	25
Descargar herramientas	27
Enrutamiento del tráfico de DNS a un sitio web estático de Amazon S3	27
Requisitos previos	28
Paso 1: Dirija el tráfico de DNS de su dominio al depósito de su sitio web	29
Paso 2: Pruebe su sitio web	31
Dirija el tráfico de DNS a una CloudFront distribución	31
Requisitos previos	32
Paso 1: Dirija el tráfico de DNS de su dominio a su distribución CloudFront	32
Integración con otros servicios de	36
Registro, monitorización y etiquetado	36
Enrutar el tráfico a otros recursos AWS	37
Formato de nombres de dominio DNS	40
Formateo de nombres de dominio para el registro de nombres de dominio	40

Formato de nombres de dominio para zonas alojadas y registros	40
Uso de un asterisco (*) en nombres de zonas alojadas y registros	41
Formato de nombres de dominio internacionalizados	42
Registro y administración de dominios	45
Registro de nuevos dominios	46
Registrar un nuevo dominio	47
Valores que especifican cuando registra o transfiere un dominio	53
Valores que Amazon Route 53 devuelve cuando registra un dominio	60
Visualización del estado de registro de un dominio	62
Actualización de la configuración de un dominio	63
Actualización de la información de contacto y la propiedad de un dominio	64
Activación o desactivación de la protección de privacidad para la información de contacto para un dominio	73
Activación o desactivación de la renovación automática de un dominio	78
Bloqueo de un dominio para impedir la transferencia no autorizada a otro registrador	79
Ampliación del periodo de registro de un dominio	80
Actualización de los servidores de nombres para utilizar otro registrador	81
Adición o modificación de servidores de nombres y registros de conexión de un dominio	82
Renovar el registro de un dominio	86
Restauración de un dominio caducado o eliminado	90
Sustitución de la zona alojada para un dominio	93
Transferencia de dominios	93
Elija el tipo de transferencia	95
Lista de verificación previa a la transferencia	97
Transferencia a Route 53	101
Problemas de transferencia comunes	121
Transferencia desde Route 53	124
Cómo transferir a una cuenta de AWS diferente	130
Estado de la transferencia	134
Impacto de la transferencia en la fecha de caducidad del dominio	137
Reenvío de los emails de autorización y confirmación	139
Actualización de la dirección de email	140
Reenvío de emails	140
Configurar DNSSEC para un dominio	146
Información general acerca de cómo DNSSEC protege su dominio	146
Requisitos previos y valores máximos para configurar DNSSEC para un dominio	148

Añadir claves públicas para un dominio	149
Eliminar claves públicas de un dominio	150
Búsqueda del registrador	151
Visualizar información sobre dominios	152
Eliminación de un registro de nombre de dominio	154
Ponerse en contacto con AWS Support sobre problemas de registro de dominios	157
Ponerte en contacto con AWS Support cuando puedas iniciar sesión en tu AWS cuenta	158
Ponerte en contacto con AWS Support cuando no puedes iniciar sesión en tu AWS cuenta	159
Descargar un informe de facturación de dominios	159
Dominios que puede registrar con Amazon Route 53	161
Índice de dominios de nivel superior compatibles	162
Dominios de nivel superior genéricos	165
Dominios geográficos de nivel superior	445
Configuración de Amazon Route 53 como servicio DNS	510
Establecer Route 53 como servicio DNS de un dominio existente	511
Establecer Route 53 como el servicio DNS para un dominio que se está utilizando	511
Establecer Route 53 como el servicio DNS de un dominio inactivo	521
Configuración del direccionamiento de DNS para un nuevo dominio	526
Direccionamiento del tráfico a sus recursos	527
Direccionamiento del tráfico de subdominios	528
Uso de zonas alojadas	535
Trabajar con zonas públicas alojadas	535
Uso de zonas alojadas privadas	568
Migración de una zona alojada a otra cuenta de AWS	583
Uso de registros	594
Elección de una política de enrutado	596
Elección entre registros de alias y sin alias	622
Tipos de registros de DNS admitidos	626
Creación de registros con la consola de Amazon Route 53	648
Permisos del conjunto de registros de recursos	651
Valores que especifica	652
Creación de registros mediante la importación de un archivo de zona	752
Editar registros	755
Eliminar registros	756
Descripción de registros	757

Configuración de la firma de DNSSEC	759
Activar la firma de DNSSEC y establecer una cadena de confianza	761
Desactivar la firma de DNSSEC	772
Trabajar con claves administradas por el cliente	777
Trabajar con claves de firma de claves () KSKs	778
Administración de claves KMS y ZSK en Route 53	780
Pruebas de inexistencia de DNSSEC en Route 53	782
Solución de problemas de firma de DNSSEC	783
Uso de AWS Cloud Map para crear registros y comprobaciones de estado	784
Restricciones y comportamientos de DNS	784
Tamaño de respuesta máximo	784
Procesamiento de sección de Authoritative	785
Procesamiento de la sección Additional	785
Temas relacionados	785
Flujo de tráfico	786
Ventajas del flujo de tráfico	786
Crear y administrar políticas de tráfico	788
Creación de una política de tráfico	788
Valores que especifica cuando crea una política de tráfico	791
Visualización de un mapa que muestra el efecto de la configuración de geoproximidad	801
Creación de versiones adicionales de una política de tráfico	805
Creación de una política de tráfico con un documento JSON	808
Consultar versiones de políticas de tráfico y los registros de políticas asociados	811
Eliminación de versiones de una política de tráfico y políticas de tráfico	815
Creación y administración de registros de política	818
Creación de registros de política	819
Valores que especifica al crear o actualizar un registro de política	821
Actualización de registros de política	823
Eliminación de registros de política	824
¿Qué es VPC Resolver?	827
Resolución de consultas de DNS entre y tu red VPCs	830
Cómo se reenvían las consultas DNS de su red a VPC Resolver	833
Cómo reenvían los puntos de conexión de Resolver las consultas de DNS de su red a su red VPCs	836
Consideraciones al crear puntos de conexión de entrada y salida	844
Disponibilidad y escalado del solucionador de VPC Route 53	848

Introducción a Route 53 VPC Resolver	850
Reenviar las consultas de DNS entrantes a tu VPCs	852
Configuración del enrutamiento entrante	852
Valores que se especifican al crear o editar puntos de conexión de entrada	853
Administración de puntos de conexión de entrada	857
Reenvío de consultas de DNS de salida a su red	860
Configuración del enrutamiento saliente	861
Valores que se especifican al crear o editar puntos de conexión de salida	862
Valores que se especifican al crear o editar reglas	865
Administración de puntos de conexión de salida	868
Administración de reglas de reenvío	870
Tutorial sobre las reglas de delegación de Resolver	879
Pasos para la delegación saliente	879
Tipos de delegación	880
Activar de la validación de DNSSEC	885
Enrutar el tráfico de Internet a sus AWS recursos	887
API de Amazon API Gateway	887
Requisitos previos	888
Configuración de Route 53 para dirigir el tráfico a un punto de conexión de interfaz de API Gateway	889
CloudFront Distribución en Amazon	893
Requisitos previos	894
Configuración de Amazon Route 53 para enrutar el tráfico a una CloudFront distribución	895
EC2 Instancia de Amazon	897
Requisitos previos	898
Configuración de Amazon Route 53 para enrutar el tráfico a una EC2 instancia de Amazon	898
Servicio de App Runner	900
Requisitos previos	901
Configuración de Amazon Route 53 para dirigir el tráfico a un servicio de App Runner	901
Global Accelerator	903
Requisitos previos	903
Configuración de Amazon Route 53 para enrutar el tráfico a un acelerador	904
AWS Elastic Beanstalk entorno	905
Implementación de una aplicación en un entorno de Elastic Beanstalk	905
Obtención del nombre de dominio del entorno de Elastic Beanstalk	906

Creación de un registro de Route 53	906
Balanceador de carga de ELB	910
Requisitos previos	910
Configuración de Amazon Route 53 para dirigir el tráfico a un balanceador de carga de ELB	911
Bucket de Amazon S3	913
Requisitos previos	914
Configuración de Amazon Route 53 para dirigir el tráfico a un bucket de S3	915
Punto de conexión de interfaz de Amazon Virtual Private Cloud	916
Requisitos previos	917
Punto de conexión de interfaz de Amazon VPC	917
Amazon WorkMail	919
OpenSearch Servicio Amazon	922
Requisitos previos	922
Configuración de Amazon Route 53 para enrutar el tráfico a un punto final OpenSearch de dominio de Amazon Service	923
VPC Lattice	924
Requisitos previos	924
Configuración de Amazon Route 53 para enrutar el tráfico a un punto de conexión del dominio del servicio de VPC Lattice	925
Otros AWS recursos	926
Creación de una comprobación de estado	928
Tipos de comprobaciones de estado	929
Cómo determina Route 53 si la comprobación de estado es correcta	931
Cómo determina Route 53 el estado de las comprobaciones de estado que monitorean un punto de conexión	931
Cómo determina Route 53 el estado de las comprobaciones de estado que monitorean otras comprobaciones de estado	933
Cómo determina Route 53 el estado de las comprobaciones de estado que monitorean las alarmas de CloudWatch	933
Creación, actualización y eliminación de comprobaciones de estado	934
Creación y actualización de comprobaciones de estado	936
Valores que especifica al crear o actualizar comprobaciones de estado	938
Valores que muestra Route 53 al crear una comprobación de estado	966
Actualizar comprobaciones de estado al cambiar la configuración de la alarma de CloudWatch	966

Desactivación o activación de las comprobaciones de estado	968
Inversión de una comprobación de estado	969
Eliminar comprobaciones de estado	970
Actualizar o eliminar comprobaciones de estado cuando está configurada la recuperación ante errores a nivel de DNS	971
Configuración de las reglas de router y de firewall para las comprobaciones de estado	972
Configuración de la recuperación ante errores a nivel de DNS	974
Lista de tareas para configurar la recuperación ante errores a nivel de DNS	975
Cómo funcionan las comprobaciones de estado en configuraciones simples	977
Cómo funcionan las comprobaciones de estado en configuraciones complejas	981
Cómo elige Route 53 registros cuando está configurado la comprobación de estado	989
Conmutación por error activa-activa y activa-pasiva	992
Configuración de la conmutación por error en una zona alojada privada	996
Cómo Route 53 evita los problemas de conmutación por error	996
Denominar y etiquetar comprobaciones de estado	998
Restricciones de las etiquetas	999
Añadir, editar y eliminar etiquetas para comprobaciones de estado	999
Usar versiones de la API que sean anteriores a 2012-12-12	1002
Monitorizar el estado de la comprobación de estado y recibir notificaciones	1003
Ver el estado de la verificación de salud y el motivo de los fallos de la verificación de salud ...	1003
Monitorización de la latencia entre los comprobadores de estado y el punto de conexión	1006
Monitorear comprobaciones de estado mediante CloudWatch	1010
Comprobación del estado de la comprobación de estado	1011
Visualización de alarmas de comprobación de estado	1014
Cómo ver métricas de comprobación de estado en la consola de CloudWatch	1017
Cómo crear una alarma con una notificación de SNS	1017
Firewall DNS Resolver	1023
Cómo funciona Resolver DNS Firewall	1024
Componentes y configuración de DNS Firewall	1024
Cómo filtra Resolver DNS Firewall las consultas de DNS	1028
Pasos generales para utilizar DNS Firewall	1029
Uso de grupos de reglas de DNS Firewall en varias regiones	1030
Disponibilidad regional de DNS Firewall	1030
Cómo empezar con Resolver DNS Firewall	1032
Ejemplo de jardín amurallado de Resolver DNS Firewall	1032
Ejemplo de lista de bloqueos de Resolver DNS Firewall	1034

Reglas y grupos de reglas de DNS Firewall	1037
Configuración del grupo de reglas en DNS Firewall	1037
Configuración de las reglas en DNS Firewall	1038
Acciones de regla en DNS Firewall	1041
Administración de reglas y grupos de reglas en DNS Firewall	1042
Listas de dominios del firewall de DNS de Resolver	1045
Listas de dominios administrados	1046
Administración de sus propias listas de dominios	1052
DNS Firewall Advanced	1054
Configuración del registro de consultas para DNS Firewall	1056
Uso compartido de grupos de reglas de entre cuentas de	1058
Habilitación de las protecciones de DNS Firewall para la VPC	1061
Administración de asociaciones entre la VPC y el grupo de reglas de firewall	1061
Configuración de la VPC de DNS Firewall	1063
¿Qué son los perfiles de Amazon Route 53?	1064
Priorización de perfiles	1065
Disponibilidad de perfiles	1065
Uso de perfiles	1066
Creación de un perfil	1066
Asociación de grupos de reglas de DNS Firewall	1068
Asociación de zonas alojadas privadas	1070
Asociación de reglas de Resolver	1071
Asociación de puntos de conexión de VPC	1071
Asocie las configuraciones de registro de consultas	1072
Edición de configuraciones de perfil	1074
Asociar VPCs	1076
Visualización y actualización de perfiles	1077
Eliminación de un perfil de	1078
Visualización y actualización de los recursos asociados a los perfiles	1080
Desasociación de un recurso	1082
Visualización VPCs asociada a un perfil	1083
Desasociación de una VPC	1085
Cómo trabajar con perfiles de Route 53 compartidos	1086
Concesión de permisos para compartir perfiles de Route 53	1087
Requisitos previos para compartir perfiles de Route 53	1087
Cómo compartir un perfil de Route 53	1088

Cómo dejar de compartir un perfil de Route 53 compartido	1089
Identificación de un perfil de Route 53 compartido	1090
Responsabilidades y permisos de los perfiles compartidos de Route 53	1090
Facturación y medición	1091
Cuotas de instancias	1091
¿Qué es Amazon Route 53 on Outposts?	1092
Información general de la arquitectura	1093
Características de Route 53 on Outposts	1093
Comportamiento del solucionador de VPC cuando AWS Outposts está desconectado de la VPC	1094
Cómo empezar a usar VPC Resolver en AWS Outposts	1094
Creación de puntos de conexión entrantes	1096
Valores que se especifican al crear o editar puntos de conexión de entrada en Outpost	1096
Creación de puntos de conexión de salida	1098
Valores que se especifican al crear o editar puntos de conexión de salida en un AWS Outposts	1099
Creación de reglas de reenvío para los puntos de conexión de salida	1101
Administración de Resolver on Outpost	1101
Edición de Resolver on Outpost	1102
Ver el estado de Resolver on Outpost	1102
Eliminación de Resolver en Outpost	1103
Administración de puntos de conexión de entrada de Resolver en Outpost	1104
Visualización y edición de puntos de conexión de entrada	1104
Visualización del estado de los puntos de conexión de entrada	1105
Eliminación de puntos de conexión de entrada	1106
Administración de puntos de conexión de salida de Resolver on Outpost	1107
Visualización y edición de puntos de conexión de salida	1107
Visualización del estado de los puntos de conexión de salida	1108
Eliminación de puntos de conexión de salida	1109
¿Qué es Global Resolver	1111
¿Por qué Route 53 Global Resolver?	1112
Conceptos y terminología	1112
Resolución de DNS para clientes en ubicaciones locales y remotas	1113
Autenticación de clientes DNS	1113
Resolución de DNS de tráfico dividido	1114
Alta disponibilidad y presencia global	1115

Resolución y reenvío de DNS	1115
Filtrado de DNS y listas de dominios	1116
Detección avanzada de amenazas de DNS	1117
Supervisión y registro	1118
Funcionamiento	1119
¿Qué ocurre cuando los clientes realizan consultas de DNS	1119
Arquitectura anycast global	1120
Filtrado y seguridad de DNS	1120
Casos de uso	1120
Servicios relacionados	1122
Acceder a Global Resolver	1123
Compatible Regiones de AWS	1124
Configurar el acceso a la cuenta	1124
Inscríbase en una Cuenta de AWS	25
Creación de un usuario con acceso administrativo	25
Crear políticas y roles	1127
Consideraciones sobre la red	1128
Tutorial: Cree su primer Route 53 Global Resolver	1128
Requisitos previos	1128
Paso 1: Crear un solucionador global	1129
Paso 2: Crear una vista de DNS y configurar la autenticación	1129
Paso 3: Configurar las reglas de filtrado de DNS (opcional)	1130
Paso 4: Pruebe la configuración	1130
Paso 5: Monitorear la actividad del DNS	1131
Paso 6: Limpiar (opcional)	1131
Siguiendo pasos	1131
Administrar las vistas de DNS	1132
Administrar las vistas de DNS	1132
Administrar las asociaciones de zonas alojadas privadas	1134
Configure los ajustes para las vistas de DNS	1135
Administrar los controles de acceso	1137
Métodos de control de acceso	1138
Configuración de las fuentes de acceso	1139
Administrar los tokens de acceso	1140
Prácticas recomendadas	1144
Asegurar el DNS	1145

Configure y administre las reglas del firewall de DNS	1145
Listas de dominios administrados	1150
Crea listas de dominios	1153
Firewall de DNS: protecciones avanzadas	1154
Administre las políticas de seguridad	1156
Configuración de asociaciones alojadas privadas	1156
Administre las asociaciones de zonas alojadas privadas	1157
Supervisión de la actividad del DNS	1158
Obtenga visibilidad sobre el DNS	1159
Configure la supervisión de DNS	1164
Solución de problemas de DNS	1165
Diagnosticque problemas de conectividad	1165
Resuelva los problemas de rendimiento	1167
Solucione los problemas de configuración	1169
Solución de problemas de acceso a los recursos internos	1171
Cuotas	1171
Cuotas flexibles	1172
Cuotas invariables	1173
Creación de recursos AWS CloudFormation	1174
Route 53, VPC Resolver y plantillas CloudFormation	1174
Prácticas recomendadas para Route 53 y CloudFormation	1175
Nociones generales sobre la consistencia final	1175
Orden y lógica de los registros de DNS IDs	1176
Gestión de los errores de reversión	1177
Obtenga más información sobre CloudFormation	1177
Ejemplos de código	1179
Route 53	1180
Conceptos básicos	1180
Registro de dominios de Route 53	1209
Conceptos básicos	1216
Seguridad	1300
Protección de datos	1301
Protección contra registros de delegación colgantes	1302
Identity and Access Management	1304
Autenticación con identidades	1304
Control de acceso	1306

Información general sobre la administración del acceso	1306
Uso de políticas de IAM para Route 53	1314
Usar roles vinculados a servicios	1326
AWS políticas gestionadas	1331
Uso de condiciones	1346
Referencia de permisos de la API de Route 53	1357
Registro y supervisión	1358
Validación de conformidad	1359
Resiliencia	1360
Seguridad de la infraestructura	1361
Envío de resultados de al CSPM de Security Hub	1362
Cómo funcionan los hallazgos en Security Hub (CSPM)	1362
Tipos de resultados que envía DNS Firewall	1363
Reintentarlo cuando el CSPM de Security Hub no está disponible	1363
Actualización de resultados existentes en el CSPM de Security Hub	1363
Resultado típico de DNS Firewall	1364
Habilitación y configuración de la integración	1366
Detener la entrega de los hallazgos a Security Hub (CSPM)	1366
Supervisión	1367
Registro de consultas de DNS públicas	1367
Configuración de registros para consultas del DNS	1369
Uso de Amazon CloudWatch para acceder a los registros de consultas de DNS	1370
Cambio del período de retención de registros y exportación de registros a Amazon S3	1371
Parar el registro de consultas	1371
Valores que aparecen en los registros de consulta de DNS	1372
Ejemplo de registro de consulta	1373
Registro de consultas de Resolver	1373
Recursos a los que puede enviar registros de consulta de Resolver	1375
Administración de la configuración	1378
Monitorizar los registros de dominios	1386
Supervisión de sus recursos con los controles de estado de Amazon Route 53 y Amazon CloudWatch	1387
Métricas y dimensiones para comprobaciones de estado	1387
Supervisión de zonas alojadas mediante Amazon CloudWatch	1390
CloudWatch métricas para las zonas alojadas públicas de Route 53	1390
CloudWatch dimensión de las métricas de zonas alojadas públicas de Route 53	1392

Supervisión de los puntos finales de resolución de VPC de Route 53 con Amazon CloudWatch	1392
Métricas y dimensiones de VPC Resolver	1393
Supervisión de los grupos de reglas de Resolver DNS Firewall con Amazon CloudWatch	1401
Métricas y dimensiones para el DNS Firewall	1401
Administrar los eventos del firewall de DNS mediante EventBridge	1404
Resolver eventos de DNS Firewall	1405
Envío de eventos de DNS Firewall	1405
Permisos	1408
Recursos adicionales	1408
Referencia detallada de eventos de DNS Firewall	1408
Registrar llamadas a la API de Amazon Route 53 con AWS CloudTrail	1416
La información de Route 53 está en CloudTrail	1417
Visualización de eventos de Route 53 en el historial de eventos	1418
Descripción de las entradas de archivos de registro de Route 53	1418
Solución de problemas	1426
Mi dominio no está disponible en Internet	1427
Ha registrado un nuevo dominio, pero no hizo clic en el enlace del correo electrónico de confirmación	1428
Ha transferido el registro de dominio a Amazon Route 53, pero no ha transferido el servicio DNS	1428
Ha transferido el registro de dominio y ha especificado los servidores de nombres incorrectos en la configuración del dominio	1430
Ha transferido el servicio DNS en primer lugar, pero no ha esperado el tiempo suficiente antes de transferir el registro de dominio	1431
Ha eliminado la zona alojada que Route 53 utiliza para dirigir el tráfico de Internet del dominio.	1432
Su dominio se ha suspendido	1433
Mi dominio está suspendido (el estado es ClientHold)	1433
Ha registrado un nuevo dominio, pero no hizo clic en el enlace del correo electrónico de confirmación	1434
Ha deshabilitado la renovación automática del dominio y este ha expirado	1435
Ha cambiado la dirección de correo electrónico del contacto del registrante, pero no ha verificado que la nueva dirección de correo electrónico sea válida	1435
No se pudo procesar el pago de la renovación de dominio automática y el dominio ha expirado	1436

Hemos suspendido el dominio debido a una vulneración de la Política de uso aceptable de AWS	1436
Hemos suspendido el dominio debido a una orden judicial	1436
Se produjo un error en mi operación de dominio	1436
Se produjo un error en la operación de dominio debido a que la información de contacto no era válida	1437
No se pudo transferir mi dominio a Amazon Route 53	1437
No hizo clic en el enlace del correo electrónico de autorización	1438
El código de autorización que ha recibido del registrador actual no es válido	1438
Error “Parameters in request are not valid” (Los parámetros de la solicitud no son válidos) al intentar transferir un dominio .es a Amazon Route 53	1439
¿El nombre de dominio internacionalizado que va a transferir a Amazon Route 53 aparece en punycode?	1439
Mensajes de error de transferencia comunes	1439
He cambiado la configuración de DNS, pero no ha tenido efecto	1442
Ha transferido el servicio DNS a Amazon Route 53 en las últimas 48 horas, por lo que el DNS sigue utilizando su servicio DNS anterior	1442
Recientemente ha transferido el servicio DNS a Amazon Route 53, pero no ha actualizado los servidores de nombres con el registrador de dominio	1443
Los solucionadores de DNS siguen usando la configuración anterior para el registro	1445
Tiene más de una zona alojada con el mismo nombre y actualizó la que no está asociada al dominio	1446
Mi navegador muestra un error “Server not found”	1447
No creó ningún registro para el nombre de dominio o subdominio	1448
Ha creado un registro, pero ha especificado el valor erróneo	1448
El recurso al que está dirigiendo el tráfico no está disponible	1448
No puedo dirigir el tráfico a un bucket de Amazon S3 configurado para hospedar sitios web ..	1448
Me han facturado dos veces por la misma zona alojada	1449
Me cobraron varias facturas por mi dominio	1449
Mi cuenta de AWS está cerrada o se ha cerrado de forma definitiva y mi dominio está registrado con Route 53.	1450
Rangos de direcciones IP	1451
Rangos de direcciones IP de los servidores de nombres de Route 53	1451
Rangos de direcciones IP de las comprobaciones de estado de Route 53	1452
Referencias de listas de prefijos	1452
Rangos de direcciones IP internas de las comprobaciones de estado de Route 53	1453

Etiquetado de recursos	1454
Tutoriales	1456
Uso de Amazon Route 53 como el servicio DNS de subdominios sin migrar el dominio principal	1457
Creación de un subdominio que usa Amazon Route 53 como el servicio DNS sin migrar el dominio principal	1458
Migración de un servicio DNS de un subdominio a Amazon Route 53 sin migrar el dominio principal	1461
Transición al direccionamiento basado en la latencia en Amazon Route 53	1466
Incorporación de otra región a su direccionamiento basado en la latencia en Amazon Route 53	1469
Uso de registros ponderados y de latencia en Amazon Route 53 para dirigir el tráfico a varias instancias de Amazon EC2 en una región	1470
Administración de más de 100 registros ponderados en Amazon Route 53	1472
Ponderación de respuestas de múltiples registros con tolerancia a errores en Amazon Route 53	1473
Prácticas recomendadas	1475
Prácticas recomendadas de Amazon Route 53 DNS	1476
Mejores prácticas para VPC Resolver	1479
Evitar las configuraciones en bucle con los puntos de enlace de Resolver	1480
Escalado de los puntos de enlace de Resolver	1480
Alta disponibilidad para puntos de enlace de Resolver	1482
Consulta exhaustiva de nombres de zona DNS	1483
Prácticas recomendadas de las comprobaciones de estado de Amazon Route 53	1483
Cuotas	1486
Uso de Service Quotas para ver y administrar cuotas	1486
Cuotas de entidades	1486
Cuotas de dominios	1487
Cuotas en zonas alojadas	1487
Cuotas de registros	1489
Cuotas en el solucionador de VPC Route 53	1489
Cuotas de comprobaciones de estado	1497
Cuotas de configuraciones de registro de consulta	1497
Cuotas de políticas de flujo de tráfico y de registros de políticas	1497
Cuotas sobre conjuntos de delegación reutilizables	1498
Cuotas en perfiles de Route 53	1498

Valores máximos de las solicitudes API	1499
Número de elementos y caracteres en las solicitudes ChangeResourceRecordSets	1499
Frecuencia de las solicitudes de la API de Amazon Route 53	1500
Frecuencia de las solicitudes de la API de resolución de VPC de Route 53	1501
Información relacionada	1502
AWSRecursos de	1502
Herramientas y bibliotecas de terceros	1503
Interfaces gráficas de usuario	1504
Historial de documentos	1505
Versiones de 2025	1505
Lanzamientos de 2024	1507
Lanzamientos de 2023	1509
Versiones de 2022	1510
Versiones de 2021	1511
Versiones de 2020	1512
Versiones de 2018	1512
Versiones de 2017	1514
Versiones de 2016	1516
Versiones de 2015	1520
Versiones de 2014	1523
Versiones de 2013	1526
Versión de 2012	1528
Versiones de 2011	1528
Versión de 2010	1528
.....	mdxxix

¿Qué es Amazon Route 53?

Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad. Puede utilizar Route 53 para realizar tres funciones principales en cualquier combinación: registro de dominio, direccionamiento de DNS y comprobación de estado.

Si decide utilizar Route 53 para las tres funciones, asegúrese de seguir el orden que se indica a continuación:

1. Registro de nombres de dominio

Su sitio web requiere un nombre, como example.com. Route 53 le permite registrar un nombre para su sitio web o aplicación web, conocido como nombre de dominio.

- Para obtener una descripción general, consulte [Cómo funciona el registro de dominios](#).
- Para consultar el procedimiento, visite [Registrar un nuevo dominio](#).
- Para ver un tutorial en el que se explica cómo registrar un dominio y crear un sitio web sencillo en un bucket de Amazon S3, consulte [Introducción a Amazon Route 53](#).

2. Direccionamiento del tráfico de Internet a los recursos del dominio

Cuando un usuario abre un navegador web y escribe el nombre del dominio (example.com) o el nombre de un subdominio (acme.example.com) en la barra de direcciones, Route 53 ayuda a conectar el navegador con su sitio web o aplicación web.

- Para obtener una descripción general, consulte [se dirige el tráfico de Internet a su sitio web o aplicación web](#).
- Para consultar los procedimientos, visite [Configuración de Amazon Route 53 como servicio DNS](#).
- Para obtener un procedimiento sobre cómo enrutar el correo electrónico a Amazon WorkMail, consulte [Enrutamiento del tráfico a Amazon WorkMail](#).

3. Comprobación del estado de los recursos

Route 53 envía solicitudes automatizadas a través de Internet a un recurso, como un servidor web, para verificar que está accesible, disponible y operativo. También puede elegir recibir notificaciones cuando un recurso deje de estar disponible y sacar el tráfico de Internet de los recursos que están en mal estado.

- Para obtener una descripción general, consulte [Cómo verifica Amazon Route 53 el estado de los recursos](#).

- Para consultar los procedimientos, visite [Creación de comprobaciones de estado de Amazon Route 53](#).

Otras características de Route 53

Además de ser un servicio web de sistema de nombres de dominio (DNS), Route 53 ofrece las siguientes características:

Solucionador de VPC

Obtenga un DNS recursivo para su Amazon VPCs en Regiones de AWS, VPCs en AWS Outposts racks o en cualquier otra red local. Cree reglas de reenvío condicional y puntos de conexión de Route 53 para resolver los nombres personalizados que se dominen en las zonas alojadas privadas de Route 53 o en los servidores DNS en las instalaciones.

Para obtener más información, consulte [¿Qué es el solucionador de VPC Route 53?](#).

Amazon Route 53 Resolver en Outposts

Conecte el Resolver de VPC en los racks de Outpost con los servidores DNS de sus centros de datos locales a través de los puntos finales de Resolver. Esto permite la resolución de consultas de DNS entre los bastidores de Outposts y los demás recursos en las instalaciones.

Para obtener más información, consulte [¿Qué es Amazon Route 53 on Outposts?](#).

Resolver DNS Firewall

Proteja sus consultas de DNS recursivas en el solucionador de VPC. Cree listas de dominios y desarrolle reglas de firewall que filtren el tráfico DNS saliente en función de estas reglas.

Para obtener más información, consulte [Uso de DNS Firewall para filtrar el tráfico de DNS saliente](#).

Flujo de tráfico

Easy-to-use y una gestión del tráfico global rentable: dirija a los usuarios finales al mejor punto final para su aplicación en función de la proximidad, la latencia, el estado y otras consideraciones.

Para obtener más información, consulte [Uso de flujo de tráfico para dirigir el tráfico DNS](#).

Perfiles de Amazon Route 53

Con los perfiles de Route 53, puede aplicar y administrar configuraciones de Route 53 relacionadas con el DNS en muchas VPCs y diferentes configuraciones. Cuenta de AWS

Para obtener más información, consulte [¿Qué son los perfiles de Amazon Route 53?](#).

Temas

- [Cómo funciona el registro de dominios](#)
- [se dirige el tráfico de Internet a su sitio web o aplicación web](#)
- [Cómo verifica Amazon Route 53 el estado de los recursos](#)
- [Conceptos de Amazon Route 53](#)
- [Primeros pasos con Amazon Route 53](#)
- [Acceso a Amazon Route 53](#)
- [AWS Identity and Access Management](#)
- [Precios y facturación de Amazon Route 53](#)
- [Uso de Route 53 con un AWS SDK](#)

Cómo funciona el registro de dominios

Si desea crear un sitio web o una aplicación web, lo primero que debe hacer es registrar el nombre de su sitio web, que recibe el nombre de [domain name](#). Su nombre de dominio es el nombre, como ejemplo.com, que los usuarios introducen en un navegador para mostrar su sitio web.

Aquí se incluye información general sobre cómo registrar un nombre de dominio con Amazon Route 53:

1. Elige un nombre de dominio y confirma que está disponible, lo que significa que nadie más ha registrado el nombre de dominio que usted desea.

Si el nombre de dominio que desea ya está en uso, puede probar otros nombres o intentar cambiar únicamente el dominio de nivel superior, como .com, por otro dominio de nivel superior, como .ninja o .hockey. Para obtener una lista de los dominios de nivel superior que Route 53 admite, consulte [Dominios que puede registrar con Amazon Route 53](#).

2. Debe registrar el nombre de dominio con Route 53. Cuando registra un dominio, proporciona nombres e información de contacto del propietario del dominio y otros contactos.

Cuando registra un dominio con Route 53, el servicio se convierte automáticamente en el servicio DNS del dominio mediante el procedimiento siguiente:

- Crea una [hosted zone](#) que tiene el mismo nombre que el dominio.
- Asigna un conjunto de cuatro servidores de nombres a la zona alojada. Cuando alguien utiliza un navegador para obtener acceso a su sitio web, como `www.example.com`, estos servidores de nombres indican al navegador dónde encontrar sus recursos, como un servidor web o un bucket de Amazon S3. ([Amazon S3](#) es el almacenamiento de objetos para almacenar y recuperar cualquier cantidad de datos desde cualquier ubicación de la web. Un bucket es un contenedor para objetos que almacena en S3).
- Obtiene los servidores de nombres de la zona alojada y los añade al dominio.

Para obtener más información, consulte [se dirige el tráfico de Internet a su sitio web o aplicación web](#).

3. Cuando finalice el proceso de registro, enviaremos su información al registrador del dominio. El [domain registrar](#) es Amazon Registrar, Inc. o nuestro registrador asociado, Gandi. Para saber quién es el registrador de su dominio, consulte [Búsqueda del registrador](#).
4. El registrador envía la información a la empresa de registro del dominio. Un registro es una empresa que vende registros de dominios para uno o más dominios de nivel superior, como `.com`.
5. La empresa de registro almacena información acerca de su dominio en su propia base de datos y también almacena parte de la información en la base de datos WHOIS pública.

Para obtener más información sobre cómo registrar un nombre de dominio, consulte [Registrar un nuevo dominio](#).

Si ya ha registrado un nombre de dominio con otro registrador, puede elegir transferir el registro de dominio a Route 53. Esto no es necesario para utilizar otras características de Route 53. Para obtener más información, consulte [Transferencia del registro de un dominio a Amazon Route 53](#).

se dirige el tráfico de Internet a su sitio web o aplicación web

Todos los equipos de Internet, desde su smartphone o laptop, se conectan a los servidores que sirven contenido a sitios web de comercio masivo y se comunican entre sí mediante números. Estos números, denominados direcciones IP, tienen alguno de los siguientes formatos:

- Formato de protocolo de Internet versión 4 (IPv4), como `192.0.2.44`

- Formato del Protocolo de Internet versión 6 (IPv6), como 2001:0 db 8:85 a 3:0000:0000:abcd:0001:2345

Cuando abre un navegador y va a un sitio web, no tiene que recordar ni escribir una larga cadena de caracteres como esa. En lugar de ello, puede introducir un nombre de dominio como example.com y aun así se le redirigirá al lugar correcto. Un servicio DNS como Amazon Route 53 le ayuda a establecer esa conexión entre los nombres de dominio y las direcciones IP.

Temas

- [Información general de cómo configurar Amazon Route 53 para dirigir el tráfico de Internet de su dominio](#)
- [Cómo dirige Amazon Route 53 el tráfico de su dominio](#)

Información general de cómo configurar Amazon Route 53 para dirigir el tráfico de Internet de su dominio

A continuación se muestra información general de cómo utilizar la consola de Amazon Route 53 para registrar un nombre de dominio y configurar Route 53 a fin de dirigir el tráfico de Internet a su sitio web o aplicación web.

1. Registra el nombre de dominio que desea que usen los usuarios para tener acceso a su contenido. Para obtener una descripción general, consulte [Cómo funciona el registro de dominios](#).
2. Después de registrar su nombre de dominio, Route 53 crea automáticamente una zona alojada pública que tiene el mismo nombre que el dominio. Para obtener más información, consulte [Trabajar con zonas públicas alojadas](#).
3. Para dirigir el tráfico a sus recursos, cree registros, que también se denominan conjuntos de registros de recursos, en su zona alojada. Cada registro incluye información acerca de cómo desea dirigir el tráfico de su dominio, como la siguiente:

Name

El nombre del registro se corresponde con el nombre del dominio (example.com) o nombre del subdominio (www.example.com, retail.example.com) para el que desea que Route 53 dirija el tráfico.

El nombre de cada registro en una zona alojada debe acabar con el nombre de la zona alojada. Por ejemplo, si el nombre de la zona alojada es ejemplo.com, todos los nombres

de registro debe terminar en ejemplo.com. La consola de Route 53 se encarga de esto automáticamente.

Tipo

El tipo de registro suele determinar el tipo de recurso al que desea dirigir el tráfico. Por ejemplo, para dirigir el tráfico a un servidor de correo electrónico, debe especificar MX para el Type (Tipo). Para enrutar el tráfico a un servidor web que tiene una dirección IP, especifique A como Tipo. IPv4

Valor

El valor está estrechamente relacionados con el tipo. Si especifica MX para el tipo, debe especificar los nombres de uno o varios servidores de correo electrónico para el valor. Si especifica A para el tipo, especifique una dirección IP en IPv4 formato, como 192.0.2.136.

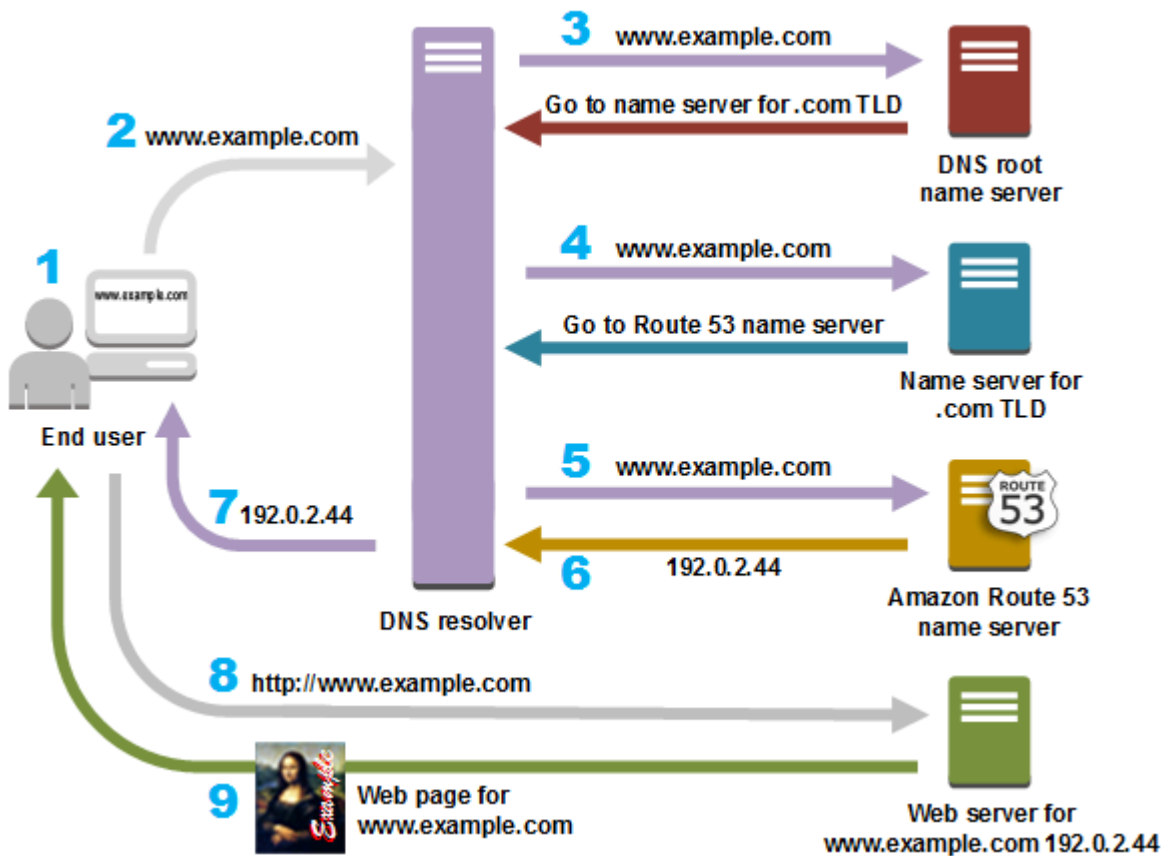
Para obtener más información acerca de los registros, consulte [Uso de registros](#).

También puede crear registros especiales de Route 53, denominados registros de alias, que dirijan el tráfico a los buckets de Amazon S3, a CloudFront las distribuciones de Amazon y a otros AWS recursos. Para obtener más información, consulte [Elección entre registros de alias y sin alias](#) y [Enrutar el tráfico de Internet a sus AWS recursos](#).

Para obtener más información sobre cómo dirigir el tráfico de Internet a sus recursos, consulte [Configuración de Amazon Route 53 como servicio DNS](#).

Cómo dirige Amazon Route 53 el tráfico de su dominio

Después de configurar Amazon Route 53 para dirigir el tráfico de Internet a sus recursos, como servidores web o buckets de Amazon S3, esto es lo que ocurre en cuestión de milisegundos cuando alguien solicita contenido de www.example.com:



1. Un usuario abre un navegador web, escribe `www.example.com` en la barra de direcciones y pulsa Enter (Intro).
2. La solicitud de `www.ejemplo.com` se envía al servicio de resolución de nombres DNS, que normalmente lo administra el proveedor de Internet (ISP) del usuario, como un proveedor de Internet por cable, un proveedor de banda ancha DSL o una red corporativa.
3. El servicio de resolución de nombres de DNS del ISP reenvía la solicitud de `www.example.com` a un servidor de nombres raíz DNS.
4. El servicio de resolución de nombres de DNS reenvía de nuevo la solicitud de `www.example.com`, esta vez a uno de los servidores de nombres TLD de los dominios `.com`. El servidor de nombres de los dominios `.com` responde a la solicitud con los nombres de cuatro servidores de nombres de Route 53 que están asociados al dominio `example.com`.

El servicio de resolución de nombres de DNS almacena en caché (almacena) los cuatro servidores de nombres de Route 53. La próxima vez que alguien busque `example.com`, el servicio de resolución de nombres omitirá los pasos 3 y 4, ya que ya tiene los servidores de nombres de `example.com`. Los servidores de nombres suelen almacenarse en caché durante dos días.

5. El servicio de resolución de nombres DNS elige un servidor de nombres de Route 53 y reenvía la solicitud de `www.example.com` a este servidor de nombres.
6. El servidor de nombres de Route 53 busca en la zona alojada de `example.com` el registro `www.example.com`, obtiene el valor asociado, como la dirección IP de un servidor web, `192.0.2.44`, y devuelve la dirección IP al servicio de resolución de nombres DNS.
7. El servicio de resolución de nombres DNS por fin tiene la dirección IP que el usuario necesita. El servicio devuelve ese valor al navegador web.

 Note

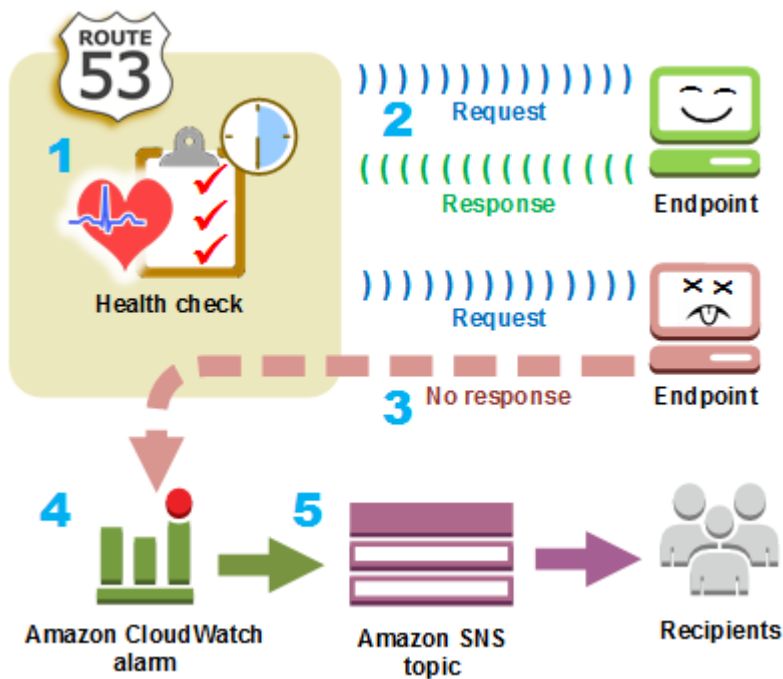
El servicio de resolución de nombres DNS también almacena en caché la dirección IP de `ejemplo.com` durante la cantidad de tiempo que usted especifique, para que pueda responder más rápidamente la próxima vez que alguien visite `ejemplo.com`. Para obtener más información, consulte [time to live \(TTL\)](#).

8. El navegador web envía una solicitud de `www.example.com` a la dirección IP que ha obtenido del servicio de resolución de nombres de DNS. Aquí es donde tu contenido es, por ejemplo, un servidor web que se ejecuta en una EC2 instancia de Amazon o un bucket de Amazon S3 que está configurado como punto final de un sitio web.
9. El servidor web u otro recurso en la dirección `192.0.2.44` devuelve la página web de `www.ejemplo.com` al navegador web y el navegador web muestra la página.

Cómo verifica Amazon Route 53 el estado de los recursos

Las comprobaciones de estado de Amazon Route 53 monitorean el estado de sus recursos, tales como servidores web y servidores de correo electrónico. Si lo desea, puede configurar CloudWatch las alarmas de Amazon para sus controles de estado, de forma que reciba una notificación cuando un recurso deje de estar disponible.

A continuación se incluye una descripción general de cómo funciona la comprobación de estado si desea recibir una notificación cuando un recurso deje de estar disponible:



1. Crea una comprobación de estado y especifica valores que definen cómo desea que funcione la comprobación de estado, como los siguientes:

- La dirección IP o el nombre de dominio del punto de conexión, como un servidor web, que desea que Route 53 monitoree. (También puede supervisar el estado de otros controles de estado o el estado de una CloudWatch alarma).
- El protocolo que desea que Amazon Route 53 utilice para realizar la comprobación: HTTP, HTTPS o TCP.
- Con qué frecuencia desea que Route 53 envíe una solicitud al punto de conexión. Este es el intervalo de la solicitud.
- Cuántas veces consecutivas debe producir un error el punto de conexión en su respuesta a las solicitudes para que Route 53 considere que está en mal estado. Este es el umbral de error.
- De manera opcional, cómo desea recibir una notificación cuando Route 53 detecte que el punto de conexión está en mal estado. Al configurar la notificación, Route 53 establece automáticamente una CloudWatch alarma. CloudWatch utiliza Amazon SNS para notificar a los usuarios que un punto de conexión no está en buen estado.

2. Route 53 comienza a enviar solicitudes al punto de conexión en el intervalo especificado en la comprobación de estado.

Si el punto de conexión responde a las solicitudes, Route 53 considera que el punto de conexión está en buen estado y no realiza ninguna acción.

3. Si el punto de conexión no responde a una solicitud, Route 53 comienza a contar el número de solicitudes consecutivas a las que el punto de conexión no responde:
 - Si el recuento alcanza el valor especificado para el umbral de error, Route 53 considera que el punto de conexión está en mal estado.
 - Si el punto final comienza a responder de nuevo antes de que el recuento alcance el umbral de error, Route 53 restablece el recuento a 0 y CloudWatch no se pone en contacto con usted.
4. Si Route 53 considera que el punto final está en mal estado y si configuraste una notificación para la comprobación de estado, Route 53 lo notificará CloudWatch.

Si no ha configurado notificaciones, puede seguir viendo el estado de las comprobaciones de estado de Route 53 en la consola de este servicio. Para obtener más información, consulte [Monitorizar el estado de la comprobación de estado y recibir notificaciones](#).

5. Si ha configurado la notificación para la comprobación de estado, CloudWatch activa una alarma y utiliza Amazon SNS para enviar la notificación a los destinatarios especificados.

Además de comprobar el estado de un puntos de conexión especificado, puede configurar una comprobación de estado para comprobar el estado de una o varias comprobaciones de estado adicionales, de forma que reciba una notificación cuando el número especificado de recursos, como dos servidores web de cinco, no estén disponibles. También puede configurar una comprobación de estado para comprobar el estado de una CloudWatch alarma, de modo que pueda recibir una notificación en función de una amplia gama de criterios, no solo de si un recurso responde a las solicitudes.

Si tiene varios recursos que realizan la misma función, como servidores web o servidores de bases de datos, y desea que Route 53 dirija el tráfico únicamente a los recursos que están en buen estado, puede configurar la conmutación por error a nivel de DNS asociando una comprobación de estado a cada registro para ese recurso. Si una comprobación de estado determina que el recurso subyacente está en mal estado, Route 53 desvía el tráfico del registro asociado.

Para obtener más información sobre cómo usar Route 53 para monitorear el estado de sus recursos, consulte [Creación de comprobaciones de estado de Amazon Route 53](#).

Conceptos de Amazon Route 53

A continuación se incluye información general de los conceptos que se han tratado a lo largo de la Guía para desarrolladores de Amazon Route 53.

Temas

- [Conceptos de registro de dominios](#)
- [Conceptos del sistema de nombres de dominio \(DNS\)](#)
- [Conceptos de plano de datos y control](#)
- [Conceptos de comprobación de estado](#)

Conceptos de registro de dominios

A continuación se incluye un resumen de los conceptos relacionados con el registro de dominios.

- [domain name](#)
- [domain registrar](#)
- [domain registry](#)
- [domain reseller](#)
- [top-level domain \(TLD\)](#)

nombre de dominio

El nombre, como ejemplo.com, que un usuario escribe en la barra de direcciones de un navegador web para tener acceso a un sitio web o una aplicación web. Para que su sitio web o aplicación web esté disponible en Internet, lo primero que tiene que hacer es registrar un nombre de dominio. Para obtener más información, consulte [Cómo funciona el registro de dominios](#).

registrador de dominios

Una empresa acreditada por la ICANN (Corporación para la Asignación de Nombres y Números de Internet) para procesar los registros de dominios de nivel superior específicos (). TLDs Para encontrar el registrador de su dominio, consulte [Búsqueda del registrador](#).

empresa de registro de dominios

Una empresa que tiene el derecho de vender dominios que tienen un dominio de nivel superior. Por ejemplo, [VeriSign](#) es el registro que posee el derecho a vender dominios que tienen un TLD .com. Una empresa de registro de dominios define las reglas para registrar un dominio, como los requisitos de residencia para un TLD geográfico. Una empresa de registro de dominios mantiene también la base de datos autorizada de todos los nombres de dominio que tienen

el mismo TLD. La base de datos de la empresa de registro contiene información como la información de contacto y los servidores de nombres de cada dominio.

distribuidor del dominio

Una empresa que vende nombres de dominio de registradores como Amazon Registrar. Amazon Route 53 es un distribuidor de dominios de Amazon Registrar y de nuestro socio registrador Gandi.

dominio de nivel superior (TLD)

La última parte de un nombre de dominio, como .com, .org o .ninja. Hay dos tipos de dominios de nivel superior:

Dominios de nivel superior genéricos

TLDs Por lo general, dan a los usuarios una idea de lo que encontrarán en el sitio web. Por ejemplo, los nombres de dominio que tienen un TLD de .bike a menudo están asociados con sitios web de empresas y organizaciones de motocicletas o bicicletas. Con algunas excepciones, puede usar cualquier TLD genérico que quiera; por ejemplo, un club de ciclismo podría usar el TLD .hockey para su nombre de dominio.

Dominios geográficos de nivel superior

TLDs Están asociados a áreas geográficas, como países o ciudades. Algunos registros geográficos TLDs tienen requisitos de residencia, mientras que otros, por ejemplo [the section called “.io \(Territorio Británico del Océano Índico\)”](#), permiten o incluso fomentan su uso como un TLD genérico.

Para obtener una lista de los TLDs que puede usar al registrar un nombre de dominio en Route 53, consulte. [Dominios que puede registrar con Amazon Route 53](#)

Conceptos del sistema de nombres de dominio (DNS)

A continuación se incluye un resumen de los conceptos relacionados con el sistema de nombres de dominio (DNS).

- [alias record](#)
- [authoritative name server](#)
- [CIDR block](#)

- [DNS query](#)
- [DNS resolver](#)
- [Domain Name System \(DNS\)](#)
- [hosted zone](#)
- [IP address](#)
- [name servers](#)
- [private DNS](#)
- [recursive name server](#)
- [record \(DNS record\)](#)
- [reusable delegation set](#)
- [routing policy](#)
- [subdomain](#)
- [time to live \(TTL\)](#)

registro de alias

Tipo de registro que puede crear con Amazon Route 53 para enrutar el tráfico a AWS recursos como CloudFront las distribuciones de Amazon y los buckets de Amazon S3. Para obtener más información, consulte [Elección entre registros de alias y sin alias](#).

servidor de nombres autorizado

Un servidor de nombres que tiene información definitiva sobre una parte del sistema de nombres de dominio (DNS) y que responde a las solicitudes de un servicio de resolución de nombres DNS devolviendo la información pertinente. Por ejemplo, un servidor de nombres autorizado para el dominio de nivel superior (TLD) .com conoce los nombres de los servidores de nombres de cada dominio .com registrado. Cuando un servidor de nombres autorizado de .com recibe una solicitud de un servicio de resolución de nombres DNS para ejemplo.com, responde con los nombres de los servidores de nombres del servicio DNS para el dominio ejemplo.com.

Los servidores de nombres de Route 53 son los servidores de nombres autorizados para cada dominio que Route 53 utiliza como servicio DNS. Los servidores de nombres saben cómo quiere usted dirigir el tráfico de su dominio y subdominios según los registros que ha creado en la zona alojada del dominio. (Los servidores de nombres de Route 53 almacenan las zonas alojadas de los dominios que utilizan Route 53 como servicio DNS).

Por ejemplo, si un servidor de nombres de Route 53 recibe una solicitud para `www.example.com`, busca ese registro y devuelve la dirección IP, como `192.0.2.33`, que está especificada en el registro.

Bloque CIDR

Un bloque CIDR es un rango IP utilizado con el enrutamiento basado en IP. En Route 53, puede especificar un bloque CIDR de `/0` a `/24` para IPv4 o `/0` a `/48` para IPv6. Por ejemplo, un bloque IPv4 CIDR `/24` incluye 256 direcciones IP contiguas. Puede agrupar conjuntos de bloques CIDR (o rangos de IP) en ubicaciones CIDR, que a su vez se agrupan en colecciones CIDR reutilizables.

consulta DNS

Normalmente, una solicitud enviada por un dispositivo, como un equipo o un smartphone, al sistema de nombres de dominio (DNS) para un recurso que está asociado a un nombre de dominio. El ejemplo más común de una consulta DNS es cuando un usuario abre un navegador y escribe el nombre de dominio en la barra de direcciones. La respuesta a una consulta DNS es normalmente la dirección IP que está asociada al recurso, como un servidor web. El dispositivo que ha iniciado la solicitud utiliza la dirección IP para comunicarse con el recurso. Por ejemplo, un navegador puede utilizar la dirección IP para obtener una página web de un servidor web.

servicio de resolución de nombres DNS

Un servidor DNS, a menudo administrado por un proveedor de Internet (ISP), que actúa como intermediario entre las solicitudes de los usuarios y los servidores de nombres DNS. Cuando abre un navegador y escribe un nombre de dominio en la barra de direcciones, su consulta se envía primero al servicio de resolución de nombres DNS. El servicio se comunica con los servidores de nombres DNS para obtener la dirección IP de los recursos correspondientes, como un servidor web. Un servicio de resolución de nombres DNS también recibe el nombre de “servidor de nombres recursivo”, ya que envía solicitudes a una secuencia de servidores de nombres DNS autorizados hasta que obtiene la respuesta (por lo general, una dirección IP), que devuelve al dispositivo de un usuario, como un navegador web de un equipo laptop.

Sistema de nombres de dominio (DNS)

Una red mundial de servidores que ayuda a los equipos, smartphones, tablets y otros dispositivos IP a que se comuniquen entre sí. El sistema de nombres de dominio traduce fácilmente nombres comprensibles como `ejemplo.com` en números, denominados direcciones IP, que permiten a los equipos encontrarse unos a otros en Internet.

Véase también [IP address](#).

zona alojada

Un contenedor de registros, que incluye información sobre cómo desea dirigir el tráfico de un dominio (como example.com) y todos sus subdominios (como www.example.com, retail.example.com y seattle.accounting.example.com). Una zona alojada tiene el mismo nombre que el dominio correspondiente.

Por ejemplo, la zona alojada de example.com podría incluir un registro que tenga información sobre el tráfico de enrutamiento de www.example.com a un servidor web que tenga la dirección IP 192.0.2.243, y un registro que tenga información sobre el enrutamiento del correo electrónico de example.com a dos servidores de correo electrónico, mail1.example.com y mail2.example.com. Cada servidor de correo electrónico requiere también su propio registro.

Véase también [record \(DNS record\)](#).

dirección IP

Un número que se asigna a un dispositivo en Internet, como un laptop, smartphone o servidor web, que permite al dispositivo comunicarse con otros dispositivos en Internet. Las direcciones IP tienen alguno de estos formatos:

- Formato de protocolo de Internet versión 4 (IPv4), como 192.0.2.44
- Formato del Protocolo de Internet versión 6 (IPv6), como 2001:0 db 8:85 a 3:0000:0000:abcd:0001:2345

IPv4 Route IPv6 53 admite ambas direcciones y para los siguientes propósitos:

- Puede crear registros que tengan un tipo A, para IPv4 las direcciones, o un tipo AAAA, para IPv6 las direcciones.
- Puede crear controles de estado que envíen solicitudes a las IPv6 direcciones IPv4 o a ellas.
- Si un solucionador de DNS está en una IPv6 red, puede usar IPv4 o IPv6 enviar solicitudes a Route 53.

servidores de nombres

Servidores del sistema de nombres de dominio (DNS) que ayudan a traducir nombres de dominio en las direcciones IP que los equipos utilizan para comunicarse entre sí. Los servidores de nombres son servidores de nombres recursivos (denominados también [DNS resolver](#)) o [authoritative name server](#).

Para obtener información general sobre cómo DNS dirige el tráfico a sus recursos, incluido el rol que desempeña Route 53 en el proceso, consulte [Cómo dirige Amazon Route 53 el tráfico de su dominio](#).

DNS privado

Una versión local del Sistema de nombres de dominio (DNS) que le permite enrutar el tráfico de un dominio y sus subdominios a EC2 instancias de Amazon dentro de una o más redes privadas virtuales de Amazon (VPCs). Para obtener más información, consulte [Uso de zonas alojadas privadas](#).

registro (registro de DNS)

Un objeto de una zona alojada que se utiliza para definir cómo desea dirigir el tráfico del dominio o un subdominio. Por ejemplo, puede crear registros para example.com y www.example.com que dirijan el tráfico a un servidor web que tenga una dirección IP de 192.0.2.234.

Para obtener más información sobre registros, incluida información sobre la funcionalidad que proporcionan registros específicos de Route 53, consulte [Configuración de Amazon Route 53 como servicio DNS](#).

servidor de nombres recursivo

Consulte [DNS resolver](#).

conjunto de delegación reutilizable

Un conjunto de cuatro servidores de nombres autorizados que puede utilizar con varias zonas hospedadas. De forma predeterminada, Route 53 asigna una selección aleatoria de servidores de nombres a cada zona alojada nueva. Para facilitar la migración del servicio DNS a Route 53 para un gran número de dominios, puede crear un conjunto de delegación reutilizable y, a continuación, asociarlo a nuevas zonas alojadas. (No puede cambiar los servidores de nombres que están asociados a una zona alojada existente).

Los conjuntos de delegación reutilizables se crean y se asocian a una zona alojada mediante programación; no se permite usar la consola de Route 53. Para obtener más información, consulte [CreateHostedZone](#) consulte [CreateReusableDelegationSet](#) la referencia de la API de Amazon Route 53. La misma función también está disponible en las [AWS SDKs](#) [AWS Command Line Interface](#), las y [AWS Tools for Windows PowerShell](#).

política de direccionamiento

Un ajuste de registros que determina cómo Route 53 responde a las consultas de DNS. Route 53 admite las siguientes políticas de direccionamiento de:

- Política de direccionamiento simple: se utiliza para dirigir el tráfico de Internet a un único recurso que realiza una función determinada para su dominio; por ejemplo, un servidor web que ofrece contenido para el sitio web `example.com`.
- Política de direccionamiento de conmutación por error: se utiliza si desea configurar la conmutación por error activa-pasiva.
- Política de direccionamiento de geolocalización: se utiliza si desea dirigir el tráfico de Internet a sus recursos en función de la ubicación de los usuarios.
- Política de direccionamiento de geoproximidad: se utiliza si desea dirigir el tráfico en función de la ubicación de los recursos y, opcionalmente, desviar el tráfico desde los recursos de una ubicación a los de otra.
- Política de direccionamiento de latencia: se utiliza si tiene recursos en varias ubicaciones y desea dirigir el tráfico al recurso que proporciona la mejor latencia.
- Política de direccionamiento basada en IP: se usa cuando se quiere enrutar el tráfico en función de la ubicación de los usuarios, y tener las direcciones IP de las que se origina el tráfico.
- Política de direccionamiento de respuesta con varios valores: se utiliza si desea que Route 53 responda a consultas de DNS con hasta ocho registros de estado seleccionados al azar.
- Política de direccionamiento ponderada: se utiliza para dirigir el tráfico a varios recursos en las proporciones que especifique.

Para obtener más información, consulte [Elección de una política de enrutado](#).

subdominio

Un nombre de dominio que tiene una o varias etiquetas delante del nombre de dominio registrado. Por ejemplo, si registra el nombre de dominio `ejemplo.com`, `www.example.com` es un subdominio. Si crea la zona alojada `madrid.ejemplo.com` para el dominio `ejemplo.com`, `contabilidad.madrid.ejemplo.com` es un subdominio.

Para dirigir el tráfico de un subdominio, cree un registro con el nombre que desee, como `www.example.com`, y especifique los valores correspondientes, como la dirección IP de un servidor web.

tiempo de vida (TTL)

La cantidad de tiempo, en segundos, que desea que un servicio de resolución de nombres DNS almacene en caché los valores de registro antes de enviar otra solicitud a Route 53 para obtener los valores actuales de ese registro. Si el servicio de resolución de nombres DNS recibe otra solicitud para el mismo dominio antes de que venza el TTL, el servicio devuelve el valor almacenado en caché.

Un TTL mayor reduce los cargos de Route 53, que se basan en parte en el número de consultas de DNS a las que Route 53 responde. Un TTL menor reduce la cantidad de tiempo que los servicios de resolución de nombres DNS dirigen tráfico a recursos más antiguos después de cambiar los valores de un registro modificando, por ejemplo, la dirección IP del servidor web de `www.example.com`.

Conceptos de plano de datos y control

A continuación, se incluye información general de los conceptos relacionados con la manera en que Amazon Route 53 divide su funcionalidad en un control y un plano de datos. El servicio Route 53, como la mayoría de Servicios de AWS, incluye un plano de control que permite realizar operaciones de gestión como la creación, actualización y eliminación de recursos, y un plano de datos que proporciona la funcionalidad principal del servicio. Si bien ambas funcionalidades están diseñadas para ser fiables, los planos de control están optimizados para garantizar la coherencia de los datos, en tanto que los planos de datos están optimizados para la disponibilidad. El diseño resistente del plano de datos le permite mantener la disponibilidad incluso durante eventos disruptivos poco frecuentes, durante los cuales el plano de control podría no estar disponible. Por este motivo, recomendamos que se utilicen funciones de plano de datos en las que la disponibilidad es importante.

Para las comprobaciones de estado y DNS públicas y privadas de Route 53, el plano de control se encuentra en la Región de AWS us-east-1 y los planos de datos se distribuyen por todo el mundo.

Amazon Route 53 se divide en planos de control y datos de la siguiente manera:

- En el caso del DNS público y privado de Route 53, el plano de control consiste en el Route 53 APIs, que permite administrar las entradas de DNS, incluidas las de Route 53 y Traffic Flow. APIs La consola de Route 53 está ubicada en la Región de AWS us-east-1, pero AWS si se determina que hay algún problema en esa región, la consola de Route 53 estará conectada por la us-west-2. Región de AWS El plano de datos es el servicio DNS autorizado, que se ejecuta en más de 200 ubicaciones de puntos de presencia (PoP) y responde a las consultas de DNS en función de las zonas alojadas y los datos de comprobación de estado.
- En el caso de las comprobaciones de estado de Route 53, el plano de control consiste en la Route 53, APIs que se puede usar para crear, actualizar y eliminar las comprobaciones de estado. La consola de chequeos de estado de Route 53 está ubicada en la Región de AWS us-east-1, pero AWS si se determina que hay una deficiencia en esa región, la consola de chequeos de estado de Route 53 estará conectada por la us-west-2. Región de AWS El plano de datos es el servicio

distribuido globalmente que realiza comprobaciones de estado, agrega los resultados y los entrega a los planos de datos de DNS público y privado de Route 53 y [AWS Global Accelerator](#).

- En el caso de [Route 53 VPC Resolver](#), el plano de control consiste en el VPC Resolver APIs que permite gestionar la configuración de Amazon VPC, las reglas del Resolver, las políticas de registro de consultas y las políticas de firewall de DNS. El plano de datos es el servicio de resolución DNS, que responde a las consultas de DNS de la VPC, los puntos de conexión que reenvían consultas a otros solucionadores y el plano de datos del firewall de DNS que aplica políticas para filtrar las consultas de DNS. VPC Resolver es un servicio regional y sus planos de control y datos funcionan de forma independiente en cada uno de ellos. Región de AWS
- Los registros de dominios de Route 53 se administran solo en el plano de control en la Región de AWS us-east-1.

Para obtener más información sobre los planos de datos, los planos de control y cómo AWS se crean servicios para cumplir los objetivos de alta disponibilidad, consulte el [artículo Static stability using Availability Zones](#) en la biblioteca de Amazon Builders.

Conceptos de comprobación de estado

A continuación se incluye información general de los conceptos relacionados con la comprobación de estado de Amazon Route 53.

- [DNS failover](#)
- [endpoint](#)
- [health check](#)

recuperación ante errores a nivel de DNS

Un método para sacar el tráfico de los recursos en mal estado y dirigirlo a recursos en buen estado. Cuando tenga más de un recurso que realice la misma función (por ejemplo, más de un servidor web o servidor de correo electrónico), puede configurar las comprobaciones de estado de Route 53 para que revisen el estado de los recursos y configurar los registros de su zona alojada para que dirijan únicamente tráfico a recursos que estén en buen estado.

Para obtener más información, consulte [Configuración de la recuperación ante errores a nivel de DNS](#).

endpoint

El recurso, como un servidor web o un servidor de correo electrónico, para el que configura una comprobación de estado para monitorizar su estado. Puede especificar un punto final por IPv4 dirección (192.0.2.243), por IPv6 dirección (2001:0 db 8:85 a 3:0000:0000:abcd: 0001:2345) o por nombre de dominio (example.com).

Note

También puede crear controles de estado que supervisen el estado de otros controles de estado o que supervisen el estado de alarma de una alarma. CloudWatch

comprobación de estado

Un componente de Route 53 que le permite hacer lo siguiente:

- Monitorizar si un puntos de conexión especificado, como un servidor web, está en buen estado
- Recibir notificaciones cuando un puntos de conexión pasa a tener un estado incorrecto
- Configurar la recuperación ante errores a nivel de DNS, que le permite redirigir el tráfico de Internet de un recurso en mal estado a un recurso en buen estado

Para obtener más información acerca de cómo crear y utilizar comprobaciones de estado, consulte [Creación de comprobaciones de estado de Amazon Route 53](#).

Primeros pasos con Amazon Route 53

Para obtener información acerca de cómo comenzar a utilizar Amazon Route 53, consulte los temas siguientes de esta guía:

- [Configuración de Amazon Route 53](#), en el que se explica cómo registrarse AWS, cómo proteger el acceso a su AWS cuenta y cómo configurar el acceso programático a Route 53
- [Introducción a Amazon Route 53](#), que describe cómo registrar un nombre de dominio, cómo crear un bucket de Amazon S3 y configurarlo para alojar un sitio web estático y cómo dirigir el tráfico de Internet al sitio web.

Acceso a Amazon Route 53

Puede acceder a Amazon Route 53 de las siguientes formas:

- Consola de administración de AWS— Los procedimientos de esta guía explican cómo utilizarlos Consola de administración de AWS para realizar tareas.
- AWS SDKs— Si usa un lenguaje de programación que AWS proporciona un SDK para, puede usar un SDK para acceder a Route 53. SDKs simplifique la autenticación, integre fácilmente su entorno de desarrollo y proporcione un acceso sencillo a los comandos de Route 53. Para obtener más información, consulte [Herramientas para Amazon Web Services](#).
- API de Route 53: si utiliza un lenguaje de programación para el que no exista un SDK, consulte la [Referencia de la API de Amazon Route 53](#) para obtener información acerca de las acciones de API y cómo realizar solicitudes de API.
- AWS Command Line Interface: para obtener más información, consulte [Configuración inicial de la AWS Command Line Interface](#) en la Guía del usuario de AWS Command Line Interface .
- AWS Tools for Windows PowerShell: para obtener más información, consulte [Configuración de AWS Tools for Windows PowerShell](#) en la Guía del usuario de Herramientas de AWS para PowerShell .

AWS Identity and Access Management

Amazon Route 53 se integra con AWS Identity and Access Management (IAM), un servicio que permite a su organización hacer lo siguiente:

- Cree usuarios y grupos en la cuenta de su organización AWS
- Comparta fácilmente los recursos de su AWS cuenta entre los usuarios de la cuenta
- Asignar credenciales de seguridad exclusivas a los usuarios
- Controlar de manera detallada el acceso de los usuarios a los servicios y recursos

Por ejemplo, puede usar IAM con Route 53 para controlar qué usuarios de su AWS cuenta pueden crear una nueva zona alojada o cambiar los registros.

Para obtener información general sobre IAM, consulte lo siguiente:

- [Identity and Access Management en Amazon Route 53](#)

- [Identity and Access Management \(IAM\)](#)
- [Guía del usuario de IAM](#)

Precios y facturación de Amazon Route 53

Al igual que con otros AWS productos, no hay contratos ni compromisos mínimos para usar Amazon Route 53. Solo se paga por las zonas alojadas que se configuran y el número de consultas de DNS a las que Route 53 responde. Para obtener más información, consulte [Precios de Amazon Route 53](#).

Para obtener información sobre la facturación de AWS los servicios, incluida la forma de ver su factura y administrar su cuenta y sus pagos, consulte la [Guía del AWS Billing usuario](#).

Uso de Route 53 con un AWS SDK

AWS Los kits de desarrollo de software (SDKs) están disponibles para muchos lenguajes de programación populares. Cada SDK proporciona una API, ejemplos de código y documentación que facilitan a los desarrolladores la creación de aplicaciones en su lenguaje preferido.

Documentación de SDK	Ejemplos de código
AWS SDK para C++	AWS SDK para C++ ejemplos de código
AWS CLI	AWS CLI ejemplos de código
AWS SDK para Go	AWS SDK para Go ejemplos de código
AWS SDK para Java	AWS SDK para Java ejemplos de código
AWS SDK para JavaScript	AWS SDK para JavaScript ejemplos de código
AWS SDK para Kotlin	AWS SDK para Kotlin ejemplos de código
AWS SDK para .NET	AWS SDK para .NET ejemplos de código
AWS SDK para PHP	AWS SDK para PHP ejemplos de código
Herramientas de AWS para PowerShell	Herramientas de AWS para PowerShell ejemplos de código

Documentación de SDK	Ejemplos de código
AWS SDK para Python (Boto3)	AWS SDK para Python (Boto3) ejemplos de código
AWS SDK para Ruby	AWS SDK para Ruby ejemplos de código
AWS SDK para Rust	AWS SDK para Rust ejemplos de código
AWS SDK para SAP ABAP	AWS SDK para SAP ABAP ejemplos de código
AWS SDK para Swift	AWS SDK para Swift ejemplos de código

Para ver ejemplos específicos de Route 53, consulte [Ejemplos de código de Route 53 con SDK de AWS](#).

 Ejemplo de disponibilidad

¿No encuentra lo que necesita? Solicite un ejemplo de código a través del enlace de Enviar comentarios que se encuentra al final de esta página.

Introducción a Amazon Route 53

Comience con los pasos básicos de registro de un dominio con Amazon Route 53 y la configuración de Route 53 para responder a las consultas de DNS que se resuelven en su sitio web. El primer tutorial aloja un sitio web estático en un bucket abierto de Amazon S3 y el segundo utiliza la CloudFront distribución de Amazon para ofrecer el sitio web con SSL/TLS.

Costo estimado

- Hay una tarifa anual para registrar un dominio, que va de 9 USD a varios centenares de dólares, según el dominio de nivel superior, como .com. Para obtener más información, consulte [Precios de Route 53 para el registro de dominio](#). Esta tarifa no es reembolsable.
- Al registrar un dominio, creamos automáticamente una zona alojada con el mismo nombre que el dominio. La zona alojada se puede usar para especificar a dónde desea que Route 53 dirija el tráfico de su dominio.
- Durante este tutorial, creará un bucket de Amazon S3 y cargará una página web de ejemplo. Si es un AWS cliente nuevo, puede empezar a utilizar Amazon S3 de forma gratuita. Si ya es AWS cliente, los cargos se basan en la cantidad de datos que almacene, en la cantidad de solicitudes de datos y en la cantidad de datos transferidos. Para obtener más información, consulte [Precios de Amazon S3](#).
- CloudFront los cargos se basan en el número de solicitudes de datos, el número de ubicaciones periféricas que utilices y la cantidad de datos transferidos. Para obtener más información, consulte [CloudFront Precios](#).

Temas

- [Configuración de Amazon Route 53](#)
- [Uso de su dominio para un sitio web estático en un bucket de Amazon S3](#)
- [Usa una CloudFront distribución de Amazon para ofrecer un sitio web estático](#)

Configuración de Amazon Route 53

La descripción general y los procedimientos de esta sección le ayudarán a empezar AWS.

Temas

- [Inscríbase en una Cuenta de AWS](#)

- [Creación de un usuario con acceso administrativo](#)
- [Descargar herramientas](#)

Inscríbase en una Cuenta de AWS

Si no tiene una Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abrir <https://portal.aws.amazon.com/billing/registro>.
2. Siga las instrucciones que se le indiquen.

Parte del procedimiento de registro consiste en recibir una llamada telefónica o mensaje de texto e indicar un código de verificación en el teclado del teléfono.

Cuando te registras en una Cuenta de AWS, Usuario raíz de la cuenta de AWS se crea uno. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar [tareas que requieren acceso de usuario raíz](#).

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. En cualquier momento, puede ver la actividad de su cuenta actual y administrarla accediendo a <https://aws.amazon.com/> y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión [Consola de administración de AWS](#) como propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

Para obtener ayuda para iniciar sesión con el usuario raíz, consulte [Iniciar sesión como usuario raíz](#) en la Guía del usuario de AWS Sign-In .

2. Active la autenticación multifactor (MFA) para el usuario raíz.

Para obtener instrucciones, consulte [Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz \(consola\)](#) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

Consulte las instrucciones en [Activar AWS IAM Identity Center](#) en la Guía del usuario de AWS IAM Identity Center .

2. En IAM Identity Center, conceda acceso administrativo a un usuario.

Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte [Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la](#) Guía del AWS IAM Identity Center usuario.

Inicio de sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, use la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte [Iniciar sesión en el portal de AWS acceso](#) en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

Para conocer las instrucciones, consulte [Create a permission set](#) en la Guía del usuario de AWS IAM Identity Center .

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

Para conocer las instrucciones, consulte [Add groups](#) en la Guía del usuario de AWS IAM Identity Center .

Descargar herramientas

Consola de administración de AWS Incluye una consola para Amazon Route 53, pero si desea acceder a los servicios mediante programación, consulte lo siguiente:

- La guía de la API documenta las operaciones que admiten los servicios y proporciona enlaces a la documentación relacionada del SDK y la CLI:
 - [Referencia de la API de Amazon Route 53](#)
- Para llamar a una API sin tener que gestionar detalles de bajo nivel, como el ensamblaje de solicitudes HTTP sin procesar, puede usar un SDK. AWS AWS SDKs Proporcionan funciones y tipos de datos que encapsulan la funcionalidad de AWS los servicios. Para descargar un AWS SDK y acceder a las instrucciones de instalación, consulta la página correspondiente:
 - [Java](#)
 - [JavaScript](#)
 - [.NET](#)
 - [Node.js](#)
 - [PHP](#)
 - [Python](#)
 - [Ruby](#)

Para obtener una lista completa AWS SDKs, consulte [Herramientas para Amazon Web Services](#).

- Puede usar AWS Command Line Interface (AWS CLI) para controlar varios AWS servicios desde la línea de comandos. También puede automatizar los comandos utilizando scripts. Para obtener más información, consulte [AWS Command Line Interface](#).
- AWS Tools for Windows PowerShell admite estos AWS servicios. Para obtener más información, consulte [Referencia de cmdlet de Herramientas de AWS para PowerShell](#).

Uso de su dominio para un sitio web estático en un bucket de Amazon S3

En este tutorial le explicaremos cómo utilizar Amazon Route 53 para enrutar el tráfico de DNS de su dominio a un bucket de Amazon Simple Storage Service que aloja un sitio web estático. Creará registros de alias que dirijan su dominio al punto de conexión del sitio web de S3.

Este tutorial forma parte de un flujo de trabajo completo de configuración de sitios web estáticos. Para obtener información general sobre cómo enrutar el tráfico a un bucket de S3, consulte [Enrutamiento del tráfico a un sitio web alojado en un bucket de Amazon S3](#).

Cuando haya terminado, los visitantes podrán acceder a su sitio web con su nombre de dominio personalizado.

Note

También puede transferir un dominio existente a Route 53, pero el proceso es más complejo y lleva más tiempo que registrar un nuevo dominio. Para obtener más información, consulte [Transferencia del registro de un dominio a Amazon Route 53](#).

Requisitos previos

Antes de comenzar, complete los pasos a continuación:

- Realice los pasos que se indican en [Configuración de Amazon Route 53](#).
- Registre un nombre de dominio mediante Amazon Route 53. Para obtener más información, consulte [Registrar un nuevo dominio](#).
- Configure un bucket de Amazon Simple Storage Service para el alojamiento de sitios web estáticos. Para obtener las instrucciones completas, consulte [Tutorial: Configuración de un sitio web estático mediante un dominio personalizado registrado con Route 53](#) en la Guía del usuario de Amazon Simple Storage Service.

Cuando haya completado el tutorial de Amazon Simple Storage Service, tendrá:

- Buckets de Amazon S3 configurados para el alojamiento y redireccionamiento de sitios web (si usa un subdominio www).
- El contenido de su sitio web cargado en el bucket.
- Acceso público configurado para el bucket de su sitio web

Paso 1: Dirija el tráfico de DNS de su dominio al depósito de su sitio web

Ahora que ya tiene un bucket de Amazon Simple Storage Service configurado para el alojamiento de sitios web estáticos, utilice Amazon Route 53 para enrutar el tráfico de DNS de su dominio al bucket. Esto permite a los visitantes acceder a su sitio web con el nombre de dominio personalizado.

Para dirigir el tráfico a su sitio web

1. Abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Zonas alojadas.

Note

Al registrar el dominio, Amazon Route 53 crea automáticamente una zona alojada con el mismo nombre. Una zona alojada contiene información sobre el modo en que desea que Route 53 dirija el tráfico del dominio.

3. En la lista de zonas alojadas, elija el nombre de su dominio.
4. Elija Crear registro.
5. Especifique los siguientes valores:

Nombre del registro

Déjelo en blanco para crear un registro para el dominio raíz.

Tipo de registro

Elija A - Dirige el tráfico a una IPv4 dirección y a algunos AWS recursos.

Alias

Active Alias.

Dirigir tráfico a

Seleccione Alias al punto de conexión del sitio web de S3.

Seleccione la región en la que creó el bucket de S3.

Seleccione el bucket de S3. El nombre del bucket debe coincidir con el nombre de su dominio. En la lista, el nombre del bucket aparece con el punto de conexión del sitio web de

Amazon S3 correspondiente a la región donde se creó el bucket, por ejemplo, `s3-website-us-west-1.amazonaws.com` (`example.com`).

Si su bucket no aparece en la lista, ingrese el punto de conexión del sitio web de Amazon S3 correspondiente a la región en la que se creó el bucket, por ejemplo, **`s3-website-us-west-2.amazonaws.com`**. Para obtener una lista completa de los puntos de enlace del sitio web de Amazon S3, consulte [Puntos de enlace de sitio web de Amazon S3](#).

Evaluate target health

Acepte el valor predeterminado de No.

6. Elija Crear registros.

(Opcional) Para agregar un registro de alias para su subdominio (**`www.example.com`**)

Si ha creado un bucket para su subdominio, agréguele también un registro de alias.

1. Elija Crear registro.
2. Especifique los siguientes valores:

Nombre del registro

Escriba **`www`**.

Tipo de registro

Elija A - Dirige el tráfico a una IPv4 dirección y a algunos AWS recursos.

Alias

Active Alias.

Dirigir tráfico a

Seleccione Alias al punto de conexión del sitio web de S3.

Seleccione la región en la que creó el bucket de S3.

Seleccione su bucket de S3 para el subdominio, por ejemplo, `s3-website-us-west-2.amazonaws.com` (`www.example.com`).

Evaluate target health

Acepte el valor predeterminado de No.

3. Elija Crear registros.

Paso 2: Pruebe su sitio web

Para comprobar que el sitio web funciona correctamente, abre un navegador web y busca lo siguiente URLs:

- `http://your-domain-name`, por ejemplo, `example.com` — Muestra el documento de índice del *your-domain-name* depósito
- `http://www.your-domain-name` por ejemplo, `www.example.com` — Redirige tu solicitud al bucket *your-domain-name*

En algunos casos, posiblemente deba eliminar la memoria caché para ver el comportamiento esperado.

Para obtener información más avanzada sobre cómo dirigir el tráfico de Internet, consulte [Configuración de Amazon Route 53 como servicio DNS](#). Para obtener información sobre cómo enrutar el tráfico de Internet a AWS los recursos, consulte [Enrutar el tráfico de Internet a sus AWS recursos](#).

Note

Amazon S3 no admite el acceso HTTPS al sitio web. Si quieres usar HTTPS, puedes usar Amazon CloudFront para ofrecer un sitio web estático alojado en Amazon S3. Para obtener más información, consulte [Usa una CloudFront distribución de Amazon para ofrecer un sitio web estático](#).

Usa una CloudFront distribución de Amazon para ofrecer un sitio web estático

En este tutorial, se muestra cómo utilizar Amazon Route 53 para enrutar el tráfico de DNS de tu dominio a CloudFront las distribuciones de Amazon que sirven a un sitio web estático. Creará registros de alias que dirijan su dominio y subdominio a CloudFront las distribuciones.

Este tutorial forma parte de un flujo de trabajo completo de configuración de sitios web estáticos. Para obtener información general sobre el enrutamiento del tráfico a cualquier CloudFront

distribución, consulte. [Enrutar el tráfico a una CloudFront distribución de Amazon mediante tu nombre de dominio](#)

Cuando haya terminado, los visitantes podrán acceder a su sitio web utilizando su nombre de dominio personalizado con la seguridad HTTPS proporcionada por CloudFront.

Requisitos previos

Antes de comenzar, complete los pasos a continuación:

- Realice los pasos que se indican en [Configuración de Amazon Route 53](#).
- Registre un nombre de dominio mediante Amazon Route 53. Para obtener más información, consulte [Registrar un nuevo dominio](#).
- Cree un sitio web estático seguro con Amazon CloudFront y Amazon Simple Storage Service. Para obtener instrucciones completas, consulta Cómo [empezar con un sitio web estático seguro](#) en la Guía para CloudFront desarrolladores de Amazon.

Cuando completes el CloudFront tutorial de Amazon, tendrás:

- Un SSL/TLS certificado para tu dominio en AWS Certificate Manager
- Buckets de Amazon S3 configurados para el alojamiento y redireccionamiento de sitios web.
- CloudFront distribuciones tanto para tu dominio raíz como para tu subdominio

Paso 1: Dirija el tráfico de DNS de su dominio a su distribución CloudFront

Ahora que tiene CloudFront distribuciones de Amazon para su sitio web, utilice Amazon Route 53 para dirigir el tráfico de DNS de su dominio a las distribuciones. Esto permite a los visitantes acceder a su sitio web con el nombre de dominio personalizado.

Para obtener más información sobre el direccionamiento del tráfico a CloudFront las distribuciones, consulte. [Enrutar el tráfico a una CloudFront distribución de Amazon mediante tu nombre de dominio](#)

Para dirigir el tráfico a su sitio web

1. Abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Zonas alojadas.

 Note

Al registrar el dominio, Amazon Route 53 crea automáticamente una zona alojada con el mismo nombre. Una zona alojada contiene información sobre el modo en que desea que Route 53 dirija el tráfico del dominio.

3. En la lista de zonas alojadas, elija el nombre de su dominio.
4. Elija Crear registro.
5. Especifique los siguientes valores:

Nombre del registro

Para el registro de su subdominio, introduzca **www**.

Tipo de registro

Elija A - Dirige el tráfico a una IPv4 dirección y a algunos AWS recursos.

Alias

Active Alias.

Dirigir tráfico a

Seleccione Alias para la CloudFront distribución.

Seleccione la región us-east-1.

Elige tu CloudFront distribución. El nombre de la distribución debe coincidir con el nombre que aparece en la columna Nombre de dominio de la CloudFront consola, por ejemplo, `dddjjjkkk.cloudfront.net`.

Evaluate target health

Acepte el valor predeterminado de No.

6. Elija Crear registros.

Para agregar un registro de alias para su dominio raíz (**example.com**)

Añada también un registro de alias para su dominio raíz, de modo que apunte a la CloudFront distribución a `www.example.com` la que redirige el tráfico.

1. Elija Crear registro.
2. Especifique los siguientes valores:

Nombre del registro

Déjelo en blanco para crear un registro para el dominio raíz.

Tipo de registro

Elija A - Dirige el tráfico a una IPv4 dirección y a algunos AWS recursos.

Alias

Active Alias.

Dirigir tráfico a

Seleccione Alias para la CloudFront distribución.

Seleccione la región us-east-1.

Elige la CloudFront distribución de tu dominio raíz.

Evaluate target health

Acepte el valor predeterminado de No.

3. Elija Crear registros.

Paso 2: Pon a prueba tu sitio web

Para comprobar que el sitio web funciona correctamente, abre un navegador web y busca lo siguiente URLs:

- <https://www.your-domain-name>, por ejemplo, www.example.com — Muestra el documento de índice en el www.your-domain-name depósito
- <https://your-domain-name> por ejemplo, example.com — Redirige la solicitud al depósito www.your-domain-name

En algunos casos, posiblemente deba eliminar la memoria caché para ver el comportamiento esperado.

Para obtener información más avanzada sobre cómo dirigir el tráfico de Internet, consulte [Configuración de Amazon Route 53 como servicio DNS](#). Para obtener información sobre cómo enrutar el tráfico de Internet a AWS los recursos, consulte [Enrutar el tráfico de Internet a sus AWS recursos](#).

Integración con otros servicios de

Puede integrar Amazon Route 53 con otros AWS servicios para registrar las solicitudes que se envían a la API de Route 53, supervisar el estado de los recursos y asignarles etiquetas. Además, puede utilizar Route 53 para dirigir el tráfico de Internet a los recursos de AWS .

Temas

- [Registro, monitorización y etiquetado](#)
- [Enrutar el tráfico a otros recursos AWS](#)

Registro, monitorización y etiquetado

AWS CloudTrail

Amazon Route 53 está integrado con AWS CloudTrail un servicio que captura información sobre todas las solicitudes que su AWS cuenta envía a la API de Route 53. Puede usar la información de los archivos de CloudTrail registro para determinar qué solicitudes se realizaron a Route 53, la dirección IP de origen desde la que se realizó cada solicitud, quién la hizo, cuándo se realizó, etc.

Para obtener más información, consulte [Registrar llamadas a la API de Amazon Route 53 con AWS CloudTrail](#).

Amazon CloudWatch

Puedes usar Amazon CloudWatch para controlar el estado (en buen estado o no) de tus controles de estado de Route 53. Las comprobaciones de estado monitorizan el estado y el desempeño de sus aplicaciones web, servidores web y otros recursos. En los intervalos regulares que especifique, Route 53 envía solicitudes automatizadas a través de Internet a su aplicación, servidor u otro recurso para comprobar que está accesible, disponible y funcional.

Para obtener más información, consulte [Monitorear comprobaciones de estado mediante CloudWatch](#).

Editor de etiquetas

Una etiqueta es una etiqueta que se asigna a un AWS recurso, incluidos los dominios de Route 53, las zonas alojadas y los controles de estado. Cada etiqueta consta de una clave y un valor, ambos definidos por el usuario. Por ejemplo, puede asignar una etiqueta a un registro de dominio

que tenga la clave "Cliente" y el valor "Example Corp.". Puede usar las etiquetas para diversos fines; uno de los usos más comunes es categorizar y realizar un seguimiento de sus AWS costos.

Para obtener más información, consulte [Etiquetado de recursos de Amazon Route 53](#).

Enrutar el tráfico a otros recursos AWS

Puede usar Amazon Route 53 para dirigir el tráfico a una variedad de AWS recursos.

Amazon API Gateway

Amazon API Gateway le permite crear, publicar, mantener, supervisar y proteger APIs a cualquier escala. Puede crear APIs ese acceso AWS u otros servicios web, así como los datos almacenados en la AWS nube.

Puede usar Route 53 para dirigir el tráfico a una API de API Gateway. Para obtener más información, consulte [Enrutamiento del tráfico a una API de Amazon API Gateway mediante su nombre de dominio](#).

Amazon CloudFront

Para acelerar la entrega de su contenido web, puede utilizar Amazon CloudFront, la red de entrega de AWS contenido (CDN). CloudFront puede ofrecer todo su sitio web (incluido el contenido dinámico, estático, de streaming e interactivo) mediante una red global de ubicaciones periféricas. CloudFront dirige las solicitudes de contenido a la ubicación perimetral que proporciona a los usuarios la latencia más baja. Puedes usar Route 53 para dirigir el tráfico de tu dominio a tu CloudFront distribución. Para obtener más información, consulte [Enrutar el tráfico a una CloudFront distribución de Amazon mediante tu nombre de dominio](#).

Amazon EC2

Amazon EC2 proporciona capacidad informática escalable en la AWS nube. Puede lanzar un entorno informático EC2 virtual (una instancia) mediante una plantilla preconfigurada (una Amazon Machine Image o AMI). Al lanzar una EC2 instancia, instala EC2 automáticamente el sistema operativo (Linux o Microsoft Windows) y el software adicional incluido en la AMI, como el software de servidor web o de base de datos.

Si aloja un sitio web o ejecuta una aplicación web en una EC2 instancia, puede dirigir el tráfico de su dominio, como example.com, a su servidor mediante Route 53. Para obtener más información, consulte [Enrutamiento del tráfico a una EC2 instancia de Amazon](#).

AWS Elastic Beanstalk

Si AWS Elastic Beanstalk solía implementar y administrar aplicaciones en la AWS nube, puede usar Route 53 para enrutar el tráfico de DNS de su dominio, como example.com, a un entorno de Elastic Beanstalk. Para obtener más información, consulte [Enrutar el tráfico a un AWS Elastic Beanstalk entorno](#).

ELB

Si alojas un sitio web en varias EC2 instancias de Amazon, puedes distribuir el tráfico a tu sitio web entre las instancias mediante un balanceador de cargas ELB (ELB). El servicio ELB escala automáticamente el balanceador de carga a medida que cambia el tráfico a su sitio web a lo largo del tiempo. Asimismo, el balanceador de carga puede monitorizar el estado de las instancias registradas y dirige el tráfico de dominio solo a las instancias con estado correcto.

Puede utilizar Route 53 para dirigir el tráfico de su dominio a su Network Load Balancer, de aplicación o clásico. Para obtener más información, consulte [Direccionamiento del tráfico a un balanceador de carga ELB](#).

Amazon Lightsail

Amazon Lightsail proporciona capacidad y funciones de informática, almacenamiento y redes para implementar y administrar sitios web, aplicaciones web y bases de datos en la nube, a un precio mensual bajo y predecible.

Si utiliza Lightsail, puede utilizar Route 53 para dirigir el tráfico a su instancia de Lightsail. Para obtener más información, consulte [Uso de Route 53 para apuntar un dominio a una instancia de Amazon Lightsail](#).

Amazon S3

Amazon Simple Storage Service (Amazon S3) proporciona un almacenamiento en la nube seguro, duradero y con un alto grado de escalabilidad. Puede configurar un bucket de S3 para alojar un sitio web estático que puede incluir páginas web y archivos de comandos de cliente. (S3 no es compatible con el scripting en el lado del servidor). Puede utilizar Route 53 para dirigir el tráfico a un bucket de Amazon S3. Para obtener más información, consulte los temas siguientes:

- Para obtener información sobre cómo dirigir el tráfico a un bucket, consulte [Enrutamiento del tráfico a un sitio web alojado en un bucket de Amazon S3](#).
- Para obtener una explicación más detallada sobre cómo hospedar un sitio web estático en un bucket de S3, consulte [Introducción a Amazon Route 53](#).

Amazon Virtual Private Cloud (Amazon VPC)

Un punto final de interfaz te permite conectarte a los servicios que funcionan con la tecnología. AWS PrivateLink Estos servicios incluyen algunos AWS servicios, los servicios alojados por otros AWS clientes y socios por sí mismos VPCs (denominados servicios de punto final) y los servicios de AWS Marketplace socios compatibles.

Puede utilizar Route 53 para dirigir el tráfico a un punto de conexión de interfaz. Para obtener más información, consulte [Enrutamiento del tráfico a un punto de conexión de interfaz de Amazon Virtual Private Cloud mediante el nombre de dominio](#).

Amazon WorkMail

Si utilizas Amazon WorkMail para el correo electrónico de tu empresa y utilizas Route 53 como servicio de DNS, puedes usar Route 53 para dirigir el tráfico a tu dominio de WorkMail correo electrónico de Amazon. Para obtener más información, consulte [Enrutamiento del tráfico a Amazon WorkMail](#).

Para obtener más información consulte [Enrutar el tráfico de Internet a sus AWS recursos](#).

Formato de nombres de dominio DNS

Los nombres de dominio (incluidos los nombres de dominios, zonas alojadas y registros) constan de una serie de etiquetas separadas por puntos. Cada etiqueta puede tener hasta 63 bytes. La longitud total de un nombre de dominio no puede superar los 255 bytes, incluidos los puntos. Amazon Route 53 admite cualquier nombre de dominio válido.

Los requisitos de nomenclatura dependen de si registra un nombre de dominio o especifica el nombre de una zona alojada o un registro. Consulte el tema correspondiente.

Formateo de nombres de dominio para el registro de nombres de dominio

En el caso del registro de nombres de dominio, un nombre de dominio puede contener únicamente los caracteres a-z, 0-9 y - (guion). No puede especificar un guion al principio o al final de una etiqueta.

Para obtener información sobre cómo registrar un nombre de dominio internacionalizado (IDN), consulte [Formato de nombres de dominio internacionalizados](#).

Formato de nombres de dominio para zonas alojadas y registros

En el caso de las zonas alojadas y los registros, el nombre de dominio puede incluir cualquiera de los siguientes caracteres ASCII imprimibles (salvo espacios):

- a-z
- 0-9
- - (guion)
- !"#\$%&'()*+,-/:;<=>?@[\\]^_`{|}~.

Amazon Route 53 almacena los caracteres alfabéticos como letras minúsculas (a-z), independientemente de la forma en que se especifiquen: como letras mayúsculas, letras minúsculas o las letras correspondientes en códigos de escape.

Si su nombre de dominio contiene alguno de los siguientes caracteres, debe especificar los caracteres usando códigos de escape en el formato *`\código octal de tres dígitos`*:

- Caracteres de 000 a 040 octales (de 0 a 32 decimales, de 0x20 a 0x00 hexadecimales)
- Caracteres de 177 a 377 octales (de 127 a 255 decimales, de 0x7F a 0xFF hexadecimales)
- . (punto), carácter 056 octal (46 decimal, 0x2E hexadecimal), cuando se usa como un carácter en un nombre de dominio. Cuando se usa . como un delimitador entre etiquetas, no es necesario utilizar un código de escape.

Si el nombre de dominio incluye caracteres distintos de a-z, 0-9, - (guion), o _ (guion bajo), las acciones de la API de Route 53 devuelven los caracteres como códigos de escape. Esto es así tanto si especifica los caracteres como caracteres o como códigos de escape cuando crea la entidad. La consola de Route 53 muestra los caracteres como caracteres, no como códigos de escape.

Para obtener una lista de los caracteres ASCII y sus códigos octales correspondientes, busque en Internet “tabla ascii”.

Para especificar un nombre de dominio internacionalizado (IDN), convierta el nombre a Punycode. Para obtener más información, consulte [Formato de nombres de dominio internacionalizados](#).

Uso de un asterisco (*) en nombres de zonas alojadas y registros

Puede crear zonas alojadas y registros que incluyan * en el nombre.

Zonas alojadas

- No puede incluir un * en la etiqueta del extremo izquierdo de un nombre de dominio. Por ejemplo, *.ejemplo.com no se permite.
- Si incluye * en otras posiciones, DNS lo trata como un carácter * (ASCII 42) y no como un carácter comodín.

Registros

DNS trata el asterisco como comodín o como el carácter ASCII (42) *, en función de dónde aparece en el nombre. Tenga en cuenta las siguientes restricciones sobre el uso de * como carácter comodín en el nombre de un registro:

- El * debe sustituir a la etiqueta del extremo izquierdo de un nombre de dominio (por ejemplo, *.example.com o *.acme.example.com.) Si incluye * en cualquier otra posición, como prod.*.example.com, DNS lo trata como un carácter * (ASCII 42) y no como un carácter comodín.

- El * debe sustituir a toda la etiqueta. Por ejemplo, no puede especificar *prod.ejemplo.com ni prod*.ejemplo.com.
- Los nombres de dominio específicos tienen preferencia. Por ejemplo, si crea registros para *.example.com y acme.example.com, Route 53 siempre responde a las consulta de DNS para acme.example.com con los valores del registro acme.example.com.
- El * se aplica a las consultas de DNS para el nivel de subdominio que incluye el asterisco, y todos los subdominios de dicho subdominio. Por ejemplo, si crea un registro denominado *.example.com, Route 53 utiliza los valores en ese registro para responder a las consultas de DNS de zenith.example.com, acme.zenith.example.com y pinnacle.acme.zenith.example.com (si no hay registros de ningún tipo para esa zona alojada).

Si crea un registro denominado *.example.com y no hay un registro example.com, Route 53 responde a las consultas de DNS para example.com con NXDOMAIN (dominio no existente).

Note

Si usa Route 53 con AWS Certificate Manager, tenga en cuenta que los certificados con comodín de ACM solo protegen un nivel de subdominio. Por ejemplo, el certificado de ACM para *.example.com protege a login.example.com y test.example.com, pero no a test.login.example.com. Para obtener más información, consulte [AWS Certificate Manager certificate characteristics and limitations](#).

- Puede configurar Route 53 para devolver la misma respuesta a las consultas de DNS tanto para todos los subdominios en el mismo nivel como para el nombre de dominio. Por ejemplo, puede configurar Route 53 para que responda a las consultas de DNS como acme.example.com y zenith.example.com utilizando el registro example.com. Siga estos pasos:
 1. Cree un registro para el dominio, como example.com.
 2. Cree un registro de alias para el subdominio, como *.example.com. Especifique el registro que ha creado en el paso 1 como el destino del registro de alias.
- No puede usar el asterisco como carácter comodín para los registros con el tipo NS.

Formato de nombres de dominio internacionalizados

Cuando registra un nuevo nombre de dominio o crea zonas alojadas y registros, puede especificar letras distintas de a-z (por ejemplo, la ç francesa), caracteres de otros alfabetos (por ejemplo, cirílico

o árabe) y caracteres en chino, japonés o coreano. Amazon Route 53 almacena estos nombres de dominio internacionalizados (IDN) en Punycode, que representa los caracteres Unicode como cadenas ASCII.

Si está registrando un nombre de dominio, tenga en cuenta lo siguiente:

- Puede utilizar caracteres distintos de a-z, 0-9 y - (guion) solo si el dominio de nivel superior (TLD) admite IDN y admite el idioma que desea utilizar. Para determinar qué idiomas admite un TLD, consulte [Dominios que puede registrar con Amazon Route 53](#).
- Puede especificar un nombre en un idioma no admitido si el nombre solo contiene letras de a-z. Por ejemplo, si un TLD no admite francés pero el nombre que desea utilizar incluye solo los caracteres a-z sin marcas diacríticas, puede seguir utilizando ese nombre. En este ejemplo, se permite un nombre que incluya una “c”, pero no un nombre que contenga una “ç”.
- Si un TLD no admite IDN o no admite el idioma que desea usar para su nombre de dominio, tampoco puede especificar el nombre en Punycode aunque el Punycode incluya solo a-z, 0-9 y -.

El siguiente ejemplo muestra la representación en Punycode del nombre de dominio internacionalizado 中国.asia:

```
xn--fiqs8s.asia
```

Cuando introduce un IDN en la barra de direcciones de un navegador moderno, el navegador lo convierte a Punycode antes de enviar una consulta DNS o realizar una solicitud HTTP.

El modo en que especifica un IDN depende de lo que vaya a crear (nombres de dominio, zonas alojadas o registros) y de cómo vaya a crearlo (API, SDK o consola de Route 53):

- Si utiliza la API de Route 53 o uno de los AWS SDK, puede convertir un valor Unicode a Punycode mediante programación. Por ejemplo, si utiliza Java, puede convertir un valor Unicode a Punycode mediante el método `toASCII` de la biblioteca de IDN de `java.net`.
- Si utiliza la consola de Route 53 para registrar un nombre de dominio, puede pegar el nombre, incluidos los caracteres Unicode, en el campo de nombre y la consola convertirá el valor a Punycode antes de guardarlo.
- Si utiliza la consola de Route 53 para crear zonas alojadas o registros, debe convertir el nombre de dominio a Punycode antes de especificar el nombre en el campo Name (Nombre) correspondiente. Para obtener información sobre convertidores online, busque en Internet “convertidor de punycode”.

Si va a registrar un nombre de dominio, tenga en cuenta que no todos los dominios de nivel superior (TLD) admiten nombres de dominio internacionalizados. Para obtener una lista de los TLD admitidos por Route 53, consulte [Dominios que puede registrar con Amazon Route 53](#). Se indican los TLD que no admiten nombres de dominio internacionalizados.

Registro y administración de dominios mediante Amazon Route 53

Cuando desee obtener un nuevo nombre de dominio, como la parte de example.com de la dirección URL <http://example.com>, puede registrarlo con Amazon Route 53. También puede transferir el registro de dominios existentes desde otros registradores a Route 53 o transferir el registro de dominios que registra con Route 53 a otro registrador.

Los procedimientos de este capítulo explican cómo registrar y transferir dominios mediante la consola de Route 53 y cómo editar la configuración del dominio y ver el estado del dominio. Si solo va a registrar y administrar algunos dominios, lo más fácil es usar la consola.

Si necesita registrar y administrar una gran cantidad de dominios, es posible que prefiera realizar los cambios mediante programación. Para obtener más información, consulte [Configuración de Amazon Route 53](#).

Note

Si utilizas un lenguaje para el que existe un AWS SDK, utilízalo en lugar de intentar trabajar con él APIs. SDKs Simplifican la autenticación, se integran fácilmente en su entorno de desarrollo y proporcionan un fácil acceso a los comandos de Route 53.

Los servicios de registro de nombres de dominio se proporcionan de acuerdo con nuestro [Acuerdo de registro de nombres de dominio](#).

Temas

- [Registro de nuevos dominios](#)
- [Actualización de la configuración de un dominio](#)
- [Renovar el registro de un dominio](#)
- [Restauración de un dominio caducado o eliminado](#)
- [Sustitución de la zona alojada para un dominio registrado con Route 53](#)
- [Transferencia de dominios](#)
- [Reenvío de los emails de autorización y confirmación](#)
- [Configurar DNSSEC para un dominio](#)

- [Búsqueda del registrador y otra información del dominio](#)
- [Eliminación de un registro de nombre de dominio](#)
- [Ponerse en contacto con AWS Support sobre problemas de registro de dominios](#)
- [Descargar un informe de facturación de dominios](#)
- [Dominios que puede registrar con Amazon Route 53](#)

Registro de nuevos dominios

En esta sección se tratan los siguientes temas relacionados con el registro de nuevos dominios en Amazon Route 53:

1. [Registrar un nuevo dominio](#):

- Aprenda el step-by-step procedimiento para registrar un nuevo dominio mediante la consola de Route 53.
- Comprenda las consideraciones y los requisitos previos para el registro de dominios, como ponerse en contacto con AWS Support en caso de problemas, los precios, los dominios de nivel superior compatibles (TLDs) y la creación automática de zonas alojadas.

2. [Valores que especifican cuando registra o transfiere un dominio](#):

- Descubra los valores que debe proporcionar al registrar o transferir un dominio, incluidas la información de contacto, la configuración de protección de la privacidad y las opciones de renovación automática.
- Comprenda las implicaciones de cambiar ciertos valores, como el titular del dominio y la dirección de correo electrónico del registrador.

3. [Valores que Amazon Route 53 devuelve cuando registra un dominio](#):

- Conozca los valores que devuelve Route 53 tras registrar de manera correcta el dominio, lo que incluye la fecha de registro, la fecha de caducidad, los códigos de estado del dominio, el estado de bloqueo de la transferencia y los servidores de nombres.

4. [Visualización del estado de registro de un dominio](#):

- Descubra cómo ver el estado actual del registro de su dominio, incluidos los códigos de estado de la ICANN, además de cualquier acción que deba realizarse de su parte, como verificar la dirección de correo electrónico del registrador.

Registrar un nuevo dominio

Registre un dominio nuevo o actualice los servidores de nombres de un dominio existente

Puede utilizar Amazon Route 53 con dominios que registre con Route 53 y con dominios que tenga registrados con otros proveedores de DNS. En función del proveedor de DNS, elija uno de los siguientes procedimientos para registrarse y usar un nuevo dominio con Route 53:

- Para registrar un nuevo dominio, consulte [Registro de un nuevo dominio mediante Route 53](#).
- Para un dominio existente, consulte [Establecer Amazon Route 53 como servicio DNS de un dominio existente](#).
- Para mover un dominio a otro registrador, consulte [Actualización de los servidores de nombres cuando desea utilizar otro servicio DNS](#).

Consideraciones sobre el registro de dominios

Antes de comenzar, tenga en cuenta lo siguiente:

Ponerse en contacto con AWS Support

Si tienes problemas al registrar un dominio, puedes ponerte en contacto con AWS Support de forma gratuita. Para obtener más información, consulte [Ponerse en contacto con AWS Support sobre problemas de registro de dominios](#).

Precios del registro de dominios

Para obtener información acerca del coste del registro de dominios, consulte [Precios de Amazon Route 53 para el registro de dominios](#).

Dominios admitidos

Para obtener una lista de los compatibles TLDs, consulte [Dominios que puede registrar con Amazon Route 53](#).

No se puede cambiar un nombre de dominio después de registrarlo

Si accidentalmente registra un nombre de dominio erróneo, no podrá cambiarlo. En su lugar, debe registrar otro nombre de dominio y especificar el nombre correcto. Tampoco puede obtener un reembolso por un nombre de dominio que haya registrado accidentalmente.

AWS créditos

No puede usar AWS los créditos para pagar la tarifa de registro de un nuevo dominio en Route 53.

Precios especiales o Premium

Los registradores de TLD han asignado precios especiales o Premium a algunos nombres de dominio. No se puede utilizar Route 53 para registrar dominios con precio especial o premium.

Cargos para zonas alojadas

Al registrar un dominio con Route 53, se creará automáticamente una zona alojada para el dominio y se cargará una pequeña tarifa mensual por dicha zona alojada, además de los cargos anuales por el registro de dominio. Esta zona alojada es donde guardas información sobre cómo enrutar el tráfico de tu dominio, por ejemplo, a una EC2 instancia de Amazon o a una CloudFront distribución. Si no desea utilizar su dominio en este momento, puede eliminar la zona alojada; si la elimina antes de que transcurran 12 horas desde el momento de registrar el dominio, no se le aplicará ningún cargo por la zona alojada en su factura de AWS . También cobramos una pequeña cuota por las consultas DNS que recibimos para su dominio. Para obtener más información, consulte [Precios de Amazon Route 53](#).

Sustitución de la zona alojada para un dominio

Si crea una zona alojada nueva para un dominio, también debe actualizar los servidores de nombres del dominio a fin de usar los mismos servidores de nombres que la nueva zona alojada. Para más información, consulte, [Sustitución de la zona alojada para un dominio registrado con Route 53](#)

Registro de un nuevo dominio mediante Route 53

Registro de un nuevo dominio mediante Route 53

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Dominios y luego Dominio registrados.
3. En la página Dominios registrados, seleccione Registrar dominios.
 - a. En la sección Buscar dominio, introduzca el nombre de dominio que desea registrar y elija Buscar para averiguar si el nombre de dominio está disponible.

Si el nombre de dominio que desea registrar contiene caracteres distintos de a-z, A-Z, 0-9 y — (guión), tenga en cuenta lo siguiente:

- Puede escribir el nombre utilizando los caracteres correspondientes. No necesita convertir el nombre a Punycode.
- Aparece una lista de idiomas. Elija el idioma del nombre especificado. Por ejemplo, si escribe příklad («ejemplo» en checo), elija checo (CES) o checo (CZE).

 Note

Para los idiomas que tienen más de un código, es posible que tenga que probar ambos. Aunque CES y CZE son sinónimos, algunos registros TLD solo admiten uno u otro.

Para obtener información sobre cómo especificar caracteres distintos de a-z, 0-9 y - (guion), y cómo especificar nombres de dominio internacionalizados, consulte [Formato de nombres de dominio DNS](#).

Si el dominio que introdujo está disponible, se mostrará; de lo contrario, se mostrarán dominios similares como sugerencias.

Puede elegir hasta cinco dominios para registrarlos. Los dominios que seleccione aparecen en la lista de Dominios seleccionados.

- b. Para registrar más dominios, repita los pasos 3a a 3b.
4. Seleccione Proceder al pago.
 5. En la página Precios, elija el número de años durante los que desea registrar el dominio y si desea que renovemos automáticamente el registro del dominio antes de la fecha de vencimiento.

 Note

Los registros y las renovaciones de nombres de dominio no son reembolsables. Si habilita la renovación automática de dominios y decide que no desea el nombre de

dominio después de renovar el registro, no podrá obtener un reembolso por el costo de la renovación.

Elija Siguiente.

6. En la página Información de contacto, escriba la información de contacto del registrador del dominio, del administrador, de los técnicos y de los contactos de facturación. Los valores que especifique aquí se aplicarán a todos los dominios que registre. Para obtener más información, consulte [Valores que especifican cuando registra o transfiere un dominio](#).

 Important

El contacto que indique como titular durante el registro del dominio tendrá determinados derechos como titular del nombre registrado del nombre de dominio, según la [Política de transferencia de la ICANN](#). La mayoría de los dominios se eliminarán cuando cierre su Cuenta de AWS (para obtener más información, consulte [Mi cuenta de AWS está cerrada o se ha cerrado de forma definitiva y mi dominio está registrado con Route 53](#)). Sin embargo, si un dominio permanece en una cuenta cerrada, el contacto que indicó como titular puede solicitar una transferencia del nombre de dominio a un registrador externo. Por lo tanto, es importante que el contacto de titular de registro que muestre sea usted mismo u otra persona en la que confíe para actuar de manera responsable.

Tenga en cuenta las siguientes consideraciones:

Nombre y apellidos

En First Name y Last Name, le recomendamos que indique el nombre que figura en su ID oficial. Para la realización de determinados cambios en la configuración del dominio, en algunos registros de dominio es necesario que se identifique. El nombre de su ID debe coincidir con el nombre del titular del dominio.

Contactos diferentes

De forma predeterminada, utilizamos la misma información para los tres contactos. Si quiere ingresar información diferente para uno o más contactos, desactive el valor Igual que el titular.

 Note

Para los dominios .it, el titular y el administrador deben ser la misma persona.

 Note

Para los dominios .jp, los contactos técnicos y administrativos deben ser los mismos.

Varios dominios

Si va a registrar más de un dominio, utilizaremos la misma información de contacto para todos los dominios.

Información adicional obligatoria

En el caso de algunos dominios de nivel superior (TLDs), debemos recopilar información adicional. Para estos TLDs, introduce los valores aplicables después del campo Código postal/postal.

Protección de la privacidad

Elija si desea ocultar su información de contacto de las consultas WHOIS.

 Note

Debe especificar la misma configuración de privacidad en los contactos administrativos, en los contactos del registrador, en los contactos técnicos y en los contactos de facturación.

Para obtener más información, consulte los temas siguientes:

- [Activación o desactivación de la protección de privacidad para la información de contacto para un dominio](#)
- [Dominios que puede registrar con Amazon Route 53](#)

 Note

Para habilitar la protección de privacidad de los dominios.uk, .co.uk, .me.uk, y .org.uk, debe abrir un caso de soporte técnico y solicitar la protección de privacidad.

Elija Siguiente.

7. En la página Revisar, verifique la información que introdujo, y corríjala si es necesario, lea los términos y condiciones del servicio, y seleccione la casilla de verificación para confirmar que los leyó.

Elija Enviar.

8. En el panel de navegación, seleccione Dominios y, a continuación, Solicitudes.

En esta página puede ver el estado del dominio y también si necesita responder el correo electrónico de verificación de contacto del titular. También puede optar por volver a enviar el correo electrónico de verificación.

Si especificó una dirección de correo electrónico para el contacto de titular que nunca se haya utilizado a fin de registrar un dominio con Route 53, algunos registros TLD necesitan que verifique que la dirección es válida.

Le enviaremos un correo electrónico de verificación desde una de las siguientes direcciones de correo electrónico:

- `noreply@registrar.amazon`: si TLDs está registrado por Amazon Registrar.
- `noreply@domainnameverification.net`: para ser TLDs registrado por nuestro registrador asociado, Gandi. Para determinar quién es el registrador de su TLD, consulte [Búsqueda del registrador](#).

 Important

El contacto del registrante debe seguir las instrucciones del correo electrónico para verificar que se ha recibido el correo electrónico, ya que, en caso contrario, suspenderemos el dominio, tal y como exige ICANN. Cuando se suspende un dominio, esté no está accesible en Internet.

- a. Cuando reciba el correo electrónico de verificación, seleccione el enlace del correo electrónico que verifica que la dirección de correo electrónico es válida. Si no recibe el correo electrónico inmediatamente, compruebe la carpeta de basura.
 - b. Volver a la página Solicitudes. Si el estado no se actualiza automáticamente para mostrar que la dirección de correo electrónico está verificada, actualice el navegador.
9. Cuando se haya completado el registro del dominio, el siguiente paso depende de si desea utilizar Route 53 u otro servicio DNS como servicio DNS para el dominio:
 - Route 53: en la zona alojada que Route 53 creó cuando registró el dominio, cree registros para indicar a Route 53 cómo desea dirigir el tráfico del dominio y los subdominios.

Por ejemplo, cuando alguien escribe su nombre de dominio en un navegador y esa consulta se reenvía a Route 53, ¿quiere que Route 53 responda a la consulta con la dirección IP de un servidor web de su centro de datos o con el nombre de un balanceador de carga de ELB?

Para obtener más información, consulte [Uso de registros](#).

 Important

Si crea registros en una zona alojada diferente de la que Route 53 crea automáticamente, debe actualizar los servidores de nombres del dominio para utilizar los servidores de nombres de la zona alojada nueva.

- Otro servicio DNS: configure su nuevo dominio para dirigir las consultas de DNS al otro servicio DNS. Realice el procedimiento [Actualización de los servidores de nombres para utilizar otro registrador](#).

Valores que especifican cuando registra o transfiere un dominio

 Note

Hemos actualizado la consola de dominios de Route 53. Durante el periodo de transición, puede seguir utilizando la consola anterior o utilizar la consola nueva. La mayoría de la información que muestra Route 53 es la misma para ambas consolas. Las diferencias se indican en la siguiente lista.

Al registrar un dominio o transferir un registro de dominio a Amazon Route 53, debe especificar los valores que se describen en este tema.

 Note

Si registra más de un dominio, Route 53 utiliza los valores que especifica para todos los dominios que están en el carro de la compra.

También puede cambiar los valores de un dominio que esté actualmente registrado con Route 53. Tenga en cuenta lo siguiente:

- Si cambia la información de contacto del dominio, enviaremos una notificación por correo electrónico al contacto del titular para informarle sobre el cambio. Este correo electrónico proviene de noreply@registrar.amazon. Para la mayoría de los cambios, no es necesario que el contacto del titular responda.
- Para los cambios en la información de contacto que también constituyen un cambio de propiedad, enviamos un correo electrónico adicional al contacto del titular. ICANN requiere que el contacto del titular confirme la recepción del correo electrónico. Para obtener más información, consulte First Name, Last Name y Organization más adelante en esta sección.

Para obtener más información sobre cómo cambiar la configuración de un dominio existente, consulte [Actualización de la configuración de un dominio](#).

Valores que especifica

- [My Registrant, Administrative, and Technical contacts are all the same](#)
- [Contact Type](#)
- [First Name, Last Name](#)
- [Organization](#)
- [Email](#)
- [Phone](#)
- [Address 1](#)
- [Address 2](#)
- [Country](#)

- [State](#)
- [City](#)
- [Postal/Zip Code](#)
- [Fields for selected top-level domains](#)
- [Privacy Protection](#)
- [Auto-renew](#)

Igual que el contacto del registrador

Esta opción especifica que desea utilizar la misma información de contacto para el titular del dominio, el contacto administrativo y el contacto técnico.

Contact Type

Categoría de este contacto. Tenga en cuenta lo siguiente:

- Si elige una opción distinta de Person, debe introducir un nombre de organización.
- Para algunos TLDs, la protección de privacidad disponible depende del valor que elijas para el tipo de contacto. Para la configuración de la protección de la privacidad de su TLD, consulte [Dominios que puede registrar con Amazon Route 53](#).
- En dominios .es, el valor de Tipo de contacto debe ser Persona para los tres contactos.

Nombre, apellido

El nombre y los apellidos del contacto.

Important

En First Name y Last Name, le recomendamos que indique el nombre que figura en su ID oficial. Para algunos cambios en la configuración de dominio, debe proporcionar pruebas que demuestren su identidad y el nombre que figura en su ID debe coincidir con el nombre del titular del dominio.

Si va a transferir un dominio a Route 53 y las siguientes condiciones son verdaderas, va a cambiar el propietario del dominio:

- El tipo de contacto es Person (Persona).

- Estás cambiando los campos Nombre and/or y Apellidos del contacto registrado desde la configuración actual.

En dicho caso, ICANN requiere que enviemos un correo electrónico al contacto del solicitante para obtener la aprobación. Le enviaremos un correo electrónico desde una de las siguientes direcciones de correo electrónico:

TLDs	Dirección de correo electrónico de donde procede el correo electrónico de aprobación
TLDs registrado por Amazon Registrar	noreply@registrar.amazon
.fr	nic@nic.fr (El correo electrónico se envía al contacto del registrante actual y al contacto del nuevo registrante).
Todos los demás	noreply@domainnameverification.net

Para determinar quién es el registrador de su TLD, consulte [Dominios que puede registrar con Amazon Route 53](#).

 Important

El contacto del registrante debe seguir las instrucciones del correo electrónico para confirmar que se ha recibido el correo electrónico, ya que, en caso contrario, suspenderemos el dominio, tal y como exige ICANN. Cuando se suspende un dominio, esté no está accesible en Internet.

Si cambia la dirección de correo electrónico del contacto del registrante, este correo electrónico se envía a la antigua dirección de correo electrónico y a la nueva dirección de correo electrónico de contacto del registrante.

Algunos registradores de TLD cobran por cambiar el propietario del dominio. Al cambiar uno de estos valores, la consola de Route 53 muestra un mensaje que le indica si tiene que abonar alguna cantidad.

Organization

La organización que está asociada con el contacto, si hay alguna. Para los contactos del titular y administrativo, suele ser la organización que registra el dominio. Para el contacto técnico, podría ser la organización que administra el dominio.

Cuando el tipo de contacto es cualquier valor salvo Person y cambia el campo Organization del contacto del registrante, cambia el propietario del dominio. ICANN requiere que enviemos un correo electrónico al contacto del titular para obtener la aprobación. Le enviaremos un correo electrónico desde una de las siguientes direcciones de correo electrónico:

TLDs	Dirección de correo electrónico de donde procede el correo electrónico de aprobación
TLDs registrado por Amazon Registrar	noreply@registrar.amazon
.fr	nic@nic.fr (El correo electrónico se envía al contacto del registrante actual y al contacto del nuevo registrante).
Todos los demás	noreply@domainnameverification.net

Para determinar quién es el registrador de su TLD, consulte [Dominios que puede registrar con Amazon Route 53](#).

Si cambia la dirección de correo electrónico del contacto del registrante, este correo electrónico se envía a la antigua dirección de correo electrónico y a la nueva dirección de correo electrónico de contacto del registrante.

Algunos registradores de TLD cobran por cambiar el propietario del dominio. Al cambiar el valor de Organization (Organización), la consola de Route 53 muestra un mensaje que le indica si tiene que abonar alguna cantidad.

Email

La dirección de correo electrónico del contacto.

Si cambia la dirección de correo electrónico del contacto del registrante, enviamos un correo electrónico de notificación a la antigua dirección de correo electrónico y a la nueva dirección de correo electrónico. Este correo electrónico proviene de `noreply@registrar.amazon`.

Phone

El número de teléfono del contacto:

- Si introduce un número de teléfono para algún lugar de Estados Unidos o Canadá, escriba 1 en el primer campo, y el código de área de 10 dígitos y el número de teléfono en el segundo campo.
- Si introduce un número de teléfono de cualquier otra ubicación, escriba el código de país en el primer campo e introduzca el resto del número de teléfono en el segundo campo. Para obtener una lista de prefijos telefónicos de países, consulte el artículo de Wikipedia [Prefijos telefónicos mundiales](#).

Dirección 1

La calle del contacto.

Dirección 2

información adicional de la dirección del contacto, como el número de apartamento o el apartado de correos.

País

El país del contacto.

Estado

El estado o provincia del contacto, si procede.

Ciudad

La ciudad del contacto.

Código postal

El código postal del contacto.

Campos para algunos dominios de nivel superior

Los siguientes dominios de nivel superior (TLDs) requieren que especifique valores adicionales:

- `.com.au` y `.net.au`
- `.ca`

- .es
- .fi
- .fr
- .it
- .ru
- .se
- .sg
- .co.uk, .me.uk y .org.uk y .uk

Además, muchos TLDs requieren un número de identificación fiscal.

Para obtener información sobre los valores válidos, consulte [ExtraParam](#) la referencia de la API de Amazon Route 53.

Privacy Protection

Si desea mostrar su información de contacto en las consultas WHOIS. Si selecciona Activar protección de privacidad (nueva consola) u Ocultar información de contacto (consola antigua), las consultas de WHOIS (“quién es”) mostrarán información de contacto del registrador o el valor “Protegido por política”.

Note

Debe especificar la misma configuración de privacidad en los contactos administrativos, en los contactos del registrador, en los contactos técnicos y en los contactos de facturación.

Si selecciona Don't hide contact information, obtendrá más spam en la dirección de correo electrónico que ha especificado.

Cualquiera puede enviar una consulta WHOIS para un dominio y obtener toda la información de contacto de dicho dominio. El comando WHOIS está disponible en muchos sistemas operativos y también como aplicación web en muchos sitios web.

Important

Aunque hay usuarios legítimos que solicitan la información de contacto asociada al dominio, los usuarios más comunes son spammers que atacan a los contactos del

dominio con correo no deseado y ofertas falsas. En general, le recomendamos que elija Hide contact information para Privacy Protection.

Para habilitar o desactivar la protección de privacidad de algunos dominios, debe abrir un caso de soporte técnico y solicitar la protección de privacidad.

Para obtener más información acerca de la protección de la privacidad, consulte los siguientes temas:

- [Activación o desactivación de la protección de privacidad para la información de contacto para un dominio](#)
- [Dominios que puede registrar con Amazon Route 53](#)

Auto Renew (solo disponible cuando se edita la configuración del dominio)

Si desea que Route 53 renueve automáticamente el dominio antes de que venza. La cuota de registro se carga a su AWS cuenta. En la consola anterior, esta configuración solo estaba disponible cuando se editaba la configuración del dominio. Para obtener más información, consulte [Renovar el registro de un dominio](#).

 Important

Si desactiva la renovación automática, el registro del dominio no se renovará cuando llegue la fecha de vencimiento y podría perder el control del nombre de dominio.

El período durante el que puede renovar un nombre de dominio varía en función del dominio de nivel superior (TLD). Si desea obtener información general sobre cómo renovar los dominios, consulte [Renovar el registro de un dominio](#). Para obtener información sobre cómo ampliar el registro del dominio durante un número específico de años, consulte [Ampliación del periodo de registro de un dominio](#).

Valores que Amazon Route 53 devuelve cuando registra un dominio

Al registrar su dominio con Amazon Route 53, Route 53 devuelve los siguientes valores, además de los valores que ha especificado.

Registered on

La fecha en que se registró originalmente el dominio con Route 53.

Expires on

La fecha y hora en que vence el periodo de registro actual, en la hora del meridiano de Greenwich (GMT).

El período de registro suele ser de un año, aunque los registros de algunos dominios de nivel superior (TLDs) tienen períodos de registro más largos. Para conocer el periodo de registro y renovación de su TLD, consulte [Dominios que puede registrar con Amazon Route 53](#).

En la mayoría de los casos TLDs, puedes ampliar el período de registro hasta diez años. Para obtener más información, consulte [Ampliación del periodo de registro de un dominio](#).

Domain name status code

El estado actual del dominio.

ICANN, la organización que mantiene una base de datos central de nombres de dominio, ha desarrollado un conjunto de códigos de estado de nombres de dominio (denominados también códigos de estado EPP) que le indican el estado de una serie de operaciones de un nombre de dominio. Por ejemplo, registrar un nombre de dominio, transferir un nombre de dominio a otro registrador, renovar el registro de un nombre de dominio, y así sucesivamente. Todos los registradores utilizan este mismo conjunto de códigos de estado.

Para ver una lista actual de códigos de estado de nombres de dominio y una explicación de cada código, visite el [sitio web de ICANN](#) y busque epp status codes. (Busque en el sitio web de la ICANN; a veces las búsquedas web devuelven una versión antigua del documento).

Transfer lock

Si el dominio está bloqueado para reducir la posibilidad de que alguien lo transfiera a otro registrador sin su permiso. Si el dominio está bloqueado, el valor de Bloqueo de transferencia es Activado. Si el dominio no está bloqueado, el valor es Desactivado.

Auto renew

Si Route 53 renovará automáticamente el registro de este dominio poco antes de la fecha de vencimiento.

Authorization code

El código necesario si desea transferir el registro de este dominio a otro registrador. El código de autorización solo se genera cuando lo solicita. Para obtener información sobre cómo transferir un dominio a otro registrador, consulte [Transferencia de un dominio de Amazon Route 53 a otro registrador](#).

Name servers

Los servidores de Route 53 que responden a las consultas de DNS de este dominio. Le recomendamos que no elimine los servidores de nombres de Route 53.

Para obtener información sobre cómo añadir, modificar o eliminar servidores de nombres, consulte [Adición o modificación de servidores de nombres y registros de conexión de un dominio](#).

Visualización del estado de registro de un dominio

ICANN, la organización que mantiene una base de datos central de nombres de dominio, ha desarrollado un conjunto de códigos de estado de nombres de dominio (denominados también códigos de estado EPP) que le indican el estado de una serie de operaciones, como registrar un nombre de dominio, transferir un nombre de dominio a otro registrador, renovar el registro de un nombre de dominio, etc. Todos los registradores utilizan este mismo conjunto de códigos de estado.

Para ver el código de estado de sus dominios, siga el procedimiento que se indica a continuación.

Para ver el código de estado de ICANN de un dominio.

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, expanda Dominios y elija Dominios registrados.
3. Seleccione el nombre vinculado de su dominio.
4. Si necesita realizar alguna acción, como volver a enviar el correo electrónico de verificación al contacto del titular, aparecerá un banner en la parte superior de la página en el que se indicará la acción que debe realizar.
5. Para ver el estado actual de su dominio, consulte el valor del campo Código de estado del dominio.

Para ver una lista actual de códigos de estado de nombres de dominio y una explicación de cada código, visite el [sitio web de ICANN](#) y busque epp status codes. (Busque en el sitio web de la ICANN; a veces las búsquedas web devuelven una versión antigua del documento).

También puede ver el estado del registro en la página Solicitudes.

Para ver el estado del registro

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, expanda Dominios y elija Solicitudes.
3. En la página Solicitudes, puede ver el estado del registro y, adicionalmente, el estado de cualquier otra acción, como eliminar dominios, bloquear transferencias de dominio, agregar o eliminar claves DNSSEC, que haya realizado en dominios,

También se muestra cualquier acción que deba realizar para completar un proceso, como verificar su correo electrónico.

- Para responder a una solicitud de acción, seleccione el botón de radio situado junto al nombre de dominio y, a continuación, seleccione la acción en el menú desplegable Acción.

Actualización de la configuración de un dominio

En esta sección, se proporciona información sobre los siguientes temas relacionados con la administración de la configuración del dominio en Route 53:

1. [Actualización de la información de contacto y la propiedad de un dominio:](#)
 - Aprenda a actualizar la información de contacto de un dominio, incluidos los contactos administrativos, técnicos, del registrador y de facturación.
 - Comprenda el proceso para cambiar el propietario de un dominio cuando el registro requiere un formulario de cambio de propiedad de dominio.
2. [Activación o desactivación de la protección de privacidad para la información de contacto para un dominio:](#)
 - Descubra cómo activar o desactivar la protección de la privacidad de la información de contacto, que oculta o revela sus datos personales en las consultas de WHOIS.

3. [Activación o desactivación de la renovación automática de un dominio](#):

- Descubra cómo activar o desactivar la renovación automática de un dominio, que determina si Route 53 renueva de manera automática el registro antes de su caducidad.

4. [Bloqueo de un dominio para impedir la transferencia no autorizada a otro registrador](#):

- Obtenga información sobre cómo bloquear un dominio para impedir la transferencia no autorizada a otro registrador, así como cómo deshabilitar el bloqueo cuando sea necesario.

5. [Ampliación del periodo de registro de un dominio](#):

- Comprenda el proceso de ampliar el período de registro de un dominio, normalmente hasta diez años con incrementos de forma anual.

6. [Actualización de los servidores de nombres para utilizar otro registrador](#) y [Adición o modificación de servidores de nombres y registros de conexión de un dominio](#):

- Descubra cómo actualizar los servidores de nombres para que usen otro servicio de DNS o cómo configurar servidores de nombres de etiqueta blanca (personalizados).
- Obtenga información sobre las consideraciones y las prácticas recomendadas a la hora de cambiar los servidores de nombres y los registros de adherencia.

Actualización de la información de contacto y la propiedad de un dominio

Para los contactos administrativos y técnicos para un dominio, puede cambiar toda la información de contacto sin tener que autorizar los cambios. Para obtener más información, consulte [Actualización de la información de contacto de un dominio](#).

Para el contacto del registrante, puede cambiar la mayoría de valores sin tener que autorizar los cambios. Sin embargo, para algunos TLD, el cambio de propietario de un dominio requiere autorización. Para obtener más información, consulte el tema correspondiente.

Temas

- [¿Qué desencadena un cambio de titularidad de dominio?](#)
- [TLD que requieren procesamiento especial para cambiar el propietario](#)
- [Actualización de la información de contacto de un dominio](#)
- [Cambio del propietario de un dominio cuando el registro requiere un formulario de cambio de propiedad de dominio](#)

¿Qué desencadena un cambio de titularidad de dominio?

Important

El contacto que indique como titular tendrá determinados derechos como titular del nombre registrado del nombre de dominio, según la [Política de transferencia de la ICANN](#). La mayoría de los dominios se eliminarán cuando cierre su Cuenta de AWS (para obtener más información, consulte [Mi cuenta de AWS está cerrada o se ha cerrado de forma definitiva y mi dominio está registrado con Route 53](#)). Sin embargo, si un dominio permanece en una cuenta cerrada, el contacto que indicó como titular puede solicitar una transferencia del nombre de dominio a un registrador externo. Por lo tanto, es importante que el contacto de titular de registro que muestre sea usted mismo u otra persona en la que confíe para actuar de manera responsable.

Los siguientes cambios en la información de contacto del titular desencadenan el proceso de cambio de propiedad del dominio:

Para contactos que son personas

Cuando se cambian los campos Nombre o Apellido, se produce un cambio de propiedad.

Para tipos de contacto que no son personas (empresa, asociación, organismo público)

Cuando se cambia el campo Organización, se produce un cambio de propiedad.

Activadores adicionales (todos los tipos de contacto)

Según los requisitos del TLD de su dominio, es posible que otros cambios en el campo de contacto también activen el proceso de cambio de titularidad, como los siguientes:

- Cambios en la dirección de correo electrónico del titular
- Cambios en otros campos de información identificatoria

Los campos específicos que provocan los cambios de propiedad varían según el TLD y están determinados por las políticas del registro de dominios.

Warning

Riesgo de interrupción del servicio: cuando se produzca un cambio de propiedad, recibirá un correo electrónico de autorización. Si no responde a este correo electrónico en un plazo de 3

a 15 días (según el TLD), se cancelará el registro del dominio según lo exija la ICANN, lo que interrumpirá su sitio web y sus servicios de correo electrónico.

Asegúrese siempre de poder acceder a la dirección de correo electrónico de contacto del titular antes de hacer cambios en el contacto.

Tenga en cuenta lo siguiente sobre el cambio del propietario de un dominio:

- Para algunos LTD hay una cuota para cambiar al propietario de un dominio. Para determinar si hay una tarifa para el TLD para su dominio, consulte la columna “Change Ownership Price” (Cambiar precio de la propiedad) en [Precios de Amazon Route 53 para el registro de dominios](#).

 Note

No se pueden utilizar los créditos de AWS para pagar la tarifa, en caso de tener alguno, a fin de cambiar el propietario de un dominio.

- Para algunos TLD, al cambiar el propietario de un dominio, enviamos un email de autorización a la dirección de email del contacto del registrante. El contacto del registrante debe seguir las instrucciones del email para autorizar el cambio.
- Para algunos TLD, debe rellenar un formulario de cambio de propiedad de dominio y proporcionar una prueba de identidad para que un ingeniero de soporte de Amazon Route 53 pueda actualizar los valores en su nombre. Si el TLD de su dominio requiere un formulario de cambio de propiedad de dominio, la consola muestra un mensaje con un enlace a un formulario para abrir un caso de soporte. Para obtener más información, consulte [Cambio del propietario de un dominio cuando el registro requiere un formulario de cambio de propiedad de dominio](#).

TLD que requieren procesamiento especial para cambiar el propietario

Cuando cambia el propietario de un dominio, los registros de algunos TLD requieren un procesamiento especial. Si va a cambiar el propietario de cualquiera de los siguientes dominios, lleve a cabo el procedimiento aplicable. Si va a cambiar el propietario de cualquier otro dominio, puede cambiarlo usted mismo, ya sea mediante programación o mediante la consola de Route 53. Consulte [Actualización de la información de contacto de un dominio](#).

Los siguientes TLD requieren un procesamiento especial para cambiar el propietario del dominio:

[.be](#), [.cl](#), [.com.br](#), [.es](#), [.fi](#), [.ru](#), [.se](#), [.sh](#)

.be

Debe obtener un código de transferencia del registro para dichos dominios y, a continuación, abrir un caso con AWS Support.

- Para obtener el código de transferencia, consulte <https://www.dnsbelgium.be/en/manage-your-domain-name/change-holder#transfer> y siga las instrucciones.
- Para abrir un caso, consulte [Ponerse en contacto con AWS Support sobre problemas de registro de dominios](#).

.cl

Debe completar y enviar un formulario a AWS Support. Consulte [Cambio del propietario de un dominio cuando el registro requiere un formulario de cambio de propiedad de dominio](#).

.com.ar

Debe completar y enviar un formulario a AWS Support. Consulte [Cambio del propietario de un dominio cuando el registro requiere un formulario de cambio de propiedad de dominio](#).

.com.br

Debe completar y enviar un formulario a AWS Support. Consulte [Cambio del propietario de un dominio cuando el registro requiere un formulario de cambio de propiedad de dominio](#).

.es

Debe completar y enviar un formulario a AWS Support. Consulte [Cambio del propietario de un dominio cuando el registro requiere un formulario de cambio de propiedad de dominio](#).

.fi

Inicie el cambio de propietario en la consola de Route 53. Una vez iniciado el cambio, recibirá una clave de transferencia de titularidad desde la dirección de correo electrónico `fi-domain-tech@traficom.fi`. Una vez que reciba la clave, abra un caso de soporte con el servicio de asistencia de AWS y comparta el código de la clave con nosotros. Consulte [Ponerse en contacto con AWS Support sobre problemas de registro de dominios](#).

.qa

Debe completar y enviar un formulario a AWS Support. Consulte [Cambio del propietario de un dominio cuando el registro requiere un formulario de cambio de propiedad de dominio](#).

.ru

Debe completar y enviar un formulario a AWS Support. Consulte [Cambio del propietario de un dominio cuando el registro requiere un formulario de cambio de propiedad de dominio](#).

.se

Debe completar y enviar un formulario a AWS Support. Consulte [Cambio del propietario de un dominio cuando el registro requiere un formulario de cambio de propiedad de dominio](#).

.sh

Debe completar y enviar un formulario a AWS Support. Consulte [Cambio del propietario de un dominio cuando el registro requiere un formulario de cambio de propiedad de dominio](#).

Actualización de la información de contacto de un dominio

Para actualizar la información de contacto de un dominio, realice el siguiente procedimiento.

Warning

Riesgo de interrupción del servicio: si el cambio en la información de contacto provoca un cambio de propiedad, recibirá un correo electrónico de autorización. Si no responde a este correo electrónico en un plazo de 3 a 15 días (según el TLD), se cancelará el registro del dominio según lo exija la ICANN, lo que interrumpirá su sitio web y sus servicios de correo electrónico.

Asegúrese de poder acceder a la dirección de correo electrónico de contacto del titular antes de hacer cambios en el contacto.

Antes de actualizar los contactos del dominio

Antes de realizar cualquier cambio en la información de contacto del titular de su dominio, complete esta lista de verificación:

1. ☐ Verifique el acceso al correo electrónico: confirme que puede recibir correos electrónicos en la dirección de correo electrónico del titular actual.
2. ☐ Comprenda los factores que provocan el cambio de propietario: consulte [the section called “¿Qué desencadena un cambio de titularidad de dominio?”](#) para comprender qué cambios podrían activar el proceso de cambio de propietario.

3. ☐ Prepárese para un posible tiempo de inactividad: si se produce un cambio de propietario, dispone de 3 a 15 días para responder al correo electrónico de autorización o se cancelará su dominio.

Para actualizar la información de contacto de un dominio

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Registered domains.
3. Elija el nombre del dominio cuya información de contacto desea actualizar.
4. En la pestaña Información de contacto, seleccione Editar.
5. Si no tiene acceso a la dirección de correo electrónico del contacto del registrador, siga los siguientes pasos. Si tiene acceso a la dirección de correo electrónico del contacto del registrador, vaya al paso 6.
 - a. Cambie solo la dirección de correo electrónico del contacto del registrante. No cambie ningún otro valor correspondiente a ninguno de los contactos del dominio. Si también desea cambiar otros valores, modifíquelos más adelante en el proceso.

Seleccione Save changes (Guardar cambios).

Para verificar la nueva dirección de correo electrónico, enviamos un correo electrónico de verificación a la nueva dirección (si el TLD lo requiere). Debe seleccionar el enlace del correo electrónico para verificar que la nueva dirección de correo electrónico es válida. Si se requiere verificación y no se verifica la nueva dirección de correo electrónico, Route 53 suspende el dominio, conforme a lo requerido por la ICANN.

Si necesita volver a enviar el correo electrónico de verificación, vaya a la página Dominios registrados, seleccione el botón de radio situado junto al nombre del dominio que actualizó y elija el nombre del dominio que va a actualizar. En la alerta Verificar su correo electrónico para evitar la suspensión del dominio, seleccione Enviar correo de nuevo.

- b. Si desea cambiar otros valores para los contactos del registrador, del administrador, de los técnicos o de facturación respecto del dominio, vuelva al paso 1 y repita el procedimiento.
6. Actualice los valores aplicables. También puede seleccionar Copiar el contacto del titular para rellenar automáticamente la misma información que ingresó para el contacto del titular. Para obtener más información, consulte [Valores que especifican cuando registra o transfiere un dominio](#).

En función del TLD de su dominio y los valores que esté cambiando, la consola puede mostrar el siguiente mensaje:

"Para cambiar el nombre o la organización del registrante, abrir un caso".

Si se muestra ese mensaje, omita el resto de este procedimiento y consulte [Cambio del propietario de un dominio cuando el registro requiere un formulario de cambio de propiedad de dominio](#) para obtener más información.

7. Seleccione Save.
8. Si ha cambiado el propietario del dominio, como se describe en [¿Qué desencadena un cambio de titularidad de dominio?](#), enviaremos un email al contacto del registrante del dominio. En el correo electrónico, se solicita autorización para el cambio de propietario.

Si no recibimos la autorización para el cambio en un plazo de 3 a 15 días, en función del dominio de nivel superior, debemos cancelar la solicitud según lo requiere la ICANN.

El email proviene de una de las siguientes direcciones de email.

TLD	Dirección de email de donde procede el email de autorización
.fr	nic@nic.fr
.com.au .net.au	noreply@emailverification.info
Todos los demás	Una de las siguientes direcciones de email: • noreply@registrar.amazon • noreply@domainnameverification.net

9. Si surge algún problema al actualizar la información de contacto, puede ponerse en contacto con AWS Support de forma gratuita. Para obtener más información, consulte [Ponerse en contacto con AWS Support sobre problemas de registro de dominios](#).

Para obtener información sobre la API que puede usar para actualizar la información de contacto, consulte [UpdateDomainContact](#).

Cambio del propietario de un dominio cuando el registro requiere un formulario de cambio de propiedad de dominio

Si el registro de su dominio requiere que complete un cambio de propiedad del dominio y envíe el formulario a AWS Support, lleve a cabo el procedimiento siguiente. Para determinar si necesita realizar este procedimiento, consulte los temas siguientes:

- Para determinar si el valor que está cambiando se considera un cambio de propietario, consulte [¿Qué desencadena un cambio de titularidad de dominio?](#).
- Para determinar si es necesario un formulario de cambio de propiedad de dominio para su dominio, consulte [TLD que requieren procesamiento especial para cambiar el propietario](#).

Para cambiar el propietario de un dominio cuando el registro requiere un formulario de cambio de propiedad del dominio

1. Consulte la introducción de este tema para determinar si el registro de su dominio requiere un procesamiento especial para cambiar el propietario del dominio. Si es así, y si se requiere un formulario de cambio de titularidad de dominio, continúe con este procedimiento.

Si no se requiere un formulario de cambio de titularidad de dominio, realice el procedimiento del tema correspondiente.

2. Descargue el [formulario para modificar la propiedad del dominio](#). El archivo está comprimido en un archivo .zip.
3. Rellene el formulario.
4. Para el contacto del titular del antiguo propietario del dominio y por el nuevo propietario, obtenga una copia de prueba de identidad firmada (documento de identidad, carné de conducir, pasaporte o cualquier otro tipo de prueba legal de identidad).

Además, si una entidad jurídica se muestra como la organización del titular, recopile la siguiente información para el anterior propietario del dominio y para el nuevo propietario:

- Prueba de que existe la organización en la que se ha registrado el dominio.
 - Prueba de que los representantes del propietario anterior y el nuevo propietario están autorizados a actuar en nombre de la organización. Este documento tiene que ser un certificado legal que contenga el nombre de la organización y los nombres de los representantes como firmantes (por ejemplo, consejero delegado, presidente o director ejecutivo).
5. Escanee el formulario de cambio de propiedad de dominio y la prueba solicitada. Guarde los documentos escaneados en un formato común, como un archivo .pdf o .png.
 6. Con la cuenta de AWS en la que está registrado actualmente el dominio, inicie sesión en el [Centro de asistencia de AWS](#).

 Important

Debe iniciar sesión con el usuario de la cuenta raíz o bien con un usuario al que se hayan concedido permisos de IAM de una o varias de las siguientes formas:

- Se asigna al usuario la política administrada AdministratorAccess.
- Se asigna al usuario la política administrada AmazonRoute53DomainsFullAccess.
- Se asigna al usuario la política administrada AmazonRoute53FullAccess.

Si no inicia sesión con la cuenta raíz o con un usuario que tenga los permisos necesarios, no podremos actualizar el propietario del dominio. Este requisito impide que los usuarios no autorizados cambien el propietario de un dominio.

7. Especifique los siguientes valores:

Regarding

Acepte el valor predeterminado de Cuenta y facturación.

Servicio

Acepte el valor predeterminado de Domains.

Categoría

Acepte el valor predeterminado de Cambio de propiedad.

Gravedad

Acepte el valor predeterminado de la Pregunta general.

Elija Paso siguiente: Información adicional.

Asunto

Especifique Change the owner of a domain (Cambiar el nombre de un dominio).

Descripción

Proporcione la información siguiente:

- Dominio cuyo propietario desea cambiar
- [El ID de cuenta de 12 dígitos](#) de la cuenta de AWS en la que está registrado el dominio.

Añadir un archivo adjunto

Cargue los documentos que ha escaneado en el paso 5.

Método de contacto

Especifique un método de contacto y escriba los valores aplicables.

8. Elija Enviar.

Un ingeniero de AWS Support revisa la información proporcionada y actualiza la configuración. El ingeniero se pondrá en contacto con usted cuando haya finalizado la actualización o para obtener más información.

Activación o desactivación de la protección de privacidad para la información de contacto para un dominio

Al registrar un dominio con Amazon Route 53 o transferir un dominio a Route 53, habilitamos la protección de privacidad de forma predeterminada para todos los contactos del dominio. De este modo, normalmente se oculta la mayor parte de la información de contacto de consultas WHOIS ("¿quién es?") y reduce la cantidad de spam que recibe. Cuando se habilita la protección de la privacidad, la información de contacto se reemplaza con la información de contacto del registrador o la frase "REDACTED FOR PRIVACY" (OCULTO POR MOTIVOS DE PRIVACIDAD), o bien "On behalf of <nombre de dominio> owner" (En nombre del propietario de <nombre de dominio>).

Si decide desactivar la protección de privacidad, debe hacerlo en todos los contactos del dominio. Si la desactiva, cualquiera podría enviar una consulta WHOIS sobre el dominio y, en la mayoría de dominios de nivel superior (TLD), podría obtener toda la información de contacto que proporcionó al registrar o transferir el dominio, incluido el nombre, la dirección, el número de teléfono y la dirección de correo electrónico. El comando WHOIS tiene una amplia disponibilidad; se incluye en muchos sistemas operativos y también como aplicación web en numerosos sitios web.

Si está transfiriendo un dominio a otro registrador y la protección de privacidad esté habilitada para los contactos del dominio, el correo electrónico para verificar la transferencia se entregará desde las direcciones de identity-protect.org de los TLD registrados en Amazon Registrar. Para determinar quién es el registrador de su TLD, consulte [Búsqueda del registrador](#).

La información que puede ocultar a las consultas WHOIS depende de dos factores principales:

Registro del dominio de nivel superior

La mayoría de registros de TLD ocultan automáticamente toda la información de contacto, otros permiten optar por ocultar toda la información de contacto, algunos permiten ocultar solo algunos datos y otros no permiten ocultar ninguna información. Algunos registros de TLD suprimen intencionalmente la protección de la privacidad para cumplir con las normativas o políticas de registro locales.

Cuando se habilita la protección de la privacidad en un dominio, la información de contacto se reemplaza con la información de contacto del servicio de protección de la privacidad, o bien con la frase “REDACTED FOR PRIVACY” (OCULTO POR MOTIVOS DE PRIVACIDAD). El servicio de protección de la privacidad aplica funciones de prevención del spam (rotación de direcciones y análisis de SPF/DKIM/spam) y reenviará automáticamente, en la mayoría de casos, los correos electrónicos que superen estos filtros. Sin embargo, no se recomienda enviar correos electrónicos críticos a direcciones de correo electrónico protegidas por motivos de privacidad, ya que el mecanismo de spam podría impedir que se reenvíen.

Además, la elección del mecanismo de protección de la privacidad que se utiliza para un dominio no se puede configurar, sino que el sistema lo selecciona automáticamente. Los detalles de contacto de nuestro servicio de protección de la privacidad no se pueden actualizar manualmente.

Note

Para habilitar o desactivar la protección de privacidad de algunos dominios, debe abrir un caso de soporte técnico y solicitar la protección de privacidad. Para obtener más

información, consulte la sección correspondiente en [Dominios que puede registrar con Amazon Route 53](#):

- [.co.uk \(Reino Unido\)](#)
- [.me.uk \(Reino Unido\)](#)
- [.org.uk \(Reino Unido\)](#)
- [.link](#)

Registrador

Al registrar un dominio en Route 53 o transferir un dominio al mismo, el titular del dominio es Amazon Registrar o nuestro registrador asociado, Gandi. Amazon Registrar y Gandi ocultan diferente información de forma predeterminada:

- Amazon Registrar: de forma predeterminada, toda la información de contacto está oculta. Sin embargo, tienen prioridad la normativa del registro de TLD.
- Gandi: de forma predeterminada, toda la información de contacto está oculta, excepto el nombre de la organización, si consta. Sin embargo, tienen prioridad la normativa del registro de TLD.

Para [TLD geográficos](#) que no permiten la protección de privacidad, su información personal se marcará como "eliminada" en la página de [búsqueda en el directorio Whois](#) del sitio web de Gandi. Sin embargo, su información personal puede estar disponible en el registro de dominios o en sitios web WHOIS de terceros.

Para saber qué información está oculta para el TLD de su dominio, consulte [Dominios que puede registrar con Amazon Route 53](#).

Cuando desee habilitar o desactivar la protección de privacidad de un dominio que ha registrado mediante Route 53, siga este procedimiento.

Important

Disponibilidad de la protección de la privacidad: la protección de la privacidad no está disponible para todos los TLD. Los TLD más comunes que no admiten la protección de la privacidad incluyen .de, .us, .com.au, .es y varios otros.

Si no ve la sección «Protección de la privacidad» al editar la información de contacto de su dominio, significa que la protección de la privacidad no está disponible para el TLD de su dominio.

Para ver una lista completa de los TLD que no admiten la protección de la privacidad, consulte [TLD que no admiten la protección de la privacidad](#). Para obtener información detallada sobre la disponibilidad de la protección de la privacidad para un TLD, consulte [Dominios que puede registrar con Amazon Route 53](#).

Para habilitar o desactivar la protección de privacidad para la información de contacto de un dominio

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Registered domains.
3. Elija el nombre del dominio cuya protección de privacidad desea habilitar o desactivar.
4. En la sección Información de contacto, seleccione Editar.
5. En la sección Protección de la privacidad, elija si desea ocultar la información de contacto. Debe especificar la misma configuración de privacidad para los cuatro contactos: administrador, registrador, técnico y facturación.

 Note

Si no aparece la sección Protección de la privacidad, significa que esta no está disponible para el TLD de su dominio. Su información de contacto será visible públicamente en las consultas de WHOIS que correspondan a los dominios que no admiten la protección de la privacidad.

6. Seleccione Save changes (Guardar cambios).
7. Si surge algún problema al activar o desactivar la protección de privacidad, puede ponerse en contacto con AWS Support de forma gratuita. Para obtener más información, consulte [Ponerse en contacto con AWS Support sobre problemas de registro de dominios](#).

TLD que no admiten la protección de la privacidad

Los siguientes TLD no admiten la protección de la privacidad. Si su dominio usa uno de estos TLD, su información de contacto será visible públicamente en las consultas de WHOIS:

TLD genéricos

.audio, .ceo, .diet, .flowers, .guitars, .hosting, .juegos, .property, .sexy

TLD geográficos

.cl (Chile), .com.ar (Argentina), .com.au (Australia), .com.br (Brasil), .com.sg (Singapur), .de (Alemania), .es (España), .in (India), .net.au (Australia), .qa (Catar), .ru (Rusia), .sg (Singapur), .us (Estados Unidos), .vg (Islas Vírgenes Británicas)

Note

Esta lista incluye los TLD más comunes que no admiten la protección de la privacidad. Para obtener información completa y actualizada sobre la disponibilidad de la protección de la privacidad para un TLD específico, consulte la página del TLD individual en [Dominios que puede registrar con Amazon Route 53](#).

Solución de problemas de protección de la privacidad

La opción de protección de la privacidad no está disponible en la consola

Esto indica que el TLD de su dominio no admite la protección de la privacidad. Su información de contacto será visible públicamente en las consultas de WHOIS. Este comportamiento es normal en algunos TLD debido a las políticas de registro o a las normativas locales.

Para comprobar si su TLD admite la protección de la privacidad, consulte la página individual del TLD en [Dominios que puede registrar con Amazon Route 53](#) o consulte [TLD que no admiten la protección de la privacidad](#).

La información de contacto sigue siendo visible después de activar la protección de la privacidad

Algunos registros mantienen sus propias bases de datos de WHOIS y es posible que sigan mostrando la información de contacto incluso cuando la protección de la privacidad está activada para Route 53. Esto lo controla el registro de TLD, no Route 53.

Además, algunos registros de TLD mantienen intencionalmente servicios de protección de la privacidad o anonimización limitados para sus dominios.

Activación o desactivación de la renovación automática de un dominio

Cuando desee cambiar si Amazon Route 53 renueva automáticamente el registro de un dominio poco antes de la fecha de vencimiento o no, o desee ver la configuración actual de la renovación automática, siga este procedimiento.

Tenga en cuenta que no puede utilizar los créditos de AWS para pagar la cuota de renovación de registro de un dominio.

Note

Asegúrese de desactivar la renovación automática si tiene intención de cancelar su cuenta de AWS. De lo contrario, seguirá recibiendo avisos de renovación de AWS. Sin embargo, su dominio no se renovará a menos que vuelva a activar su cuenta.

Para habilitar o desactivar la renovación automática de un dominio

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Registered domains.
3. Elija el nombre del dominio que desea actualizar.
4. En la sección Detalles, en el menú desplegable Acciones, seleccione Activar la renovación automática

En el menú ¿Activar la renovación automática para <domain name>? acepte pagar la tarifa anual y seleccione Activar.

Note

El precio indicado corresponde al periodo de registro actual y puede cambiar. Para obtener más información, consulte [Precios de Amazon Route 53 para el registro de dominio](#).

5. Para desactivar la renovación automática, seleccione Desactivar la renovación automática en el menú desplegable Acciones.

6. Si surge algún problema al activar o desactivar la renovación automática, puede ponerse en contacto con AWS Support de forma gratuita. Para obtener más información, consulte [Ponerse en contacto con AWS Support sobre problemas de registro de dominios](#).

Bloqueo de un dominio para impedir la transferencia no autorizada a otro registrador

Los registros de dominio de todos los TLD genéricos y muchos TLD geográficos le permiten bloquear un dominio para evitar que nadie transfiera el dominio a otro registrador sin su permiso. Para determinar si el registro de su dominio le permite bloquear el dominio, consulte [Dominios que puede registrar con Amazon Route 53](#). Si se admite el bloqueo y desea bloquear el dominio, realice el siguiente procedimiento. También puede utilizar el procedimiento para desactivar el bloqueo si desea transferir un dominio a otro registrador.

Para bloquear un dominio para impedir la transferencia no autorizada a otro registrador

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Registered Domains.
3. Elija el nombre del dominio que desea actualizar.
4. En la sección Detalles, en el menú desplegable Acciones, seleccione Activar el bloqueo de transferencia o Desactivar el bloqueo de transferencia, dependiendo de si desea activar o desactivar el bloqueo de transferencia.

Puede ir a la página Solicitudes para ver el progreso de su solicitud.

5. Si surge algún problema al bloquear un dominio, puede ponerse en contacto con AWS Support de forma gratuita. Para obtener más información, consulte [Ponerse en contacto con AWS Support sobre problemas de registro de dominios](#).

En la búsqueda en WHOIS, este estado aparece como: `clientTransferProhibited`. Es posible que algunos TLD tengan, además, estos estados:

- `clientUpdateProhibited`
- `clientDeleteProhibited`

Ampliación del periodo de registro de un dominio

Cuando registra un dominio con Amazon Route 53 o transfiere un registro de dominio a Route 53, lo configuramos para que se renueve automáticamente. El periodo de renovación automática suele ser de un año, aunque los registradores de algunos dominios de nivel superior (TLD) tienen periodos de renovación más prolongados.

Tenga en cuenta lo siguiente:

Periodo máximo de renovación

Todos los TLD genéricos y muchos TLD de código de país permiten ampliar el registro del dominio durante periodos más largos, normalmente hasta diez años con incrementos anuales. Para determinar si puede ampliar el periodo de registro de su dominio, consulte [Dominios que puede registrar con Amazon Route 53](#). Si se permiten periodos de registros más largos, siga este procedimiento.

Restricciones sobre cuándo puede renovar o ampliar el registro de un dominio

Algunos registros de TLD tienen restricciones sobre cuándo puede renovar o ampliar un registro de dominio, por ejemplo, los últimos dos meses antes del vencimiento del dominio. Aunque el registro permita ampliar el periodo de registro de un dominio, es posible que no lo permitas en el número de días actual antes del vencimiento del dominio.

Note

Por ejemplo, si el período de renovación máximo permitido es de 5 años para los TLD con los que tiene su dominio, puede añadir renovaciones anuales en cualquier momento hasta alcanzar el límite de 5 años. Más específicamente, si tiene un dominio que actualmente tiene 2,5 años de validez, solo puede renovarlo por un máximo de 2 años más.

AWSCréditos de

No se pueden utilizar los créditos de AWS para ampliar el período de registro de un dominio.

Para ampliar el periodo de registro de su dominio

1. Abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.

2. En el panel de navegación, elija Registered Domains.
3. Elija el nombre del dominio cuyo periodo de registro desee ampliar.
4. En la sección Detalles, en el menú desplegable Acciones, seleccione Renovar el registro de dominio.
5. En el cuadro de diálogo Renovar los registros de dominio, en el menú desplegable Periodo de renovación, elija el número de años durante los que desea extender el registro.

La lista muestra todas las opciones actuales en función de la fecha de vencimiento actual y el periodo de registro máximo que permite el registro para este dominio. La fecha de vencimiento con la aplicación de ese número de años aparece debajo de la duración.

6. Seleccione Renovar el registro de dominio.

Cuando recibamos la confirmación del registro de que ha actualizado su fecha de vencimiento, le enviaremos un email para confirmar que hemos cambiado la fecha de vencimiento.

7. Si surge algún problema al ampliar el período de registro de un dominio, puede ponerse en contacto con AWS Support de forma gratuita. Para obtener más información, consulte [Ponerse en contacto con AWS Support sobre problemas de registro de dominios](#).

Actualización de los servidores de nombres para utilizar otro registrador

Si desea trasladar la administración de DNS a otro registrador, debe actualizar los servidores de nombres para que apunten a

Para actualizar los servidores de nombres de su dominio cuando desea utilizar otro servicio DNS

1. Utilice el proceso proporcionado por su servicio DNS para obtener los servidores de nombres del dominio.
2. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
3. En el panel de navegación, elija Registered domains.
4. Elija el nombre del dominio que desea configurar para utilizar otro servicio DNS.
5. En la sección Detalles, en el menú desplegable Acciones, seleccione Editar servidores de nombres.
6. Elimine los servidores de nombres existentes y, a continuación, añada los nombres de los servidores de nombres a los servidores de nombres que obtuvo de su servicio de DNS en el paso 1.

7. Seleccione Save changes (Guardar cambios).
8. (Opcional) Elimine la zona alojada que Route 53 creó automáticamente cuando registró su dominio. Esto impide que se le cobre por una zona alojada que no utiliza.
 - a. En el panel de navegación, elija Hosted Zones.
 - b. Seleccione el botón de opción de la zona alojada que tiene el mismo nombre que el dominio.
 - c. Seleccione Delete Hosted Zone.
 - d. Elija Confirm para confirmar que desea eliminar la zona alojada.

Adición o modificación de servidores de nombres y registros de conexión de un dominio

Al registrar un dominio con Route 53, se creará automáticamente una zona alojada para el dominio, se asignarán cuatro servidores de nombres a la zona alojada y luego se actualizará el registro de dominio para usar dichos servidores de nombres. Por lo general, no es necesario cambiar esa configuración a menos que desee utilizar otro servicio DNS o desee utilizar servidores de nombres de etiqueta blanca.

El número máximo de servidores de nombres por dominio en Route 53 es 6.

Warning

Si cambia los servidores de nombres por valores erróneos, especifique las direcciones IP incorrectas en los registros de conexión o elimine uno o varios servidores de nombres sin especificar los nuevos, es posible que su sitio web o aplicación dejen de estar disponibles en Internet hasta un máximo de dos días.

Temas

- [Consideraciones sobre la modificación de servidores de nombres y registros de conexión](#)
- [Adición o modificación de servidores de nombres o registros de conexión](#)

Consideraciones sobre la modificación de servidores de nombres y registros de conexión

Tenga en cuenta los siguientes aspectos antes de cambiar la configuración.

Temas

- [You want to make Route 53 the DNS service for your domain](#)
- [You want to use another DNS service](#)
- [You want to use white-label name servers](#)
- [You're changing name servers for a .it domain](#)

Desea que Route 53 sea el servicio DNS de su dominio

Si está utilizando actualmente otro servicio DNS y desea convertir Route 53 en el servicio DNS para su dominio, consulte en [Establecer Amazon Route 53 como servicio DNS de un dominio existente](#) las instrucciones detalladas sobre cómo migrar el servicio DNS a Route 53.

Important

Si no sigue rigurosamente el proceso de migración, su dominio puede dejar de estar disponible en Internet durante un máximo de dos días.

Desea utilizar otro servicio DNS

Si desea utilizar un servicio DNS que no sea Route 53 para su dominio, utilice el siguiente procedimiento a fin de cambiar los servidores de nombres del registro de dominio por los servidores de nombres que proporciona el otro servicio DNS.

Note

Si cambia los servidores de nombres y Route 53 devuelve el siguiente mensaje de error, el registro del TLD no reconoce los servidores de nombres que especificó como servidores de nombres válidos:

```
"We're sorry to report that the operation failed after we forwarded your request to our registrar associate. This is because: One or more of the specified name servers are not known to the domain registry."
```

Los registros de TLD normalmente admiten servidores de nombres que proporcionan servicios DNS públicos, pero no admiten servidores DNS privados, como, por ejemplo, servidores DNS que ha configurado en instancias de Amazon EC2, a menos que el

registro tenga direcciones IP para los servidores de nombres. Route 53 no admite el uso de servidores de nombres que no los reconozca el registro de TLD. Si detecta este error, debe cambiar a servidores de nombres para Route 53 u otro servicio DNS público.

Desea utilizar servidores de nombres de etiqueta blanca

Si desea que los nombres de los servidores de nombres sean subdominios de su nombre de dominio, puede crear servidores de nombres de etiqueta blanca. (Los servidores de nombres de etiqueta blanca también son conocidos como servidores de nombres personalizados o servidores de nombres privados). Por ejemplo, puede crear servidores de nombres ns1.example.com a través de ns4.example.com para el dominio example.com. Para utilizar servidores de nombres de etiqueta blanca, utilice el siguiente procedimiento para especificar las direcciones IP de sus servidores de nombres en lugar de los nombres. Estas direcciones IP se conocen como registros de conexión.

Para obtener más información sobre cómo configurar servidores de nombres de etiqueta blanca, consulte [Configuración de servidores de nombres de etiqueta blanca](#).

Está cambiando los servidores de nombres de un dominio .it

Los servidores de nombres para el dominio IT deben superar una comprobación de DNS. Le recomendamos que revise los servidores de nombres en <https://dns-check.nic.it/> antes de enviar la solicitud de cambio. La empresa de registro sigue respondiendo a las consultas de DNS con los servidores de nombres anteriores a que realizara el cambio. Si los servidores de nombres anteriores ya no están disponibles, su dominio deja de estar disponible en Internet.

Important

Cada vez que cambie los servidores de nombres de un dominio, confirme que DNS responde a las consultas con los nuevos servidores de nombres antes de cancelar el antiguo servicio DNS o elimine la zona alojada de Route 53 que utilizaba los antiguos servidores de nombres.

Para obtener más información acerca de cómo obtener ayuda de AWS para corregir los nombres de los servidores de nombres con la empresa de registro de dominios .it, consulte [Ponerse en contacto con AWS Support sobre problemas de registro de dominios](#).

Adición o modificación de servidores de nombres o registros de conexión

Para añadir o cambiar servidores de nombres o registros de conexión, realice el siguiente procedimiento.

Note

De forma predeterminada, los solucionadores DNS suelen almacenar en caché los nombres de los servidores de nombres durante dos días. Como resultado, los cambios pueden tardar dos días en surtir efecto. Para obtener más información, consulte [Cómo dirige Amazon Route 53 el tráfico de su dominio](#).

Para añadir o cambiar servidores de nombres o registros de conexión de un dominio

1. Consulte [Consideraciones sobre la modificación de servidores de nombres y registros de conexión](#) y resuelva los problemas correspondientes, si los hubiera.
2. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
3. En el panel de navegación, elija Registered domains.
4. Elija el nombre del dominio cuya configuración desea editar.
5. En la sección Detalles, en el menú desplegable Acciones, seleccione Editar servidores de nombres.
6. En el cuadro de diálogo Editar servidores de nombres puede hacer lo siguiente:
 - Lleve a cabo una de las siguientes acciones para cambiar el servicio DNS del dominio:
 - Reemplazar los servidores de nombres de otro servicio DNS con los servidores de nombres para una zona alojada de Route 53
 - Reemplazar los servidores de nombres de una zona alojada de Route 53 con los servidores de nombres de otro servicio DNS
 - Reemplazar los servidores de nombres de una zona alojada de Route 53 con los servidores de nombres de otra zona alojada de Route 53

Para obtener información acerca de cómo cambiar el servicio DNS para un dominio, consulte [Establecer Amazon Route 53 como servicio DNS de un dominio existente](#). Para obtener información sobre cómo obtener los servidores de nombres para la zona alojada de Route

53 que desea utilizar para el servicio DNS del dominio, consulte [Obtener los servidores de nombres para una zona alojada pública](#).

- Añadir uno o varios servidores de nombres.
- Reemplazar el nombre de un servidor de nombres existente.
- Si especifica servidores de nombres de etiqueta blanca, añada o cambie las direcciones IP en los registros de conexión. Puede escribir las direcciones en formato IPv4 o IPv6. Si un servidor de nombres tiene varias direcciones IP, escriba cada dirección en una línea independiente.

Un servidor de nombres de etiqueta blanca incluye su nombre de dominio, como example.com, en el nombre del servidor de nombres, por ejemplo, ns1.example.com. Al especificar un servidor de nombres de etiqueta blanca, Route 53 le pedirá que especifique una o más direcciones IP para el servidor de nombres. La dirección IP se conoce como un registro de conexión. Para obtener más información, consulte [Configuración de servidores de nombres de etiqueta blanca](#).

- Elimine un servidor de nombres. Elija el icono x en la parte derecha del campo para ese servidor de nombres.

Warning

Si cambia los servidores de nombres por valores erróneos, especifique las direcciones IP incorrectas en los registros de conexión o elimine uno o varios servidores de nombres sin especificar los nuevos, es posible que su sitio web o aplicación dejen de estar disponibles en Internet hasta un máximo de dos días.

7. Elija Actualizar.
8. Si surge algún problema al agregar o cambiar los servidores de nombre o registros de adherencia, puede ponerse en contacto con AWS Support de forma gratuita. Para obtener más información, consulte [Ponerse en contacto con AWS Support sobre problemas de registro de dominios](#).

Renovar el registro de un dominio

Cuando registra un dominio con Amazon Route 53 o transfiere un registro de dominio a Route 53, lo configuramos para que se renueve automáticamente. El período de renovación automática suele ser de un año, aunque los registros de algunos dominios de nivel superior (TLDs) tienen períodos

de renovación más largos. Para conocer el periodo de registro y renovación de su TLD, consulte [Dominios que puede registrar con Amazon Route 53](#).

 Note

No puedes usar los AWS créditos para pagar la tarifa de renovación del registro de un dominio.

En la mayoría de los dominios de nivel superior (TLDs), puedes cambiar la fecha de caducidad de un dominio. Para obtener más información, consulte [Ampliación del periodo de registro de un dominio](#).

 Important

Si desactiva la renovación automática, debe conocer los siguientes efectos que esta desactivación tendrá en su dominio:

- Algunos registradores de TLD eliminan los dominios incluso antes de la fecha de vencimiento si no se renuevan con la suficiente antelación. Recomendamos encarecidamente que deje la renovación automática habilitada si desea mantener un nombre de dominio.
- También le recomendamos que no piense en volver a registrar un dominio después de que haya caducado. Algunos registradores permiten que otras personas registren los dominios inmediatamente después de que vencen, por lo que es posible que no pueda volver a registrar el dominio antes de que lo obtenga otra persona.
- Algunos registradores cobran una prima muy alta por restaurar dominios caducados.
- Cuando se aproxime o llegue la fecha de vencimiento, el dominio dejará de estar disponible en Internet.

Para determinar si la renovación automática está habilitada para su dominio, consulte [Activación o desactivación de la renovación automática de un dominio](#).

Si la renovación automática está habilitada, esto es lo que ocurre:

45 días antes de la fecha de vencimiento

Enviamos un correo electrónico al contacto del registrante que indica que la renovación automática está habilitada y ofrece instrucciones sobre cómo desactivarla. Mantenga actualizada

la dirección de correo electrónico del contacto del registrante para que no pierda este correo electrónico.

35 o 30 días antes de la fecha de vencimiento

Para todos los dominios, excepto los dominios.com.ar y .com.br, renovamos el registro del dominio 35 días antes de la fecha de caducidad para tener tiempo de resolver cualquier problema relacionado con la renovación antes de que caduque el nombre de dominio.

Los registros de los dominios.com.ar y .com.br requieren que los renovemos no más de 30 días antes de su caducidad. Recibirá un correo electrónico de renovación de Gandi, nuestro socio registrador, 30 días antes de la fecha de vencimiento, que es el mismo día que renovamos su dominio si ha habilitado la renovación automática.

Note

Cuando renovamos su dominio, le enviamos un mensaje de correo electrónico para informarle de que lo hemos renovado. Si no se puede realizar la renovación, le enviaremos un correo electrónico para explicarle por qué no se ha podido realizar.

Si la renovación automática está deshabilitada, esto es lo que sucede cuando se aproxima la fecha de vencimiento de un nombre de dominio:

45 días antes de la fecha de vencimiento

Enviamos un correo electrónico al contacto del registrante del dominio que indica que la renovación automática está deshabilitada actualmente y ofrece instrucciones sobre cómo activarla. Mantenga actualizada la dirección de correo electrónico del contacto del registrante para que no pierda este correo electrónico.

30 y 7 días antes de la fecha de vencimiento

Si la renovación automática está deshabilitada para el dominio, la ICANN, el organismo que rige el registro de dominios, exige que el registrador le envíe un correo electrónico. El correo electrónico proviene de una de las siguientes direcciones de correo electrónico:

- `noreply@registrar.amazon`: para dominios cuyo registrador es Amazon Registrar.
- `noreply@domainnameverification.net`: para dominios cuyo registrador es nuestro socio de registro, Gandi.

Para determinar quién es el registrador de su TLD, consulte [Dominios que puede registrar con Amazon Route 53](#).

Si habilita la renovación automática en un plazo menor de 30 días antes de la fecha de vencimiento y aún no ha transcurrido el periodo de renovación, renovaremos el dominio en 24 horas.

 Important

Algunos registradores de TLD tienen restricciones respecto de cuándo puede renovar un dominio. Para obtener información específica sobre el dominio, consulte [Dominios que puede registrar con Amazon Route 53](#). Además, el procesamiento de una renovación puede tardar hasta un día. Si deja pasar mucho tiempo antes de habilitar la renovación automática, el dominio podría caducar antes de que se procese la renovación, y es posible que pierda el dominio. Si se aproxima la fecha de vencimiento, le recomendamos que amplíe manualmente la fecha de vencimiento del dominio. Para obtener más información, consulte [Ampliación del periodo de registro de un dominio](#).

Para obtener más información acerca de los periodos de renovación, consulte la sección Plazos para renovar y restaurar dominios de su TLD en [Dominios que puede registrar con Amazon Route 53](#).

Después de la fecha de vencimiento

El registrador conserva la mayoría de los dominios durante un breve periodo después de la fecha de vencimiento, por lo que es posible que pueda renovar un dominio que ha vencido después de la fecha de vencimiento, pero es absolutamente recomendable que mantenga la renovación automática habilitada si desea conservar su dominio. Para obtener información sobre cómo intentar renovar un dominio después de la fecha de vencimiento, consulte [Restauración de un dominio caducado o eliminado](#).

Si el dominio caduca pero se permite una renovación tardía para el dominio, puede renovar el dominio por el precio de la renovación estándar. Para determinar si un dominio sigue estando dentro del periodo de renovación tardía, realice el procedimiento en la sección [Ampliación del periodo de registro de un dominio](#). Si el dominio sigue estando en la lista, está dentro del periodo de renovación tardía.

Para obtener más información acerca de los periodos de renovación, consulte la sección Plazos para renovar y restaurar dominios de su TLD en [Dominios que puede registrar con Amazon Route 53](#).

Restauración de un dominio caducado o eliminado

Si no renuevas un dominio antes de que finalice el período de renovación tardía o si lo eliminas accidentalmente, en el caso de algunos registros de dominios de nivel superior (TLDs), puedes restaurar el dominio antes de que esté disponible para que otros lo registren.

Cuando se elimina un dominio o cumple el final del periodo de renovación tardía, ya no aparece en la consola de Amazon Route 53.

Important

El precio de restauración de un dominio suele ser superior y en ocasiones mucho mayor que el precio de registro o de renovación de un dominio. Para conocer el precio actual de restauración de un dominio, consulte la columna Precio de la restauración en la sección [Precios para el registro de dominios de Amazon Route 53](#).

No puedes usar los AWS créditos para pagar la tarifa de restauración de un dominio caducado.

Para probar a restaurar el registro de dominio cuando se ha eliminado un dominio o ha caducado el período de renovación tardía

1. Determine si el registro del dominio de nivel superior (TLD) del dominio es compatible con la restauración de dominios y, en tal caso, el período durante el cual se permite la restauración.
 - a. Vaya a [Dominios que puede registrar con Amazon Route 53](#).

Important

En el caso de los dominios de TLD genéricos que se eliminan dentro de los primeros 5 días después del registro, no se aplica el período de canje estándar de 30 días (para verificar el número real de días del período de canje, consulte [Dominios que puede registrar con Amazon Route 53](#)). En su lugar, estos dominios pasan inmediatamente a estar disponibles para nuevos registros.

- b. Encuentre el TLD para el dominio y revise los valores en la sección Plazos para renovar y restaurar dominios.

 Important

Reenviaremos las solicitudes de restauración a Gandi, que procesa las solicitudes durante el horario comercial, de lunes a viernes. Gandi tiene su sede en París, donde el tiempo es de UTC/GMT 1 hora. Por tanto, dependiendo de cuándo se envíe su solicitud, en algunas ocasiones es posible que se tarde una semana o más en procesar la solicitud.

2. Revise el precio de restauración de un dominio, que suele ser superior y en ocasiones mucho mayor que el precio de registro o de renovación de un dominio. En [Precios para el registro de dominios de Amazon Route 53](#), busque el TLD de su dominio (por ejemplo, .com) y compruebe el precio en la columna Precio de restauración. Si sigue queriendo restaurar el dominio, anote el precio, ya que lo necesitará en un paso posterior.
3. Con la AWS cuenta en la que se registró el dominio, inicie sesión en el [AWS Support Center](#).
4. Especifique los siguientes valores:

Regarding

Acepte el valor predeterminado de Cuenta y facturación.

Servicio

Acepte el valor predeterminado de Domains.

Categoría

Acepte el valor predeterminado de Recuperación.

Gravedad

Acepte el valor predeterminado de la Pregunta general.

Elija Paso siguiente: Información adicional.

Asunto

Escriba Restore an expired domain (Restaurar un dominio caducado) o Restore a deleted domain (Restaurar un dominio eliminado).

Description (Descripción)

Proporcione la información siguiente:

- El dominio que desea restaurar
- El [identificador de cuenta de 12 dígitos](#) de la AWS cuenta en la que se registró el dominio
- Confirmación de que acepta el precio de restauración del dominio Utilice el siguiente texto:

"I agree to the price of \$____ for restoring my domain" (Acepto el precio de ____ USD por la restauración del dominio).

Sustituya el espacio en blanco con el precio que ha anotado en el paso 2.

Método de contacto

Especifique un método de contacto y escriba los valores aplicables.

5. Elija Enviar.
6. Cuando sepamos si hemos podido restaurar su dominio, un representante de AWS Support se pondrá en contacto con usted. Además, si hemos podido restaurar su dominio, el dominio reaparecerá en la consola. La fecha de vencimiento depende de si el dominio ha caducado o se ha eliminado accidentalmente:

El dominio ha caducado

La nueva fecha de vencimiento suele ser de uno o dos años (en función del TLD) después de la fecha de vencimiento anterior.

Note

La nueva fecha de vencimiento no se calcula a partir de la fecha en que se restauró el dominio.

El dominio se ha eliminado accidentalmente

Normalmente, la fecha de vencimiento no cambia.

Sustitución de la zona alojada para un dominio registrado con Route 53

Si [elimina la zona alojada](#) para un dominio, debe crear otra zona alojada cuando esté listo para hacer que el dominio esté disponible en Internet. Realice el siguiente procedimiento.

Para sustituir la zona alojada para un dominio

1. Creación de una zona alojada pública. Para obtener más información, consulte [Crear una zona alojada pública](#).
2. Creación de registros en la zona alojada. Los registros definen cómo desea dirigir el tráfico para el dominio (example.com) y los subdominios (acme.example.com, zenith.example.com). Para obtener más información, consulte [Uso de registros](#).
3. Actualización de la configuración del dominio para usar los servidores de nombres para la nueva zona alojada. Para obtener más información, consulte [Adición o modificación de servidores de nombres y registros de conexión de un dominio](#).

Important

Al crear una zona alojada, Route 53 asigna un conjunto de cuatro servidores de nombres a la zona alojada. Si elimina una zona alojada y crea una, Route 53 asigna otro conjunto de cuatro servidores de nombres. Normalmente, ninguno de los servidores de nombres de la nueva zona alojada coincide con ninguno de los servidores de nombres de la zona alojada anterior. Si no actualiza la configuración de dominio para usar los servidores de nombres para la nueva zona alojada, el dominio seguirá sin estar disponible en Internet.

4. Si tienes problemas al sustituir la zona alojada por un dominio, puedes ponerte en contacto con AWS Support de forma gratuita. Para obtener más información, consulte [Ponerse en contacto con AWS Support sobre problemas de registro de dominios](#).

Transferencia de dominios

Puede transferir el registro de un dominio desde otro registrador hasta Amazon Route 53, desde una cuenta de AWS a otra o desde Route 53 a otro registrador. La transferencia de dominios de una cuenta de AWS a otra es gratuita.

En esta sección se tratan los siguientes temas relacionados con la transferencia de dominios:

1. [Elija el tipo de transferencia](#)

- Comprenda la diferencia entre transferir el registro de dominio a Route 53 y usar Route 53 únicamente para el alojamiento de DNS.
- Descubra qué opción es la adecuada para sus necesidades en función de sus objetivos de administración de dominios y alojamiento de DNS.

2. [Lista de verificación previa a la transferencia](#)

- Complete los pasos de preparación esenciales antes de transferir su dominio a Route 53 para evitar que se produzcan errores de transferencia comunes.
- Verifique la elegibilidad del dominio, obtenga los códigos de autorización y prepare su configuración de DNS para que el proceso de transferencia sea fluido.

3. [Transferencia del registro de un dominio a Amazon Route 53](#)

- Conozca el procedimiento paso a paso para transferir un dominio de otro registrador a Route 53, incluidos los requisitos previos, los códigos de autorización y la actualización de la configuración de DNS.
- Comprenda cómo la transferencia de un dominio afecta a la fecha de caducidad, así como las consideraciones de los distintos dominios de nivel superior (TLD).

4. [Problemas de transferencia comunes](#)

- Comprenda los requisitos del dominio, los procesos de autorización y las consideraciones de tiempo para evitar los problemas de transferencia más comunes.
- Obtenga información sobre cómo resolver los problemas de transferencia y qué hacer si su transferencia se retrasa o se rechaza.

5. [Transferencia de un dominio de Amazon Route 53 a otro registrador](#)

- Comprenda el proceso de transferir un dominio de Route 53 a otro registrador, que incluye obtener el código de autorización, actualizar la configuración de DNS y responder a los correos electrónicos de confirmación.
- Tenga en cuenta las consideraciones al momento de transferir el servicio de DNS a otro proveedor y el posible impacto en las características específicas de Route 53, como los registros de alias y las políticas de enrutamiento.

6. [Transferencia de un dominio a otra cuenta de AWS](#)

- Descubra cómo transferir un dominio de una cuenta de AWS a otra, incluidos los roles y permisos necesarios para iniciar y aceptar la transferencia.

- Obtenga información sobre el paso opcional de migrar la zona alojada a la nueva cuenta tras la transferencia del dominio.

7. [Estado de la transferencia](#)

- Descubra cómo ver el estado de una solicitud de transferencia de dominio y el significado de los diferentes códigos de estado durante el proceso de transferencia.

8. [Cómo la transferencia de un dominio a Amazon Route 53 afecta a la fecha de vencimiento del registro del dominio](#)

- Descubra cómo la transferencia de un dominio a Route 53 puede afectar la fecha de caducidad del dominio.

Si sigue la información proporcionada en los temas mencionados con anterioridad, podrá transferir dominios de forma eficaz desde y hacia Route 53, administrar el proceso de transferencia y garantizar una transición fluida y, al mismo tiempo, mantener una configuración y un enrutamiento de DNS adecuados.

Elija el tipo de transferencia en Route 53.

Si desea utilizar Amazon Route 53 con su dominio, tiene dos opciones. Entender la diferencia lo ayudará a elegir el método adecuado para satisfacer sus necesidades:

Transferencia del registro de dominio a Route 53

Con esta opción, Route 53 se convierte en su registrador de dominios. Esto significa que administrará las renovaciones de su dominio, la información de contacto y la configuración de DNS a través de Route 53.

Elija esta opción cuando quiera:

- Consolidar la administración de dominios y el alojamiento de DNS en un solo lugar.
- Aprovechar las características de administración de dominios de Route 53.
- Simplificar la facturación mediante la inclusión de las renovaciones de dominio en su factura de AWS.

Qué esperar:

- Plazo de finalización: de 5 a 7 días

- Requisitos previos: obtener el código de autorización del registrador actual, desbloquear el dominio, verificar el correo electrónico del titular
- A quién paga por las renovaciones: Route 53

Siguiente paso: complete la [Lista de verificación previa a la transferencia para transferencias de dominios](#) para preparar la transferencia.

Uso de Route 53 únicamente para el alojamiento de DNS

Con esta opción, conserva su registrador de dominios actual, pero utiliza Route 53 como su servicio DNS.

Elija esta opción cuando quiera:

- Mantener su registrador actual.
- Utilizar las características de DNS avanzadas de Route 53 sin cambiar de registrador.
- Comenzar rápidamente con los requisitos previos mínimos.

Qué esperar:

- Tiempo de finalización: hasta 2 días (depende de la propagación del DNS)
- Requisitos previos: ninguno
- A quién paga por las renovaciones: su registrador actual

Siguiente paso: vaya a [Configuración de Amazon Route 53 como servicio DNS](#) para configurar el alojamiento de DNS.

Important

No es necesario que transfiera el registro de su dominio para poder utilizar Route 53 como su servicio de DNS. Puede conservar su registrador actual y usar Route 53 solo para el alojamiento de DNS.

Lista de verificación previa a la transferencia para transferencias de dominios

Antes de empezar a transferir el registro de dominio a Amazon Route 53, realice los siguientes controles para evitar errores de transferencia comunes y garantizar que el proceso fluya.

Decida qué quiere transferir

Elija la opción que mejor se adapte a sus necesidades.

Transferencia del registro de dominio a Route 53

Su registrador pasa a ser Amazon Route 53. Usted paga a Route 53 por las renovaciones de dominio y administra la configuración del dominio a través de la consola de Route 53.

Siguiente paso: continúe con esta lista de verificación y, a continuación, siga los pasos en [Transferencia del registro de un dominio a Amazon Route 53](#).

Uso de Route 53 únicamente para el alojamiento de DNS

Conserve su registrador actual, pero utilice los servidores de nombres de Route 53 para la resolución de DNS. Sigue pagando a su registrador actual por las renovaciones.

Siguiente paso: omita esta lista de verificación y siga los pasos en [Configuración de Amazon Route 53 como servicio DNS](#).

Lista de verificación de requisitos previos

Complete todos los pasos siguientes antes de iniciar la transferencia de dominio.

Lista de verificación previa a la transferencia (complete todos los puntos)

1. ☐ Verifique el acceso al correo electrónico del titular

Confirme que puede recibir correos electrónicos en la dirección de correo electrónico del titular, ya que recibirá el correo electrónico de autorización de la transferencia de dominio.

 Important

Si no puede acceder a la dirección de correo electrónico del titular actual, actualice la dirección de correo electrónico de contacto del titular con su registrador actual y espere 60 días para hacer la transferencia.

2. ☐ Desbloquee el dominio

Acceda a la configuración del dominio de su registrador actual y desactive la protección «Bloqueo de dominio» o «Bloqueo de transferencia» si está activada.

 Note

Tras desactivar el bloqueo, espere unos minutos hasta que el cambio se efectúe para iniciar la transferencia.

3. ☐ Obtenga el código de autorización

Solicite un código de autorización a su registrador actual y mantenga su confidencialidad. Deberá ingresar este código en la consola de Route 53 en un paso posterior del procedimiento de transferencia.

4. ☐ Verifique la antigüedad y la elegibilidad del dominio

Confirme que su dominio cumpla con los requisitos de transferencia de la ICANN:

- El dominio debe tener al menos 60 días de antigüedad desde el registro inicial.
- Si el registro del dominio caducó y se restauró, debe haberse restaurado al menos hace 60 días.

 Tip

Las normas de la ICANN pueden bloquear temporalmente las transferencias si los datos de contacto del titular se actualizaron recientemente (por ejemplo, si se cambió su nombre o correo electrónico). Algunos registradores le permiten eximirlo de esta retención; consulte con su registrador actual si no lo sabe con seguridad.

5. ☐ Prepare el método de pago

Asegúrese de que su cuenta de AWS tenga un método de pago válido. Cuando transfiere un dominio a Route 53, la tarifa de transferencia que se aplica a su cuenta de AWS varía según el dominio de nivel superior.

Para conocer los precios actuales, consulte [Precios de Route 53](#).

 Note

No se pueden usar créditos de AWS para pagar transferencias de dominio. Route 53 cobra la tarifa de transferencia antes de iniciar el proceso y proporciona un reembolso inmediato si la transferencia no se realiza correctamente.

6. ☐ **Deshabilite DNSSEC (si está habilitado)**

Si DNSSEC está habilitado actualmente con su registrador actual, deshabilítelo temporalmente antes de iniciar la transferencia. Esto garantiza que la transferencia se pueda completar sin problemas de validación del DNS.

Por qué es importante

Cuando se transfiere un dominio, las claves DNSSEC (KSK/ZSK) y los registros DS almacenados en su registrador actual no se transfieren automáticamente a Route 53. Si vuelve a habilitar DNSSEC sin volver a configurar estas claves en Route 53, es posible que su dominio no supere la validación del DNS.

Enfoque seguro (recomendado):

1. Deshabilite DNSSEC en su registrador actual antes de iniciar la transferencia.
2. Complete la transferencia de dominio y cree su zona alojada de Route 53 (si aún no la ha creado).
3. Compruebe que todos los registros de DNS se estén resolviendo correctamente sin que DNSSEC esté habilitado.
4. Configure DNSSEC en Route 53 con los nuevos valores KSK/ZSK de la zona alojada.
5. Vuelva a habilitar DNSSEC. Para ello, publique el nuevo registro DS en su registrador de TLD (ahora Route 53).

 Tip

Si planea transferir su dominio junto con la creación de una nueva zona alojada en Route 53, deshabilite DNSSEC antes de realizar la transferencia y espere a que se verifique la configuración de la zona alojada y la resolución de DNS funcione correctamente. Una vez confirmado, puede volver a habilitar DNSSEC de forma segura desde la consola de Route 53. Compruebe siempre la configuración de DNS en Route 53 antes de volver a habilitar DNSSEC. Para obtener más información acerca de DNSSEC en relación con Route 53, consulte [Configurar DNSSEC para un dominio](#).

Opcional: transfiera primero el servicio de DNS

Considere la posibilidad de transferir su servicio de DNS a Route 53 antes de transferir el registro de dominio. A continuación se enumeran los beneficios de este enfoque:

- Reduce el riesgo de que el sitio web o el correo electrónico tengan tiempo de inactividad durante la transferencia.
- Le permite probar la funcionalidad del DNS de Route 53 antes de realizar la transferencia completa.
- Proporciona una alternativa si se producen problemas durante la transferencia de dominio.

Para transferir primero el servicio de DNS, consulte [Configuración de Amazon Route 53 como servicio DNS](#).

Pasos a seguir a continuación

Después de completar esta lista de verificación:

1. Siga paso a paso el proceso de transferencia explicado en [Transferencia del registro de un dominio a Amazon Route 53](#).
2. Controle su correo electrónico en busca de mensajes de autorización durante el proceso de transferencia.

Transferencia del registro de un dominio a Amazon Route 53

Important

Durante la transferencia de cualquier dominio de nivel superior (ccTLDs) con código de país a Route 53, excepto .cc y .tv, se ignoran las actualizaciones del contacto propietario y se utilizan los datos de contacto del propietario del registro. Una vez realizada la transferencia, puede actualizar el contacto del propietario. Para obtener más información, consulte [Actualización de la información de contacto y la propiedad de un dominio](#).

Para transferir el registro de un dominio a Amazon Route 53, siga los procedimientos de este tema prestando especial atención.

Información general del proceso de transferencia

La transferencia de dominio incluye estos pasos clave:

1. Completar la lista de verificación previa a la transferencia

Verifique los requisitos previos para evitar errores en la transferencia. Consulte [Lista de verificación previa a la transferencia para transferencias de dominios](#).

2. Solicitar la transferencia en la consola de Route 53

Introduzca el nombre de dominio y el código de autorización. Consulte [Paso 5: Solicitar la transferencia](#).

3. Autorizar por correo electrónico (es necesaria la acción del cliente)

Haga clic en el enlace de autorización enviado al correo electrónico del titular en un plazo de 5 días. Consulte [Paso 6: Hacer clic en el enlace de los correos electrónicos de confirmación y autorización..](#)

4. Esperar a que se complete

La transferencia se completa automáticamente, a menos que el registrador actual la rechace. Supervise el estado en la consola.

Puntos de error más comunes

A continuación se explican las soluciones para los problemas comunes:

- Correo electrónico no recibido: compruebe que se pueda acceder al correo electrónico del titular y controle la carpeta de correo no deseado.
- Dominio bloqueado: desbloquéelo en el registrador actual antes de iniciar la transferencia.
- Código de autenticación no válido: solicite un nuevo código de autorización al registrador actual.
- Infracción de la regla de 60 días: norma de la ICANN de 60 días (plazo de elegibilidad). Las transferencias se bloquean en un plazo de 60 días a partir del registro inicial o del cambio de contacto del titular. Algunos registradores permiten darse de baja antes del cambio; pregunte a su registrador actual, si corresponde.

 Important

Si se salta un paso, su dominio podría dejar de estar disponible en Internet.

Tenga en cuenta lo siguiente:

Ponerse en contacto con AWS Support

Si surge algún problema al transferir un dominio, puede ponerse en contacto con AWS Support de forma gratuita. Para obtener más información, consulte [Ponerse en contacto con AWS Support sobre problemas de registro de dominios](#).

Fecha de vencimiento

Para obtener información sobre cómo la transferencia de su dominio afecta a la fecha de vencimiento actual, consulte [Cómo la transferencia de un dominio a Amazon Route 53 afecta a la fecha de vencimiento del registro del dominio](#).

Cuota de transferencia

Cuando transfiere un dominio a Route 53, la tarifa de transferencia que aplicamos a su AWS cuenta depende del dominio de nivel superior, como .com o .org. Para obtener más información, consulte [Precios de Route 53](#).

No puedes usar los AWS créditos para pagar la tarifa, si la hubiera, de transferir un dominio a Route 53.

 Note

Route 53 cobra la tarifa por la transferencia de su dominio antes de que comencemos el proceso de transferencia. Si una transferencia falla por algún motivo, le abonaremos inmediatamente en su cuenta el costo de la transferencia.

Nombres de dominio premium y especiales

Los registradores de TLD han asignado precios especiales o Premium a algunos nombres de dominio. No se puede transferir un dominio a Route 53 si el dominio tiene un precio especial o premium.

Cuotas de dominio

La cantidad máxima predeterminada de dominios por AWS cuenta es 20. Puede [solicitar una mayor cuota](#). Para obtener más información, consulte [Cuotas de dominios](#).

Límite de servidores de nombres

El número máximo de servidores de nombres por dominio en Route 53 es 6.

Temas

- [Requisitos de transferencia de dominios de nivel superior](#)
- [Paso 1: Confirmar que Amazon Route 53 admite el dominio de nivel superior](#)
- [Paso 2 \(opcional\): transferir su servicio DNS a Amazon Route 53 o a otro proveedor del servicio DNS](#)
- [Paso 3: Cambiar la configuración con el registrador actual](#)
- [Paso 4: Obtener los nombres de sus servidores de nombres](#)
- [Paso 5: Solicitar la transferencia](#)
- [Paso 6: Hacer clic en el enlace de los correos electrónicos de confirmación y autorización.](#)
- [Paso 7: Actualizar la configuración del dominio.](#)

Requisitos de transferencia de dominios de nivel superior

La mayoría de los registradores de dominios aplican requisitos para transferir un dominio a otro registrador. El objetivo principal de estos requisitos es evitar que los propietarios de dominios

fraudulentos transfieran repetidamente los dominios a otros registradores. Los requisitos varían, pero los siguientes son los más comunes:

- Debe haber registrado el dominio con el registrador actual o transferido el registro del dominio al registrador actual al menos hace 60 días.
- Si el registro de un nombre de dominio ha vencido y tenía que restaurarse, debería haberse restaurado al menos hace 60 días.
- El dominio no puede tener ninguno de los siguientes códigos de estado de nombres de dominio:
 - clientTransferProhibited
 - pendingDelete
 - pendingTransfer
 - redemptionPeriod
 - serverTransferProhibited
- Los registradores de algunos dominios de nivel superior no permiten las transferencias hasta que se realizan los cambios, como los cambios del propietario del dominio.

Para ver una lista actual de códigos de estado de nombres de dominio y una explicación de cada código, visite el [sitio web de ICANN](#) y busque códigos de estado de EPP. (Busque en el sitio web de la ICANN; a veces las búsquedas web devuelven una versión antigua del documento).

 Note

ICANN es la organización que establece las políticas que rigen el registro y la transferencia de nombres de dominio.

También puede buscar su nombre de dominio en el [sitio web de Whois](#) para ver los códigos de estado y otra información de tu dominio.

Paso 1: Confirmar que Amazon Route 53 admite el dominio de nivel superior

Consulte [Dominios que puede registrar con Amazon Route 53](#). Si el dominio de nivel superior del dominio que desea transferir figura en la lista, puede transferirlo a Amazon Route 53.

Si un TLD no figura en la lista, no puede transferir actualmente el registro del dominio a Route 53. De vez en cuando añadimos más TLDs a la lista, así que vuelve a comprobar si hemos añadido compatibilidad con tu dominio.

Paso 2 (opcional): transferir su servicio DNS a Amazon Route 53 o a otro proveedor del servicio DNS

¿Por qué transferir el DNS primero?

Algunos registradores proporcionan un servicio DNS gratuito que puede desactivarse en cuanto reciban una solicitud de Route 53 para transferir el registro del dominio. Si desea que Route 53 proporcione servicio DNS para su dominio, consulte [Establecer Amazon Route 53 como servicio DNS de un dominio existente](#).

Paso 3: Cambiar la configuración con el registrador actual

Con el método que proporciona el registrador actual, realice lo siguiente para cada dominio que desee transferir.

- [Confirm that the email for the registrant contact for your domain is up to date](#)
- [Unlock the domain so it can be transferred](#)
- [Confirm that the domain status allows you to transfer the domain](#)
- [Disable DNSSEC for the domain](#)
- [Get an authorization code](#)
- [Renew your domain registration before you transfer the domain \(selected geographic TLDs\)](#)

Confirme que el correo electrónico del contacto del registrante del dominio está actualizado

Enviaremos un correo electrónico a la dirección de correo electrónico para solicitar autorización para la transferencia. Tendrá que hacer clic en un enlace del correo electrónico para autorizar la transferencia. Si no hace clic en el enlace, tendremos que cancelar la transferencia.

Important

El contacto que indique como titular tendrá determinados derechos como titular del nombre registrado del nombre de dominio, según la [Política de transferencia de la ICANN](#). La mayoría de los dominios se eliminarán al cerrar tu dominio Cuenta de AWS (para obtener más información, consulta [Mi cuenta de AWS está cerrada o se ha cerrado de forma definitiva y mi dominio está registrado con Route 53](#)). Sin embargo, si un dominio permanece en una cuenta cerrada, el contacto que indicaste como registrante podrá solicitar la transferencia del nombre de dominio a un registrador externo. Por lo tanto,

es importante que el contacto de titular de registro que muestre sea usted mismo u otra persona en la que confíe para actuar de manera responsable.

Desbloquee el dominio para que se pueda transferir

ICANN, el organismo que rige los registros de dominios, exige que se desbloquee el dominio antes de transferirlo.

Confirme que el estado del dominio le permite transferir el dominio

Para obtener más información, consulte [Requisitos de transferencia de dominios de nivel superior](#).

Deshabilite DNSSEC para el dominio

Si utiliza DNSSEC con un dominio y transfiere el registro de dominio a Route 53, primero debe desactivar DNSSEC en el registrador anterior. A continuación, después de transferir el registro de dominio, siga los pasos necesarios a fin de configurar DNSSEC para el dominio en Route 53. Route 53 admite DNSSEC para el registro de dominios y la firma de DNSSEC. Para obtener más información, consulte [Configuración de la firma de DNSSEC en Amazon Route 53](#).

 Important

Si transfiere un registro de dominio a Route 53 mientras DNSSEC está configurado, también se transfieren las claves públicas de DNSSEC. Si transfiere el servicio DNS a un proveedor que no admite DNSSEC, la resolución DNS produce un error de forma intermitente hasta que elimine las claves de DNSSEC del dominio. Para obtener más información, consulte [Eliminar claves públicas de un dominio](#).

Obtenga un código de autorización

Un código de autorización del registrador actual nos autoriza a solicitar que el registro del dominio se transfiera a Route 53. Ingresará este código en la consola de Route 53 más adelante en este procedimiento.

Algunos dominios de nivel superior tienen requisitos adicionales:

Dominios .co.za

No es necesario que obtenga un código de autorización para transferir un dominio .co.za a Route 53.

Dominios .uk, .co.uk, .me.uk y .org.uk

Si va a transferir un dominio .uk, .co.uk, .me.uk o .org.uk a Route 53, no es necesario que obtenga un código de autorización. En lugar de ello, use el método proporcionado por el registrador del dominio actual para actualizar el valor de la etiqueta IPS del dominio a GANDI (con todos los caracteres en mayúsculas). (Nominet, la empresa de registro de nombres de dominio .uk, requiere una etiqueta IPS). Si su registrador no proporciona una forma de cambiar el valor de la etiqueta IPS, [póngase en contacto con Nominet](#).

Tenga en cuenta lo siguiente sobre el cambio de la etiqueta IPS:

Debe solicitar la transferencia en un plazo de cinco días

Si no solicita la transferencia en un plazo de cinco días después de cambiar la etiqueta IPS, la etiqueta vuelve a cambiar al valor anterior. Debe cambiar el valor de la etiqueta IPS de nuevo o la solicitud de transferencia fallará.

Visualización de la etiqueta IPS en consultas WHOIS

El cambio en la etiqueta IPS no aparece en las consultas WHOIS hasta después de que se haya completado la transferencia a Route 53.

Correo electrónico de Gandi

Es posible que reciba un correo electrónico de nuestro registrador asociado, Gandi, relativo al proceso de transferencia. Si recibe un correo electrónico de Gandi (transfer-auth@gandi.net) acerca de la transferencia de su dominio, pase por alto las instrucciones del correo electrónico, ya que no son pertinentes para los dominios .uk, .co.uk, .me.uk ni .org.uk. En su lugar, siga las instrucciones de este tema para hacerlo.

Renueva el registro de tu dominio antes de transferirlo (zona geográfica TLDs seleccionada)

En la mayoría de los casos TLDs, cuando transfieres un dominio, el registro se prolonga automáticamente un año. Sin embargo, en algunas zonas geográficas TLDs, el registro no se prolonga al transferir el dominio. Si va a transferir un dominio a Route 53 que tenga una de estas características TLDs, le recomendamos que renueve el registro del dominio antes de transferirlo, especialmente si se acerca la fecha de caducidad.

 Important

Si no renueva el dominio antes de transferirlo, el registro podría caducar antes de que se completase la transferencia. En este caso, el dominio deja de estar disponible en Internet y el nombre de dominio podría estar disponible para que otros lo compren.

El registro no se prolonga automáticamente cuando transfiere los siguientes dominios a otro registrador:

- .ch (Suiza)
- .cl (Chile)
- .co.uk (Reino Unido)
- .co.za (Sudáfrica)
- .com.au (Australia)
- .cz (Czech Republic)
- .es (España)
- .fi (Finlandia)
- .im (Isla de Man)
- .jp (Japón)
- .me.uk (Reino Unido)
- .net.au (Australia)
- .org.uk (Reino Unido)
- .se (Suecia)
- .uk (Reino Unido)

Paso 4: Obtener los nombres de sus servidores de nombres

Si utiliza Amazon Route 53 como su servicio DNS o va a seguir utilizando el servicio DNS existente, obtendremos los nombres de los servidores de nombres automáticamente más adelante en este proceso. Vaya a [Paso 5: Solicitar la transferencia](#).

Si desea cambiar el servicio DNS a un proveedor distinto de Route 53 al mismo tiempo que transfiere el dominio a Route 53, utilice el procedimiento que proporciona el proveedor del servicio DNS para obtener los nombres de los servidores de nombres de cada dominio que desea transferir.

⚠ Important

Si el registrador de su dominio es también el proveedor del servicio DNS del dominio, transfiera su servicio DNS a Route 53 o a otro proveedor del servicio DNS antes de continuar con el proceso de transferencia del registro del dominio.

Si transfiere el servicio DNS al mismo tiempo que el registro del dominio, su sitio web, correo electrónico y aplicaciones web asociados con el dominio podrían dejar de estar disponibles.

Para obtener más información, consulte [Paso 2 \(opcional\): transferir su servicio DNS a Amazon Route 53 o a otro proveedor del servicio DNS](#).

Paso 5: Solicitar la transferencia

Para transferir un registro de dominio del registrador actual a Amazon Route 53, utilice la consola de Route 53 a fin de solicitar la transferencia. Route 53 se encarga de la comunicación con el registrador actual del dominio.

Puede utilizar la consola para transferir hasta cinco dominios.

El procedimiento que utilice depende de si desea transferir hasta un solo dominio o hasta cinco:

- [Para transferir el registro de dominio de un solo dominio a Route 53](#)
- [Transferencia de un registro de dominios a Route 53 para hasta cinco dominios](#)

Use el proceso Transferir dominio a su cuenta para transferir un solo dominio a su cuenta.

Para transferir el registro de dominio de un solo dominio a Route 53

1. Abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Registered domains.
3. En la página Dominios registrados, elija Dominio único en el menú desplegable Transferencia entrante.
4. En la página Transferir dominio a su cuenta, en la sección Comprobar si el dominio se puede transferir, introduzca el nombre del dominio cuyo registro desea transferir a Route 53 y seleccione Comprobar.
5. Si el registro de dominio está disponible para ser transferido, compruebe que ha completado los requisitos de transferencia para los dominios de nivel superior y seleccione Siguiente.

Si el registro del dominio no está disponible para su transferencia, el motivo se indicará en la consola de Route 53. Póngase en contacto con su registrador para obtener información acerca de cómo resolver los problemas que le impiden transferir el registro.

6. En la página Servicio de DNS, revise la información sobre los servidores de nombres y seleccione Siguiente.
7. Si se lo solicita, introduzca el código de autorización o etiqueta IPS que obtuvo de su registrador actual en [Paso 3: Cambiar la configuración con el registrador actual](#).

 Note

No es necesario que ingrese un código de autorización para transferir un dominio .co.za, .uk, .co.uk, .me.uk o .org.uk a Route 53.

Elija Siguiente.

8. En la página Opciones de precios de dominios, elija el número de años durante los que desea registrar el dominio que va a transferir y si desea que renovemos automáticamente el registro del dominio antes de la fecha de vencimiento.

 Note

Los registros y las renovaciones de nombres de dominio no son reembolsables. Si habilita la renovación automática de dominios y decide que no desea el nombre de dominio después de renovar el registro, no podrá obtener un reembolso por el costo de la renovación.

Elija Siguiente.

9. En la página Información de contacto, escriba la información de contacto del registrador del dominio, del administrador, de los técnicos y de los contactos de facturación. Los valores que especifique aquí se aplicarán a todos los dominios que registre. Para obtener más información, consulte [Valores que especifican cuando registra o transfiere un dominio](#).

Tenga en cuenta las siguientes consideraciones:

Nombre y apellidos

En First Name y Last Name, le recomendamos que indique el nombre que figura en su ID oficial. Para la realización de determinados cambios en la configuración del dominio, en algunos registros de dominio es necesario que se identifique. El nombre de su ID debe coincidir con el nombre del titular del dominio.

Contactos diferentes

De forma predeterminada, utilizamos la misma información para los tres contactos. Si quiere ingresar información diferente para uno o más contactos, desactive el valor Igual que el titular.

Note

Para los dominios .it, el titular y el administrador deben ser la misma persona.

Información adicional obligatoria

Para algunos dominios de nivel superior (TLDs), debemos recopilar información adicional. Para estos TLDs, introduce los valores aplicables después del campo Código postal/postal.

Protección de la privacidad

Elija si desea ocultar su información de contacto de las consultas WHOIS.

Note

Debe especificar la misma configuración de privacidad para los contactos de administrador, titular y los contactos técnicos.

Para obtener más información, consulte los temas siguientes:

- [Activación o desactivación de la protección de privacidad para la información de contacto para un dominio](#)
- [Dominios que puede registrar con Amazon Route 53](#)

 Note

Para habilitar la protección de privacidad de los dominios.uk, .co.uk, .me.uk, y .org.uk, debe abrir un caso de soporte técnico y solicitar la protección de privacidad.

Elija Siguiente.

10. En la página Revisar, compruebe la información que introdujo y, si lo desea, corríjala. Lea los términos y condiciones del servicio, y seleccione la casilla de verificación para confirmar que los leyó.

Elija Submit request (Enviar solicitud).

11. En el panel de navegación, seleccione Dominios y, a continuación, Solicitudes.

En esta página, puede ver el estado del dominio y también si necesita responder el correo electrónico de verificación de contacto del titular. También puede optar por volver a enviar el correo electrónico de verificación.

Si especificó una dirección de correo electrónico para el contacto de titular que nunca se haya utilizado a fin de registrar un dominio con Route 53, algunos registros TLD necesitan que verifique que la dirección es válida.

Le enviaremos un correo electrónico de verificación desde una de las siguientes direcciones de correo electrónico:

- `noreply@registrar.amazon`: si TLDs está registrado por Amazon Registrar.
- `noreply@domainnameverification.net`: para ser TLDs registrado por nuestro registrador asociado, Gandi. Para determinar quién es el registrador de su TLD, consulte [Búsqueda del registrador](#).

 Important

El contacto del registrante debe seguir las instrucciones del correo electrónico para verificar que se ha recibido el correo electrónico, ya que, en caso contrario, suspenderemos el dominio, tal y como exige ICANN. Cuando se suspende un dominio, esté no está accesible en Internet.

- a. Cuando reciba el correo electrónico de verificación, seleccione el enlace del correo electrónico que verifica que la dirección de correo electrónico es válida. Si no recibe el correo electrónico inmediatamente, compruebe la carpeta de basura.
 - b. Volver a la página Solicitudes. Si el estado no se actualizará automáticamente indicando email-address is verified, seleccione Refresh status.
12. Cuando se haya completado el registro del dominio, el siguiente paso depende de si desea utilizar Route 53 u otro servicio DNS como servicio DNS para el dominio:

- Route 53: en la zona alojada que Route 53 creó cuando registró el dominio, cree registros para indicar a Route 53 cómo desea dirigir el tráfico del dominio y los subdominios.

Por ejemplo, cuando alguien escribe su nombre de dominio en un navegador y esa consulta se reenvía a Route 53, ¿quiere que Route 53 responda a la consulta con la dirección IP de un servidor web de su centro de datos o con el nombre de un balanceador de carga de ELB?

Para obtener más información, consulte [Uso de registros](#).

 Important

Si crea registros en una zona alojada diferente de la que Route 53 crea automáticamente, debe actualizar los servidores de nombres del dominio para utilizar los servidores de nombres de la zona alojada nueva.

- Otro servicio DNS: configure su nuevo dominio para dirigir las consultas de DNS al otro servicio DNS. Realice el procedimiento [Actualización de los servidores de nombres para utilizar otro registrador](#).

Use el siguiente procedimiento para transferir hasta cinco dominios a su cuenta.

Transferencia de un registro de dominios a Route 53 para hasta cinco dominios

1. Abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Registered domains.
3. En la página Dominios registrados, seleccione Varios dominios en el menú desplegable Transferencia entrante.

4. En la página Transferir varios dominios a su cuenta, introduzca hasta cinco dominios que desee transferir y su código de autorización, si es necesario, por línea y seleccione Comprobar.
5. Si el registro de dominio está disponible para su transferencia, aparecerá en la lista de Disponibilidad del dominio como disponible. Seleccione la casilla de verificación situada junto a cada dominio cuyo registro quiera transferir, compruebe que haya cumplido los requisitos de transferencia para los dominios de nivel superior y seleccione Siguiente.

Si el registro del dominio no está disponible para su transferencia, el motivo se indicará en la consola de Route 53. Póngase en contacto con su registrador para obtener información acerca de cómo resolver los problemas que le impiden transferir el registro.

6. En la página Servicio de DNS, revise la información sobre los servidores de nombres y seleccione Siguiente.

 Note

Los registros y las renovaciones de nombres de dominio no son reembolsables. Si habilita la renovación automática de dominios y decide que no desea el nombre de dominio después de renovar el registro, no podrá obtener un reembolso por el costo de la renovación.

7. En la página Información de contacto, escriba la información de contacto del titular, del administrador y de los contactos técnicos del dominio. Los valores que especifique aquí se aplicarán a todos los dominios que transfiera.

 Important

Le recomendamos que especifique los siguientes valores en el contacto del registrante (el propietario del dominio):

- First and last name (Nombre y apellidos): le recomendamos que indique el nombre que figura en su ID oficial. Para la realización de determinados cambios en la configuración del dominio, en algunos registros de dominio es necesario que se identifique. El nombre de su ID debe coincidir con el nombre del titular del dominio.
- Contact details (Datos de contacto): durante la transferencia del dominio, le recomendamos que especifique los mismos valores tal y como se especifican en el registrador actual. Al cambiar los datos del contacto del registrante, cambia el propietario del dominio y algunos registros de TLD no le permiten cambiar el

propietario del dominio durante una transferencia de dominio. Si cambia los datos del contacto del registrante, la transferencia podría producir un error. Puede cambiar los datos del contacto del registrante después de transferir el dominio.

De forma predeterminada, utilizamos la misma información para los tres contactos. Si quiere ingresar información diferente para uno o más contactos, desactive el valor Igual que el titular.

 Note

Para los dominios .it, el titular y el administrador deben ser la misma persona.

Para obtener más información, consulte [Valores que especifican cuando registra o transfiere un dominio](#).

8. En algunos casos TLDs, debemos recopilar información adicional. Para ello TLDs, introduce los valores aplicables después del campo Código postal/postal.
9. Si el valor de For each domain name that you want to transfer, enter the applicable values es Person, elija si desea ocultar su información de contacto en las consultas WHOIS. Para obtener más información, consulte [Activación o desactivación de la protección de privacidad para la información de contacto para un dominio](#).
10. Seleccione Enviar.
11. Revise la información que ha introducido, lea los términos y condiciones del servicio, y seleccione la casilla para confirmar que ha leído los términos y condiciones del servicio.
12. Elija Submit request (Enviar solicitud).

Confirmaremos que los dominios se pueden transferir y enviaremos un correo electrónico a los contactos del titular del dominio para solicitar autorización para transferirlo.

13. En el panel de navegación, seleccione Dominios y, a continuación, Solicitudes.

En esta página puede ver el estado del dominio y también si necesita responder el correo electrónico de verificación de contacto del titular. También puede optar por volver a enviar el correo electrónico de verificación.

Si especificó una dirección de correo electrónico para el contacto de titular que nunca se haya utilizado a fin de registrar un dominio con Route 53, algunos registros TLD necesitan que verifique que la dirección es válida.

Le enviaremos un correo electrónico de verificación desde una de las siguientes direcciones de correo electrónico:

- `noreply@registrar.amazon`: si TLDs está registrado por Amazon Registrar.
- `noreply@domainnameverification.net`: para ser TLDs registrado por nuestro registrador asociado, Gandi. Para determinar quién es el registrador de su TLD, consulte [Búsqueda del registrador](#).

 Important

El contacto del registrante debe seguir las instrucciones del correo electrónico para verificar que se ha recibido el correo electrónico, ya que, en caso contrario, suspenderemos el dominio, tal y como exige ICANN. Cuando se suspende un dominio, esté no está accesible en Internet.

- a. Cuando reciba el correo electrónico de verificación, seleccione el enlace del correo electrónico que verifica que la dirección de correo electrónico es válida. Si no recibe el correo electrónico inmediatamente, compruebe la carpeta de basura.
 - b. Volver a la página Solicitudes. Si el estado no se actualizará automáticamente indicando email-address is verified, seleccione Refresh status.
14. Cuando se haya completado el registro del dominio, el siguiente paso depende de si desea utilizar Route 53 u otro servicio DNS como servicio DNS para el dominio:
- Route 53: en la zona alojada que Route 53 creó cuando registró el dominio, cree registros para indicar a Route 53 cómo desea dirigir el tráfico del dominio y los subdominios.

Por ejemplo, cuando alguien escribe su nombre de dominio en un navegador y esa consulta se reenvía a Route 53, ¿quiere que Route 53 responda a la consulta con la dirección IP de un servidor web de su centro de datos o con el nombre de un balanceador de carga de ELB?

Para obtener más información, consulte [Uso de registros](#).

 Important

Si crea registros en una zona alojada diferente de la que Route 53 crea automáticamente, debe actualizar los servidores de nombres del dominio para utilizar los servidores de nombres de la zona alojada nueva.

- Otro servicio DNS: configure su nuevo dominio para dirigir las consultas de DNS al otro servicio DNS. Realice el procedimiento [Actualización de los servidores de nombres para utilizar otro registrador](#).

Paso 6: Hacer clic en el enlace de los correos electrónicos de confirmación y autorización.

Poco después de solicitar la transferencia, es posible que enviemos uno o varios correos electrónicos al contacto del titular del dominio:

Email para confirmar que se puede contactar con el titular

Si nunca ha registrado un dominio en Route 53 ni ha transferido un dominio a Route 53, le enviaremos un correo electrónico donde se le solicita que confirme que la dirección de correo electrónico es válida. Conservaremos esta información para no tener que volver a enviar este email de confirmación de nuevo.

Email para obtener la autorización para transferir el dominio

En algunos TLDs casos, es necesario responder a un correo electrónico para autorizar la transferencia del dominio.

Genéricos TLDs como .com, .net y .org

No se requiere autorización para los dominios que tienen un [TLD genérico](#), como .com, .net u .org.

Geográficos TLDs , como .co.uk y .jp

En el caso de los dominios que tienen un [TLD geográfico](#), se requiere su autorización para transferir el dominio. Si transfiere 10 dominios, tenemos que enviarle 10 emails, y tendrá que hacer clic en el enlace de autorización en cada uno de ellos.

Todos estos emails van al contacto del titular del dominio:

- Si usted es el contacto del registrante del dominio, siga las instrucciones del correo electrónico para autorizar la transferencia.
- Si otra persona es el contacto del registrante, pida a esa persona que siga las instrucciones del correo electrónico para autorizar la transferencia.

Important

Si va a transferir un dominio que tiene un TLD geográfico, esperaremos hasta cinco días a que el contacto del registrador autorice la transferencia. Si el contacto del registrante no responde en cinco días, cancelamos la operación de transferencia y enviamos un mensaje de correo electrónico al contacto del registrante para informarle de la cancelación.

Temas

- [Correo electrónico de autorización para un nuevo propietario o una nueva dirección de correo electrónico](#)
- [Direcciones de correo electrónico de donde proceden los correos electrónicos de autorización](#)
- [Aprobación del registrador actual](#)
- [¿Qué ocurre a continuación?](#)

Correo electrónico de autorización para un nuevo propietario o una nueva dirección de correo electrónico

Si ha cambiado los valores siguientes, le enviaremos un correo electrónico aparte para solicitar su autorización:

Propietario del dominio

Si cambia el propietario del dominio, como se describe en [¿Qué desencadena un cambio de titularidad de dominio?](#), enviaremos un email al contacto del registrante del dominio.

Dirección de correo electrónico del contacto del registrante (solo para algunos) TLDs

En algunos casos TLDs, si cambias la dirección de correo electrónico del contacto registrado, enviamos un correo electrónico a la antigua y a la nueva dirección de correo electrónico del contacto registrado. Alguien en ambas direcciones de email debe seguir las instrucciones del email para autorizar el cambio.

Para hacer cambios en la información del propietario del dominio o de la dirección de correo electrónico de contacto del titular, si no recibimos autorización para dicho cambio en un plazo de 3 a 15 días, en función del dominio de nivel superior, tendremos que cancelar la solicitud, tal y como lo exige ICANN.

Direcciones de correo electrónico de donde proceden los correos electrónicos de autorización

Todos los mensajes de correo electrónico provienen de una de las siguientes direcciones de correo electrónico.

TLDs	Dirección de email de donde procede el email de autorización
.com.au y .net.au	no-reply@ispapi.net El correo electrónico contiene un enlace a http://transfers.ispapi.net.
.fr	nic@nic.fr, si cambia el contacto del registrante de un nombre de dominio .fr al mismo tiempo que transfiere el dominio. (El correo electrónico se envía al contacto del registrante actual y al contacto del nuevo registrante).
Todos los demás	Una de las siguientes direcciones de email: • noreply@registrar.amazon • noreply@domainnameverification.net

Para determinar quién es el registrador de su TLD, consulte [Dominios que puede registrar con Amazon Route 53](#).

Aprobación del registrador actual

Si el contacto del registrante autoriza la transferencia, empezamos a trabajar con el registrador actual para transferir el dominio. Este paso podría tardar hasta diez días, en función del dominio de nivel superior de su dominio:

- [Dominios de nivel superior genéricos](#): tardan hasta siete días.
- [Dominios geográficos de nivel superior](#) (denominados también dominios de nivel superior de código de país): tardan hasta diez días.

Si el registrador actual no responde a nuestra solicitud de transferencia, algo habitual entre los registradores, la transferencia se produce de forma automática. Si el registrador actual rechaza la solicitud de transferencia, enviaremos una notificación por correo electrónico al contacto del registrante actual. El registrante tendrá que ponerse en contacto con el registrador actual y resolver los problemas con la transferencia.

¿Qué ocurre a continuación?

Cuando se ha aprobado la transferencia de su dominio, enviamos otro correo electrónico al contacto del registrante. Para obtener información sobre el proceso, consulte [Ver el estado de una transferencia de dominio](#).

Cobramos a tu AWS cuenta la transferencia de dominio tan pronto como se complete la transferencia. Para obtener una lista de los cargos por TLD, consulte [Precios de Amazon Route 53 para el registro de dominios](#).

Note

Se trata de un cargo único, por lo que no aparecerá en sus métricas de facturación de CloudWatch. Para obtener más información sobre CloudWatch las métricas, consulta [Uso de CloudWatch las métricas de Amazon](#) en la Guía del CloudWatch usuario de Amazon.

Paso 7: Actualizar la configuración del dominio.

Una vez que se haya completado la transferencia, puede cambiar los siguientes ajustes:

Transfer lock

Para transferir el dominio a Route 53, tuvo que desactivar el bloqueo de transferencia. Si desea volver a habilitar el bloqueo para impedir transferencias no autorizadas, consulte [Bloqueo de un dominio para impedir la transferencia no autorizada a otro registrador](#).

Renovación automática

Configuramos el dominio transferido para que se renueve automáticamente cuando se aproxime la fecha de vencimiento. Para obtener información sobre cómo cambiar esta configuración, consulte [Activación o desactivación de la renovación automática de un dominio](#).

Periodo de registro ampliado

De forma predeterminada, Route 53 renueva el dominio anualmente. Si desea registrar el dominio durante un periodo mayor, consulte [Ampliación del periodo de registro de un dominio](#).

DNSSEC

Para obtener información sobre la configuración de DNSSEC del dominio, consulte [Configurar DNSSEC para un dominio](#).

Prevención de problemas comunes con las transferencias a Route 53

Si tiene problemas mientras la transferencia de dominio está en curso, a continuación se detallan los problemas más comunes y cómo resolverlos:

Note

Si la transferencia ya ha fallado, consulte [No se pudo transferir mi dominio a Amazon Route 53](#) para solucionar problemas posteriores a un error.

No recibió el correo electrónico de autorización

Si no recibe el correo electrónico de autorización de Route 53, estas son las causas más comunes y las soluciones:

- Revise su carpeta de correo no deseado: los proveedores de correo electrónico a veces filtran los correos electrónicos de autorización.
- Verifique su dirección de correo electrónico: confirme que la dirección de correo electrónico del titular que figura en la información de contacto de su dominio esté actualizada y sea accesible.
- Actualice su información de contacto: si la dirección de correo electrónico no está actualizada, actualícela con su registrador actual antes de iniciar la transferencia.
- Reenvíe el correo electrónico de autorización: en la consola de Route 53, haga clic en «Reenviar el correo electrónico de autorización» para el dominio en estado de transferencia.

Aparece un error «Invalid authorization code»

Si recibe un error «Invalid authorization code», pruebe estas soluciones:

- Vuelva a verificar que el código sea correcto: los códigos de autorización distinguen entre mayúsculas y minúsculas. Copie y pegue el código directamente desde la interfaz de su registrador para evitar errores de escritura.
- Compruebe si el código ha caducado: los códigos de autorización pueden caducar después de 5 a 30 días, según su registrador actual. Solicite un código nuevo si el suyo ha caducado.
- Elimine los espacios adicionales: asegúrese de que no haya espacios al principio ni al final cuando introduzca el código.
- Obtenga un nuevo código de autorización: si el código sigue fallando, solicite un nuevo código de autorización a su registrador actual.

Su dominio está bloqueado en el registrador actual

Las transferencias de dominio pueden fallar si su registrador actual tiene activado el bloqueo de transferencias (también conocido como «bloqueo de dominio» o «transferencia de clientes prohibida»). Se trata de una configuración de seguridad común que impide las transferencias no autorizadas.

Para resolver este problema, siga estos pasos:

- Desbloquee su dominio: inicie sesión en el panel de control de su registrador actual y desactive el bloqueo de transferencias de dominio.
- Verifique que se haya eliminado el bloqueo: puede usar cualquier herramienta pública de búsqueda de WHOIS para confirmar que el estado del dominio sea «OK» en lugar de «clientTransferProhibited».
- Pida ayuda a su registrador: si no ve ninguna opción para desbloquear su dominio, comuníquese con el equipo de asistencia de su registrador actual. Pueden ayudarlo a eliminar el bloqueo.

Su dominio no es elegible para la transferencia

Si se rechaza la transferencia de dominio debido a problemas de elegibilidad, controle lo siguiente:

- Verifique la antigüedad del dominio: su dominio debe tener al menos 60 días de antigüedad desde el registro o la última transferencia.

- Compruebe la compatibilidad con los TLD: confirme que Route 53 sea compatible con el dominio de nivel superior (TLD) de su dominio. Consulte [Dominios que puede registrar con Amazon Route 53](#) para conocer los TLD compatibles.
- Revise el estado del dominio: los dominios con determinados códigos de estado (como «pendingTransfer» o «redemptionPeriod») no se pueden transferir.
- Compruebe la fecha de caducidad: es posible que los dominios que estén vencidos o que estén a menos de 15 días de caducar no sean transferibles.
- Resuelva los problemas de facturación: asegúrese de pagar todas las tarifas pendientes correspondientes a su registrador actual.

Su transferencia está tardando más de lo esperado

Si parece que su transferencia se ha retrasado, debe saber lo siguiente:

- Plazo normal: la mayoría de las transferencias se completan en un plazo de 5 a 7 días, pero pueden tardar hasta 10 días.
- Controle el estado de la transferencia: compruebe el progreso de la transferencia en la consola de Route 53. Para obtener más información, consulte [Ver el estado de una transferencia de dominio](#).
- Responda rápidamente a los correos electrónicos: es posible que ambos registradores envíen correos electrónicos de confirmación que requieran su respuesta para continuar.
- Póngase en contacto con su registrador actual: si la transferencia se retrasa, comuníquese con su registrador actual para asegurarse de que no esté bloqueando la transferencia.

Cuándo ponerse en contacto con AWS Support

Comuníquese con AWS Support si ha probado las soluciones anteriores y sigue teniendo problemas, o si se encuentra con:

- Errores en la transferencia después de varios intentos con la información correcta
- Problemas de facturación o pago durante el proceso de transferencia
- Errores técnicos en la consola de Route 53 que le impiden iniciar una transferencia
- Transferencias que permanecen en estado «pendiente» durante más de 10 días

Cuando se ponga en contacto con el servicio de asistencia, incluya su nombre de dominio, el identificador de la solicitud de transferencia (si está disponible) y los detalles sobre el error o problema específico que está experimentando.

Transferencia de un dominio de Amazon Route 53 a otro registrador

Cuando transfiere un dominio desde Amazon Route 53 a otro registrador, obtiene información de Route 53 y se la proporciona al nuevo registrador. El nuevo registrador se encargará de lo demás.

Important

Si en la actualidad utiliza Route 53 como su proveedor del servicio DNS y desea también transferir el servicio DNS a otro proveedor, debe saber que las siguientes características de Route 53 no tienen un paralelismo directo con las características que proporcionan otros proveedores de servicios DNS. Tendrá que contactar con el nuevo proveedor del servicio DNS para determinar cómo conseguir funcionalidades equivalentes:

- Registros de alias. Para obtener más información, consulte [Elección entre registros de alias y sin alias](#).
- Políticas de direccionamiento distintas de la política de direccionamiento simple. Para obtener más información, consulte [Elección de una política de enrutado](#).
- Comprobaciones de estado que están asociadas con registros. Para obtener más información, consulte [Configuración de la recuperación ante errores a nivel de DNS](#).

La mayoría de los registradores de dominios aplican requisitos para transferir un dominio a otro registrador. El objetivo principal de estos requisitos es evitar que los propietarios de dominios fraudulentos transfieran repetidamente los dominios a otros registradores. Los requisitos varían, pero los siguientes son los más comunes:

- Debe haber registrado el dominio con el registrador actual o transferido el registro del dominio al registrador actual al menos hace 14 días.
- El dominio no puede tener ninguno de los siguientes códigos de estado de nombres de dominio:
 - pendingDelete
 - pendingTransfer
 - redemptionPeriod
 - clientTransferProhibited
 - serverTransferProhibited

Para ver una lista actual de códigos de estado de nombres de dominio y una explicación de cada código, visite el [sitio web de ICANN](#) y busque epp status codes. (Busque en el sitio web de la ICANN; a veces las búsquedas web devuelven una versión antigua del documento).

 Note

Si desea transferir su dominio a otro registrador de dominio, pero la cuenta de AWS con la que está registrado el dominio está cerrada, suspendida o terminada, puede ponerse en contacto con AWS Support para obtener asistencia. Los dominios no se pueden transferir durante los primeros 14 días de registro. Para obtener más información, consulte [Ponerse en contacto con AWS Support sobre problemas de registro de dominios](#).

 Note

Si el nuevo registrador requiere un código REG-ID, puede ponerse en contacto con AWS Support para obtener ayuda. Para obtener más información, consulte [Ponerse en contacto con AWS Support sobre problemas de registro de dominios](#).

Transferencia de un dominio de Route 53 a otro registrador

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Registered domains.
3. Elija el nombre del dominio que desea transferir a otro registrador.
4. En la página de nombre de dominio, compruebe el valor del código de estado del nombre de dominio. Si es alguno de los siguientes valores, no puede transferir el dominio en este momento:
 - pendingDelete
 - pendingTransfer
 - redemptionPeriod
 - clientTransferProhibited
 - serverTransferProhibited

Para ver una lista actual de códigos de estado de nombres de dominio y una explicación de cada código, visite el [sitio web de ICANN](#) y busque epp status codes. (Busque en el sitio web de la ICANN; a veces las búsquedas web devuelven una versión antigua del documento).

Si el valor de Domain name status code (Código de estado del nombre de dominio) es serverTransferProhibited (serverTransferProhibited), puede ponerse en contacto con AWS Support de forma gratuita para saber lo que debe hacer a fin de poder transferir el dominio. Para obtener más información, consulte [Ponerse en contacto con AWS Support sobre problemas de registro de dominios](#).

5. Si el valor de Bloqueo de transferencia está Activado, seleccione Desactivar el bloqueo de transferencia en el menú desplegable Acciones.
6. Todos los dominios, excepto .be, .co.za, .ru, .uk, .co.uk, .me.uk y .org.uk: en la página Nombre de dominio, seleccione Transferir a otro registrador en el menú desplegable Transferencia saliente.

En el cuadro de diálogo Transferir a otro registrador, seleccione Copiar para copiar el código de autorización de la transferencia de dominio. Proporcionará este valor a su registrador más adelante en este procedimiento.

 Note

En el caso de los dominios.eu, también puede generar el código de autenticación mediante el panel “Mi.eu” del registro: <https://my.eurid.eu/>.

Dominios .be, .co.za, .es, .ru, .uk, .co.uk, .me.uk, and .org.uk: haga lo siguiente:

Dominios .be

Obtenga el código de autorización del registro para los dominios .be en el [sitio web de DNS Bélgica](#).

Dominios .co.za

No es necesario que obtenga un código de autorización para transferir un dominio .co.za a otro registrador.

Dominios .ru

Obtenga el código de autorización del registro para dominios .ru en <https://www.nic.ru/en/auth/recovery/>:

- a. Elija la opción para recuperar las credenciales por nombre de dominio.
- b. Escriba su nombre de dominio y seleccione Continue (Continuar).
- c. Siga las instrucciones en pantalla para obtener acceso a la página de administración de RU-CENTER.
- d. En la sección Manage your account (Administrar su cuenta), elija Domain transfer (Transferencia de dominio).
- e. Confirme la transferencia con REGRU-RU.

Dominios .uk, .co.uk, .me.uk y .org.uk

Cambie la etiqueta IPS por el valor del nuevo registrador:

- a. Vaya a la página [Find a Registrar](#) del sitio web de Nominet y busque la etiqueta IPS del nuevo registrador. (Nominet es la empresa de registro de los dominios .uk, .co.uk, .me.uk y .org.uk).
- b. En la página Dominios registrados > Nombre de dominio, seleccione el menú desplegable Transferencia saliente y, a continuación, Actualizar etiqueta IPS, y especifique el valor que obtuvo en el paso 6a.
- c. Elija Actualizar.

Note

También puede actualizar la etiqueta IPS en la consola Nominet. Para obtener instrucciones, consulte este artículo sobre [cómo cambiar el registrador](#).

7. Si no está usando actualmente Route 53 como el proveedor del servicio DNS de su dominio, vaya al paso 10.

Si está utilizando actualmente Route 53 como el proveedor del servicio DNS para el dominio, realice los pasos siguientes:

- a. Elija Zonas alojadas.
- b. Elija el nombre de la zona alojada de su dominio. El dominio y la zona alojada tienen el mismo nombre.

- c. Si desea seguir utilizando Route 53 como el proveedor del servicio DNS del dominio: obtenga los nombres de los cuatro servidores de nombres que Route 53 ha asignado a su zona alojada. Para obtener más información, consulte [Obtener los servidores de nombres para una zona alojada pública](#).

Si no desea seguir utilizando Route 53 como el proveedor del servicio DNS del dominio: tome nota de la configuración de todos los registros, excepto los registros SOA y NS. Para las características específicas de Route 53, como los registros de alias, tendrá que ponerse en contacto con el nuevo proveedor del servicio DNS para determinar cómo conseguir una funcionalidad equivalente.

8. Si va a transferir el servicio DNS a otro proveedor, emplee los métodos ofrecidos por el nuevo servicio DNS para llevar a cabo las siguientes tareas:
 - Creación de una zona alojada
 - Creación de registros que reproduzcan la funcionalidad de sus registros de Route 53
 - Obtención de los servidores de nombres que el nuevo servicio DNS ha asignado a su zona alojada
9. Siga el proceso proporcionado por el nuevo registrador para solicitar una transferencia del dominio.

Todos los dominios, excepto co.za, .uk, .co.uk, .me.uk y .org.uk: se le pedirá que ingrese el código de autorización que obtuvo de la consola de Route 53 en el paso 6 de este procedimiento.

10. Si aún desea utilizar Route 53 como proveedor de servicios DNS, siga el proceso que proporciona el nuevo registrador para especificar los nombres de los servidores de nombres de Route 53 que obtuvo en el paso 7. Si desea utilizar otro proveedor del servicio DNS, especifique los nombres de los servidores de nombres que el nuevo proveedor le proporcionó al crear una zona alojada nueva en el paso 8.
11. Responda al correo electrónico de confirmación:

Todos los dominios, excepto .jp

Route 53 envía un correo electrónico de confirmación a la dirección de correo electrónico del titular del dominio:

- Si no responde al correo electrónico, la transferencia se efectúa automáticamente en la fecha especificada.

- Si desea que la transferencia se complete antes o desea cancelar la transferencia, elija el enlace del correo electrónico para ir a la página web de Route 53 y elegir la opción aplicable.
- Según el TLD, el correo electrónico de confirmación puede contener un enlace a <https://approvemove.com> donde puede aprobar o rechazar la transferencia. Cuando la protección de privacidad esté habilitada para los contactos del dominio, el correo electrónico se entregará desde las direcciones de identity-protect.org de los TLD registrados en Amazon Registrar. Para determinar quién es el registrador de su TLD, consulte [Búsqueda del registrador](#).

Dominios .jp

Route 53 envía un correo electrónico de confirmación a la dirección de correo electrónico del titular del dominio `noreply@domainnameverification.net` con un enlace para confirmar la transferencia:

- Si no responde al correo electrónico, la transferencia se cancela en la fecha especificada.
- Si desea que la transferencia se complete antes o desea cancelar la transferencia, elija el enlace del correo electrónico para ir a la página web de Route 53 y elegir la opción aplicable. Se le pedirá que proporcione el código de autorización de dominio que obtuvo en el paso 7.

Además, es posible que reciba un correo electrónico de WIXI.jp. Puede omitir este correo electrónico.

12. Si el registrador al que transfiere el dominio informa de que ha habido un error en la transferencia, póngase en contacto con él para obtener más información. Cuando transfiere un dominio a otro registrador, todas las actualizaciones de estado van al nuevo registrador, por lo que Route 53 no tiene información acerca de por qué no se ha realizado una transferencia.

Si el nuevo registrador informa de que se ha producido un error en la transferencia debido a que el código de autorización que obtuvo de Route 53 no es válido, abra un caso con AWS Support. (No es necesario un contrato de soporte y no hay cargos). Para obtener más información, consulte [Ponerse en contacto con AWS Support sobre problemas de registro de dominios](#).

 Note

Los códigos de autorización generados por Gandi son válidos durante unos 5 días. Si intenta hacer la transferencia después de este período, es posible que se produzca un error debido a que el código ha caducado.

13. Si se transfirió el servicio DNS a otro proveedor de servicios DNS, puede eliminar los registros de la zona alojada y eliminar la zona alojada después de que los solucionadores de DNS dejen de responder a las consultas de DNS con los nombres de servidores de nombres de Route 53. Esto suele tardar dos días; es decir, la cantidad de tiempo que los solucionadores de DNS tienen en caché los nombres de servidores de nombres de dominio.

 Important

Si elimina la zona alojada mientras que los solucionadores de DNS siguen respondiendo a las consultas de DNS con los nombres de servidores de nombres de Route 53, el dominio dejará de estar disponible en Internet.

Después de eliminar la zona alojada, Route 53 dejará de facturarle la tarifa mensual para una zona alojada. Para obtener más información, consulte la documentación siguiente:

- [Eliminar registros](#)
- [Eliminación de una zona alojadas pública](#)
- [Precios de Route](#)

Transferencia de un dominio a otra cuenta de AWS

Si registró un dominio con una cuenta de AWS y quiere transferir el dominio a otra cuenta de AWS, puede hacerlo usted mismo utilizando la consola nueva o AWS CLI u otros métodos programáticos.

Temas

- [Paso 1: Transferir un dominio a otra cuenta de AWS](#)
- [Paso 2 \(opcional\): migrar de una zona alojada a otra cuenta de AWS](#)

Paso 1: Transferir un dominio a otra cuenta de AWS

Los dominios no se pueden transferir durante los primeros 14 días de registro.

Cuando se inicie la transferencia del dominio, debe iniciar sesión con el usuario de la cuenta raíz o bien con un usuario al que se hayan concedido permisos de IAM de una o varias de las siguientes formas:

- Se asigna al usuario la política administrada AdministratorAccess.
- Se asigna al usuario la política administrada AmazonRoute53DomainsFullAccess.
- Se asigna al usuario la política administrada AmazonRoute53FullAccess.
- Al usuario se le asigna la política administrada PowerUserAccess.
- El usuario tiene permiso para realizar todas las acciones siguientes: TransferDomains, DisableDomainTransferLock y RetrieveDomainAuthCode.

Si no inicia sesión con el usuario de la cuenta raíz ni con un usuario que tenga los permisos necesarios, no podemos realizar la transferencia. Este requisito impide que los usuarios no autorizados transfieran dominios a otras cuentas de Cuentas de AWS.

El proceso de transferencia consta de dos pasos. En primer lugar, el propietario de la cuenta de origen inicia la transferencia: en el procedimiento [iniciar una transferencia a otra Cuenta de AWS](#) y, a continuación, el propietario de la cuenta de destino acepta la transferencia; en el procedimiento [aceptar una transferencia desde otra Cuenta de AWS](#).

Transferir un dominio a una AWS diferente

1. Debe iniciar sesión en AWS usando la Cuenta de AWS en la que está registrado actualmente el dominio.
2. Abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
3. En el panel de navegación, elija Registered domains.
4. Elija el nombre del dominio que desea transferir a otra Cuenta de AWS.
5. Sobre la sección Detalles, en el menú desplegable Transferencia saliente, seleccione Transferir a otra Cuenta de AWS.
6. En el cuadro de diálogo Transferir a otra Cuenta de AWS, escriba el ID de la cuenta de destino. Puede obtener este ID del propietario de la Cuenta de AWS de destino.
7. Elija Confirmar.

8. En el cuadro de diálogo Generar contraseña, copie la contraseña y reenvíela al propietario receptor de la Cuenta de AWS.

En la página Solicitudes, el Estado del dominio mostrará En curso y el Tipo mostrará Transferencia interna saliente.

Para aceptar una transferencia de dominio desde una cuenta de AWS diferente

1. Inicie sesión en AWS con la Cuenta de AWS que recibirá el dominio.
2. Abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
3. En el panel de navegación, elija Solicitudes.
4. En la página Solicitudes, seleccione el botón de radio que se encuentra junto al nombre de dominio que va a transferir desde otra Cuenta de AWS. Si el dominio está listo para ser transferido, el Estado es Acción requerida y el Tipo es Transferencia interna de dominio entrante.

Dispone de tres días para aceptar la solicitud. Si no se ha aceptado la transferencia en 3 días, la solicitud de transferencia se cancelará.

5. En el menú desplegable Acción, seleccione Aceptar.

También puede elegir Rechazar para cancelar el proceso de transferencia.

6. Si aceptó, en la página Transferir dominio a su cuenta, en la sección Contraseña, escriba la contraseña que recibió del propietario de la cuenta de origen.

Lea los términos y las condiciones, y elija Aceptar.

7. Vaya a la página Solicitudes para controlar el estado de la transferencia y los demás pasos que debe seguir.
8. Una vez completada la transferencia, puede actualizar la información de contacto. Para obtener más información, consulte [Actualización de la información de contacto y la propiedad de un dominio](#).

Transferencia del dominio mediante programación

De igual forma, puede transferir el dominio mediante programación, utilizando la AWS CLI, uno de los SDK de AWS o la API de Route 53. Para obtener más información, consulte la documentación siguiente:

- Para obtener información general sobre el proceso de transferencia y la documentación acerca de las acciones de la API que utiliza a fin de transferir un dominio mediante la API de registro de dominio de Route 53, consulte [TransferDomainToAnotherAwsAccount](#) en la Referencia de la API de Amazon Route 53.
- Para obtener documentación sobre otras opciones a fin de transferir dominios mediante programación, consulte “SDK y conjuntos de herramientas” en la sección [Guías y referencias de la API](#) de la página “Documentación de AWS”.
- La cuenta receptora dispone de tres días para aceptar la transferencia de la cuenta de origen mediante la API [transfer-domain-to-another-aws-account](#). Si no se ha aceptado la transferencia en 3 días, la solicitud de transferencia se cancelará.

 Important

Cuando transfiere un dominio a una cuenta de AWS diferente, la zona alojada para el dominio no se transfiere. Si también quiere transferir la zona alojada, espere hasta que el dominio se haya transferido y luego consulte [Paso 2 \(opcional\): migrar de una zona alojada a otra cuenta de AWS](#).

Paso 2 (opcional): migrar de una zona alojada a otra cuenta de AWS

Si utiliza Route 53 como servicio DNS para el dominio, no transferirá la zona alojada al transferir un dominio a otra cuenta de AWS. Si el registro del dominio está asociado a una cuenta y la zona alojada correspondiente está asociada a otra cuenta, ni el registro del dominio ni la funcionalidad de DNS resultan afectados. El único efecto es que tendrá que iniciar sesión en la consola de Route 53 con una cuenta para ver el dominio e iniciar sesión con la otra cuenta a fin de ver la zona alojada.

Si es el propietario de la cuenta desde la que se transfiere el dominio y de la cuenta a la que transfiere el dominio, tiene la opción de migrar la zona alojada del dominio a otra cuenta, pero esto no es necesario. Route 53 seguirá utilizando los registros de la zona alojada existente para dirigir el tráfico del dominio.

 Important

Si no es el propietario de la cuenta desde la que transfiere el dominio ni de la cuenta a la que lo transfiere, debe migrar la zona alojada existente a la cuenta de AWS a la que transfiere el dominio o crear una zona alojada en una cuenta de AWS de su propiedad. Si no es el

propietario de la cuenta que ha creado la zona alojada que redirige el tráfico del dominio, no puede controlar la forma en que se dirige el tráfico.

Para migrar la zona alojada existente a la nueva cuenta, consulte [Migración de una zona alojada a otra cuenta de AWS](#).

Para crear una nueva zona alojada, consulte [Establecer Amazon Route 53 como servicio DNS de un dominio existente](#). Este tema se utiliza normalmente cuando se transfieren dominios de otro registrador a Route 53, pero el proceso es el mismo cuando se transfieren dominios de una cuenta de AWS a otra.

Important

Servidores de nombres de etiqueta blanca: si su dominio utiliza servidores de nombres de etiqueta blanca (nombres de host del servidor de nombres personalizados como ns1.example.com), es necesario seguir pasos adicionales:

- Al transferir el registro de un dominio: actualice los registros de adherencia con su nuevo registrador una vez finalizada la transferencia.
- Al migrar zonas alojadas: actualice los registros de adherencia con su registrador de dominios después de la migración de la zona, ya que las direcciones IP cambian aunque los nombres de host sigan siendo los mismos.

Para obtener instrucciones detalladas, consulte [the section called “Paso 7: Crear registros de adherencia y cambiar los servidores de nombres del registrador”](#).

Ver el estado de una transferencia de dominio

Después de iniciar la transferencia de un dominio desde otro registrador de dominios a Amazon Route 53, puede realizar un seguimiento del estado en la página Solicitudes (consola nueva) o en la página Solicitudes pendientes (consola anterior) de la consola de Route 53. La columna Status incluye una breve descripción del paso actual. La siguiente lista incluye el texto de la consola y una descripción más detallada de cada paso.

 Note

Cuando envía una solicitud de transferencia, el estado inicial es Domain transfer request submitted, que indica que hemos recibido su solicitud.

Determinando si el dominio cumple los requisitos de transferencia (paso 1 de 14)

Estamos confirmando si el estado de su dominio es apto para la transferencia. Debe desbloquear el dominio y el dominio no puede tener ninguno de los siguientes códigos de estado cuando envíe la solicitud de transferencia:

- clientTransferProhibited
- pendingDelete
- pendingTransfer
- redemptionPeriod

Solo TLD geográficos: comprobar la información de WHOIS (paso 2 de 14)

Si va a transferir un dominio que tiene un [TLD geográfico](#), hemos enviado una consulta de WHOIS para su dominio con el fin de determinar si ha deshabilitado la protección de privacidad del dominio. Si la protección de privacidad sigue estando habilitada con el registrador actual, no podremos tener acceso a la información que necesitamos para transferir el dominio.

 Note

No se requiere autorización para los dominios que tienen un [TLD genérico](#), como .com, .net u .org.

Solo TLD geográficos: correo electrónico enviado al contacto del titular para obtener la autorización de la transferencia (paso 3 de 14)

Si va a transferir un dominio que tiene un [TLD geográfico](#), hemos enviado un correo electrónico al contacto del titular del dominio. El objetivo del correo electrónico se confirmar que un contacto autorizado del dominio solicitó la transferencia.

 Note

No se requiere autorización para los dominios que tienen un [TLD genérico](#), como .com, .net u .org.

Verificando la transferencia con el registrador actual (paso 4 de 14)

Hemos enviado una solicitud al registrador actual del dominio para iniciar la transferencia.

Solo TLD geográficos: esperando autorización del contacto del titular (paso 5 de 14)

Hemos enviado un correo electrónico al contacto del registrante del dominio (véase el paso 3 de 14) y estamos esperando a que el contacto del registrante haga clic en un enlace del correo electrónico para autorizar la transferencia. Si va a transferir un dominio que tiene un [TLD geográfico](#) y no ha recibido el correo electrónico por algún motivo, consulte [Reenvío de los emails de autorización y confirmación](#).

Se ha contactado con el registrador actual para solicitar la transferencia (paso 6 de 14)

Estamos trabajando con el registrador actual del dominio para finalizar la transferencia.

Esperando a que el registrador actual complete la transferencia (paso 7 de 14)

Su registrador actual está confirmando que el dominio cumple los requisitos para que se pueda transferir. Este paso podría tardar hasta diez días, en función del dominio de nivel superior de su dominio:

- [Dominios de nivel superior genéricos](#): tardan hasta siete días.
- [Dominios geográficos de nivel superior](#) (denominados también dominios de nivel superior de código de país): tardan hasta diez días.

 Note

Si ha aprobado el email de confirmación enviado por Route 53 al transferir un dominio .JP, pero se ha detenido durante varios días en el PASO 7, póngase en contacto con el [Centro de soporte de AWS](#) para obtener ayuda.

Para la mayoría de registradores, el proceso está completamente automatizado y no se puede acelerar. Algunos registradores le envían un correo electrónico que le solicita que apruebe la transferencia; si el registrador envía este correo electrónico de confirmación, el proceso de transferencia puede ser mucho más rápido que de siete a diez días.

Para obtener información sobre los motivos que un registrador podría tener para rechazar la transferencia, consulte [Requisitos de transferencia de dominios de nivel superior](#).

Confirmando con el contacto del registrante que el contacto inició la transferencia (paso 8 de 14)

Algunos registradores de TLD envían al contacto del registrante otro correo electrónico para confirmar que un usuario autorizado solicitó la transferencia del dominio.

Sincronizando los servidores de nombres con la empresa de registro (paso 9 de 14)

Este paso se produce únicamente si los servidores de nombres que proporcionó como parte de la solicitud de transferencia son diferentes de los servidores de nombres que figuran en el registrador actual. Intentaremos actualizar los servidores de nombres a los nuevos servidores de nombres que ha proporcionado.

Sincronizando la configuración con la empresa de registro (paso 10 de 14)

Estamos comprobando que la transferencia se ha completado correctamente y estamos sincronizando los datos relacionados con su dominio con nuestro registrador asociado.

Enviando información de contacto actualizada a la empresa de registro (paso 11 de 14)

Si modificó la propiedad del dominio cuando solicitó la transferencia, estamos intentando realizar este cambio. Sin embargo, la mayoría de los registradores no permiten una transferencia de propiedad como parte del proceso de transferencia del dominio.

Finalizando la transferencia a Route 53 (paso 12 de 14)

Estamos confirmando que el proceso de transferencia se ha realizado correctamente.

Finalizando la transferencia (paso 13 de 14)

Estamos configurando su dominio en Route 53.

Transferencia completa (paso 14 de 14)

Su transferencia se ha realizado correctamente.

Cómo la transferencia de un dominio a Amazon Route 53 afecta a la fecha de vencimiento del registro del dominio

Cuando transfiere un dominio entre registradores, algunos registradores de TLD le permiten mantener la misma fecha de vencimiento para su dominio, algunos registradores añaden un año a la fecha de vencimiento y algunos registradores cambian la fecha de vencimiento a un año después de la fecha de transferencia.

Note

Para la mayoría de los TLD, puede ampliar el período de registro de un dominio hasta diez años después de transferirlo a Amazon Route 53. Para obtener más información, consulte [Ampliación del periodo de registro de un dominio](#).

TLD genéricos

Cuando transfiere un dominio que tiene un TLD genérico (por ejemplo, .com) a Route 53, la nueva fecha de vencimiento del dominio es la fecha de vencimiento con el registrador anterior más un año.

TLD geográficos

Cuando transfiere un dominio que tiene un TLD geográfico (por ejemplo, .co.uk) a Route 53, la nueva fecha de vencimiento del dominio depende del TLD. Encuentre su TLD en la siguiente tabla para determinar cómo la transferencia de su dominio afecta a la fecha de vencimiento.

Continente	TLD geográficos y el efecto de transferir un dominio en la fecha de vencimiento
África	.co.za: la fecha de vencimiento no cambia.
América	.cl, .com.ar, .com.br: la fecha de vencimiento no cambia. .ca, .co, .mx, .us: se agrega un año a la antigua fecha de vencimiento.
Asia/Oceanía	.com.au, .com.sg, .jp, .net.au, .sg: la fecha de vencimiento no cambia. .co.nz, .in, .net.nz, .org.nz: se agrega un año a la antigua fecha de vencimiento.
Europa	.ch, .co.uk, .es, .fi, .me.uk, .org.uk, .se: la fecha de vencimiento no cambia. .berlin, .eu, .io, .me, .ruhr, .wien: se agrega un año a la antigua fecha de vencimiento.

Continente	TLD geográficos y el efecto de transferir un dominio en la fecha de vencimiento
	.be, .de, .fr, .it, .nl: la nueva fecha de vencimiento se fija un año después de la fecha de transferencia.

Reenvío de los emails de autorización y confirmación

En varias operaciones relacionadas con el registro de dominio, ICANN requiere que obtengamos la autorización del contacto del registrante del dominio o la confirmación de que la dirección de email del contacto del registrante es válida. Para obtener la autorización o la confirmación, le enviamos un email que contiene un enlace. Tiene entre 3 y 15 días para hacer clic en el enlace, según la operación y el dominio de nivel superior. Transcurrido ese tiempo, el enlace deja de funcionar.

Si no hace clic en el enlace del email en el tiempo asignado, ICANN suele requerir que suspendamos el dominio o cancelemos la operación, en función de lo que intentaba hacer:

Registrar un dominio

Suspendemos el dominio, por lo que no está accesible en Internet. Para volver a enviar el email de confirmación, consulte [Para reenviar el email de confirmación para un registro de dominio](#).

Solo TLD geográficos: Transferir un dominio a Amazon Route 53

Si va a transferir un dominio que tiene un [TLD geográfico](#), cancelamos la transferencia. Para volver a enviar el email de autorización, consulte [Para reenviar el email de autorización para una transferencia de dominio](#).

Note

No se requiere autorización para los dominios que tienen un [TLD genérico](#), como .com, .net u .org.

Cambiar el nombre o la dirección de email del contacto del registrante para el dominio (el propietario)

Cancelamos el cambio. Para volver a enviar el email de autorización, consulte [Para reenviar el email de autorización para actualizar el contacto del registrante o eliminar un dominio](#).

Eliminar un dominio

Cancelamos la solicitud de eliminación. Para volver a enviar el email de autorización, consulte [Para reenviar el email de autorización para actualizar el contacto del registrante o eliminar un dominio](#).

Solo TLD geográficos: Transferir un dominio de Route 53 a otro registrador

Si va a transferir un dominio que tiene un [TLD geográfico](#), el nuevo registrador cancela la transferencia.

Note

No se requiere autorización para los dominios que tienen un [TLD genérico](#), como .com, .net u .org.

Temas

- [Actualización de la dirección de email](#)
- [Reenvío de emails](#)

Actualización de la dirección de email

Siempre enviamos emails de confirmación y autorización a la dirección de email del contacto del registrante de un dominio. Para algunos TLD, debemos enviar un email a las direcciones de email antigua y nueva al contacto del registrante en los casos siguientes:

- Cambio de la dirección de correo electrónico de un dominio que ya está registrado con Amazon Route 53
- Cambio de la dirección de correo electrónico de un dominio que se está transfiriendo a Route 53

Reenvío de emails

Utilice el procedimiento aplicable para reenviar los emails de autorización o confirmación.

- [Para reenviar el email de confirmación para un registro de dominio](#)
- [Para reenviar el email de autorización para una transferencia de dominio](#)

- [Para reenviar el email de autorización para actualizar el contacto del registrante o eliminar un dominio](#)

Para reenviar el email de confirmación para un registro de dominio

1. Compruebe la dirección de email del contacto del registrante y, si es necesario, actualícela. Para obtener más información, consulte [Actualización de la información de contacto y la propiedad de un dominio](#).
2. Busque en la carpeta de spam de su aplicación de email un mensaje de una de las siguientes direcciones.

Si ha transcurrido demasiado tiempo, el enlace ya no funcionará, pero sabrá dónde buscar el email de confirmación cuando le enviemos otro.

TLD	Dirección de email de la que procede el email de aprobación o confirmación
.fr	nic@nic.fr
Todos los demás	Una de las siguientes direcciones de email: • noreply@registrar.amazon • noreply@domainnameverification.net

 Note

Los correos electrónicos pueden contener un enlace a www.verify-whois.com. Es seguro utilizar este enlace.

3. Utilice la consola de Amazon Route 53 para reenviar el correo electrónico de confirmación:
 - a. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.

- b. En el panel de navegación, elija Registered domains.
- c. Elija el nombre del dominio cuyo email desea reenviar.
- d. En el cuadro de advertencia con el título "Your domain might be suspended", elija Send email again.

 Note

Si no hay ningún cuadro de advertencia, significa que ya ha confirmado que la dirección de email del contacto del registrante es válida.

4. Si surge algún problema al volver a enviar el correo electrónico de confirmación, puede ponerse en contacto con AWS Support de forma gratuita. Para obtener más información, consulte [Ponerse en contacto con AWS Support sobre problemas de registro de dominios](#).

Para reenviar el email de autorización para una transferencia de dominio

Este método no funciona para solicitudes de transferencia de salida de dominio.jp.

1. Utilice el método proporcionado por el registrador de dominio actual para confirmar que la protección de privacidad del dominio está deshabilitada. Si no lo está, deshabilítela.

Enviamos el email de autorización a la dirección de email que el registrador actual ha guardado en la base de datos WHOIS. Si la protección de la privacidad está habilitada, la dirección de email normalmente está oculta. El registrador actual no podría reenviar a su dirección de correo electrónico real el correo electrónico que Amazon Route 53 envía a la dirección de correo electrónico de la base de datos WHOIS.

 Note

Si el titular actual del dominio no le permite desactivar la protección de privacidad, podemos transferir el dominio si hubiera especificado un código de autorización válido en [Paso 5: Solicitar la transferencia](#).

2. Compruebe la dirección de email del contacto del registrante y, si es necesario, actualícela. Utilice el método proporcionado por el registrador actual para el dominio.
3. Busque en la carpeta de spam de su aplicación de email un mensaje de una de las siguientes direcciones.

Si ha transcurrido demasiado tiempo, el enlace ya no funcionará, pero sabrá dónde buscar el email de autorización cuando le enviemos otro.

TLD	Dirección de email de la que procede el email de aprobación o confirmación
.com.au y .net.au	no-reply@ispapi.net El email contiene un enlace a https://approve.domainadmin.com .
.fr	nic@nic.fr
Todos los demás	Una de las siguientes direcciones de email: • noreply@registrar.amazon • noreply@domainnameverification.net

 Note

Los correos electrónicos pueden contener un enlace a www.verify-whois.com. Es seguro utilizar este enlace.

4. Si la transferencia ya no está en proceso (si ya la hemos cancelado porque ha pasado demasiado tiempo), vuelva a solicitar la transferencia y le enviaremos otro email de autorización.

 Note

Durante los primeros 15 días después de solicitar una transferencia, puede determinar su estado consultando la tabla Notifications (Notificaciones) de la página Dashboard (Panel) en la consola de Route 53. Después de 15 días, utilice la AWS CLI para obtener

el estado. Para obtener más información, consulte [route53domains](#) en la Referencia de comandos de la AWS CLI.

Si la transferencia continúa en curso, siga estos pasos para reenviar el email de autorización.

- a. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
 - b. En la tabla Notifications (Notificaciones), busque el dominio que desea transferir.
 - c. En la columna Status (Estado) de dicho dominio, seleccione Resend email (Volver a enviar el email).
5. Si surge algún problema al volver a enviar el correo electrónico de autorización para una transferencia de dominio, puede ponerse en contacto con AWS Support de forma gratuita. Para obtener más información, consulte [Ponerse en contacto con AWS Support sobre problemas de registro de dominios](#).

Para reenviar el email de autorización para actualizar el contacto del registrante o eliminar un dominio

1. Compruebe la dirección de email del contacto del registrante y, si es necesario, actualícela. Para obtener más información, consulte [Actualización de la información de contacto y la propiedad de un dominio](#).
2. Busque en la carpeta de spam de su aplicación de email un mensaje de una de las siguientes direcciones.

Si ha transcurrido demasiado tiempo, el enlace ya no funcionará, pero sabrá dónde buscar el email de autorización cuando le enviemos otro.

TLD	Dirección de email de donde procede el email de autorización
.fr	nic@nic.fr
Todos los demás	Una de las siguientes direcciones de email: • noreply@registrar.amazon

TLD	Dirección de email de donde procede el email de autorización
	noreply@domainnameverification.net

 Note

Los correos electrónicos pueden contener un enlace a www.verify-whois.com. Es seguro utilizar este enlace.

3. Cancele el cambio o la eliminación. Dispone de dos opciones para hacerlo:

- Puede dejar que transcurra el periodo de espera de 3 a 15 días, tras el cual se cancelará automáticamente la operación solicitada.
- También puede ponerse en contacto con AWS Support y solicitar la cancelación de la operación.

 Important

Tipos de transferencia y métodos de cancelación: el método de cancelación depende del tipo de transferencia:

- Del registrador externo a Route 53: siga los procedimientos de este tema (espere a que se cancele automáticamente o póngase en contacto con AWS Support).
- Entre cuentas de AWS: utilice la API `CancelDomainTransferToAnotherAwsAccount` o póngase en contacto con AWS Support.

No se ponga en contacto con su registrador externo actual para cancelar una transferencia a Route 53, ya que ellos no pueden cancelar transferencias que ya estén en curso en AWS.

4. Después de que se cancele el cambio o la eliminación, puede modificar la información de contacto o eliminar el dominio de nuevo, y le enviaremos otro email de autorización.

5. Si surge algún problema al volver a enviar el correo electrónico de autorización, puede ponerse en contacto con AWS Support de forma gratuita. Para obtener más información, consulte [Ponerse en contacto con AWS Support sobre problemas de registro de dominios](#).

Configurar DNSSEC para un dominio

Los atacantes a veces llevan el tráfico a puntos de conexión de Internet como servidores web interceptando las consultas DNS y devolviendo sus propias direcciones IP a los servicios de resolución de nombres DNS en lugar de a las direcciones IP reales de esos puntos de conexión. Los usuarios son redirigidos a las direcciones IP proporcionadas por los atacantes en la respuesta fraudulenta como, por ejemplo, sitios web falsos.

Puede proteger su dominio de este tipo de ataque, conocido como suplantación de DNS o ataque "man-in-the-middle", configurando DNSSEC (Extensiones de seguridad del sistema de nombres de dominio), un protocolo para proteger el tráfico DNS.

Important

Amazon Route 53 admite DNSSEC para el registro de dominios y la firma de DNSSEC. Si desea configurar la firma de DNSSEC para un dominio que esté registrado con Route 53, consulte [Configuración de la firma de DNSSEC en Amazon Route 53](#).

Temas

- [Información general acerca de cómo DNSSEC protege su dominio](#)
- [Requisitos previos y valores máximos para configurar DNSSEC para un dominio](#)
- [Añadir claves públicas para un dominio](#)
- [Eliminar claves públicas de un dominio](#)

Información general acerca de cómo DNSSEC protege su dominio

Cuando configura DNSSEC para su dominio, un servicio de resolución de nombres DNS establece una cadena de confianza para las respuestas de los servicios de resolución intermedios. La cadena de confianza comienza con la empresa de registro del TLD del dominio (la zona principal del dominio) y termina con los servidores de nombres autorizados en su proveedor del servicio DNS.

No todos los solucionadores de DNS admiten DNSSEC. Solo los Resolver que admiten DNSSEC realizan cualquier validación de firma o de autenticidad.

Esta es la manera de configurar DNSSEC para los dominios registrados con Amazon Route 53 a fin de proteger sus hosts de Internet de la suplantación de DNS, en un formato simplificado:

1. Utilice el método proporcionado por el proveedor del servicio DNS para firmar los registros de su zona alojada con la clave privada de un par de claves asimétricas.

 Important

Route 53 admite DNSSEC para el registro de dominios y la firma de DNSSEC. Para obtener más información, consulte [Configuración de la firma de DNSSEC en Amazon Route 53](#).

2. Proporcione la clave pública del par de claves a su registrador del dominio y especifique el algoritmo que se utilizó para generar el par de claves. El registrador del dominio reenvía la clave pública y el algoritmo a la empresa de registro del dominio de nivel superior (TLD).

Para obtener información sobre cómo realizar este paso para dominios que haya registrado con Route 53, consulte [Añadir claves públicas para un dominio](#).

Después de configurar DNSSEC, así es cómo debe proteger su dominio de la suplantación de DNS:

1. Envíe una consulta DNS, por ejemplo, navegando a un sitio web o enviando un mensaje de correo electrónico.
2. La solicitud se redirige a una servicio de resolución de nombres DNS. Los servicios de resolución de nombres son responsables de devolver el valor adecuado a los clientes en función de la solicitud, por ejemplo, la dirección IP del host que ejecuta un servidor web o un servidor de correo electrónico.
3. Si la dirección IP está almacenada en la caché del servicio de resolución de nombres DNS porque alguien ya ha enviado la misma consulta de DNS y el servicio ya ha obtenido el valor, el servicio de resolución devuelve la dirección IP al cliente que presentó la solicitud. El cliente utiliza entonces la dirección IP para tener acceso al host.

Si la dirección IP no está almacenada en la caché del servicio de resolución de nombres DNS, el servicio envía una solicitud a la zona principal de su dominio, en la empresa de registro del TLD, que proporciona dos valores:

- El registro DS (Delegation Signer), que es una clave pública que se corresponde con la clave privada que se usó para firmar el registro.
 - Las direcciones IP de los servidores de nombres autorizados de su dominio.
4. El servicio de resolución de nombres DNS envía la solicitud original a otro servicio DNS. Si ese servicio no tiene la dirección IP, repite el proceso hasta que un servicio de resolución de nombres envíe la solicitud a un servidor de nombres de su proveedor del servicio DNS. El servidor de nombres devuelve dos valores:
- El registro del dominio, como example.com. Normalmente este conjunto contiene la dirección IP de un host.
 - La firma del registro, que creó al configurar DNSSEC.
5. El solucionador de DNS utiliza la clave pública que proporcionó al registrador de dominio, y que el registrador reenvió a la empresa de registro del TLD para realizar lo siguiente:
- Establecer una cadena de confianza.
 - Verificar que la respuesta firmada del proveedor del servicio DNS es legítima y no se ha reemplazado por una respuesta falsa de un atacante.
6. Si la respuesta es auténtica, el servicio de resolución de nombres devuelve el valor al cliente que presentó la solicitud.

Si la respuesta no se puede verificar, el servicio de resolución de nombres devuelve un error al usuario.

Si la empresa de registro del TLD del dominio no tiene la clave pública del dominio, el servicio de resolución de nombres responde a la consulta DNS con la respuesta que obtuvo del proveedor del servicio DNS.

Requisitos previos y valores máximos para configurar DNSSEC para un dominio

Para configurar DNSSEC para un dominio, el dominio y el proveedor del servicio DNS deben cumplir los siguientes requisitos previos:

- La empresa de registro del TLD debe admitir DNSSEC. Para determinar si la empresa de registro de su TLD admite DNSSEC, consulte [Dominios que puede registrar con Amazon Route 53](#).
- El proveedor del servicio DNS del dominio debe admitir DNSSEC.

 Important

Route 53 admite DNSSEC para el registro de dominios y la firma de DNSSEC. Para obtener más información, consulte [Configuración de la firma de DNSSEC en Amazon Route 53](#).

- Debe configurar DNSSEC con el proveedor del servicio DNS de su dominio antes de agregar las claves públicas del dominio a Route 53.
- El número de claves públicas que se pueden añadir a un dominio depende del TLD del dominio:
 - Dominios .com y .net: hasta 13 claves
 - Todos los demás dominios: hasta cuatro claves

Añadir claves públicas para un dominio

Cuando rota las claves o habilita DNSSEC para un dominio, realiza el siguiente procedimiento después de configurar DNSSEC con el proveedor del servicio DNS del dominio.

Para añadir claves públicas para un dominio

1. Si aún no ha configurado DNSSEC con su proveedor del servicio DNS, utilice el método proporcionado por su proveedor del servicio para configurar DNSSEC.
2. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
3. En el panel de navegación, elija Registered domains.
4. Elija el nombre del dominio para el que desea añadir claves.
5. En la pestaña Claves de DNSSEC, elija Agregar clave.
6. Especifique los siguientes valores:

Tipo de clave

Elija si desea cargar una clave de firma de claves (KSK) o una clave de firma de zonas (ZSK).

Algoritmo

Elija el algoritmo que utilizó para firmar los registros de la zona alojada.

Clave pública

Especifique la clave pública del par de claves asimétricas que utilizó para configurar DNSSEC con su proveedor del servicio DNS.

Tenga en cuenta lo siguiente:

- Especifique la clave pública, no el resumen.
- Debe especificar la clave en base 64.

7. Elija Agregar.

Note

Solo puede añadir las claves públicas de una en una. Si necesita agregar más claves, espere hasta que reciba un correo electrónico de confirmación de Route 53.

8. Cuando Route 53 recibe una respuesta de la empresa de registro, enviamos un correo electrónico al contacto del registrante del dominio. El correo electrónico confirma que la clave pública se ha añadido al dominio en la empresa de registro o explica por qué no se pudo agregar la clave.

Eliminar claves públicas de un dominio

Cuando rota las claves o deshabilita DNSSEC para el dominio, elimina las claves públicas usando el siguiente procedimiento antes de deshabilitar DNSSEC con el proveedor del servicio DNS. Tenga en cuenta lo siguiente:

- Si rota las claves públicas, le recomendamos que espere hasta tres días después de añadir las nuevas claves públicas para eliminar las claves públicas antiguas.
- Si deshabilita DNSSEC, elimine primero las claves públicas del dominio. Le recomendamos que espere hasta tres días antes de deshabilitar DNSSEC con el servicio DNS del dominio.

Important

Si DNSSEC está habilitado para el dominio y deshabilita DNSSEC con el servicio DNS, los servicios de resolución de nombres DNS que admiten DNSSEC devolverán un error

SERVFAIL a los clientes y los clientes no podrán tener acceso a los puntos de conexión asociados al dominio.

Para eliminar claves públicas de un dominio

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Registered domains.
3. Elija el nombre del dominio del que desea eliminar las claves.
4. En la pestaña de Claves de DNSSEC elija el botón de radio situado junto a la clave que desea eliminar y, a continuación, elija Eliminar clave.
5. En el cuadro de diálogo Eliminar la clave de DNSSEC, escriba eliminar en el cuadro de texto para confirmar que desea eliminar la clave y, a continuación, elija Eliminar.

 Note

Solo puede eliminar las claves públicas de una en una. Si necesita eliminar más claves, espere hasta que reciba un email de confirmación de Amazon Route 53.

6. Cuando Route 53 recibe una respuesta de la empresa de registro, enviamos un correo electrónico al contacto del registrante del dominio. El correo electrónico confirma que la clave pública se ha eliminado del dominio en la empresa de registro o explica por qué no se pudo eliminar la clave.

Búsqueda del registrador y otra información del dominio

Para ver la información del dominio mediante la [GetDomainDetail](#) API, puedes usar cualquiera de las siguientes SDKs opciones AWS CLI: Para obtener más información, consulte [get-domain-detail](#).

Para ver la información de los dominios con la CLI **get-domain-detail**

- Para ello, utilice la siguiente CLI:

```
aws route53domains get-domain-detail \  
    --region us-east-1 \  
    --domain-name example.com
```

```
--domain-name example.com
```

 Note

Este comando solo se ejecuta en us-east-1 Región de AWS.

Toda la información sobre el dominio aparecerá en la salida, incluido el registrador, la fecha de registro, la configuración de privacidad, etc.

Visualización de la información sobre dominios registrados con Route 53

 Note

A partir del 28 de enero de 2025, es posible que algunos registros de dominios pasen del WHOIS al Protocolo de acceso a los datos de registro (RDAP) para las consultas de datos de los registros de dominios. Si accede a información de los registros de dominios directamente desde los registros a través de WHOIS, es posible que tenga que actualizar sus aplicaciones para utilizar los puntos de conexión del RDAP si el registro correspondiente deja de funcionar con WHOIS.

La funcionalidad del servicio de los dominios de Route 53 permanece sin cambios. Este aviso se aplica únicamente a las consultas de WHOIS de registro directas realizadas fuera de los servicios de Route 53.

Puede ver información sobre los dominios que se hayan registrado con Route 53. Esta información incluye detalles como, por ejemplo, cuándo se registró originalmente el dominio, información de contacto del propietario del dominio y los contactos técnicos, administrativos y de facturación.

WHOIS

WHOIS es un directorio gratuito y de acceso público que contiene información sobre los dominios patrocinados por los registradores y registros de dominios. Se proporciona como un servicio que acepta consultas en el puerto 43 y como un sitio web, al que se puede acceder a cada uno mediante y. IPv4 IPv6 WHOIS es una búsqueda jerárquica distribuida. Para obtener más información, consulte [Acerca de WHOIS](#).

Una solicitud de WHOIS a diferentes niveles de la jerarquía puede proporcionar información diferente:

- Una solicitud al WHOIS raíz (whois.iana.org) proporciona información sobre el registro.
- Una solicitud de registro de WHOIS proporciona información sobre el registrador y cierta información pública sobre el dominio.
- Una solicitud al registrador WHOIS proporciona toda la información pública sobre el dominio.

Como hay varios niveles de WHOIS, incluidas las búsquedas de WHOIS gestionadas por el registro de TLD y el registrador de dominios, es posible que, si se desactiva la protección de la privacidad en la consola de Route 53, solo se desactive en el WHOIS proporcionado por el registrador. Algunos registros mantienen intencionalmente servicios de protección de la privacidad o de eliminación de contenido confidencial para sus servicios de búsqueda en WHOIS, independientemente de si los has desactivado con Route 53. Para obtener información completa sobre su dominio, le recomendamos que utilice el WHOIS proporcionado por el registrador.

Tenga en cuenta lo siguiente:

El envío de correos electrónicos a los contactos del dominio cuando la protección de privacidad está habilitada

Si la protección de privacidad está habilitada para el dominio, la información de contacto del registrante y de los responsables técnicos y administrativos se sustituye por la información de contacto del servicio de privacidad de Amazon Registrar. Por ejemplo, si el dominio ejemplo.com se registró con Amazon Registrar y la protección de privacidad está habilitada, el valor de Correo electrónico del titular en la respuesta a una consulta para WHOIS será similar a propietario1234@ejemplo.com.identity-protect.org.

Para dirigirse a uno o varios de los contactos del dominio cuando la protección de privacidad está habilitada, envíe un correo electrónico a las direcciones de correo electrónico correspondientes. Reenviamos automáticamente el correo electrónico al contacto correspondiente.

Denuncia de abusos

Para denunciar cualquier actividad ilegal o infracción de la [Política de uso aceptable](#), como contenido inapropiado, suplantación de identidad, malware o spam, envía un correo electrónico a trustandsafety@support.aws.com.

Para ver información sobre los dominios registrados con Route 53

1. En un navegador web, vaya a uno de los siguientes sitios web:
 - [WHOIS de Amazon Registrar: https://registrar.amazon.com/whois](https://registrar.amazon.com/whois)
 - [Amazon Registrar RDAP: /rdap https://registrar.amazon.com](https://registrar.amazon.com/rdap)
 - WHOIS de Gandi: <https://whois.gandi.net>
2. Escriba el nombre del dominio cuya información desea ver y elija Search (Buscar).

Eliminación de un registro de nombre de dominio

En la mayoría de los dominios de nivel superior (TLDs), puede eliminar el registro si ya no lo desea. Si la empresa de registro le permite eliminar el registro, realice el procedimiento de este tema.

Tenga en cuenta lo siguiente:

La cuota de registro no es reembolsable

Si elimina un registro de nombre de dominio antes de la fecha de vencimiento programada, AWS no le reembolsará la cuota de registro.

TLDs que te permiten eliminar un registro de dominio

Para determinar si puede eliminar el registro de su dominio, consulte [Dominios que puede registrar con Amazon Route 53](#). Si la selección del TLD no incluye una subsección de "Eliminación de registro del dominio", puede eliminar el dominio. Antes de eliminar el dominio, asegúrese de haber deshabilitado el bloqueo de dominio. Para obtener más información sobre cómo deshabilitar el bloqueo de dominio, consulte [DisableDomainTransferLock](#).

¿Qué sucede si no puede eliminar un registro de dominio?

Si el registro de su dominio no le permite eliminar el registro de un nombre de dominio, debe esperar a que el dominio venza. Para garantizar que el dominio no se renueva automáticamente, desactive la renovación automática del dominio. Cuando transcurra la fecha especificada en Expires on (Caduca el), Route 53 eliminará automáticamente el registro del dominio. Para obtener información sobre cómo cambiar la configuración de renovación automática, consulte [Activación o desactivación de la renovación automática de un dominio](#).

Retraso antes de que se elimine un dominio y esté disponible para volverlo a registrar

Casi todos los registros evitan que cualquiera registre de inmediato un dominio que acabe de vencer. El retraso habitual es de entre uno y tres meses, según el TLD. Para obtener más información, consulte la sección «Plazos para renovar y restaurar dominios» de su TLD en [Dominios que puede registrar con Amazon Route 53](#).

Important

No elimines un dominio y esperes volver a registrarlo si solo quieres transferir el dominio entre AWS cuentas o transferir el dominio a otro registrador. En su lugar, consulte la documentación correspondiente:

- [Transferencia de un dominio a otra cuenta de AWS](#)
- [Transferencia de un dominio de Amazon Route 53 a otro registrador](#)

Para eliminar un registro de nombre de dominio

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/route53/>
2. En el panel de navegación, elija Registered domains.
3. Seleccione el nombre de su dominio.

Si desea eliminar un dominio .co.uk, .me.uk, .org.uk o .uk, consulte [Cómo eliminar los registros de nombres de dominio .co.uk, .me.uk, .org.uk y .uk](#).

4. Si la empresa de registro de su TLD permite eliminar un registro de nombre de dominio, seleccione Delete Domain.

Algunos dominios requieren que enviemos un correo electrónico al titular del dominio para comprobar que desea eliminar el dominio. Si recibe un correo electrónico, será de una de las siguientes direcciones de correo electrónico:

- noreply@registrar.amazon: si TLDs está registrado por Amazon Registrar.
- noreply@domainnameverification.net: para ser TLDs registrado por nuestro registrador asociado, Gandi.

Para determinar quién es el registrador de su TLD, consulte [Dominios que puede registrar con Amazon Route 53](#).

5. Si recibe el correo electrónico de verificación, seleccione el enlace del correo y apruebe o rechace la solicitud para eliminar el dominio.

 Important

El contacto del registrador debe seguir las instrucciones del correo electrónico o tendremos que cancelar la solicitud de eliminación un día después, tal como lo exige la ICANN.

Recibirá otro correo electrónico cuando su dominio se haya eliminado. Para determinar el estado actual de su solicitud, consulte [Visualización del estado de registro de un dominio](#).

6. Elimine los registros de la zona alojada del dominio eliminado y, a continuación, elimine la zona alojada. Después de eliminar la zona alojada, Route 53 dejará de facturarle la tarifa mensual para una zona alojada. Para obtener más información, consulte la siguiente documentación sobre :
 - [Eliminar registros](#)
 - [Eliminación de una zona alojadas pública](#)
 - [Precios de Route 53](#)
7. Si tienes problemas al eliminar el registro de un nombre de dominio, puedes ponerte en contacto con AWS Support de forma gratuita. Para obtener más información, consulte [Ponerse en contacto con AWS Support sobre problemas de registro de dominios](#).

Cómo eliminar los registros de nombres de dominio .co.uk, .me.uk, .org.uk y .uk

Si desea eliminar un dominio .co.uk, .me.uk, .org.uk o .uk, cree una cuenta con Nominet, el registro de dominios .uk. Para obtener más información, consulte «Cancelación del nombre de dominio» en el sitio web de Nominet, <https://www.nominet.uk/domain-support/>.

 Important

Si elimina (cancela) un nombre de dominio .uk, se eliminará en unos días y estará disponible para que cualquier persona lo registre. Si solo desea transferir el dominio, no lo elimine.

A continuación se ofrece información general sobre el proceso:

1. En el sitio web de Nominet, siga las instrucciones para iniciar sesión por primera vez. Consulte <https://secure.nominet.org.uk/auth/login.html>. Nominet le enviará un correo electrónico con instrucciones para crear una contraseña.
2. Siga las instrucciones del correo electrónico que reciba de Nominet.
3. Inicie sesión en el sitio web de Nominet y siga las instrucciones para cancelar (eliminar) un nombre de dominio.

Ponerse en contacto con AWS Support sobre problemas de registro de dominios

AWS ofrece un plan de soporte básico, gratuito, para todos los AWS clientes. El plan incluye asistencia para los siguientes problemas relacionados con el registro del dominio:

- Transferencia de dominios a Amazon Route 53 o desde este
- Transferencia de dominios entre AWS cuentas
- Incremento de las cuotas de las entidades de Route 53, tales como el número de dominios que puede registrar (consulte [Cuotas](#))
- Cambio del propietario de un dominio
- Cambio de la información de contacto del propietario de un dominio
- Reenvío de correos electrónicos de confirmación y autorización
- Renovación de dominios
- Restauración de dominios caducado
- Obtención de información de facturación de Route 53
- Aportación de pruebas de identidad para dominios .uk
- Eliminar dominios o deshabilitar la renovación automática después de cerrar la cuenta AWS

Para ponerse en contacto con AWS Support sobre estos y otros problemas relacionados con el registro de dominios, realice el procedimiento correspondiente.

Temas

- [Ponerse en contacto con AWS Support cuando puedas iniciar sesión en tu AWS cuenta](#)
- [Ponerse en contacto con AWS Support cuando no puedes iniciar sesión en tu AWS cuenta](#)

Ponerse en contacto con AWS Support cuando puedas iniciar sesión en tu AWS cuenta

Para ponerte en contacto con AWS Support cuando puedas iniciar sesión en tu AWS cuenta, realiza el siguiente procedimiento:

1. Con la AWS cuenta en la que está registrado el dominio actualmente, inicie sesión en [AWS Support](#).

Important

Debe iniciar sesión con la cuenta raíz en la que está registrado actualmente el dominio. Este requisito impide que los usuarios no autorizados se apropien de su cuenta.

2. Elija Cuenta y facturación.
3. Especifique los siguientes valores:

Regarding

Acepte el valor predeterminado de Account and Billing Support.

Servicio

Acepte el valor predeterminado de Domains.

Categoría

Acepte el valor predeterminado de Registration Issue.

Gravedad

Elija la gravedad que corresponda.

Asunto

Escriba un breve resumen del problema.

Description (Descripción)

Describa el problema que tenga con más detalle y adjunte los documentos o capturas de pantalla pertinentes.

Método de contacto

Elija el método de contacto, Web. Nos pondremos en contacto contigo mediante la dirección de correo electrónico asociada a tu AWS cuenta.

4. Elija Enviar.

Ponerte en contacto con AWS Support cuando no puedes iniciar sesión en tu AWS cuenta

Para ponerte en contacto con AWS Support cuando no puedas iniciar sesión en tu AWS cuenta, realiza el siguiente procedimiento:

1. Ve a la página [Soy AWS cliente y estoy buscando asistencia sobre facturación o cuentas](#).
2. Rellene el formulario.
3. Elija Enviar.

Descargar un informe de facturación de dominios

Si administra varios dominios y desea ver los cargos por dominio durante un periodo de tiempo determinado, puede descargar un informe de facturación de dominios. Este informe incluye todos los cargos que se aplican al registro de dominio, incluidos los siguientes:

- Registrar un dominio
- Renovar el registro de un dominio
- Transferencia de un dominio a Amazon Route 53
- Cambiar el propietario de un dominio (para algunos TLDs, esta operación es gratuita)

A veces, el informe de facturación puede mostrar períodos de facturación a futuro. Esto ocurre porque el proceso de renovación automática del dominio comienza un mes antes de que este caduque. Por lo tanto, y esto es un ejemplo, en tu informe de agosto, es posible que veas un período de facturación que comienza en septiembre siguiente y termina en septiembre del año siguiente.

Al ejecutar el informe mediante la consola, puede elegir las opciones siguientes:

- Last 12 months (12 últimos meses): el informe incluye los cargos desde un año antes de que ejecutara el informe hasta el día actual. Por ejemplo, si ejecuta el informe el 3 de junio, incluye cargos desde el 3 de junio del año anterior hasta el día actual.
- Individual months in the last year (Meses individuales del último año): el informe incluye los cargos correspondientes al mes especificado.

Si ejecuta el informe mediante programación, puede obtener los cargos para cualquier intervalo de fechas, a partir del 31 de julio de 2014. Dicha fecha fue la fecha en que Route 53 comenzó a admitir el registro de dominios. Por ejemplo, consulte [view-billing](#) en la Referencia de los comandos de AWS CLI .

El informe de facturación está en formato CSV y la [ViewBilling](#) API describe su contenido.

Para descargar un informe de facturación de dominios

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Registered Domains.
3. Elija Domain billing report.
4. Elija el intervalo de fechas del informe y, a continuación, seleccione Download domain report.
5. Siga las instrucciones para abrir el informe o para guardarlo.
6. Si tienes problemas al descargar el informe de facturación de un dominio, puedes ponerte en contacto con AWS Support de forma gratuita. Para obtener más información, consulte [Ponerse en contacto con AWS Support sobre problemas de registro de dominios](#).

Dominios que puede registrar con Amazon Route 53

Important

Las siguientes restricciones de dominio de nivel superior se aplican únicamente al registro de dominios. Puede usar el servicio DNS de Route 53 con cualquier dominio de nivel superior que elija y con cualquier registrador de dominios. La información de esta página se refiere únicamente a los dominios que se pueden registrar en Route 53. Para obtener más información acerca de Route 53 como servicio DNS, consulte [se dirige el tráfico de Internet a su sitio web o aplicación web](#).

Las siguientes listas de dominios de nivel superior genéricos y geográficos muestran los dominios de nivel superior (TLDs) que puede usar para registrar dominios en Amazon Route 53.

Registro de dominios con Route 53

Los registradores de TLD han asignado precios especiales o Premium a algunos nombres de dominio. No se puede utilizar Route 53 para registrar dominios con precio especial o premium. Los TLDs que puede registrar en Route 53 se incluyen en las siguientes listas. Si el TLD no está incluido, no puede registrar el dominio con Route 53.

Transferencia de dominios a Route 53

Puede transferir un dominio a Route 53 si el TLD está incluido en la siguiente lista. Si el TLD no está incluido, no puede transferir el dominio a Route 53.

En la mayoría de los casos TLDs, necesita obtener un código de autorización del registrador actual para transferir un dominio. Para determinar si necesita un código de autorización, consulte la sección “Código de autorización necesario para transferencias” para su TLD.

Precios del registro y las transferencias de dominios

Para obtener información acerca del coste del registro de dominios o su transferencia a Route 53, consulte [Precios de Amazon Route 53 para el registro de dominios](#).

Uso de Route 53 como servicio DNS

Puede utilizar Route 53 como el servicio DNS para cualquier dominio, incluso si el TLD del dominio no está incluido en la siguiente lista. Para obtener más información acerca de Route 53 como servicio DNS, consulte [se dirige el tráfico de Internet a su sitio web o aplicación web](#). Para

obtener información sobre cómo transferir el servicio DNS de un dominio a Route 53, consulte [Establecer Amazon Route 53 como servicio DNS de un dominio existente](#).

Nombres de dominio internacionalizados

No todos TLDs admiten nombres de dominio internacionalizados (IDNs), es decir, nombres de dominio que incluyen caracteres distintos de los caracteres ASCII a-z, 0-9 y - (guión). La lista de cada TLD indica si ese TLD es compatible. IDNs Para obtener más información acerca de los nombres de dominio internacionalizados, consulte [Formato de nombres de dominio DNS](#).

Registrar dominios geográficos con TLDs

Las normas de registro geográfico TLDs varían según el país. Algunos países no tienen restricciones, lo que significa que cualquier persona del mundo puede registrar estas extensiones, mientras que otros tienen algunas restricciones, como la residencia. La descripción de cada TLD geográfico indica cualquier restricción.

Índice de dominios de nivel superior compatibles

Temas

- [Dominios de nivel superior genéricos](#)
- [Dominios geográficos de nivel superior](#)

Dominios de nivel superior genéricos

[A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [WXYZ](#)

A

[.ac](#), [.academy](#), [.accountants](#), [.actor](#), [.adult](#), [.agency](#), [.airforce](#), [.apartments](#), [.associates](#), [.auction](#),
[.audio](#)

B

[.band](#), [.bargains](#), [.beer](#), [.bet](#), [.bid](#), [.bike](#), [.bingo](#), [.bio](#), [.biz](#), [.black](#), [.blue](#), [.boutique](#), [.builders](#),
[.business](#), [.buzz](#)

C

[.cab](#), [.cafe](#), [.camera](#), [.camp](#), [.capital](#), [.cards](#), [.care](#), [.careers](#), [.cash](#), [.casino](#), [.catering](#), [.cc](#), [.center](#),
[.ceo](#), [.chat](#), [.cheap](#), [.christmas](#), [.church](#), [.city](#), [.claims](#), [.cleaning](#), [.click](#), [.clinic](#), [.clothing](#), [.cloud](#),

[.club](#), [.coach](#), [.codes](#), [.coffee](#), [.college](#), [.com](#), [.community](#), [.company](#), [.computer](#), [.condos](#),
[.construction](#), [.consulting](#), [.contact](#), [.contractors](#), [.cool](#), [.coupons](#), [.credit](#), [.creditcard](#), [.cruises](#)

D

[.dance](#), [.dating](#), [.deals](#), [.degree](#), [.delivery](#), [.democrat](#), [.dental](#), [.design](#), [.diamonds](#), [.diet](#), [.digital](#),
[.direct](#), [.directory](#), [.discount](#), [.dog](#), [.domains](#)

E

[.education](#), [.email](#), [.energy](#), [.engineering](#), [.enterprises](#), [.equipment](#), [.estate](#), [.events](#), [.exchange](#),
[.expert](#), [.exposed](#), [.express](#)

F

[.fail](#), [.fan](#), [.farm](#), [.finance](#), [.financial](#), [.fish](#), [.fitness](#), [.flights](#), [.florist](#), [.flowers](#), [.fm](#), [.football](#), [.forsale](#),
[.foundation](#), [.fun](#), [.fund](#), [.furniture](#), [.futbol](#), [.fyi](#)

G

[.gallery](#), [.games](#), [.gift](#), [.gifts](#), [.gives](#), [.glass](#), [.global](#), [.gmbh](#), [.gold](#), [.golf](#), [.graphics](#), [.gratis](#), [.green](#),
[.gripe](#), [.group](#), [.guide](#), [.guitars](#), [.guru](#)

H

[.haus](#), [.healthcare](#), [.help](#), [.hiv](#), [.hockey](#), [.holdings](#), [.holiday](#), [.host](#), [.hosting](#), [.house](#)

I

[.im](#), [.immo](#), [.immobilien](#), [.industries](#), [.info](#), [.ink](#), [.institute](#), [.insure](#), [.international](#), [.investments](#), [.io](#),
[.irish](#)

J

[.jewelry](#), [.juegos](#)

K

[.kaufen](#), [.kim](#), [.kitchen](#), [.kiwi](#)

L

[.land](#), [.law](#), [.lease](#), [.legal](#), [.lgbt](#), [.life](#), [.lighting](#), [.limited](#), [.limo](#), [.link](#), [.live](#), [.llc](#), [.loan](#), [.loans](#), [.lol](#), [.ltd.](#)

M

[.maison](#), [.management](#), [.marketing](#), [.mba](#), [.media](#), [.memorial](#), [.mobi](#), [.moda](#), [.money](#), [.mortgage](#),
[.movie](#)

N

[.name](#), [.net](#), [.network](#), [.news](#), [.ninja](#)

O

[.onl](#), [.online](#), [.org](#)

P

[.partners](#), [.parts](#), [.photo](#), [.photography](#), [.photos](#), [.pics](#), [.pictures](#), [.pink](#), [.pizza](#), [.place](#), [.plumbing](#),
[.plus](#), [.poker](#), [.porn](#), [.press](#), [.pro](#), [.productions](#), [.properties](#), [.property](#), [.pub](#), [.pw \(Palau\)](#)

Q

[.qpon](#)

R

[.recipes](#), [.red](#), [.reise](#), [.reisen](#), [.rentals](#), [.repair](#), [.report](#), [.republican](#), [.restaurant](#), [.reviews](#), [.rip](#), [.rocks](#),
[.run](#)

S

[.sale](#), [.sarl](#), [.school](#), [.schule](#), [.services](#), [.sex](#), [.sexy](#), [.shiksha](#), [.shoes](#), [.shopping](#), [.show](#), [.singles](#),
[.site](#), [.ski](#), [.soccer](#), [.social](#), [.solar](#), [.solutions](#), [.software](#), [.space](#), [.store](#), [.stream](#), [.studio](#), [.style](#),
[.sucks](#), [.supplies](#), [.supply](#), [.support](#), [.surgery](#), [.systems](#)

T

[.tattoo](#), [.tax](#), [.taxi](#), [.team](#), [.tech](#), [.technology](#), [.tennis](#), [.theater](#), [.tienda](#), [.tips](#), [.tires](#), [.today](#), [.tools](#),
[.tours](#), [.town](#), [.toys](#), [.trade](#), [.training](#), [.tv](#)

U

[.university](#), [.uno](#)

V

[.vacations](#), [.vegas](#), [.ventures](#), [.vg](#), [.viajes](#), [.video](#), [.villas](#), [.vision](#), [.vote](#), [.voyage](#)

WXYZ

[.watch](#), [.website](#), [.wedding](#), [.wiki](#), [.wine](#), [.work](#), [.works](#), [.world](#), [.wtf](#), [.xxx](#), [.xyz](#), [.zone](#)

Dominios geográficos de nivel superior

África

[.ac](#) (Isla Ascensión), [.co.za](#) (Sudáfrica), [.sh](#) (Santa Elena)

América

[.ca](#) (Canadá), [.cl](#) (Chile), [.co](#) (Colombia), [.com.ar](#) (Argentina), [.com.br](#) (Brasil), [.com.mx](#) (México), [.mx](#) (México), [.us](#) (Estados Unidos), [.vc](#) (San Vicente y las Granadinas), [.vg](#) (Islas Vírgenes Británicas)

Asia/Oceanía

[.au](#) (Australia), [.cc](#) (Islas Cocos (Keeling)), [.co.nz](#) (Nueva Zelanda), [.com.au](#) (Australia), [.com.sg](#) (República de Singapur), [.fm](#) (Estados Federados de Micronesia), [.in](#) (India), [.jp](#) (Japón), [.io](#) (Territorio Británico del Océano Índico), [.net.au](#) (Australia), [.net.nz](#) (Nueva Zelanda), [.org.nz](#) (Nueva Zelanda), [.pw](#) (Palau), [.qa](#) (Qatar), [.ru](#) (Federación Rusa), [.sg](#) (República de Singapur)

Europa

[.be](#) (Bélgica), [.berlin](#) (ciudad de Berlín de Alemania), [.ch](#) (Suiza), [.co.uk](#) (Reino Unido), [.cz](#) (Czech Republic), [.de](#) (Alemania), [.es](#) (España), [.eu](#) (Unión Europea), [.fi](#) (Finlandia), [.fr](#) (Francia), [.gg](#) (Guernsey), [.im](#) (Isla de Man), [.it](#) (Italia), [.me](#) (Montenegro), [.me.uk](#) (Reino Unido), [.nl](#) (Países Bajos), [.org.uk](#) (Reino Unido), [.ruhr](#) (región del Ruhr, parte occidental de Alemania), [.se](#) (Suecia), [.uk](#) (Reino Unido), [.wien](#) (ciudad de Viena en Austria)

Dominios de nivel superior genéricos

Los dominios genéricos de nivel superior (gTLDs) son extensiones globales que se utilizan y reconocen en todo el mundo, como .com, .net y .org. También incluyen dominios especiales como .bike, .condos y .marketing.

[A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [WXYZ](#)

A

[.ac](#), [.academy](#), [.accountants](#), [.actor](#), [.adult](#), [.agency](#), [.airforce](#), [.apartments](#), [.associates](#), [.auction](#), [.audio](#)

B

[.band](#), [.bargains](#), [.beer](#), [.bet](#), [.bid](#), [.bike](#), [.bingo](#), [.bio](#), [.biz](#), [.black](#), [.blue](#), [.boutique](#), [.builders](#),
[.business](#), [.buzz](#)

C

[.cab](#), [.cafe](#), [.camera](#), [.camp](#), [.capital](#), [.cards](#), [.care](#), [.careers](#), [.cash](#), [.casino](#), [.catering](#), [.cc](#), [.center](#),
[.ceo](#), [.chat](#), [.cheap](#), [.church](#), [.christmas](#), [.city](#), [.claims](#), [.cleaning](#), [.click](#), [.clinic](#), [.clothing](#), [.cloud](#),
[.club](#), [.coach](#), [.codes](#), [.coffee](#), [.college](#), [.com](#), [.community](#), [.company](#), [.computer](#), [.condos](#),
[.construction](#), [.consulting](#), [.contact](#), [.contractors](#), [.cool](#), [.coupons](#), [.credit](#), [.creditcard](#), [.cruises](#)

D

[.dance](#), [.dating](#), [.deals](#), [.degree](#), [.delivery](#), [.democrat](#), [.dental](#), [.design](#), [.diamonds](#), [.diet](#), [.digital](#),
[.direct](#), [.directory](#), [.discount](#), [.dog](#), [.domains](#)

E

[.education](#), [.email](#), [.energy](#), [.engineering](#), [.enterprises](#), [.equipment](#), [.estate](#), [.events](#), [.exchange](#),
[.expert](#), [.exposed](#), [.express](#)

F

[.fail](#), [.fan](#), [.farm](#), [.finance](#), [.financial](#), [.fish](#), [.fitness](#), [.flights](#), [.florist](#), [.flowers](#), [.fm](#), [.football](#), [.forsale](#),
[.foundation](#), [.fun](#), [.fund](#), [.furniture](#), [.futbol](#), [.fyi](#)

G

[.gallery](#), [.games](#), [.gift](#), [.gifts](#), [.gives](#), [.glass](#), [.global](#), [.gmbh](#), [.gold](#), [.golf](#), [.graphics](#), [.gratis](#), [.green](#),
[.gripe](#), [.group](#), [.guide](#), [.guitars](#), [.guru](#)

H

[.haus](#), [.healthcare](#), [.help](#), [.hiv](#), [.hockey](#), [.holdings](#), [.holiday](#), [.host](#), [.hosting](#), [.house](#)

I

[.im](#), [.immo](#), [.immobilien](#), [.industries](#), [.info](#), [.ink](#), [.institute](#), [.insure](#), [.international](#), [.investments](#), [.io](#),
[.irish](#)

J

[.jewelry](#), [.juegos](#)

K

[.kaufen](#), [.kim](#), [.kitchen](#), [.kiwi](#)

L

[.land](#), [.law](#), [.lease](#), [.legal](#), [.lgbt](#), [.life](#), [.lighting](#), [.limited](#), [.limo](#), [.link](#), [.live](#), [.llc](#), [.loan](#), [.loans](#), [.lol](#), [.ltd.](#)

M

[.maison](#), [.management](#), [.marketing](#), [.mba](#), [.media](#), [.memorial](#), [.mobi](#), [.moda](#), [.money](#), [.mortgage](#), [.movie](#)

N

[.name](#), [.net](#), [.network](#), [.news](#), [.ninja](#)

O

[.onl](#), [.online](#), [.org](#)

P

[.partners](#), [.parts](#), [.photo](#), [.photography](#), [.photos](#), [.pics](#), [.pictures](#), [.pink](#), [.pizza](#), [.place](#), [.plumbing](#), [.plus](#), [.poker](#), [.porn](#), [.press](#), [.pro](#), [.productions](#), [.properties](#), [.property](#), [.pub](#)

Q

[.qpon](#)

R

[.recipes](#), [.red](#), [.reise](#), [.reisen](#), [.rentals](#), [.repair](#), [.report](#), [.republican](#), [.restaurant](#), [.reviews.](#), [.rip](#), [.rocks](#), [.run](#)

S

[.sale](#), [.sarl](#), [.school](#), [.schule](#), [.services](#), [.sex](#), [.sexy](#), [.shiksha](#), [.shoes](#), [.shopping](#), [.show](#), [.singles](#), [.site](#), [.ski](#), [.soccer](#), [.social](#), [.solar](#), [.solutions](#), [.software](#), [.space](#), [.store](#), [.stream](#), [.studio](#), [.style](#), [.sucks](#), [.supplies](#), [.supply](#), [.support](#), [.surgery](#), [.systems](#)

T

[.tattoo](#), [.tax](#), [.taxi](#), [.team](#), [.tech](#), [.technology](#), [.tennis](#), [.theater](#), [.tienda](#), [.tips](#), [.tires](#), [.today](#), [.tools](#), [.tours](#), [.town](#), [.toys](#), [.trade](#), [.training](#), [.tv](#)

U

[.university](#), [.uno](#)

V

[.vacations](#), [.vegas](#), [.ventures](#), [.vg](#), [.viajes](#), [.video](#), [.villas](#), [.vision](#), [.vote](#), [.voyage](#)

WXYZ

[.watch](#), [.website](#), [.wedding](#), [.wiki](#), [.wine](#), [.work](#), [.works](#), [.world](#), [.wtf](#), [.xxx](#), [.xyz](#), [.zone](#)

.ac

Consulte [.ac \(Isla Ascensión\)](#).

[Return to index](#)

.academy

Utilizado por instituciones educativas, como escuelas y universidades. También lo utilizan reclutadores, asesores, anunciantes, estudiantes, profesores y administradores afiliados a instituciones educativas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento

- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.accountants

Usado por empresas, grupos y particulares relacionados con la profesión de contabilidad.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento

- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.actor

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

compatible

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.adult

Utilizado para los sitios web que alojan contenido solo para adultos.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.agency

Utilizado por empresas o grupos que se identifican como agencias.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.airforce

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

compatible

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.apartments

Utilizado por agentes inmobiliarios, propietarios y arrendatarios.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.associates

Utilizado por empresas y firmas que incluyen el término “associates” en su título. Utilizado también por los grupos o agencias que desean indicar la naturaleza profesional de sus organizaciones.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.auction

Usado para eventos relacionados con las subastas y operaciones de compra y venta basadas en subastas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para chino, francés, alemán, español y alfabeto latino.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.audio

Important

Ya no puede usar Route 53 para registrar nuevos dominios .audio o transferir dominios .audio a Route 53. Seguiremos ofreciendo soporte a dominios .audio que ya están registrados en Route 53.

Utilizado por la industria audiovisual y por cualquier persona interesada en la radiodifusión, equipos de sonido, producción de audio y transmisión de audio.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, español, francés, italiano, lenguas cirílicas (principalmente el ruso) y portugués.

Código de autorización necesario para transferencias

No admitido. Ya no se pueden transferir dominios .audio a Route 53.

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.band

Usado para compartir información sobre las bandas musicales y eventos de las bandas. Usado también por los músicos para contactar con sus fans y vender artículos relacionados con la banda.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para chino, francés, alemán, español y alfabeto latino.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.bargains

Usado para ofrecer información sobre ventas y promociones.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.beer

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.bet

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.bid

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento

- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.bike

Utilizado por las empresas o grupos que suministran artículos a los ciclistas o motoristas, como tiendas de bicicletas, concesionarios de motocicletas y talleres de reparación.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento

- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.bingo

Utilizado para los sitios web de apuestas o para compartir información sobre el juego del bingo.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.bio

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.biz

Utilizado para uso comercial o empresarial.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Compatible con alemán, chino simplificado, chino tradicional, coreano, danés, español, finlandés, húngaro, japonés, letón, lituano, noruego, polaco, portugués y sueco.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.black

Utilizado por aquellos que les gusta el color negro o que desean asociar el color negro a su negocio o marca.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.blue

Utilizado por aquellos que les gusta el color azul o que desean asociar el color azul a su negocio o marca.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.boutique

Usado para ofrecer información sobre boutiques y pequeñas tiendas de moda.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.builders

Utilizado por empresas y particulares asociados al sector de la construcción.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.business

Usado por cualquier tipo de empresa. Se puede utilizar como una alternativa a la extensión .biz.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.buzz

Usado para ofrecer información sobre las últimas noticias y eventos.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.cab

Utilizado por empresas y particulares asociados al sector de los taxis.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.cafe

Usado por las empresas de café y personas interesadas en la cultura del café.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español y francés.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento

- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.camera

Usado por los entusiastas de la fotografía y cualquiera que desee compartir fotos.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento

- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.camp

Usado por parques y departamentos de recreo, campamentos de verano, talleres para escritores, campamentos de fitness y entusiastas de la acampada.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento

- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.capital

Usado como una categoría general que describe cualquier tipo de capital, como una capital financiera o la capital de una ciudad.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento

- El dominio se elimina del registro: 75 días después del vencimiento

.cards

Utilizado por empresas especializadas en tarjetas como tarjetas electrónicas, tarjetas de felicitación impresas, tarjetas de visita y barajas de cartas. Ideal también para los jugadores que deseen comentar las normas y estrategias de los juegos de cartas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento

- El dominio se elimina del registro: 75 días después del vencimiento

.care

Utilizado por empresas u organismos relacionados con la prestación de cuidados. Usado también por organizaciones benéficas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.careers

Usado para ofrecer información sobre contratación laboral.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.cash

Usado por cualquier organización, grupo o particular involucrado en actividades relacionadas con el dinero.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.casino

Usado por el sector de las apuestas o por los jugadores que desean compartir información acerca de las apuestas y los juegos de casino.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.catering

Usado por las empresas de restauración o aquellos que desean compartir información sobre los eventos relacionados con la alimentación.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.cc

Consulte [.cc \(Islas Cocos \(Keeling\)\)](#).

[Return to index](#)

.center

Se utiliza como extensión genérica para cualquier cosa, desde organizaciones de investigación a centros comunitarios.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.ceo

Se utilizan para obtener información sobre sus CEOs homólogos y sus equivalentes.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán.

Código de autorización necesario para transferencias

Sí

DNSSEC

No admitido.

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.chat

Usado por cualquier tipo de sitio web de chat online.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.cheap

Usado por los sitios web de comercio electrónico para promocionar y vender productos económicos.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.christmas

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 43 días después de la fecha de vencimiento.
- El dominio se elimina de Route 53: 44 días después del vencimiento
- Es posible restaurarlo a través del registro: entre 44 y 86 días después del vencimiento.
- El dominio se elimina del registro: 86 días después de la fecha de vencimiento.

.church

Usado por las iglesias de cualquier tamaño o denominación para conectar con sus congregaciones y para publicar información sobre los eventos y las actividades relacionados con la iglesia.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.city

Se utiliza para proporcionar información sobre ciudades específicas, como puntos de interés, lugares de visita destacados y actividades del vecindario.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.claims

Utilizado por las empresas que tramitan reclamaciones de seguros o proporcionan servicios jurídicos.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.cleaning

Utilizado por empresas y particulares que proporcionan servicios de limpieza.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento

- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.click

Usado por las empresas que desean asociar la acción de hacer clic con sus sitios web, como hacer clic en productos de un sitio web para comprarlos.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

Soportado.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, español, francés, italiano, lenguas cirílicas (principalmente el ruso) y portugués.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento

- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.clinic

Usado por el sector sanitario y por los profesionales médicos.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento

- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.clothing

Utilizado por aquellos que trabajan en el sector de la moda, incluidos minoristas, grandes almacenes, diseñadores, sastres y outlets.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento

- El dominio se elimina del registro: 75 días después del vencimiento

.cloud

Se utiliza como una extensión general, pero es ideal para las empresas que proporcionan tecnologías y servicios de informática en la nube.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.club

Usado por cualquier tipo de club u organización.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para español y japonés.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.coach

Utilizado por cualquier persona interesada en el entrenamiento, como profesionales del deporte, asesores de estilo de vida o entrenadores corporativos.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.codes

Se utiliza como una extensión genérica para todos los tipos de código, como códigos de conducta, códigos de construcción o código de programación.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.coffee

Utilizado por las personas relacionadas con la industria del café.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.college

Utilizado por instituciones educativas, como escuelas y universidades. También lo utilizan reclutadores, asesores, anunciantes, estudiantes, profesores y administradores afiliados a instituciones educativas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para árabe, chino tradicional y simplificado, cirílico, griego, hebreo, japonés y tailandés.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.com

Usado para sitios web comerciales. Es la extensión más popular en Internet.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

Toda la información está oculta.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.community

Usado por cualquier tipo de comunidad, club, organización o grupo de interés especial.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.company

Usado como extensión genérica por empresas de todo tipo.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.computer

Se utiliza como extensión genérica para proporcionar información sobre los equipos informáticos.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.condos

Usado por personas y empresas relacionadas con condominios.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.construction

Usado por los integrantes del sector de la construcción, como constructores y contratistas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento

- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.consulting

Usado por consultores y otras personas relacionadas con el sector de la consultoría.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Compatible con alemán, árabe, chino, cirílico, coreano, devanagari, español, francés, griego, hebreo, japonés, latino, tamil y tailandés.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento

- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.contact

Usado por las iglesias de cualquier tamaño o denominación para conectar con sus congregaciones y para publicar información sobre los eventos y las actividades relacionados con la iglesia.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento

- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.contractors

Usado por contratistas, como los del sector de la construcción.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.cool

Usado por organizaciones y grupos que desean asociar su marca con las últimas tendencias.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.coupons

Usado por vendedores y fabricantes que proporcionan cupones y códigos de cupón online.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español y francés.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.credit

Usado por la industria crediticia.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.creditcard

Usado por empresas o bancos que emiten tarjetas de crédito.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.cruises

Usado por la industria de los cruceros.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.dance

Usado por bailarines, profesores de baile y escuelas de baile.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español, francés y alfabeto latino.

Código de autorización necesario para transferencias

Sí

DNSSEC

No admitido.

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.dating

Usado para sitios web de citas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.deals

Se utiliza para proporcionar información sobre gangas y ventas online.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.degree

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

compatible

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.delivery

Usado por las empresas que entregan cualquier tipo de mercancía o servicio.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento

- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.democrat

Usado para proporcionar información sobre el partido democrático. También lo utilizan los funcionarios electos, entusiastas de la política, consultores y asesores.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español, francés y alfabeto latino.

Código de autorización necesario para transferencias

Sí

DNSSEC

No admitido.

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento

- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.dental

Usado por profesionales de la odontología y proveedores dentales.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento

- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.design

Usado por las iglesias de cualquier tamaño o denominación para conectar con sus congregaciones y para publicar información sobre los eventos y las actividades relacionados con la iglesia.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento

- El dominio se elimina del registro: 75 días después del vencimiento

.diamonds

Usado por los entusiastas de los diamantes y los integrantes de la industria del diamante, incluidos vendedores, distribuidores y comerciantes.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.diet

Important

Ya no puede usar Route 53 para registrar nuevos dominios .diet o transferir dominios .diet a Route 53. Seguiremos ofreciendo soporte a dominios .diet que ya están registrados en Route 53.

Usado por profesionales de la salud y el deporte.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, español, francés, italiano, lenguas cirílicas (principalmente el ruso) y portugués.

Código de autorización necesario para transferencias

No admitido. Ya no se pueden transferir dominios .diet a Route 53.

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento

- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.digital

Usado para cualquier cosa digital, pero ideal para empresas tecnológicas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento

- El dominio se elimina del registro: 75 días después del vencimiento

.direct

Usado como extensión general, pero ideal para aquellos que venden productos directamente a los clientes a través de un sitio web de comercio electrónico.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.directory

Usado por el sector de los medios de comunicación.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.discount

Usado por los sitios web de descuentos y empresas que bajan los precios.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.dog

Usado por los amantes de los perros y aquellos que proporcionan servicios y productos caninos.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español y francés.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.domains

Usado para proporcionar información sobre los nombres de dominio.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.education

Usado para ofrecer información sobre educación.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.email

Usado para ofrecer información sobre cómo promocionar el correo electrónico.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.energy

Usado como una extensión general, pero ideal para aquellos que trabajan en el campo de la energía o del ahorro energético.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.engineering

Usado por empresas y profesionales de ingeniería.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.enterprises

Usado para ofrecer información sobre empresas y negocios.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.equipment

Usado para ofrecer información sobre equipos, minoristas o fabricantes de equipos y tiendas de alquiler.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento

- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.estate

Usado para ofrecer información sobre la vivienda y el sector de la vivienda.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento

- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.events

Usado para ofrecer información sobre eventos de todo tipo.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento

- El dominio se elimina del registro: 75 días después del vencimiento

.exchange

Usado para cualquier tipo de intercambio: la bolsa, intercambio de bienes o incluso un simple intercambio de información.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.expert

Usado por aquellos que tienen conocimientos especializados en una serie de campos.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.exposed

Usado como extensión genérica para una serie de asuntos, como fotografía, publicaciones sensacionalistas y periodismo de investigación.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.express

Usado como extensión general, pero ideal para aquellos que desean hacer hincapié en la rápida entrega de bienes o servicios.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español y francés.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.fail

Usado por cualquiera que haya cometido errores, pero ideal para publicar tropiezos y meteduras de pata graciosos.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.fan

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.farm

Usado por los integrantes del sector agrícola, como agricultores e ingenieros agrícolas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.finance

Usado por el sector financiero.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.financial

Usado por el sector financiero.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.fish

Usado como extensión general, pero ideal para los sitios web relacionados con los peces y la pesca.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.fitness

Usado para promocionar el fitness y los servicios de fitness.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento

- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.flights

Usado por agencias de viajes, líneas aéreas y cualquier persona relacionada con el sector de viajes.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento

- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.florist

Utilizado por los floricultores.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.flowers

Important

Ya no puede usar Route 53 para registrar nuevos dominios .flowers o transferir dominios .flowers a Route 53. Seguiremos ofreciendo soporte a dominios .flowers que ya están registrados en Route 53.

Usado para cualquier cosa relacionada con las flores, como venta de flores online o información sobre el cultivo de flores.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, español, francés, italiano, lenguas cirílicas (principalmente el ruso) y portugués.

Código de autorización necesario para transferencias

No admitido. Ya no se pueden transferir dominios .flowers a Route 53.

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento

- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.fm

Consulte [.fm \(Estados Federados de Micronesia\)](#).

[Return to index](#)

.football

Usado por cualquiera implicado en el deporte de fútbol americano.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento

- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.forsale

Usado para vender bienes y servicios.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español, francés y alfabeto latino.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.foundation

Utilizado por organizaciones sin ánimo de lucro, organizaciones benéficas y otros tipos de fundaciones.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.fun

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.fund

Usado como extensión general para todo lo relacionado con la financiación.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.furniture

Usado por los fabricantes y vendedores de muebles y cualquier persona relacionada con el sector de los muebles.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.futbol

Usado para ofrecer información sobre fútbol.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español, francés y alfabeto latino.

Código de autorización necesario para transferencias

Sí

DNSSEC

No admitido.

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.fyi

Usado como extensión general, pero ideal para compartir información de todo tipo. “FYI” es el acrónimo de “for your information” (para su información).

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español y francés.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.gallery

Usado por propietarios de galerías de arte.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.games

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

compatible

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.gift

Usado por empresas u organizaciones que venden regalos o proporcionan servicios relacionados con regalos.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, español, francés, italiano, lenguas cirílicas (principalmente el ruso) y portugués.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento

- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.gifts

Usado por empresas u organizaciones que venden regalos o proporcionan servicios relacionados con regalos.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento

- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.gives

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.glass

Usado por los integrantes del sector del vidrio, como cortadores de vidrio e instaladores de ventanas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.global

Usado por empresas o grupos con un mercado o una visión internacional.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, árabe, bielorruso, bosnio, búlgaro, chino (simplificado), chino (tradicional), coreano, danés, español, hindi, húngaro, islandés, letón, lituano, macedonio, montenegrino, polaco, ruso, serbio, sueco y ucraniano.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.gmbh

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

compatible

Nombres de dominio internacionalizados

compatible

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.gold

Usado como extensión general, pero ideal para las empresas que compran o venden oro o productos relacionados con el oro.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español y francés.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.golf

Usado para los sitios web dedicados al juego de golf.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español y francés.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.graphics

Utilizado por las personas relacionadas con el sector de los gráficos.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.gratis

Usado por sitios web que ofrecen productos gratis, como artículos promocionales, descargas o vales. Proviene de la palabra española “gratis”.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.green

Usado por los sitios web dedicados a la conservación, la ecología, el medio ambiente y el estilo de vida ecológico.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.gripe

Se utiliza para compartir quejas y críticas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.group

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

compatible

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento

- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.guide

Usado como extensión general, pero ideal para los sitios web centrados en los destinos, servicios y productos de viaje.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.guitars

Important

Ya no puede usar Route 53 para registrar nuevos dominios .guitars o transferir dominios .guitars a Route 53. Seguiremos ofreciendo soporte a dominios .guitars que ya están registrados en Route 53.

Usado por los entusiastas de la guitarra.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, español, francés, italiano, lenguas cirílicas (principalmente el ruso) y portugués.

Código de autorización necesario para transferencias

No admitido. Ya no se pueden transferir dominios .guitars a Route 53.

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento

- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.guru

Usado por aquellos que desean compartir sus conocimientos sobre una serie de temas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.haus

Usado por el sector inmobiliario y de la construcción. “Haus” es una palabra alemana que significa “casa”.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español, francés y alfabeto latino.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.healthcare

Usado por el sector sanitario.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.help

Usado como extensión general, pero ideal para los sitios web que proporcionan ayuda e información online.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, español, francés, italiano, lenguas cirílicas (principalmente el ruso) y portugués.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.hiv

Usado para los sitios web dedicados a la lucha contra el VIH.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, español, francés, italiano, lenguas cirílicas (principalmente el ruso) y portugués.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.hockey

Usado para los sitios web dedicados al juego de hockey.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español y francés.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.holdings

Usado por asesores financieros, agentes de bolsa y aquellas personas que trabajan con inversiones.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.holiday

Utilizado por las personas que trabajan en el sector de viajes, y particulares y empresas dedicados a la planificación de fiestas y ocasiones especiales.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.host

Usado por empresas que proporcionan plataformas y servicios de alojamiento web.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Compatible con árabe, chino simplificado, chino tradicional, coreano, griego, hebreo y tailandés.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.hosting

Important

Ya no puede usar Route 53 para registrar nuevos dominios .hosting o transferir dominios .hosting a Route 53. Seguiremos ofreciendo soporte a dominios .hosting que ya están registrados en Route 53.

Usados por sitios web de hospedaje y personas que trabajan en la industria del hospedaje.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español y francés.

Código de autorización necesario para transferencias

No admitido. Ya no se pueden transferir dominios .hosting a Route 53.

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.house

Usado por agentes inmobiliarios y compradores y vendedores de viviendas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.im

Consulte [.im \(Isla de Man\)](#).

[Return to index](#)

.immo

Usado por el sector inmobiliario.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.immobilien

Usado para ofrecer información sobre el mercado inmobiliario.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español y francés.

Código de autorización necesario para transferencias

Sí

DNSSEC

No admitido.

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.industries

Usado por cualquier negocio o empresa comercial que desea identificarse como un sector de la industria.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.info

Usado para la divulgación de información.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento

- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.ink

Usado por los entusiastas del tatuaje o cualquier sector relacionado con la tinta, como imprentas y editoriales.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para los alfabetos árabe y latino.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento

- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.institute

Usado por cualquier organización o grupo, especialmente por las organizaciones de investigación y educativas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.insure

Usado por las compañías de seguros y agentes de seguros.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.international

Usado por empresas que tienen cadenas internacionales, particulares que viajan al extranjero u organizaciones benéficas con influencia internacional.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.investments

Usado como extensión general, pero ideal para promocionar oportunidades de inversión.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.io

Consulte [.io \(Territorio Británico del Océano Índico\)](#).

[Return to index](#)

.irish

Usado para promocionar la cultura y las organizaciones irlandesas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Compatible con alemán, árabe, chino simplificado, chino tradicional, coreano, francés, español, griego, hebreo, japonés, tamil y tailandés.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.jewelry

Usado por los vendedores y compradores de joyas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español y francés.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.juegos

Important

Ya no puede usar Route 53 para registrar nuevos dominios .juegos o transferir dominios .juegos a Route 53. Seguiremos ofreciendo soporte a dominios .juegos que ya están registrados en Route 53.

Usado para sitios web de juegos de todo tipo. Proviene de la palabra española “juegos”.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, español, francés, italiano, lenguas cirílicas (principalmente el ruso) y portugués.

Código de autorización necesario para transferencias

No admitido. Ya no se pueden transferir dominios .juegos a Route 53.

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.kaufen

Usado para ofrecer información sobre comercio electrónico.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español, francés y alfabeto latino.

Código de autorización necesario para transferencias

Sí

DNSSEC

No admitido.

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.kim

Usado por las personas cuyo nombre o apellido es Kim.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.kitchen

Utilizado por los vendedores de cocinas, cocineros, bloggers de comida y cualquier persona relacionada con la industria alimentaria.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.kiwi

Usado por las empresas y particulares que desean respaldar la cultura del kiwi de Nueva Zelanda. También se utiliza como plataforma para ayudar en la reconstrucción de Christchurch, afectado por los terremotos de 2010 y 2011.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para maorí.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.land

Utilizado por agricultores, agentes inmobiliarios, promotores comerciales y todas aquellas personas interesadas en la propiedad.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.law

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.lease

Utilizado por inmobiliarias, agentes inmobiliarios y arrendatarios.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento

- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.legal

Usado por los miembros de la abogacía.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento

- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.lgbt

Usado por la comunidad de lesbianas, gays, bisexuales y transexuales.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento

- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.life

Usado como extensión general y adecuado para una amplia variedad de empresas, grupos y particulares.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento

- El dominio se elimina del registro: 75 días después del vencimiento

.lighting

Usado por fotógrafos, diseñadores, arquitectos, ingenieros y otras personas interesadas en la iluminación.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.limited

Usado como extensión general y adecuado para una amplia variedad de empresas, grupos y particulares.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.limo

Usado por chóferes, empresas de limusinas y agencias de alquiler de vehículos.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.link

Usado para ofrecer información sobre la creación de enlaces de acceso directo online.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

Uniregistry es el registro de los dominios .LINK. Debido a la política de Uniregistry, el [WHOIS](#) de registro muestra “REDACTADO POR PRIVACIDAD”. Eliminar nuestra característica de protección de la privacidad sólo afectará a la información mostrada en el [WHOIS del registrador de Amazon](#).

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, español, francés, italiano, lenguas cirílicas (principalmente el ruso) y portugués.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.live

Usado como extensión general y adecuado para una amplia variedad de empresas, grupos y particulares.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español, francés y alfabeto latino.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.llc

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.loan

Usado por prestamistas, prestatarios y especialistas en crédito.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, danés, noruego y sueco.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.loans

Usado por prestamistas, prestatarios y especialistas en crédito.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.lol

Usado para sitios web de humor. “LOL” es el acrónimo de “laugh out loud” (reírse a carcajadas).

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, cirílico, español, francés, italiano y portugués.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

ltd.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.maison

Usado por el sector inmobiliario.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento

- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.management

Usado para ofrecer información sobre el mundo empresarial y la administración de empresas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento

- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.marketing

Usado por el sector de marketing para distintos fines.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.mba

Usado por los sitios web que proporcionan información sobre másteres en administración de empresas (MBA).

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español y francés.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.media

Usado por los sectores de medios de comunicación y entretenimiento.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.memorial

Usado por organizaciones conmemorativas dedicadas a honrar eventos y personas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.mobi

Usado por empresas y particulares que desean que sus sitios web estén accesibles desde teléfonos móviles.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.moda

Usado para ofrecer información sobre moda.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español, francés y alfabeto latino.

Código de autorización necesario para transferencias

Sí

DNSSEC

No admitido.

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.money

Usado para sitios web centrados en el dinero y en actividades relacionadas con el dinero.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.mortgage

Usado por el sector hipotecario.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español, francés y alfabeto latino.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.movie

Usado para sitios web que proporcionan información sobre películas y realización de películas. Adecuado para profesionales y aficionados.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español y francés.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento

- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.name

Usado por cualquiera que desee crear una presencia web personalizada.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

Verisign, el registro de .name TLDs, le permite registrar dominios de segundo nivel (nombre .name) y dominios de tercer nivel (nombre). apellido (.name). Route 53 admite únicamente dominios de segundo nivel, tanto para registrar dominios como para transferir dominios existentes a Route 53.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.net

Usado para todo tipo de sitios web. La extensión .net es una abreviatura de “network” (red).

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

Toda la información está oculta.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento

- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.network

Usado por los integrantes del sector de las redes o por aquellos que desean crear conexiones a través de redes de contactos.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento

- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.news

Usado para la distribución de cualquier información de interés periodístico, como acontecimientos actuales e información relacionada con el periodismo y la comunicación.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español, francés y alfabeto latino.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento

- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.ninja

Usado por las personas y empresas que desean relacionarse a sí mismas con las habilidades de un ninja.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español, francés y alfabeto latino.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento

- El dominio se elimina del registro: 75 días después del vencimiento

.onl

La extensión .onl es una abreviatura de “online” y también es la abreviatura española de “organización no lucrativa”.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.online

La extensión .onl es una abreviatura de “online” y también es la abreviatura española de “organización no lucrativa”.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.org

Usado por todo tipo de organizaciones.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

Toda la información está oculta.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.partners

Usado por bufetes de abogados, inversores y una gran variedad de empresas. También se utiliza para sitios web sociales de establecimiento de relaciones.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.parts

Usado como extensión general, pero ideal para los fabricantes, vendedores y compradores de piezas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.photo

Usado por fotógrafos y cualquier persona interesada en la fotografía.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, español, francés, italiano, lenguas cirílicas (principalmente el ruso) y portugués.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.photography

Usado por fotógrafos y cualquier persona interesada en la fotografía.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.photos

Usado por fotógrafos y cualquier persona interesada en la fotografía.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.pics

Usado por fotógrafos y cualquier persona interesada en la fotografía.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, español, francés, italiano, lenguas cirílicas (principalmente el ruso) y portugués.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.pictures

Usado por cualquier persona interesada en la fotografía, el arte y el contenido multimedia.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.pink

Utilizado por aquellos que les gusta el color rosa o que desean asociar el color rosa a su negocio o marca.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento

- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.pizza

Utilizado por las pizzerías y amantes de las pizzas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento

- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.place

Usado como extensión general, pero ideal para los sectores de hogar y viajes.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.plumbing

Utilizado por las personas relacionadas con el sector de la fontanería.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.plus

Usado como extensión general, pero ideal para las tallas grandes de ropa, complementos de software y cualquier producto que ofrezca característica o dimensiones “extra”.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español y francés.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.poker

Usado por jugadores de póker y sitios web de apuestas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.porn

Usado para sitios web solo para adultos.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.press

Usado para sitios web solo para adultos.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

compatible

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.pro

Usado por profesionales acreditados y reconocidos y organizaciones profesionales.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.productions

Usado por estudios y productoras que hacen publicidad, anuncios de radio y vídeos musicales.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.properties

Usado para ofrecer información sobre cualquier tipo de propiedad, incluido el sector inmobiliario o la propiedad intelectual. Lo usan también quienes tienen casas, edificios o parcelas que venden, arriendan o alquilan.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.property

Usado para ofrecer información sobre cualquier tipo de propiedad, incluido el sector inmobiliario o la propiedad intelectual. Lo usan también quienes tienen casas, edificios o parcelas que venden, arriendan o alquilan.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, español, francés, italiano, lenguas cirílicas (principalmente el ruso) y portugués.

Código de autorización necesario para transferencias

No admitido. Ya no se pueden transferir dominios .property a Route 53.

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.pub

Utilizado por las personas relacionadas con empresas de publicación, publicidad o cerveza.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español, francés y alfabeto latino.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.qpon

Usado para cupones y códigos promocionales.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.recipes

Usado por quienes desean compartir recetas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento

- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.red

Utilizado por aquellos que les gusta el color rojo o que desean asociar el color rojo a su negocio o marca.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento

- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.reise

Usado por sitios web relacionados con viajes. “Reise” es una palabra alemana que significa “aumento”, “elevación” o “la acción de emprender un viaje”.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español y francés.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento

- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.reisen

Usado por sitios web relacionados con viajes. “Reisen” es una palabra alemana que significa “viajar”.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.rentals

Usado para todo tipo de alquileres.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.repair

Usado por servicios de reparación o por aquellos que desean enseñar a reparar todo tipo de artículos.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.report

Usado como extensión general, pero ideal para ofrecer información sobre los informes empresariales, publicaciones de la comunidad, reseñas de libros o informes de noticias.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.republican

Usado para proporcionar información sobre el partido republicano. También lo utilizan los funcionarios electos, entusiastas de la política, consultores y asesores.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español, francés y alfabeto latino.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.restaurant

Usado por el sector de los restaurantes.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

reviews.

Usado por aquellos que desean dar su opinión y leer los comentarios de otras personas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español, francés y alfabeto latino.

Código de autorización necesario para transferencias

Sí

DNSSEC

No admitido.

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.rip

Usado para sitios web dedicado a la muerte y los funerales. “RIP” es el acrónimo de “rest in pace” (descanse en paz).

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español, francés y alfabeto latino.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.rocks

Extensión .rocks utilizada de manera general pero sobre todo por músicos, geólogos, joyeros, escaladores y más.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español, francés y alfabeto latino.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.run

Usado como extensión general, pero ideal para el sector del fitness y los deportes.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español y francés.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.sale

Utilizado por los sitios web de comercio electrónico.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español, francés y alfabeto latino.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento

- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.sarl

Usado por sociedades anónimas emplazadas normalmente en Francia. “SARL” es un acrónimo de “Société à Responsabilité Limitée”.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento

- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.school

Usado para ofrecer información sobre educación, instituciones educativas y actividades relacionadas con la escuela.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.schule

Usado para ofrecer información sobre educación, instituciones educativas y actividades relacionadas con la escuela en Alemania. “Schule” es una palabra alemana que significa “escuela”.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.services

Usado por los sitios web centrados en servicios de todo tipo.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.sex

Usado para contenido solo para adultos.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.sexy

Usado para contenido sexual. Se utiliza también para describir las marcas, productos, información y sitios web más populares y estimulantes.

[Return to index](#)

Important

Ya no puede usar Route 53 para registrar nuevos dominios .sexy o transferir dominios .sexy a Route 53. Seguiremos ofreciendo soporte a dominios .sexy que ya están registrados en Route 53.

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, español, francés, italiano, lenguas cirílicas (principalmente el ruso) y portugués.

Código de autorización necesario para transferencias

No admitido. Ya no se pueden transferir dominios .sexy a Route 53.

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.shiksha

Usado por instituciones educativas. “Shiksha” es una palabra india que significa “escuela”.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.shoes

Usado por vendedores, diseñadores y fabricantes de zapatos o bloggers de moda.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.shopping

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.show

Usado como extensión general, pero ideal para el sector del entretenimiento.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español y francés.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.singles

Usado por servicios de citas, complejos turísticos y otras empresas dirigidas a aquellas personas que desean establecer relaciones.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.site

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

compatible

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.ski

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento

- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.soccer

Usado para los sitios web dedicados al fútbol.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español y francés.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.social

Usado para ofrecer información sobre redes sociales, foros y conversaciones online.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español, francés y alfabeto latino.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.solar

Usado para ofrecer información sobre el sistema solar o la energía solar.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.solutions

Utilizado por consultores, do-it-yourself servicios y asesores de todo tipo.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.software

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.space

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

compatible

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.store

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

compatible

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.stream

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.studio

Usado como una extensión general, pero ideal para aquellos que trabajan en el sector inmobiliario, del arte o del entretenimiento.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español, francés y alfabeto latino.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento

- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.style

Usado como extensión general, pero ideal para los sitios web dedicados a las últimas tendencias, en particular tendencias de moda, diseño, arquitectura y arte.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento

- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.sucks

Usado como extensión general, pero ideal para aquellos que desean compartir experiencias negativas o advertir a otras personas sobre timos, fraudes o productos defectuosos.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.supplies

Usado por empresas que venden productos online.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.supply

Usado por empresas que venden productos online.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.support

Usado por empresas, grupos u organizaciones benéficas que ofrecen cualquier tipo de ayuda, incluida asistencia a los clientes, productos o sistemas, o ayuda emocional, financiera o espiritual.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.surgery

Usado para ofrecer información sobre la cirugía, la medicina y la atención sanitaria.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.systems

Usado principalmente por el sector de la tecnología y aquellas personas que ofrecen servicios tecnológicos.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.tattoo

Usado por los entusiastas del tatuaje y el sector del tatuaje.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, español, francés, italiano, lenguas cirílicas (principalmente el ruso) y portugués.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.tax

Usado para ofrecer información sobre los impuestos, la preparación de declaraciones de impuestos y la legislación fiscal.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.taxi

Usado por empresas de taxis, chóferes y traslados.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español y francés.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.team

Usado por cualquier empresa u organización que desea identificarse como un equipo.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español y francés.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento

- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.tech

Usado por los entusiastas de la tecnología y aquellas personas dedicadas a la tecnología en empresas, servicios y fábricas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

compatible

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento

- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.technology

Usado por los entusiastas de la tecnología y aquellas personas dedicadas a la tecnología en empresas, servicios y fábricas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento

- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.tennis

Usado para ofrecer información relacionada con el juego de tenis.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.theater

Usado por los sitios web dedicados al cine, obras de teatro y musicales.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español y francés.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.tienda

Usado por empresas minoristas que desea conectar con consumidores hispanohablantes.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.tips

Usado por aquellas personas que desean compartir sus conocimientos y asesorar sobre prácticamente cualquier tema.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.tires

Usado por fabricantes, distribuidores o compradores de neumáticos.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.today

Usado para ofrecer información sobre los acontecimientos actuales, noticias, climatología, entretenimiento, etc.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.tools

Usado para ofrecer información sobre cualquier tipo de herramienta.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.tours

Usado como extensión general, pero ideal para las empresas de viajes.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español y francés.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.town

Usado para promocionar las características, cultura y comunidad de una ciudad.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.toys

Usado por la industria de los juguetes.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento

- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.trade

Usado como extensión general, pero ideal para sitios web de comercio o servicios comerciales.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, danés, noruego y sueco.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento

- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.training

Usado por instructores, entrenadores y educadores.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento

- El dominio se elimina del registro: 75 días después del vencimiento

.tv

Usado para ofrecer información sobre la televisión y los medios de comunicación.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

Ninguna.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.university

Usado por universidades y otras organizaciones educativas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.uno

Usado para ofrecer información sobre las comunidades hispana, portuguesa e italiana.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.vacations

Usado por el sector de viajes y turismo.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.vegas

Usado para promocionar la ciudad de Las Vegas y el estilo de vida de Las Vegas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.ventures

Usado por empresarios, empresas emergentes, inversores de capital riesgo, bancos de inversión y financieros.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.vg

Consulte [.vg \(Islas Vírgenes Británicas\)](#).

[Return to index](#)

.viajes

Usado por agencias de viaje, operadores turísticos, blogs de viajes, compañías turísticas, servicios de alquiler, bloggers de viajes y minoristas de viajes.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.video

Usado por el sector de los medios de comunicación y vídeo.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español, francés y alfabeto latino.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.villas

Usado por agentes inmobiliarios y propietarios de inmuebles que venden, alquilan o arrendan villas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.vision

Usado como extensión general, pero ideal para los especialistas en la visión, como optometristas y oftalmólogos.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.vote

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.voyage

Usado por agencias de viaje, operadores turísticos, blogs de viajes, compañías turísticas, servicios de alquiler, bloggers de viajes y minoristas de viajes.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento

- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.watch

Se utiliza para obtener información sobre sitios web de streaming TVs, páginas web, vídeos o relojes.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento

- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.website

Usado para ofrecer información sobre el desarrollo, promoción, mejoras y experiencias de sitios web.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Compatible con árabe, chino simplificado, chino tradicional, coreano, griego, hebreo, japonés y tailandés.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento

- El dominio se elimina del registro: 75 días después del vencimiento

.wedding

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

Ninguna.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alemán, chino, español y francés.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.wiki

Usado para ofrecer información sobre documentación online.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para los alfabetos árabe y latino.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.wine

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad

Soportado.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

compatible

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.work

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.works

Usado por empresas, organizaciones y particulares que desean ofrecer información sobre el trabajo y los servicios de empleo. Esta extensión puede utilizarse como una alternativa a las extensiones .com, .net y .org.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.world

Usado por cualquiera que desee proporcionar información sobre temas mundiales.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.wtf

Usado por cualquiera que desee identificarse con el acrónimo popular (pero soez) “WTF”.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.XXX

Utilizado para los sitios web que alojan contenido solo para adultos.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.xyz

Usado como extensión general para cualquier fin.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

La empresa de registro de dominios .xyz, Generation XYZ, considera que algunos nombres de dominio son premium. No puede registrar dominios .xyz premium ni transferirlos a Route 53. Para obtener más información, consulte el sitio web de [Generation XYZ](#).

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.zone

Usado para ofrecer información sobre cualquier tipo de zona, incluidas zonas horarias, zonas climáticas y zonas deportivas.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para francés y español.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

Dominios geográficos de nivel superior

Las siguientes extensiones de dominio están agrupadas por zonas geográficas e incluyen extensiones oficiales específicas de cada país, conocidas como dominios de nivel superior con código de país (cc). TLDs Algunos ejemplos son .be (Bélgica), .in (India) y .mx (México). Las normas de registro de los cc TLDs varían según el país. Algunos países no tienen restricciones, lo que significa que cualquier persona del mundo puede registrar estas extensiones, mientras que otros tienen algunas restricciones, como la residencia. La descripción de cada ccTLD indica cualquier restricción.

Important

Al transferir cualquier cc TLDs a Route 53, excepto .cc y .tv, se ignoran las actualizaciones del contacto propietario y se utilizan los datos de contacto del propietario del registro. Una vez realizada la transferencia, puede actualizar el contacto del propietario. Para obtener más información, consulte [Actualización de la información de contacto y la propiedad de un dominio](#).

[Return to index](#)

África

[.ac \(Isla Ascensión\)](#), [.co.za \(Sudáfrica\)](#), [.sh \(Santa Elena\)](#)

América

[.ca](#) (Canadá), [.cl](#) (Chile), [.co](#) (Colombia), [.com.ar](#) (Argentina), [.com.br](#) (Brasil), [.com.mx](#) (México), [.mx](#) (México), [.us](#) (Estados Unidos), [.vc](#) (San Vicente y las Granadinas), [.vg](#) (Islas Vírgenes Británicas)

Asia/Oceanía

[.au](#) (Australia), [.cc](#) (Islas Cocos (Keeling)), [.co.nz](#) (Nueva Zelanda), [.com.au](#) (Australia), [.com.sg](#) (República de Singapur), [.fm](#) (Estados Federados de Micronesia), [.in](#) (India), [.jp](#) (Japón), [.io](#) (Territorio Británico del Océano Índico), [.net.au](#) (Australia), [.net.nz](#) (Nueva Zelanda), [.org.nz](#) (Nueva Zelanda), [.pw](#) (Palau), [.qa](#) (Qatar), [.ru](#) (Federación Rusa), [.sg](#) (República de Singapur)

Europa

[.be](#) (Bélgica), [.berlin](#) (ciudad de Berlín de Alemania), [.ch](#) (Suiza), [.co.uk](#) (Reino Unido), [.cz](#) (Czech Republic), [.de](#) (Alemania), [.es](#) (España), [.eu](#) (Unión Europea), [.fi](#) (Finlandia), [.fr](#) (Francia), [.gg](#) (Guernsey), [.im](#) (Isla de Man), [.it](#) (Italia), [.me](#) (Montenegro), [.me.uk](#) (Reino Unido), [.nl](#) (Países Bajos), [.org.uk](#) (Reino Unido), [.ruhr](#) (región del Ruhr, parte occidental de Alemania), [.se](#) (Suecia), [.uk](#) (Reino Unido), [.wien](#) (ciudad de Viena en Austria)

África

Puede usar los siguientes dominios de nivel superior (TLDs) para África para registrar dominios en Amazon Route 53.

, ,

[Return to index](#)

[.ac](#) (Isla Ascensión)

[Return to index](#)

Se utiliza también como un TLD genérico popular entre las personas del sector académico.

Periodo de alquiler para el registro y la renovación

Un año.

Restricciones

Abierto al público, sin restricciones.

Protección de la privacidad

Determinada por la empresa de registro.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 80 días después de la fecha de vencimiento

.co.za (Sudáfrica)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

Un año.

Restricciones

Solo los dominios de segundo nivel están disponibles para la extensión .za. Route 53 admite el dominio de segundo nivel .co.za.

Abierto al público, con algunas restricciones:

- El registro está abierto a entidades legales identificables (particulares y personas jurídicas).
- El nombre de dominio debe superar una comprobación de zona durante el proceso de registro.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

No

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Es posible la renovación: Hasta un día antes de la fecha de vencimiento
- La renovación tardía con Route 53 es posible: No
- El dominio se elimina de Route 53: 1 día antes de la fecha de vencimiento
- Es posible restaurarlo a través del registro: Entre 1 día y 9 días después del vencimiento
- El dominio se elimina del registro: 9 días después del vencimiento

.sh (Santa Elena)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

Abierto al público, sin restricciones.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 80 días después de la fecha de vencimiento

América

Puede usar los siguientes dominios de nivel superior (TLDs) para América para registrar dominios en Amazon Route 53.

, , , , , , , ,

[Return to index](#)

.ca (Canadá)

[Return to index](#)

Las variantes de un nombre de dominio, con tilde (à) o sin tilde (a), se reservan de manera automática para el registrador y pasan a formar parte de un paquete administrativo. A fin de activar un dominio en un paquete, el registrador debe realizar una solicitud de registro para el dominio. Todos los dominios de un paquete deben estar registrados por el mismo registrador y ante el mismo registrador. El registrador también deberá presentar una solicitud de transferencia para todos los dominios de un paquete a fin de completar la transferencia.

Correo electrónico de confirmación de la empresa de registro del TLD

Cuando registre un dominio .ca, recibirá un correo electrónico con un enlace al procedimiento de aceptación del contrato del solicitante. Debe completar el procedimiento en un plazo de siete días o su dominio no se registrará.

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

Abierto al público, con algunas restricciones:

- El registro está abierto a los particulares u organizaciones relacionados con Canadá, tal y como se describe en Canadian Presence Requirements for Registrants.
- Contacto del solicitante: debe proporcionar el nombre legal completo y exacto del propietario del dominio.
- Contactos administrativos y técnicos: debe especificar Person como el tipo de contacto y proporcionar información de contacto para las personas que viven en Canadá.
- Debe seleccionar uno de los siguientes tipos legales durante el proceso de registro:
 - ABO: pueblos aborígenes (individuos o grupos) indígenas de Canadá
 - ASS: asociación canadiense sin personalidad jurídica
 - CCO: corporación, provincia o territorio canadiense
 - CCT: ciudadano canadiense
 - EDU: institución educativa canadiense
 - GOV: Gobierno o entidad gubernamental de Canadá
 - HOP: hospital canadiense
 - INB: banda india reconocida por la Ley India de Canadá
 - LAM: biblioteca, archivo o museo canadiense
 - LGR: representante legal de un ciudadano canadiense o un residente permanente

- MAJ: Her/His Majestad la Reina/Rey
- OMK: marca oficial registrada en Canadá
- PLT: partido político canadiense
- PRT: asociación registrada en Canadá
- RES: residente permanente de Canadá
- TDM: marca registrada en Canadá (por un tipo de propietario no canadiense)
- TRD: sindicato canadiense
- TRS: fideicomiso establecido en Canadá

Protección de la privacidad

- Persona: para todos los contactos, el nombre de contacto, la dirección, el número de teléfono, el número de fax y la dirección de correo electrónico están ocultos, ya que [CIRA](#) aplica de forma automática su protección de la privacidad a una persona. La opción de protección de la privacidad se aplicará únicamente al registrador Whois.
- Empresa, asociación u organismo público: no se admiten en el nivel del registro.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento

- El dominio se elimina del registro: Varía. Contacte con [AWS Support](#).

Eliminación de registro del dominio

La empresa de registro de dominios .ca no permite eliminar registros de dominios. En lugar de ello, debe desactivar la renovación automática y esperar a que el dominio caduque. Para obtener más información, consulte [Eliminación de un registro de nombre de dominio](#).

.cl (Chile)

Important

Ya no puede usar Route 53 para registrar nuevos dominios .cl o transferir dominios .cl a Route 53. Seguiremos ofreciendo soporte a dominios .cl que ya están registrados en Route 53.

[Return to index](#)

Período de renovación

Dos años.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

No admitido. Le recomendamos que impida las transferencias no autorizadas restringiendo el acceso a la acción de la [RetrieveDomainAuthCode](#) API. (Al restringir el acceso a esta API de Route 53, también restringe quién puede generar un código de autorización mediante la consola de Route 53 y otros métodos programáticos). AWS SDKs Para obtener más información, consulte [Identity and Access Management en Amazon Route 53](#).

Código de autorización necesario para transferencias

No admitido. Ya no se pueden transferir dominios .cl a Route 53.

DNSSEC

No admitido.

Plazos para renovar y restaurar dominios

- Es posible la renovación: póngase en contacto con [AWS Support](#).
- La renovación tardía con Route 53 es posible: póngase en contacto con [AWS Support](#).
- Se ha eliminado el dominio de Route 53: póngase en contacto con [AWS Support](#).
- Es posible restaurarlo a través del registro: póngase en contacto con [AWS Support](#).
- El dominio se ha eliminado del registro: póngase en contacto con [AWS Support](#).

.co (Colombia)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a cinco años.

Restricciones

Abierto al público, sin restricciones.

Protección de privacidad (se aplica a: persona)

Toda la información está oculta.

Si el tipo de contacto no es una persona, WHOIS muestra el nombre de la compañía y el país.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento

- Es posible la renovación tardía con Route 53: hasta 29 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 30 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 30 días y 45 días después del vencimiento
- El dominio se elimina del registro: 50 días después del vencimiento

.com.ar (Argentina)

 Important

Ya no puede usar Route 53 para registrar nuevos dominios .com.ar o transferir dominios .com.ar a Route 53. Seguiremos ofreciendo soporte a dominios .com.ar que ya están registrados en Route 53.

[Return to index](#)

Período de renovación

Un año.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

No admitido. Para evitar transferencias no autorizadas, restrinja el acceso a la dirección de correo electrónico del registrante y a Route 53, ya APIs que esto podría permitir el cambio de propietario, por ejemplo. [UpdateDomainContact](#) Para obtener más información, consulte [Acciones, recursos y claves de condición para Amazon Route 53 Domains](#) en la Referencia de autorizaciones de servicio y [Permisos de ejemplo para el propietario de un registro de dominio](#).

Código de autorización necesario para transferencias

No admitido. Ya no se pueden transferir dominios .com.ar a Route 53.

DNSSEC

No admitido.

Plazos para renovar y restaurar dominios

- Es posible la renovación: póngase en contacto con [AWS Support](#).
- La renovación tardía con Route 53 es posible: póngase en contacto con [AWS Support](#).
- Se ha eliminado el dominio de Route 53: póngase en contacto con [AWS Support](#).
- Es posible restaurarlo a través del registro: póngase en contacto con [AWS Support](#).
- El dominio se ha eliminado del registro: póngase en contacto con [AWS Support](#).

.com.br (Brasil)

Important

Ya no puede usar Route 53 para registrar nuevos dominios .com.br o transferir dominios .com.br a Route 53. Seguiremos ofreciendo soporte a dominios .com.br que ya están registrados en Route 53.

[Return to index](#)

Período de renovación

Un año.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Código de autorización necesario para transferencias

No admitido. Ya no se pueden transferir dominios .com.br a Route 53.

DNSSEC

No admitido.

Plazos para renovar y restaurar dominios

- Es posible la renovación: entre 30 días antes del vencimiento y la fecha de vencimiento

- Es posible la renovación tardía con Route 53: hasta 119 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 119 días después del vencimiento
- Es posible restaurarlo a través del registro: No
- El dominio se elimina del registro: 119 días después del vencimiento

.com.mx (México)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

Abierto al público, sin restricciones.

Protección de la privacidad

Determinada por la empresa de registro.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento

- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.mx (México)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

Abierto al público, sin restricciones.

Protección de la privacidad

Determinada por la empresa de registro.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.us (Estados Unidos)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

La empresa de registro para los dominios .us no permite nombres de dominio que contengan alguna de las siete palabras identificadas en el “Appendix to Opinion of the Court” de [Federal Communications Commission v. Pacifica Foundation n.º 77-528](#).

Abierto al público, con una restricción:

- La extensión .us es para sitios web o actividades que se realizan en los Estados Unidos de América.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 29 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 30 días después del vencimiento

- Es posible restaurarlo a través del registro: Entre 30 días y 60 días después del vencimiento
- El dominio se elimina del registro: 65 días después del vencimiento

.vc (San Vicente y las Granadinas)

También se utiliza como TLD genérico, a menudo por aquellas personas que participan en la financiación de capital de riesgo, universidades, etc.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

Abierto al público, sin restricciones.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento

- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 80 días después de la fecha de vencimiento

.vg (Islas Vírgenes Británicas)

También se utiliza como TLD genérico, a menudo por las organizaciones relacionadas con los videojuegos.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

Abierto al público, sin restricciones.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Sí

DNSSEC

No admitido.

Plazos para renovar y restaurar dominios

- Es posible la renovación: hasta 44 días después de la fecha de vencimiento
- La renovación tardía con Route 53 es posible: Sí
- El dominio se elimina de Route 53: 45 días después del vencimiento

- El dominio se elimina del registro: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: entre 45 días y 74 días después del vencimiento
- El dominio vuelve a ser de acceso público: 80 días después del vencimiento

Asia/Oceanía

Puede usar los siguientes dominios de nivel superior (TLDs) para Asia y Oceanía para registrar dominios en Amazon Route 53.

, , , , , , , , , , , , , , ,

[Return to index](#)

.au (Australia)

[Return to index](#)

Correo electrónico de confirmación de la empresa de registro del TLD

Nuestro registrador asociado, Gandi, revende los dominios.au a través de. DomainDirectors
 Cuando transfiere un nombre de dominio a Route 53, DomainDirectors envía un correo electrónico al contacto registrante del dominio para verificar la información de contacto o autorizar las solicitudes de transferencia.

Periodo de alquiler para el registro y la renovación

De uno a cinco años.

Restricciones

Abierto al público, con algunas restricciones:

- Los dominios .au están abiertos a las personas jurídicas, empresas mercantiles, sociedades o agentes independientes registrados en Australia; a las empresas extranjeras con licencia para operar en Australia; y a los propietarios o solicitantes de una marca comercial registrada en Australia. Los particulares no pueden registrar dominios.au. El contacto del solicitante de registro debe ser una empresa.
- Durante el proceso de registro, debe indicar la siguiente información:
 - El tipo de registro: ABN (Australian Business Number), ACN (Australian Company Number),) o TM (Trademark) si el nombre de dominio se corresponde con su marca comercial.

- Su número de ID, que puede ser un número de empresa australiana (ABN), número de compañía australiana (ACN), o marca comercial (TM).
- El nombre de su titular, que es el nombre de la entidad legal que registra los dominios. Este valor debe coincidir exactamente con el nombre del ABN (número de empresa australiana), ACN (número de compañía australiana) o TM (marca comercial) proporcionados.
- Su tipo de elegibilidad, que se refiere al tipo de entidad legal que registra el nombre de dominio.
- El motivo por el que se le permite registrar este nombre de dominio (motivo de la política):
 - El nombre de dominio coincide con la sigla o la abreviatura del nombre de la empresa, el nombre comercial, el nombre de la organización o asociación o la marca comercial del titular. (Motivo de la política 1)
 - El nombre de dominio cumple con las reglas de asignación, pero no es una sigla ni la abreviatura del nombre de la empresa, el nombre comercial, el nombre de la organización o asociación ni la marca comercial del titular. (Motivo de la política 2) Para ver las reglas de asignación de .au, consulte el ANEXO A del [registro .au](#).
- La información de contacto incorrecta o que no coincida, incluido el nombre, ABN o número de marca registrada (TM) provocará errores en el registro, la comercialización y las renovaciones. Es posible que se requiera un cambio de propiedad para corregir la información de los dominios existentes.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

No admitido. Le recomendamos que evite las transferencias no autorizadas restringiendo el acceso a la acción de la [RetrieveDomainAuthCode](#) API. (Al restringir el acceso a esta API de Route 53, también restringe quién puede generar un código de autorización mediante la consola de Route 53 y otros métodos programáticos). AWS SDKs Para obtener más información, consulte [Identity and Access Management en Amazon Route 53](#).

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Sí. Además de la consola de Route 53, también puede obtener el código de transferencia en el [registro .au](#).

DNSSEC

Admitido para el registro del dominio. Al configurar la clave, debe elegir el algoritmo de seguridad DNS 2 (DH). Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Es posible la renovación: entre 60 días antes del vencimiento y la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 29 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 29 días después del vencimiento
- Es posible restaurarlo a través del registro: No
- El dominio se elimina del registro: 30 días después del vencimiento

Eliminación de registro del dominio

La empresa de registro de dominios .au no permite eliminar registros de dominios. En lugar de ello, debe desactivar la renovación automática y esperar a que el dominio caduque. Para obtener más información, consulte [Eliminación de un registro de nombre de dominio](#).

Cambio de propiedad

Cambie el propietario utilizando la consola de Route 53. Consulte [Actualización de la información de contacto de un dominio](#). A continuación, complete el siguiente proceso para completar el cambio de propiedad:

1. Tanto los inscritos antiguos como los nuevos deben hacer clic en el enlace que reciben en un correo electrónico enviado por transfers@1api.net a las direcciones de correo electrónico que figuran en la lista. Si esto no se completa en un plazo de 14 días, tiene que iniciar el proceso de nuevo.
2. Una vez confirmadas las respuestas, el cambio de propietario en el registro se procesará en poco tiempo sin ninguna confirmación adicional.

.cc (Islas Cocos (Keeling))

[Return to index](#)

También se utiliza como TLD genérico, a menudo por las organizaciones con “cc” en sus nombres, como empresas de consultoría (consulting companies), empresas de informática en la nube (cloud computing companies) o clubes de ciclismo. La extensión es una alternativa popular a “.com”

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

Abierto al público, sin restricciones.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

- Oculto: dirección, número de teléfono, número de fax y dirección de correo electrónico
- No oculto: nombre de contacto y nombre de la organización

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 30 días y 60 días después del vencimiento
- El dominio se elimina del registro: 65 días después del vencimiento

.co.nz (Nueva Zelanda)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

Puede registrar los siguientes dominios de segundo nivel con Route 53: .co.nz, .net.nz y .org.nz. No puede registrar los dominios .nz (primer nivel) con Route 53 ni transferir dominios .nz a Route 53.

Abierto al público, con algunas restricciones:

- Los particulares deben tener al menos 18 años.
- Las organizaciones deben estar registradas.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

No admitido. Te recomendamos que impidas las transferencias no autorizadas restringiendo el acceso a la acción de la [RetrieveDomainAuthCode](#) API. (Al restringir el acceso a esta API de Route 53, también restringe quién puede generar un código de autorización mediante la consola de Route 53 y otros métodos programáticos). AWS SDKs Para obtener más información, consulte [Identity and Access Management en Amazon Route 53](#).

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 44 días después del vencimiento

- Es posible restaurarlo a través del registro: entre 44 y 134 días después del vencimiento
- El dominio se elimina del registro: 134 días después de la fecha de vencimiento

.com.au (Australia)

[Return to index](#)

Correo electrónico de confirmación de la empresa de registro del TLD

Nuestro registrador asociado, Gandi, revende los dominios.com.au a través de. DomainDirectors Cuando transfiere un nombre de dominio a Route 53, DomainDirectors envía un correo electrónico al contacto registrante del dominio para verificar la información de contacto o autorizar las solicitudes de transferencia.

Periodo de alquiler para el registro y la renovación

De uno a cinco años.

Restricciones

Abierto al público, con algunas restricciones:

- Los dominios .com.au y .net.au están abiertos a las sociedades o agentes independientes registrados en Australia; a las empresas extranjeras con licencia para operar en Australia; y a los propietarios o solicitantes de una marca comercial registrada en Australia. Las personas físicas no pueden registrar dominios .com.au o .net.au. El contacto del solicitante de registro debe ser una empresa.
- Su nombre de dominio debe ser idéntico a su nombre (tal como lo ha registrado en los organismos australianos pertinentes) o a su marca comercial (o abreviatura o acrónimo de su marca comercial).
- El nombre de dominio debe indicar su actividad. Por ejemplo, debe indicar un producto que vende o un servicio que proporciona.
- Durante el proceso de registro, debe proporcionar la siguiente información:
 - El tipo de registro: ABN (Australian Business Number), ACN (Australian Company Number),) o TM (Trademark) si el nombre de dominio se corresponde con su marca comercial.
 - Su número de ID que puede ser un número de empresa australiana (Australian Business Number, ABN), número de compañía australiana (Australian Company Number, ACN),) o marca registrada (Trademark, TM) si el nombre de dominio se corresponde con su marca comercial.

- El nombre de su titular, que es el nombre de la entidad legal que registra el dominio. Este valor debe coincidir exactamente con el nombre proporcionado.
- Su tipo de elegibilidad, que se refiere al tipo de entidad legal que registra este nombre de dominio.
- El motivo por el que se le permite registrar este nombre de dominio (motivo de la política):
 - El nombre de dominio coincide con la sigla o la abreviatura del nombre de la empresa, el nombre comercial, el nombre de la organización o asociación o la marca comercial del titular. (Motivo de la política 1)
 - El nombre de dominio cumple con las reglas de asignación, pero no es una sigla ni la abreviatura del nombre de la empresa, el nombre comercial, el nombre de la organización o asociación ni la marca comercial del titular. (Motivo de la política 2) Para ver las reglas de asignación de .com.au, consulte el ANEXO C del [registro .com.au](#).
- La información de contacto incorrecta o que no coincida, incluido el nombre, ABN o número de marca registrada (TM) provocará errores en el registro, la comercialización y las renovaciones. Es posible que se requiera un cambio de propiedad para corregir la información de los dominios existentes.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

No admitido. Le recomendamos que evite las transferencias no autorizadas restringiendo el acceso a la acción de la [RetrieveDomainAuthCode](#) API. (Al restringir el acceso a esta API de Route 53, también restringe quién puede generar un código de autorización mediante la consola de Route 53 y otros métodos programáticos). AWS SDKs Para obtener más información, consulte [Identity and Access Management en Amazon Route 53](#).

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Al configurar la clave, debe elegir el algoritmo de seguridad DNS 2 (DH). Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Es posible la renovación: entre 60 días antes del vencimiento y la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 29 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 29 días después del vencimiento
- Es posible restaurarlo a través del registro: No
- El dominio se elimina del registro: 30 días después del vencimiento

Eliminación de registro del dominio

La empresa de registro de dominios .com.au no permite eliminar registros de dominios. En lugar de ello, debe desactivar la renovación automática y esperar a que el dominio caduque. Para obtener más información, consulte [Eliminación de un registro de nombre de dominio](#).

Cambio de propiedad

Cambie el propietario, ya sea mediante programación o mediante la consola de Route 53. Consulte [Actualización de la información de contacto de un dominio](#). A continuación, complete el siguiente proceso para completar el cambio de propiedad:

1. Tanto los inscritos antiguos como los nuevos deben hacer clic en el enlace que reciben en un correo electrónico enviado por transfers@1api.net a las direcciones de correo electrónico que figuran en la lista. Si esto no se completa en un plazo de 14 días, tiene que iniciar el proceso de nuevo.
2. Una vez confirmadas las respuestas, el cambio de propietario en el registro se procesará en poco tiempo sin ninguna confirmación adicional.

.com.sg (República de Singapur)

Important

Ya no puede usar Route 53 para registrar nuevos dominios .com.sg o transferir dominios .com.sg a Route 53. Seguiremos ofreciendo soporte a dominios .com.sg que ya están registrados en Route 53.

[Return to index](#)

Período de renovación

Uno o dos años.

Eliminación de registro del dominio

La empresa de registro de dominios .com.sg no permite eliminar registros de dominios. En lugar de ello, debe desactivar la renovación automática y esperar a que el dominio caduque. Para obtener más información, consulte [Eliminación de un registro de nombre de dominio](#).

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Código de autorización necesario para transferencias

No admitido. Ya no se pueden transferir dominios .com.sg a Route 53.

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 29 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 30 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 30 días y 60 días después del vencimiento
- El dominio se elimina del registro: 60 días después del vencimiento

.fm (Estados Federados de Micronesia)

También se utiliza como TLD genérico, a menudo por las organizaciones relacionadas con medios de comunicación y radiodifusión online.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

Abierto al público, sin restricciones.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 44 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 44 días y 79 días después del vencimiento
- El dominio se elimina del registro: 84 días después del vencimiento

.in (India)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

Abierto al público, sin restricciones.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Sí

DNSSEC

No admitido.

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 29 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 30 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 30 días y 60 días después del vencimiento
- El dominio se elimina del registro: 65 días después del vencimiento

.jp (Japón)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

Un año.

Restricciones

Abierto al público, con una restricción:

- Solo los particulares o las empresas de Japón pueden registrar un nombre de dominio .jp.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

No admitido. Te recomendamos que impidas las transferencias no autorizadas restringiendo el acceso a la acción de la [RetrieveDomainAuthCode](#) API. (Al restringir el acceso a esta API de Route 53, también restringe quién puede generar un código de autorización mediante la consola de Route 53 y otros métodos programáticos). AWS SDKs Para obtener más información, consulte [Identity and Access Management en Amazon Route 53](#).

Nombres de dominio internacionalizados

Admitidos para japonés.

Código de autorización necesario para transferencias

Sí.

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- La renovación es posible: hasta 16 días antes de la fecha de caducidad
- La renovación tardía con Route 53 es posible: No
- El dominio se elimina de Route 53: 6 días antes del vencimiento
- Es posible restaurarlo a través del registro: póngase en contacto con [AWS Support](#).
- El dominio se ha eliminado del registro: póngase en contacto con [AWS Support](#).

Note

Por el non-general-purpose momento, no es posible registrar dominios japoneses como .co.jp y .or.jp.

.io (Territorio Británico del Océano Índico)

También se utiliza como TLD genérico, a menudo por organizaciones relacionadas con la informática, como servicios online, juegos basados en navegador y empresas startup.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

Abierto al público, sin restricciones.

Protección de la privacidad

Toda la información está oculta excepto el país. state/province

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

El registro de dominios .io también utiliza el código de autorización como contraseña de un solo uso en determinadas operaciones como, por ejemplo, para activar o desactivar la protección de privacidad. Si desea realizar más de una operación que requiere una contraseña, deberá generar otro código de autorización para cada operación.

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 90 días después de la fecha de vencimiento

.net.au (Australia)

[Return to index](#)

Correo electrónico de confirmación de la empresa de registro del TLD

Nuestro registrador asociado, Gandi, revende dominios.net.au a través de. DomainDirectors
Cuando transfiere un nombre de dominio a Route 53, DomainDirectors envía un correo electrónico al contacto registrante del dominio para verificar la información de contacto o autorizar las solicitudes de transferencia.

Periodo de alquiler para el registro y la renovación

De uno a cinco años.

Restricciones

Solo están disponibles los dominios de segundo nivel. Route 53 admite los dominios de segundo nivel .com.au y net.au.

Abierto al público, con algunas restricciones:

- Los dominios .com.au y .net.au están abiertos a las personas jurídicas, empresas mercantiles, sociedades o agentes independientes registrados en Australia; a las empresas extranjeras con licencia para operar en Australia; y a los propietarios o solicitantes de una marca comercial registrada en Australia.
- Su nombre de dominio debe ser idéntico a su nombre (tal como lo ha registrado en los organismos australianos pertinentes) o a su marca comercial (o abreviatura o acrónimo).
- El nombre de dominio debe indicar su actividad. Por ejemplo, debe indicar un producto que vende o un servicio que proporciona.
- Durante el proceso de registro, debe indicar la siguiente información:
 - El tipo de registro: ABN (Australian Business Number), ACN (Australian Company Number),) o TM (Trademark) si el nombre de dominio se corresponde con su marca comercial.
 - Su número de ID que puede ser un número de empresa australiana (Australian Business Number, ABN), número de compañía australiana (Australian Company Number, ACN),) o marca registrada (Trademark, TM) si el nombre de dominio se corresponde con su marca comercial.
 - El nombre de su titular, que es el nombre de la entidad legal que registra el dominio. Este valor debe coincidir exactamente con el nombre proporcionado.

- Su tipo de elegibilidad, que se refiere al tipo de entidad legal que registra este nombre de dominio.
- El motivo por el que se le permite registrar este nombre de dominio (motivo de la política):
 - El nombre de dominio coincide con la sigla o la abreviatura del nombre de la empresa, el nombre comercial, el nombre de la organización o asociación o la marca comercial del titular. (Motivo de la política 1)
 - El nombre de dominio cumple con las reglas de asignación, pero no es una sigla ni la abreviatura del nombre de la empresa, el nombre comercial, el nombre de la organización o asociación ni la marca comercial del titular. (Motivo de la política 2) Para ver las reglas de asignación de .net.au, consulte el ANEXO E del [registro de net.au](#).
- La información de contacto incorrecta o que no coincida, incluido el nombre, ABN o número de marca registrada (TM) provocará errores en el registro, la comercialización y las renovaciones. Es posible que se requiera un cambio de propiedad para corregir la información de los dominios existentes.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

No admitido. Le recomendamos que evite las transferencias no autorizadas restringiendo el acceso a la acción de la [RetrieveDomainAuthCode](#) API. (Al restringir el acceso a esta API de Route 53, también restringe quién puede generar un código de autorización mediante la consola de Route 53 y otros métodos programáticos). AWS SDKs Para obtener más información, consulte [Identity and Access Management en Amazon Route 53](#).

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Al configurar la clave, debe elegir el algoritmo de seguridad DNS 2 (DH). Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Es posible la renovación: entre 60 días antes del vencimiento y la fecha de vencimiento

- Es posible la renovación tardía con Route 53: hasta 29 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 29 días después del vencimiento
- Es posible restaurarlo a través del registro: No
- El dominio se elimina del registro: 30 días después del vencimiento

Eliminación de registro del dominio

La empresa de registro de dominios .net.au no permite eliminar registros de dominios. En lugar de ello, debe desactivar la renovación automática y esperar a que el dominio caduque. Para obtener más información, consulte [Eliminación de un registro de nombre de dominio](#).

Cambio de propiedad

Cambie el propietario, ya sea mediante programación o mediante la consola de Route 53.

Consulte [Actualización de la información de contacto de un dominio](#). A continuación, complete el siguiente proceso para completar el cambio de propiedad:

1. Tanto los inscritos antiguos como los nuevos deben hacer clic en el enlace que reciben en un correo electrónico enviado por transfers@1api.net a las direcciones de correo electrónico que figuran en la lista. Si esto no se completa en un plazo de 14 días, tiene que iniciar el proceso de nuevo.
2. Una vez confirmadas las respuestas, el cambio de propietario en el registro se procesará en poco tiempo sin ninguna confirmación adicional.

.net.nz (Nueva Zelanda)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

Puede registrar los siguientes dominios de segundo nivel con Route 53: .co.nz, .net.nz y .org.nz. No puede registrar los dominios .nz (primer nivel) con Route 53 ni transferir dominios .nz a Route 53.

Abierto al público, con algunas restricciones:

- Los particulares deben tener al menos 18 años.
- Las organizaciones deben estar registradas.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

No admitido. Te recomendamos que impidas las transferencias no autorizadas restringiendo el acceso a la acción de la [RetrieveDomainAuthCode](#) API. (Al restringir el acceso a esta API de Route 53, también restringe quién puede generar un código de autorización mediante la consola de Route 53 y otros métodos programáticos). AWS SDKs Para obtener más información, consulte [Identity and Access Management en Amazon Route 53](#).

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 44 días después del vencimiento
- Es posible restaurarlo a través del registro: entre 44 y 134 días después del vencimiento
- El dominio se elimina del registro: 134 días después de la fecha de vencimiento

.org.nz (Nueva Zelanda)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

Puede registrar los siguientes dominios de segundo nivel con Route 53: .co.nz, .net.nz y .org.nz. No puede registrar los dominios .nz (primer nivel) con Route 53 ni transferir dominios .nz a Route 53.

Abierto al público, con algunas restricciones:

- Los particulares deben tener al menos 18 años.
- Las organizaciones deben estar registradas.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

No admitido. Le recomendamos que impida las transferencias no autorizadas restringiendo el acceso a la acción de la [RetrieveDomainAuthCode](#) API. (Al restringir el acceso a esta API de Route 53, también restringe quién puede generar un código de autorización mediante la consola de Route 53 y otros métodos programáticos). AWS SDKs Para obtener más información, consulte [Identity and Access Management en Amazon Route 53](#).

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 44 días después del vencimiento
- Es posible restaurarlo a través del registro: entre 44 y 134 días después del vencimiento

- El dominio se elimina del registro: 134 días después de la fecha de vencimiento

.pw (Palau)

[Return to index](#)

El dominio .pw estaba originalmente reservado para los residentes de Palau, un país insular en la subregión de Micronesia de Oceanía, en el Pacífico occidental; sin embargo, ahora se usa comúnmente para representar “Web profesional” y está disponible para todos.

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Protección de la privacidad (se aplica a todos los tipos de contacto: persona, empresa, asociación y organismo público)

Toda la información está oculta, excepto el nombre de la organización.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 75 días después del vencimiento

.qa (Qatar)

Important

Ya no puede usar Route 53 para registrar nuevos dominios .qa o transferir dominios .qa a Route 53. Seguiremos ofreciendo soporte a dominios .qa que ya están registrados en Route 53.

[Return to index](#)

Período de renovación

De uno a cinco años.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

No admitido. Le recomendamos que impida las transferencias no autorizadas restringiendo el acceso a la acción de la [RetrieveDomainAuthCode](#) API. (Al restringir el acceso a esta API de Route 53, también restringe quién puede generar un código de autorización mediante la consola de Route 53 y otros métodos programáticos). AWS SDKs Para obtener más información, consulte [Identity and Access Management en Amazon Route 53](#).

Código de autorización necesario para transferencias

No admitido. Ya no se pueden transferir dominios .qa a Route 53.

DNSSEC

No admitido.

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 29 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 30 días después del vencimiento
- Es posible restaurarlo a través del registro: No

- El dominio se elimina del registro: 31 días después del vencimiento

.ru (Federación Rusa)

 Important

Ya no puede usar Route 53 para registrar nuevos dominios .ru o transferir dominios .ru a Route 53. Seguiremos ofreciendo soporte a dominios .ru que ya están registrados en Route 53.

[Return to index](#)

Periodo de alquiler para el registro y la renovación

Un año.

 Note

La empresa de registro de dominios .ru actualiza la fecha de vencimiento de un dominio el día del vencimiento del dominio. Las consultas de WHOIS mostrarán la fecha de vencimiento anterior del dominio hasta dicha fecha, independientemente de cuándo renueve el dominio con Route 53.

Restricciones

Abierto al público, con algunas restricciones:

- Es posible que los particulares necesiten proporcionar un número de pasaporte o número de identificación emitido por el gobierno.
- Las empresas extranjeras tal vez tengan que proporcionar un ID o número de registro de la empresa.

Protección de la privacidad

Determinada por la empresa de registro.

Bloqueo de dominio para evitar transferencias no autorizadas

No admitido. Le recomendamos que impida las transferencias no autorizadas restringiendo el acceso a la acción de la [RetrieveDomainAuthCode](#) API. (Al restringir el acceso a esta API de

Route 53, también restringe quién puede generar un código de autorización mediante la consola de Route 53 y otros métodos programáticos). AWS SDKs Para obtener más información, consulte [Identity and Access Management en Amazon Route 53](#).

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

No admitido. Ya no se pueden transferir dominios .ru a Route 53.

DNSSEC

No admitido.

Plazos para renovar y restaurar dominios

- Es posible la renovación: Hasta 2 días antes de la fecha de vencimiento
- La renovación tardía con Route 53 es posible: No
- El dominio se elimina de Route 53: 2 días antes del vencimiento
- Es posible restaurarlo a través del registro: Entre 2 días antes y 28 días después del vencimiento
- El dominio se elimina del registro: 28 días después del vencimiento

Eliminación de registro del dominio

La empresa de registro de dominios .ru no permite eliminar registros de dominios. En lugar de ello, debe desactivar la renovación automática y esperar a que el dominio caduque. Para obtener más información, consulte [Eliminación de un registro de nombre de dominio](#).

.sg (República de Singapur)

Important

Ya no puede usar Route 53 para registrar nuevos dominios .sg o transferir dominios .sg a Route 53. Seguiremos ofreciendo soporte a dominios .sg que ya están registrados en Route 53.

[Return to index](#)

.be (Bélgica)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

Un año.

Restricciones

Abierto al público, sin restricciones.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí. Puede obtener el código de transferencia en el [sitio web de DNS Bélgica](#).

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- La renovación tardía con Route 53 es posible: No
- Se elimina el dominio de Route 53: en la fecha de vencimiento
- Es posible restaurarlo a través del registro: Hasta 40 días después del vencimiento
- El dominio se elimina del registro: 40 días después del vencimiento

.berlin (ciudad de Berlín de Alemania)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

Abierto al público, con algunas restricciones:

- El propietario, contacto administrativo o contacto técnico debe proporcionar una dirección de contacto en Berlín y el contacto administrativo debe ser una persona.
- Debe activar y utilizar su dominio .berlin en un plazo de 12 meses a partir de su registro (se aplica a un sitio web, redirección o dirección de correo electrónico).
- Si publica un sitio web bajo su dominio .berlin, o si su dominio .berlin redirige a otro sitio web, el contenido del sitio web debe estar relacionado con Berlín.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alfabeto latino y cirílico.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 80 días después de la fecha de vencimiento

.ch (Suiza)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

Un año.

Restricciones

Abierto al público, sin restricciones.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

No admitido. Le recomendamos que impida las transferencias no autorizadas restringiendo el acceso a la acción de la [RetrieveDomainAuthCode](#) API. (Al restringir el acceso a esta API de Route 53, también restringe quién puede generar un código de autorización mediante la consola de Route 53 y otros métodos programáticos). AWS SDKs Para obtener más información, consulte [Identity and Access Management en Amazon Route 53](#).

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 9 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 9 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 9 días y 49 días después del vencimiento
- El dominio se elimina del registro: 49 días después del vencimiento

.co.uk (Reino Unido)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

Abierto al público, sin restricciones.

Protección de la privacidad

Toda la información está oculta.

Bloqueo de dominio para evitar transferencias no autorizadas

compatible

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Si va a transferir un dominio .co.uk a Route 53, no es necesario que obtenga un código de autorización. En lugar de ello, use el método proporcionado por el registrador del dominio actual para actualizar el valor de la etiqueta IPS del dominio a GANDI (con todos los caracteres en mayúsculas). (Nominet, la empresa de registro de nombres de dominio .uk, requiere una etiqueta IPS). Si su registrador no va a cambiar el valor de la etiqueta IPS, [póngase en contacto con Nominet](#).

 Note

Cuando registra un dominio .co.uk, Route 53 ajusta automáticamente la etiqueta IPS del dominio en GANDI.

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Es posible la renovación: Entre 180 días antes y 30 días después de la fecha de vencimiento

- Es posible la renovación tardía con Route 53: entre 30 días y 90 días después del vencimiento
- El dominio se elimina de Route 53: 90 días después del vencimiento
- Es posible restaurarlo a través del registro: No
- El dominio se elimina del registro: 92 días después del vencimiento

Eliminación de registro del dominio

La empresa de registro de dominios .co.uk no permite eliminar registros de dominios. En lugar de ello, debe desactivar la renovación automática y esperar a que el dominio caduque. Para obtener más información, consulte [Eliminación de un registro de nombre de dominio](#).

.cz (Czech Republic)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

Abierto al público, sin restricciones.

Protección de la privacidad

No se admite, pero la dirección de correo electrónico y el número de teléfono están ocultos para todos los contactos.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Sí

Si el registrador actual no proporciona un código de autorización, vaya a <https://www.nic.cz/whois/send-password/> para solicitar que el registro de dominios CZ lo envíe a la dirección de correo electrónico del solicitante.

DNSSEC

No admitido.

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 58 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 59 días después del vencimiento
- Es posible restaurarlo a través del registro: No
- El dominio se elimina del registro: 60 días después del vencimiento

.de (Alemania)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

Un año.

Restricciones

Abierto al público, con algunas restricciones:

- Debe residir en Alemania o tener un contacto administrativo (persona física) que resida en Alemania y tener una dirección que no sea un apartado de correos.
- Durante el registro, el DNS (A, MX y CNAME) del nombre de dominio debe estar configurado correctamente para que pueda superar la comprobación de zona de la empresa de registro. Se requieren tres servidores de clases C diferentes.
- Si utiliza un servicio DNS distinto de Route 53, los servidores de nombres del dominio deben pasar una comprobación para asegurarse de que están configurados correctamente. Para determinar si los servidores de nombres de su dominio pasarán la comprobación, consulte <https://www.denic.de/en/service/tools/nast/>.
- Debe proporcionar información de contacto que cumpla con los requisitos de validación del registro. Los datos de contacto no válidos o con un formato incorrecto pueden provocar que no se puedan renovar los dominios.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

No admitido. Le recomendamos que impida las transferencias no autorizadas restringiendo el acceso a la acción de la [RetrieveDomainAuthCode](#) API. (Al restringir el acceso a esta API de Route 53, también restringe quién puede generar un código de autorización mediante la consola de Route 53 y otros métodos programáticos). AWS SDKs Para obtener más información, consulte [Identity and Access Management en Amazon Route 53](#).

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- La renovación tardía con Route 53 es posible: No
- Se elimina el dominio de Route 53: en la fecha de vencimiento
- Es posible restaurarlo a través del registro: póngase en contacto con [AWS Support](#).
- El dominio se ha eliminado del registro: póngase en contacto con [AWS Support](#).

.es (España)

[Return to index](#)

Compra o transferencia del dominio

Important

Actualmente, puede comprar nuevos nombres de dominio .es o transferir dominios .es a Route 53. El tipo de contacto para el contacto del registrador no tiene ninguna restricción. El tipo de contacto administrativo, técnico o de facturación debe ser una persona.

Periodo de alquiler para el registro y la renovación

De uno a cinco años.

Restricciones

Abierto al público, para aquellas personas interesadas en España o que guardan alguna relación con España.

A partir de 2016, los solicitantes del dominio .ES deberán proporcionar un correo electrónico de contacto. Si no ha proporcionado esta información, debe hacerlo en el registrador actual antes de transferir su dominio a Route 53.

Necesitará la siguiente información:

- Identificador de ESNIC similar a. *AAAA0-ESNIC-F0*
- Si no conoce su identificador ESNIC, puede obtenerlo del registrador actual. Puede encontrar su registrador en: <https://www.dominios.es/en>.

En función de si recuerda o no su contraseña en el registrador, puede seguir uno de los siguientes procedimientos para actualizar el correo electrónico del solicitante:

- Si recuerda su contraseña, inicie sesión en <https://www.nic.es/sgnd/login.action> utilizando su nombre de usuario y contraseña de ESNIC.

Una vez que haya iniciado sesión, podrá editar el contacto de correo electrónico del solicitante al seleccionar la pestaña Editar de la página de registro.

- Si ha olvidado su contraseña, vaya a https://www.nic.es/sgnd/peticion/editCorreo¿.acción?request_locale=es.

Complete el formulario con su identificador de ESNIC, su correo electrónico de contacto nuevo y válido para registrarse. A continuación, valide el formulario al seleccionar Procesamiento sin eID/Certificate y cargue el documento de identidad solicitado.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

compatible

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

El registro.es gestiona el código de autorización con un time-to-live y es posible que haya caducado. Puedes actualizar el código de autenticación quitando el estado de bloqueo de transferencia (clientTransferProhibited) de tu dominio, si está presente. Si el dominio no tiene ningún bloqueo de transferencia, puede actualizar el código de autorización, para lo cual debe activarlo y luego desactivarlo.

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Es posible la renovación: Hasta 6 días antes de la fecha de vencimiento
- La renovación tardía con Route 53 es posible: No
- El dominio se elimina de Route 53: 6 días antes del vencimiento
- Es posible restaurarlo a través del registro: Entre 6 días antes y 4 días después del vencimiento
- El dominio se elimina del registro: 4 días después del vencimiento

.eu (Unión Europea)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

Abierto al público, con una restricción:

- Debe proporcionar una dirección postal válida de uno de los 30 Estados del Espacio Económico Europeo (EEE) o, si es ciudadano de uno de los 27 Estados miembros de la Unión Europea (UE), debe especificar su país de ciudadanía de la UE.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

No admitido. Te recomendamos que impidas las transferencias no autorizadas restringiendo el acceso a la acción de la [RetrieveDomainAuthCodeAPI](#). (Al restringir el acceso a esta API de Route 53, también restringe quién puede generar un código de autorización mediante la consola de Route 53 y otros métodos programáticos). AWS SDKs Para obtener más información, consulte [Identity and Access Management en Amazon Route 53](#).

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

También puede generar el código de autenticación mediante el panel “My.eu” del registro: <https://my.eurid.eu/>.

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- La renovación tardía con Route 53 es posible: No
- Se elimina el dominio de Route 53: en la fecha de vencimiento
- Es posible restaurarlo a través del registro: Hasta 40 días después del vencimiento
- El dominio se elimina del registro: 40 días después del vencimiento

Búsqueda en WHOIS

Para obtener información sobre dominios .eu existentes, consulte <https://whois.eurid.eu/en/>.

.fi (Finlandia)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a cinco años.

Restricciones

Abierto al público, con algunas restricciones:

- La extensión .fi está disponible para las personas que tienen domicilio en Finlandia y poseen un número de identidad finlandés, y para las personas jurídicas o empresarios privados registrados en Finlandia.
- Si la dirección de contacto de la titularidad se encuentra en Finlandia, se requiere el número de identidad finlandés para la titularidad individual y el número de compañía finlandesa para el registro de una compañía, y se debe proporcionar la siguiente información durante el registro:
 - Si el contacto es o no es una persona física o jurídica en Finlandia.
 - El identificador del registro donde está registrado el nombre, si se trata del nombre de una persona jurídica.
 - El número de registro del nombre, si se trata del nombre de una persona jurídica.
 - El número de identificación de una persona jurídica en Finlandia.
 - El número de identificación de una persona física en Finlandia.
 - Si el registrador es una empresa no finlandesa, debe proporcionar su número de empresa como número de IVA.
- Si la dirección del registrante no se encuentra en Finlandia, entonces no se requiere una identidad finlandesa ni un número de compañía.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

No admitido. Le recomendamos que impida las transferencias no autorizadas restringiendo el acceso a la acción de la [RetrieveDomainAuthCode](#) API. (Al restringir el acceso a esta API de Route 53, también restringe quién puede generar un código de autorización mediante la consola de Route 53 y otros métodos programáticos). AWS SDKs Para obtener más información, consulte [Identity and Access Management en Amazon Route 53](#).

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 29 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 30 días después del vencimiento
- Es posible restaurarlo a través del registro: No
- El dominio se elimina del registro: No

Eliminación de registro del dominio

Para obtener más información sobre la eliminación de dominios, consulte [Eliminación de un registro de nombre de dominio](#).

.fr (Francia)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

Abierto al público, con algunas restricciones:

- Las personas deben tener al menos 18 años y deben proporcionar su date-of-birth
- Las organizaciones deben estar emplazadas en el Espacio Económico Europeo o en Suiza.
- Las organizaciones deben rellenar todos los campos de identificación de la empresa (número de IVA, SIREN, WALDEC, DUNS, etc.), ya que esto facilitará cualquier verificación que AFNIC pueda realizar posteriormente.
- Los mismos requisitos se aplican al contacto administrativo.
- Los nombres y términos están sujetos a una revisión previa de AFNIC (Artículo del reglamento de nomenclatura 2.4) y a las siguientes condiciones adicionales:

- Los nombres de dominio reservados previamente o prohibidos están abiertos a los solicitantes que justifiquen un derecho legítimo y actúen de buena fe.
- Los nombres que empiezan por ville, mairie, agglo, cc, cg y cr están sujetos a las convenciones de nomenclatura de AFNIC.

Protección de la privacidad

Determinada por la empresa de registro.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 27 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 28 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 28 días y 58 días después del vencimiento
- El dominio se elimina del registro: 58 días después del vencimiento

.gg (Guernsey)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

Un año.

Restricciones

Abierto al público, sin restricciones.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 29 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 30 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 30 días y 35 días después del vencimiento
- El dominio se elimina del registro: 35 días después del vencimiento

.im (Isla de Man)

También se utiliza como TLD genérico, a menudo por servicios de mensajería instantánea o personas que desea desarrollar una marca personal “I am” (yo soy).

[Return to index](#)

Periodo de alquiler para el registro y la renovación

Uno o dos años.

Restricciones

Abierto al público, sin restricciones.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Sí

DNSSEC

No admitido.

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 29 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 30 días después del vencimiento
- Es posible restaurarlo a través del registro: No
- El dominio se elimina del registro: 30 días después del vencimiento

.it (Italia)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

Un año.

Restricciones

Abierto al público, con algunas restricciones:

- Los particulares o las organizaciones deben tener una dirección registrada en la Unión Europea.
- Si su país de origen es Italia, debe indicar un código fiscal. Si su país de origen está dentro de la Unión Europea, debe indicar un número de documento de identidad.
- Los servidores de nombres de su dominio deben superar una comprobación de DNS. Le recomendamos que revise los servidores de nombres en <https://dns-check.nic.it/> antes de enviar la solicitud de cambio. Si su nombre de dominio no cumple los requisitos técnicos (por ejemplo, no está asociado a un servidor de nombres operativo) y no corrige esta situación en un plazo de 30 días, la empresa de registro eliminará su nombre de dominio. No emitimos reembolsos por dominios que se hayan eliminado por no cumplir los requisitos técnicos.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

No admitido. Te recomendamos que impidas las transferencias no autorizadas restringiendo el acceso a la acción de la [RetrieveDomainAuthCodeAPI](#). (Al restringir el acceso a esta API de Route 53, también restringe quién puede generar un código de autorización mediante la consola de Route 53 y otros métodos programáticos). AWS SDKs Para obtener más información, consulte [Identity and Access Management en Amazon Route 53](#).

Nombres de dominio internacionalizados

Soportado.

Código de autorización necesario para transferencias

Sí

DNSSEC

No admitido.

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: Hasta 13 días después de la fecha de vencimiento
- El dominio se elimina del registro: 49 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 14 días y 44 días después del vencimiento
- El dominio se ha eliminado del registro: póngase en contacto con [AWS Support](#).

.me (Montenegro)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

Domain.me, la empresa de registro de dominios .me, considera nombres de dominio premium los nombres de dominio de dos letras y algunos nombres más largos. No puede registrar dominios .me premium ni transferirlos a Route 53. Para obtener más información sobre nombres de dominio .me premium, consulte el sitio web de domain.me.

Protección de la privacidad

Toda la información está oculta.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Compatible con alemán, árabe, bielorruso, bosnio, búlgaro, chino simplificado, chino tradicional, coreano, croata, danés, español, francés, hindi, húngaro, islandés, italiano, letón, lituano, mongol, polaco, portugués, ruso, serbio, sueco, turco y ucraniano.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 29 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 30 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 30 días y 60 días después del vencimiento
- El dominio se elimina del registro: 65 días después del vencimiento

.me.uk (Reino Unido)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

Abierto al público, sin restricciones.

Protección de la privacidad

Toda la información está oculta.

Bloqueo de dominio para evitar transferencias no autorizadas

compatible

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Si va a transferir un dominio .me.uk a Route 53, no es necesario que obtenga un código de autorización. En lugar de ello, use el método proporcionado por el registrador del dominio actual para actualizar el valor de la etiqueta IPS del dominio a GANDI (con todos los caracteres en mayúsculas). (Nominet, la empresa de registro de nombres de dominio .uk, requiere una etiqueta IPS). Si su registrador no va a cambiar el valor de la etiqueta IPS, [póngase en contacto con Nominet](#).

 Note

Cuando registra un dominio .me.uk, Route 53 ajusta automáticamente la etiqueta IPS del dominio en GANDI.

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Es posible la renovación: Entre 180 días antes y 30 días después de la fecha de vencimiento
- Es posible la renovación tardía con Route 53: entre 30 días y 90 días después del vencimiento
- El dominio se elimina de Route 53: 90 días después del vencimiento
- Es posible restaurarlo a través del registro: No
- El dominio se elimina del registro: 92 días después del vencimiento

Eliminación de registro del dominio

La empresa de registro de dominios .me.uk no permite eliminar registros de dominios. En lugar de ello, debe desactivar la renovación automática y esperar a que el dominio caduque. Para obtener más información, consulte [Eliminación de un registro de nombre de dominio](#).

.nl (Países Bajos)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

Un año.

Restricciones

Abierto al público, con algunas restricciones:

- El propietario o el contacto administrativo deben proporcionar una dirección válida en los Países Bajos. Se requiere presencia local.
- Si no tiene una dirección válida en los Países Bajos, la empresa de registro SIDN le proporcionará una dirección de domicilio, de acuerdo con el procedimiento de direcciones de domicilio.
- El nombre de dominio debe tener entre 3 y 63 caracteres, excluyendo .nl.

Protección de la privacidad

Determinada por la empresa de registro.

Bloqueo de dominio para evitar transferencias no autorizadas

No admitido. Le recomendamos que impida las transferencias no autorizadas restringiendo el acceso a la acción de la [RetrieveDomainAuthCode](#)API. (Al restringir el acceso a esta API de

Route 53, también restringe quién puede generar un código de autorización mediante la consola de Route 53 y otros métodos programáticos). AWS SDKs Para obtener más información, consulte [Identity and Access Management en Amazon Route 53](#).

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Es posible la renovación: Hasta 1 día antes de la fecha de vencimiento
- La renovación tardía con Route 53 es posible: No
- El dominio se elimina de Route 53: 1 día antes de la fecha de vencimiento
- Es posible restaurarlo a través del registro: Entre 1 día antes y 39 días después del vencimiento
- El dominio se elimina del registro: 39 días después del vencimiento

.org.uk (Reino Unido)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

Abierto al público, sin restricciones.

Protección de la privacidad

Toda la información está oculta.

Bloqueo de dominio para evitar transferencias no autorizadas

compatible

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Si va a transferir un dominio .org.uk a Route 53, no es necesario que obtenga un código de autorización. En lugar de ello, use el método proporcionado por el registrador del dominio actual para actualizar el valor de la etiqueta IPS del dominio a GANDI (con todos los caracteres en mayúsculas). (Nominet, la empresa de registro de nombres de dominio .uk, requiere una etiqueta IPS). Si su registrador no va a cambiar el valor de la etiqueta IPS, [póngase en contacto con Nominet](#).

Note

Cuando registra un dominio .org.uk, Route 53 establece automáticamente la etiqueta IPS del dominio en GANDI.

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Es posible la renovación: Entre 180 días antes y 30 días después de la fecha de vencimiento
- Es posible la renovación tardía con Route 53: entre 30 días y 90 días después del vencimiento
- El dominio se elimina de Route 53: 90 días después del vencimiento
- Es posible restaurarlo a través del registro: No
- El dominio se elimina del registro: 92 días después del vencimiento

Eliminación de registro del dominio

La empresa de registro de dominios .org.uk no permite eliminar registros de dominios. En lugar de ello, debe desactivar la renovación automática y esperar a que el dominio caduque. Para obtener más información, consulte [Eliminación de un registro de nombre de dominio](#).

.ruhr (región del Ruhr, parte occidental de Alemania)

[Return to index](#)

La extensión .ruhr es para la región del Ruhr (parte occidental de Alemania).

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

Abierto al público, con una restricción:

- El contacto administrativo debe ser una persona que tenga una dirección en Alemania.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos (ä, ö, ü, ß).

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se ha eliminado del registro: póngase en contacto con [AWS Support](#).

.se (Suecia)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

Abierto al público, con algunas restricciones:

- Si se encuentra en Suecia, debe proporcionar un número de identificación sueco válido. El formato del número de ID es YYMMDD-NNNN.
- Si se encuentra fuera de Suecia, debe indicar un número de identificación válido, como un número de identificación fiscal.

Requisitos de verificación adicionales

A partir del 1 de octubre de 2025, los registros de dominios .se requerirán una verificación de identidad adicional para cumplir con los nuevos requisitos de NIS 2.0 del registro. Cuando registre un dominio .se, nos pondremos en contacto con usted para solicitarle los documentos de verificación. El registro de su dominio permanecerá pendiente hasta que proporcione los documentos necesarios y se complete la verificación. Para enviar sus documentos, [póngase en contacto con AWS Support](#).

El registro .se también lleva a cabo auditorías periódicas de los dominios existentes y puede que solicite una verificación adicional de los dominios registrados recientemente o cuando haga ciertos cambios en su dominio (como actualizar el propietario del dominio o la información de contacto). Si su dominio aparece en estado `serverHold`, significa que el registro requiere una verificación antes de que el dominio pueda activarse por completo.

Documentos que deberá proporcionar:

- Para personas físicas: un documento de identidad emitido por el gobierno (como un documento de identidad o un pasaporte) y un comprobante de domicilio de menos de 3 meses de antigüedad.
- Para empresas u organizaciones: el certificado de registro de la empresa u organización y comprobante de domicilio si difiere del certificado de registro.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

No admitido. Te recomendamos que impidas las transferencias no autorizadas restringiendo el acceso a la acción de la [RetrieveDomainAuthCodeAPI](#). (Al restringir el acceso a esta API de

Route 53, también restringe quién puede generar un código de autorización mediante la consola de Route 53 y otros métodos programáticos). AWS SDKs Para obtener más información, consulte [Identity and Access Management en Amazon Route 53](#).

Nombres de dominio internacionalizados

Admitidos para alfabeto latino, sueco y yiddish.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Es posible la renovación: Hasta 1 día antes de la fecha de vencimiento
- La renovación tardía con Route 53 es posible: No
- El dominio se elimina de Route 53: 1 día antes de la fecha de vencimiento
- Es posible restaurarlo a través del registro: Entre 1 día antes y 59 días después del vencimiento
- El dominio se elimina del registro: 64 días después del vencimiento

.uk (Reino Unido)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

Abierto al público, sin restricciones.

Protección de la privacidad

Toda la información está oculta.

Bloqueo de dominio para evitar transferencias no autorizadas

compatible

Nombres de dominio internacionalizados

No admitido.

Código de autorización necesario para transferencias

Si va a transferir un dominio .uk a Route 53, no es necesario que obtenga un código de autorización. En lugar de ello, use el método proporcionado por el registrador del dominio actual para actualizar el valor de la etiqueta IPS del dominio a GANDI (con todos los caracteres en mayúsculas). (Nominet, la empresa de registro de nombres de dominio .uk, requiere una etiqueta IPS). Si su registrador no va a cambiar el valor de la etiqueta IPS, [póngase en contacto con Nominet](#).

Note

Cuando registra un dominio .uk, Route 53 ajusta automáticamente la etiqueta IPS del dominio a GANDI.

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Es posible la renovación: Entre 180 días antes y 30 días después de la fecha de vencimiento
- Es posible la renovación tardía con Route 53: entre 30 días y 90 días después del vencimiento
- El dominio se elimina de Route 53: 90 días después del vencimiento
- Es posible restaurarlo a través del registro: No
- El dominio se elimina del registro: 92 días después del vencimiento

Eliminación de registro del dominio

La empresa de registro de dominios .uk no permite eliminar registros de dominios. En lugar de ello, debe desactivar la renovación automática y esperar a que el dominio caduque. Para obtener más información, consulte [Eliminación de un registro de nombre de dominio](#).

.wien (ciudad de Viena en Austria)

[Return to index](#)

Periodo de alquiler para el registro y la renovación

De uno a diez años.

Restricciones

Abierto al público, con algunas restricciones:

- Debe mostrar una relación económica, cultural, histórica, social u otra afinidad con la ciudad austriaca de Viena.
- Los nombres de dominio .wien se deben utilizar con arreglo a las condiciones anteriores, durante todo el periodo del registro.

Protección de la privacidad

No admitido.

Bloqueo de dominio para evitar transferencias no autorizadas

Soportado.

Nombres de dominio internacionalizados

Admitidos para alfabeto latino.

Código de autorización necesario para transferencias

Sí

DNSSEC

Admitido para el registro del dominio. Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

Plazos para renovar y restaurar dominios

- Se puede renovar: Hasta la fecha de vencimiento
- Es posible la renovación tardía con Route 53: hasta 44 días después de la fecha de vencimiento
- El dominio se elimina de Route 53: 45 días después del vencimiento
- Es posible restaurarlo a través del registro: Entre 45 días y 75 días después del vencimiento
- El dominio se elimina del registro: 80 días después de la fecha de vencimiento

Configuración de Amazon Route 53 como servicio DNS

Puede utilizar Amazon Route 53 como el servicio DNS de su dominio, como example.com. Cuando Route 53 es su servicio DNS, dirige el tráfico de Internet a su sitio web convirtiendo los nombres de dominio legibles, como www.example.com, en direcciones IP numéricas, como 192.0.2.1, que los sistemas utilizan para conectarse entre sí. Cuando un usuario escribe su nombre de dominio en un navegador o le envía un mensaje de email, se reenvía una consulta de DNS a Route 53, que responde con el valor correspondiente. Por ejemplo, Route 53 podría responder con la dirección IP del servidor web correspondiente a example.com.

Comparación del alojamiento de DNS con el registro de dominios

Este capítulo trata sobre el uso de Route 53 únicamente para el alojamiento de DNS. Esto significa que el registro de su dominio permanece con su registrador actual y usted seguirá pagándole por las renovaciones de dominio. Route 53 solo administrará su configuración de DNS y gestionará las consultas de DNS correspondientes a su dominio.

Si quiere transferir también el registro de su dominio a Route 53 (lo que convertiría a Route 53 en su registrador y en su servicio de DNS), consulte [Lista de verificación previa a la transferencia para transferencias de dominios](#) y [Transferencia del registro de un dominio a Amazon Route 53](#).

En este capítulo, explicamos cómo configurar Route 53 para dirigir su tráfico de Internet a los lugares correctos. También se explica cómo migrar el servicio DNS a Route 53 si utiliza otro servicio DNS y cómo utilizar Route 53 como el servicio DNS para un nuevo dominio.

Temas

- [Establecer Amazon Route 53 como servicio DNS de un dominio existente](#)
- [Configuración del direccionamiento de DNS para un nuevo dominio](#)
- [Direccionamiento del tráfico a sus recursos](#)
- [Uso de zonas alojadas](#)
- [Uso de registros](#)
- [Configuración de la firma de DNSSEC en Amazon Route 53](#)
- [Uso de AWS Cloud Map para crear registros y comprobaciones de estado](#)

- [Restricciones y comportamientos de DNS](#)
- [Temas relacionados](#)

Establecer Amazon Route 53 como servicio DNS de un dominio existente

Si va a transferir uno o varios registros de dominio a Route 53 y está utilizando actualmente un registrador de dominios que no proporciona un servicio DNS de pago, debe migrar el servicio DNS antes de migrar el dominio. De lo contrario, el registrador dejará de proporcionar el servicio DNS cuando transfiera sus dominios y los sitios y aplicaciones web asociados dejarán de estar disponible en Internet. (También puede migrar el servicio DNS desde el registrador actual a otro proveedor de servicios DNS. No es necesario usar Route 53 como el proveedor de servicios DNS para los dominios que están registrados con Route 53).

El proceso depende de si está utilizando actualmente el dominio:

- Si el dominio tiene actualmente tráfico (por ejemplo, si los usuarios utilizan el nombre de dominio para navegar por un sitio web u obtener acceso a una aplicación web), consulte [Establecer Route 53 como el servicio DNS para un dominio que se está utilizando](#).
- Si el dominio no tiene tráfico (o tiene muy poco tráfico), consulte [Establecer Route 53 como el servicio DNS de un dominio inactivo](#).

En ambas opciones, su dominio debe permanecer disponible durante todo el proceso de migración. Sin embargo, en el caso poco probable de que haya problemas, la primera opción le permite restaurar la migración de forma rápida. Con la segunda opción, su dominio podría no estar disponible durante un par de días.

Si desea ponerse en contacto con un experto en AWS, visite [Soporte de ventas](#).

Establecer Route 53 como el servicio DNS para un dominio que se está utilizando

Si desea migrar el servicio DNS a Amazon Route 53 en el caso de un dominio que tenga actualmente tráfico (por ejemplo, si los usuarios utilizan el nombre de dominio para navegar a un sitio web u obtener acceso a una aplicación web), siga los procedimientos que indicamos en esta sección.

Temas

- [Paso 1: Obtener la configuración de DNS actual del proveedor de servicios DNS actual \(opcional pero recomendado\)](#)
- [Paso 2: Crear una zona alojada](#)
- [Paso 3: Crear los registros](#)
- [Paso 4: Reducir la configuración de TTL](#)
- [Paso 5: \(Si DNSSEC está configurado\) Quitar el registro de DS de la zona principal](#)
- [Paso 6: Esperar a que caduque el TTL anterior](#)
- [Paso 7: Actualizar los registros NS para utilizar servidores de nombres de Route 53](#)
- [Paso 8: Monitorear el tráfico del dominio](#)
- [Paso 9: Volver a cambiar el TTL del registro NS a un valor más alto](#)
- [Paso 10: Transferir el registro del dominio a Amazon Route 53](#)
- [Paso 11: Volver a habilitar la firma de DNSSEC \(si es necesario\)](#)

Paso 1: Obtener la configuración de DNS actual del proveedor de servicios DNS actual (opcional pero recomendado)

Al migrar el servicio DNS desde otro proveedor a Route 53, reproduce su configuración de DNS actual en Route 53. En Route 53, debe crear una zona alojada que tenga el mismo nombre que su dominio y crear registros en la zona alojada. Cada registro indica cómo desea dirigir el tráfico de un nombre de dominio o subdominio especificado. Por ejemplo, cuando alguien escribe su nombre de dominio en un navegador web, ¿desea que el tráfico se dirija a un servidor web de su centro de datos, a una instancia de Amazon EC2, a una distribución de CloudFront o a cualquier otra ubicación?

El proceso que utilice dependerá de la complejidad de la configuración de DNS que tenga:

- Si la configuración de DNS actual es sencilla. Si está dirigiendo tráfico de Internet solo para unos cuantos subdominios a un pequeño número de recursos, como servidores web o buckets de Amazon S3, puede crear manualmente varios registros en la consola de Route 53.
- Si la configuración de DNS actual es más compleja y solo quiere reproducir su configuración actual. Puede simplificar la migración si puede obtener un archivo de zona del proveedor de servicios DNS actual e importar dicho archivo a Route 53. (No todos los proveedores de servicios DNS ofrecen archivos de zona). Al importar un archivo de zona, Route 53 reproduce automáticamente la configuración existente creando los registros correspondientes en la zona alojada.

Pregunte al servicio de atención al cliente de su proveedor de servicios DNS actual cómo obtener un archivo de zona o una lista de registros. Para obtener más información acerca del formato que un archivo de zona ha de tener, consulte [Creación de registros mediante la importación de un archivo de zona](#).

- Si su configuración de DNS actual es más compleja y está interesado en las características de enrutamiento de Route 53. Lea la documentación siguiente para ver si quiere utilizar las características de Route 53 que no están disponibles en otros proveedores de servicios DNS. En caso afirmativo, puede crear registros manualmente o puede importar un archivo de zona y, a continuación, crear o actualizar registros en otro momento:
 - [Elección entre registros de alias y sin alias](#) explica las ventajas de los registros de alias de Route 53, que dirigen el tráfico a algunos recursos de AWS de forma gratuita, como distribuciones de CloudFront y buckets de Amazon S3.
 - [Elección de una política de enrutado](#) explica las opciones de direccionamiento de Route 53, como, por ejemplo, el enrutamiento basado en la ubicación de los usuarios, el enrutamiento basado en la latencia entre sus usuarios y los recursos, el enrutamiento basado en si los recursos son correctos y el que está basado en ponderaciones que usted mismo especifica.

 Note

También puede importar un archivo de zona y más tarde cambiar la configuración para aprovechar los registros de alias y las políticas de direccionamiento complejas.

Si no puede obtener un archivo de zona o si desea crear manualmente registros en Route 53, los registros que probablemente migrará son los siguientes:

- Registros A (dirección): asocian un nombre de dominio o uno de subdominio a la dirección IPv4 (por ejemplo, 192.0.2.3) del recurso correspondiente
- Registros AAAA (dirección): asocian un nombre de dominio o uno de subdominio a la dirección IPv6 (por ejemplo, 2001:0db8:85a3:0000:0000:abcd:0001:2345) del recurso correspondiente
- Registros de servidor de correo (MX): dirigen tráfico a servidores de correo
- Registros CNAME: redirigen el tráfico de un nombre de dominio (example.net) a otro nombre de dominio (example.com)
- Registros para otros tipos de registros DNS admitidos: para consultar una lista de tipos de registros admitidos, consulte [Tipos de registros de DNS admitidos](#).

Paso 2: Crear una zona alojada

Para indicar a Amazon Route 53 cómo quiere dirigir el tráfico de su dominio, cree una zona alojada que tenga el mismo nombre que el dominio y después cree registros en la zona alojada.

Important

Puede crear una zona alojada solo para los dominios para los que tenga permiso para administrar. Por lo general, esto indicará que es el propietario del dominio, aunque también podría estar desarrollando una aplicación para el registrador del dominio.

Cuando crea una zona alojada, Route 53 genera automáticamente un registro del servidor de nombres (NS) y un registro de inicio de autoridad (SOA) para dicha zona. El registro NS identifica los cuatro servidores de nombres que Route 53 asoció a su zona alojada. Para que Route 53 sea el servicio DNS de su dominio, puede actualizar el registro del dominio para que utilice estos cuatro servidores de nombres.

Important

No cree registros de servidor de nombres (NS) o de inicio de autoridad (SOA) adicionales ni elimine los registros SOA y NS existentes.

Para crear una zona alojada

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. Si no está familiarizado con Route 53, elija Get started (Introducción) en DNS management (Administración de DNS) y, a continuación, elija Create hosted zones (Crear zonas alojadas).

Si ya trabaja con Route 53, elija Hosted zones (Zonas alojadas) en el panel de navegación y, a continuación, elija Create hosted zones (Crear zonas alojadas).

3. En el panel Create hosted zone (Crear zona alojada), ingrese un nombre de dominio y, si lo desea, un comentario. Para obtener más información sobre una configuración, elija abrir el panel de ayuda en el lado derecho.

Para obtener información sobre cómo especificar caracteres distintos de a-z, 0-9 y - (guion), y cómo especificar nombres de dominio internacionalizados, consulte [Formato de nombres de dominio DNS](#).

4. En Type (Tipo), acepte el valor predeterminado de Public hosted zone (Zona alojada pública).
5. Elija Create hosted zone (Crear zona alojada).

Paso 3: Crear los registros

Después de crear una zona alojada, debe crear registros en dicha zona que definan adónde desea dirigir el tráfico de un dominio (example.com) o subdominio (www.example.com). Por ejemplo, si desea dirigir el tráfico de example.com y www.example.com a un servidor web en una instancia de Amazon EC2, debe crear dos registros, uno denominado example.com y otro denominado www.example.com. En cada registro debe especificar la dirección IP de la instancia de EC2.

Puede crear registros de diversas formas:

Importando un archivo de zona.

Este es el método más fácil si tiene un archivo de zona de su servicio DNS actual en [Paso 1: Obtener la configuración de DNS actual del proveedor de servicios DNS actual \(opcional pero recomendado\)](#). Amazon Route 53 no puede predecir cuándo crear registros de alias o utilizar tipos de direccionamiento especiales como el direccionamiento ponderado o de conmutación por error. Como resultado, si importa un archivo de zona, Route 53 crea registros DNS estándar con la política de direccionamiento sencilla.

Para obtener más información, consulte [Creación de registros mediante la importación de un archivo de zona](#).

Creando registros individualmente en la consola

Si no ha recibido un archivo de zona y quiere crear unos cuantos registros con una política de direccionamiento sencilla para comenzar, puede crear los registros en la consola de Route 53. Puede crear registros de alias y registros sin alias.

Para obtener más información, consulte los temas siguientes:

- [Elección de una política de enrutado](#)
- [Elección entre registros de alias y sin alias](#)

- [Creación de registros con la consola de Amazon Route 53](#)

Creando registros mediante programación

Puede crear registros usando uno de los AWS SDK, la AWS CLI o AWS Tools for Windows PowerShell. Para obtener más información, consulte la [Documentación de AWS](#).

Si usa un lenguaje de programación para el que AWS no proporcione un SDK, también puede utilizar la API de Route 53. Para obtener más información, consulte la [referencia de API de Amazon Route 53](#).

Paso 4: Reducir la configuración de TTL

La opción TTL (tiempo de vida) de un registro especifica el tiempo que quiere que los solucionadores de DNS tengan en caché el registro y se use la información de la memoria caché. Cuando el TTL vence, un solucionador envía otra consulta al proveedor de servicios DNS para que un dominio obtenga la información más reciente.

Normalmente, la configuración de TTL para el registro NS es de 172 800 segundos o dos días. El registro NS muestra una lista de los servidores de nombres que el sistema de nombres de dominio (DNS) puede utilizar para obtener información acerca de cómo dirigir el tráfico para su dominio. Si reduce el TTL del registro NS, tanto en su proveedor de servicios DNS actual como en Amazon Route 53, reducirá el tiempo de inactividad de su dominio si descubre un problema mientras realiza la migración de DNS a Route 53. Si no reduce el TTL, su dominio podría no estar disponible en Internet durante un máximo de dos días si algo va mal.

Note

Algunos solucionadores completos pueden almacenar en caché el TTL del registro NS del servidor autorizado principal, por lo que también se debe reducir el TTL de los registros NS registrados en el servidor DNS autorizado principal.

Le recomendamos que cambie el TTL en los siguientes registros NS:

- En el registro NS de la zona alojada del proveedor de servicios DNS actual. (Puede que su proveedor actual utilice otra terminología).
- En el registro NS de la zona alojada que ha creado en [Paso 2: Crear una zona alojada](#).

Para reducir la configuración de TTL en el registro NS del proveedor de servicios DNS actual

- Utilice el método proporcionado por el proveedor de servicios DNS actual para que el dominio cambie el TTL del registro NS de la zona alojada de su dominio.

Para reducir la configuración de TTL en el registro NS de una zona alojada de Route 53

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. Elija Hosted Zones (Zonas alojadas) en el panel de navegación.
3. Elija el nombre de la zona alojada.
4. Elija el registro NS y, a continuación, elija Edit (Editar).
5. Cambie el valor de TTL (Seconds) (Segundos). Le recomendamos que especifique un valor entre 60 segundos y 900 segundos (15 minutos).
6. Elija Save changes (Guardar cambios).

Paso 5: (Si DNSSEC está configurado) Quitar el registro de DS de la zona principal

Si ha configurado DNSSEC para su dominio, quite el registro de Delegation Signer (DS) de la zona principal antes de migrar el dominio a Route 53.

Si la zona principal está alojada a través de Route 53 u otro registrador, contacte con él para eliminar el registro DS.

Dado que actualmente no es posible tener habilitada la firma DNSSEC en dos proveedores, debe eliminar cualquier DS o DNSKEY para desactivar DNSSEC. Esto envía una señal temporal a los solucionadores de DNS para que desactiven la validación DNSSEC. En el [paso 11](#), puede volver a habilitar la validación de DNSSEC si lo desea, una vez completada la transición a Route 53.

Para obtener más información, consulte [Eliminar claves públicas de un dominio](#).

Paso 6: Esperar a que caduque el TTL anterior

Si está utilizando el dominio, como, por ejemplo, si los usuarios utilizan el nombre de dominio para navegar a un sitio web u obtener acceso a una aplicación web, los solucionadores de DNS tienen en caché los nombres de los servidores de nombres que ha proporcionado el proveedor de servicios DNS actual. Un solucionador de DNS que haya guardado en la memoria caché esa información tan solo unos minutos antes, la guardará durante casi dos días más.

Para asegurarse de que la migración del servicio DNS a Route 53 se produzca de una sola vez, espere dos días después de haber reducido el TTL. Una vez transcurridos esos dos días, el TTL vencerá y los solucionadores solicitarán a los servidores de nombres su dominio, obtendrán los servidores de nombres actuales y también obtendrán el nuevo TTL especificado en [Paso 4: Reducir la configuración de TTL](#).

Paso 7: Actualizar los registros NS para utilizar servidores de nombres de Route 53

Para comenzar a utilizar Amazon Route 53 como servicio DNS para un dominio, utilice el método proporcionado por el proveedor de servicios DNS actual para reemplazar los servidores de nombres actuales en el registro NS por servidores de nombres de Route 53.

Note

Cuando actualiza el registro NS con el proveedor de servicios DNS actual para utilizar servidores de nombres de Route 53, actualiza la configuración DNS del dominio. (Esto equivale a la actualización del registro NS en la zona alojada de Route 53 para un dominio, con la excepción de que está actualizando la configuración con el servicio DNS desde el que está migrando).

Para actualizar el registro NS en el registrador, o en la zona principal, para utilizar los servidores de nombres de Route 53

1. En la consola de Route 53, obtenga los servidores de nombres de la zona alojada:
 - a. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
 - b. En el panel de navegación, elija Zonas alojadas.
 - c. En la página Hosted zones (Zonas alojadas), seleccione el nombre de la zona alojada pertinente.
 - d. Anote los cuatro nombres que figuran en Name servers (Servidores de nombres) en la sección Hosted zone details (Detalles de la zona alojada).
2. Utilice el método que proporciona el servicio DNS actual para que el dominio actualice el registro NS de la zona alojada. Si el dominio está registrado con Route 53, consulte [Adición o modificación de servidores de nombres y registros de conexión de un dominio](#). El proceso dependerá de si el servicio DNS actual le permite eliminar servidores de nombres:

Si puede eliminar los servidores de nombres

- Anote los nombres de los servidores de nombres actuales del registro NS para la zona alojada. Si necesita volver a la configuración de DNS actual, estos son los servidores que especificará.
- Elimine los servidores de nombres actuales del registro NS.
- Actualice el registro NS con los nombres de los cuatro servidores de nombres de Route 53 que obtuvo en el paso 1 de este procedimiento.

 Note

Cuando termine, los únicos servidores de nombres del registro NS serán los cuatro servidores de nombres de Route 53.

Si no puede eliminar los servidores de nombres

- Elija la opción para utilizar servidores de nombres personalizados.
- Añada los cuatro servidores de nombres de Route 53 que obtuvo en el paso 1 de este procedimiento.

Paso 8: Monitorear el tráfico del dominio

Monitoree el tráfico del dominio, incluido el tráfico del sitio web o la aplicación, y el correo electrónico:

- Si el tráfico se reduce o se detiene: utilice el método proporcionado por el servicio DNS anterior para cambiar los servidores de nombres del dominio por los servidores de nombres anteriores. Estos son los servidores de nombres que anotó en el paso 7 de [Para actualizar el registro NS en el registrador, o en la zona principal, para utilizar los servidores de nombres de Route 53](#). A continuación, determine qué ha fallado.
- Si el tráfico no se ve afectado: continúe en [Paso 9: Volver a cambiar el TTL del registro NS a un valor más alto](#).

Paso 9: Volver a cambiar el TTL del registro NS a un valor más alto

En la zona alojada de Amazon Route 53 del dominio, cambie el TTL del registro NS a un valor más habitual, como, por ejemplo, 172800 segundos (dos días). Esto mejorará la latencia de los usuarios, ya que no tendrán que esperar tan a menudo para que los solucionadores de DNS envíen una consulta para obtener los servidores de nombres de su dominio.

Para cambiar el TTL del registro NS de la zona alojada de Route 53

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. Elija Hosted Zones (Zonas alojadas) en el panel de navegación.
3. Elija el nombre de la zona alojada.
4. En la lista de registros de la zona alojada, elija el registro NS.
5. Seleccione Editar.
6. Cambie TTL (Seconds) por el número de segundos que desea que los solucionadores de DNS almacenen en caché los nombres de los servidores de nombres de su dominio. Le recomendamos un valor de 172 800 segundos.
7. Seleccione Save changes (Guardar cambios).

Paso 10: Transferir el registro del dominio a Amazon Route 53

Ahora que ha transferido el servicio DNS de un dominio a Amazon Route 53, tiene la opción de transferir el registro del dominio a Route 53. Para obtener más información, consulte [Transferencia del registro de un dominio a Amazon Route 53](#).

Paso 11: Volver a habilitar la firma de DNSSEC (si es necesario)

Ahora que ha transferido el servicio DNS de un dominio a Amazon Route 53, tiene la opción de volver a habilitar la firma de DNSSEC.

Habilitar la firma de DNSSEC es un proceso de dos pasos:

- Paso 1: Habilitar la firma de DNSSEC para Route 53 y solicitar que este servicio cree una clave de firma de claves (KSK) basada en una clave administrada por el cliente en AWS Key Management Service (AWS KMS).

- Paso 2: Crear una cadena de confianza para la zona alojada agregando un registro de Delegation Signer (DS) a la zona principal, de modo que las respuestas DNS se puedan autenticar con firmas criptográficas de confianza.

Para obtener instrucciones, consulte [Activar la firma de DNSSEC y establecer una cadena de confianza](#).

Establecer Route 53 como el servicio DNS de un dominio inactivo

Si desea migrar a Amazon Route 53 el servicio DNS de un dominio que no tiene tráfico (o muy poco tráfico), siga el procedimiento que se indica en esta sección.

Temas

- [Paso 1: Solicitar la configuración de DNS actual al proveedor de servicios DNS actual \(dominios inactivos\)](#)
- [Paso 2: Crear una zona alojada \(dominios inactivos\)](#)
- [Paso 3: Crear los registros \(dominios inactivos\)](#)
- [Paso 4: Actualizar el registro de dominio para que utilice los servidores de nombres de Amazon Route 53 \(dominios inactivos\)](#)

Paso 1: Solicitar la configuración de DNS actual al proveedor de servicios DNS actual (dominios inactivos)

Al migrar el servicio DNS desde otro proveedor a Route 53, reproduce su configuración de DNS actual en Route 53. En Route 53, debe crear una zona alojada que tenga el mismo nombre que su dominio y crear registros en la zona alojada. Cada registro indica cómo desea dirigir el tráfico de un nombre de dominio o subdominio especificado. Por ejemplo, cuando alguien escribe su nombre de dominio en un navegador web, ¿desea que el tráfico se dirija a un servidor web de su centro de datos, a una instancia de Amazon EC2, a una distribución de CloudFront o a cualquier otra ubicación?

El proceso que utilice dependerá de la complejidad de la configuración de DNS que tenga:

- Si la configuración de DNS actual es sencilla. Si está dirigiendo tráfico de Internet solo para unos cuantos subdominios a un pequeño número de recursos, como servidores web o buckets de Amazon S3, puede crear manualmente varios registros en la consola de Route 53.

- Si la configuración de DNS actual es más compleja y solo quiere reproducir su configuración actual. Puede simplificar la migración si puede obtener un archivo de zona del proveedor de servicios DNS actual e importar dicho archivo a Route 53. (No todos los proveedores de servicios DNS ofrecen archivos de zona). Al importar un archivo de zona, Route 53 reproduce automáticamente la configuración existente creando los registros correspondientes en la zona alojada.

Pregunte al servicio de atención al cliente de su proveedor de servicios DNS actual cómo obtener un archivo de zona o una lista de registros. Para obtener más información acerca del formato que un archivo de zona ha de tener, consulte [Creación de registros mediante la importación de un archivo de zona](#).

- Si su configuración de DNS actual es más compleja y está interesado en las características de enrutamiento de Route 53. Lea la documentación siguiente para ver si quiere utilizar las características de Route 53 que no están disponibles en otros proveedores de servicios DNS. En caso afirmativo, puede crear registros manualmente o puede importar un archivo de zona y, a continuación, crear o actualizar registros en otro momento:
 - [Elección entre registros de alias y sin alias](#) explica las ventajas de los registros de alias de Route 53, que dirigen el tráfico a algunos recursos de AWS de forma gratuita, como distribuciones de CloudFront y buckets de Amazon S3.
 - [Elección de una política de enrutado](#) explica las opciones de direccionamiento de Route 53, como, por ejemplo, el enrutamiento basado en la ubicación de los usuarios, el enrutamiento basado en la latencia entre sus usuarios y los recursos, el enrutamiento basado en si los recursos son correctos y el que está basado en ponderaciones que usted mismo especifica.

 Note

También puede importar un archivo de zona y más tarde cambiar la configuración para aprovechar los registros de alias y las políticas de direccionamiento complejas.

Si no puede obtener un archivo de zona o si desea crear manualmente registros en Route 53, los registros que probablemente migrará son los siguientes:

- Registros A (dirección): asocian un nombre de dominio o uno de subdominio a la dirección IPv4 (por ejemplo, 192.0.2.3) del recurso correspondiente
- Registros AAAA (dirección): asocian un nombre de dominio o uno de subdominio a la dirección IPv6 (por ejemplo, 2001:0db8:85a3:0000:0000:abcd:0001:2345) del recurso correspondiente

- Registros de servidor de correo (MX): dirigen tráfico a servidores de correo
- Registros CNAME: redirigen el tráfico de un nombre de dominio (example.net) a otro nombre de dominio (example.com)
- Registros para otros tipos de registros DNS admitidos: para consultar una lista de tipos de registros admitidos, consulte [Tipos de registros de DNS admitidos](#).

Paso 2: Crear una zona alojada (dominios inactivos)

Para indicar a Amazon Route 53 cómo quiere dirigir el tráfico de su dominio, cree una zona alojada que tenga el mismo nombre que el dominio y después cree registros en la zona alojada.

Important

Puede crear una zona alojada solo para los dominios para los que tenga permiso para administrar. Por lo general, esto indicará que es el propietario del dominio, aunque también podría estar desarrollando una aplicación para el registrador del dominio.

Cuando crea una zona alojada, Route 53 genera automáticamente un registro del servidor de nombres (NS) y un registro de inicio de autoridad (SOA) para dicha zona. El registro NS identifica los cuatro servidores de nombres que Route 53 asoció a su zona alojada. Para que Route 53 sea el servicio DNS de su dominio, puede actualizar el registro del dominio para que utilice estos cuatro servidores de nombres.

Important

No cree registros de servidor de nombres (NS) o de inicio de autoridad (SOA) adicionales ni elimine los registros SOA y NS existentes.

Para crear una zona alojada

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. Si no conoce Route 53, elija Get started (Introducción).

Si ya trabaja con Route 53, seleccione Hosted zones (Zonas alojadas) en el panel de navegación.

3. Elija Create hosted zone (Crear zona alojada).
4. En el panel Create hosted zone (Crear zona alojada), ingrese un nombre de dominio y, si lo desea, un comentario. Si necesita más información sobre una opción de configuración, sitúe el puntero del ratón sobre el nombre de la opción para que aparezca la información sobre herramientas.

Para obtener información sobre cómo especificar caracteres distintos de a-z, 0-9 y - (guion), y cómo especificar nombres de dominio internacionalizados, consulte [Formato de nombres de dominio DNS](#).

5. En Record type (Tipo de registro), acepte el valor predeterminado de Public hosted zone (Zona alojada pública).
6. Elija Create hosted zone (Crear zona alojada).

Paso 3: Crear los registros (dominios inactivos)

Después de crear una zona alojada, debe crear registros en dicha zona que definan adónde desea dirigir el tráfico de un dominio (example.com) o subdominio (www.example.com). Por ejemplo, si desea dirigir el tráfico de example.com y www.example.com a un servidor web en una instancia de Amazon EC2, debe crear dos registros, uno denominado example.com y otro denominado www.example.com. En cada registro debe especificar la dirección IP de la instancia de EC2.

Puede crear registros de diversas formas:

Importando un archivo de zona.

Este es el método más fácil si tiene un archivo de zona de su servicio DNS actual en [Paso 1: Solicitar la configuración de DNS actual al proveedor de servicios DNS actual \(dominios inactivos\)](#). Amazon Route 53 no puede predecir cuándo crear registros de alias o utilizar tipos de direccionamiento especiales como el direccionamiento ponderado o de conmutación por error. Como resultado, si importa un archivo de zona, Route 53 crea registros DNS estándar con la política de direccionamiento sencilla.

Para obtener más información, consulte [Creación de registros mediante la importación de un archivo de zona](#).

Creando registros individualmente en la consola

Si no ha recibido un archivo de zona y quiere crear unos cuantos registros con una política de direccionamiento sencilla para comenzar, puede crear los registros en la consola de Route 53. Puede crear registros de alias y registros sin alias.

Para obtener más información, consulte los temas siguientes:

- [Elección de una política de enrutado](#)
- [Elección entre registros de alias y sin alias](#)
- [Creación de registros con la consola de Amazon Route 53](#)

Creando registros mediante programación

Puede crear registros usando uno de los AWS SDK, la AWS CLI o AWS Tools for Windows PowerShell. Para obtener más información, consulte la [Documentación de AWS](#).

Si usa un lenguaje de programación para el que AWS no proporcione un SDK, también puede utilizar la API de Route 53. Para obtener más información, consulte la [referencia de API de Amazon Route 53](#).

Paso 4: Actualizar el registro de dominio para que utilice los servidores de nombres de Amazon Route 53 (dominios inactivos)

Cuando haya terminado de crear registros para el dominio, puede cambiar el servicio DNS de su dominio a Amazon Route 53. Ejecute el procedimiento siguiente para actualizar la configuración en el registrador de dominio.

Para actualizar los servidores de nombres del dominio

1. En la consola de Route 53, obtenga los servidores de nombres de la zona alojada de Route 53:
 - a. Abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
 - b. En el panel de navegación, elija Zonas alojadas.
 - c. En la página Hosted zones (Zonas alojadas), elija el botón de radio (no el nombre) de la zona alojada y luego View details (Ver detalles).
 - d. En la página de detalles de la zona alojada, elija Hosted zone details (Detalles de la zona alojada).
 - e. Anote los nombres de los cuatro servidores que aparecen en Name servers (Servidores de nombres).

2. Use el método proporcionado por el registrador del dominio para cambiar los servidores de nombres para que el dominio use los cuatro servidores de nombres de Route 53 que obtuvo en el paso 2 de este procedimiento.

Si el dominio está registrado en Route 53, consulte [Adición o modificación de servidores de nombres y registros de conexión de un dominio](#).

Configuración del direccionamiento de DNS para un nuevo dominio

Un dominio nuevo que compró en Route 53

Al registrar un dominio con Route 53, convertimos automáticamente a Route 53 en el servicio DNS del dominio. Route 53 crea una zona alojada que tiene el mismo nombre que el dominio, asigna cuatro servidores de nombres a la zona alojada y actualiza el dominio para utilizar esos servidores de nombres.

Un dominio nuevo que compró de otro registrador

Cuando compra un dominio de otro registrador, por ejemplo, porque Route 53 no ofrece el dominio de nivel superior (TLD), tiene dos opciones:

- Utilice Route 53 únicamente para el alojamiento de DNS: mantenga su registrador actual, pero delegue la administración del DNS a Route 53. Siga el procedimiento que se indica a continuación para crear una zona alojada y actualizar los servidores de nombres de su registrador.
- Transfiera el registro del dominio a Route 53: convierta a Route 53 en su registrador y servicio de DNS. Consulte [Lista de verificación previa a la transferencia para transferencias de dominios](#) para conocer los requisitos previos y [Transferencia del registro de un dominio a Amazon Route 53](#) para conocer el proceso de transferencia.

Para obtener más información acerca de los TLD que admite Route 53, consulte [Dominios que puede registrar con Amazon Route 53](#).

Siga estas instrucciones para crear una zona alojada pública y, a continuación, utilice los servidores de nombres creados con el registrador:

Cómo crear una zona alojada para un dominio no proveniente de Route 53

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.

2. En el panel de navegación, elija Zonas alojadas y, luego, Crear zona alojada.
3. En Nombre, introduzca el nombre del dominio para el que desea crear una zona alojada, como `example.com`, y una descripción opcional. Seleccione Zona alojada pública y, a continuación, Crear zona alojada.
4. Después de crear la zona alojada, anote los cuatro registros del servidor de nombres (NS) que se crearon. Estos empezarán con «ns-».

En el registrador de dominios, introduzca los servidores de nombres anteriores para delegar la administración de los dominios a la zona alojada de Route 53.

Enrute el tráfico de DNS

Para especificar la forma en que desea que Route 53 dirija el tráfico de Internet del dominio, debe crear registros en la zona alojada. Por ejemplo, si desea direccionar las solicitudes de `example.com` a un servidor web que se ejecuta en una instancia de Amazon EC2, debe crear un registro en la zona alojada `example.com` y especificar la dirección IP elástica de la instancia de EC2. Para obtener más información, consulte los temas siguientes:

- Para obtener información sobre cómo crear registros en su zona alojada, consulte [Uso de registros](#).
- Para obtener información sobre cómo dirigir el tráfico a recursos de AWS seleccionados, consulte [Enrutar el tráfico de Internet a sus AWS recursos](#).
- Para obtener información sobre cómo funciona DNS, consulte [se dirige el tráfico de Internet a su sitio web o aplicación web](#).
- Para comprobar el reposo del DNS, consulte [Comprobación de las respuestas de DNS de Route 53](#).

Direccionamiento del tráfico a sus recursos

Cuando los usuarios solicitan su sitio web o una aplicación web, por ejemplo, escribiendo el nombre de su dominio en un navegador web, Amazon Route 53 ayuda a dirigir a los usuarios a sus recursos, como un bucket de Amazon S3 o un servidor web de su centro de datos. Para configurar Route 53 para que dirija el tráfico a sus recursos, debe hacer lo siguiente:

1. Cree una zona alojada. Puede crear una zona alojada pública o una zona alojada privada:

Zona alojada pública

Crea una zona alojada pública si quieres enrutar el tráfico de Internet a tus recursos, por ejemplo, para que tus clientes puedan ver el sitio web de la empresa que alojas en EC2 las instancias. Para obtener más información, consulte [Trabajar con zonas públicas alojadas](#).

Zona alojada privada

Cree una zona alojada privada si desea dirigir el tráfico dentro de una Amazon VPC. Para obtener más información, consulte [Uso de zonas alojadas privadas](#).

2. Creación de registros en la zona alojada. Los registros definen a dónde quiere dirigir el tráfico para cada nombre de dominio o de subdominio. Por ejemplo, para dirigir el tráfico de `www.example.com` a un servidor web de su centro de datos, se suele crear un registro de `www.example.com` en la zona alojada de `example.com`.

Para obtener más información, consulte los temas siguientes:

- [Uso de registros](#)
- [Direccionamiento del tráfico de subdominios](#)
- [Enrutar el tráfico de Internet a sus AWS recursos](#)

Direccionamiento del tráfico de subdominios

Cuando desee dirigir el tráfico a sus recursos para un subdominio como `acme.example.com` o `zenith.example.com`, dispone de dos opciones:

Creación de registros en la zona alojada para el dominio

Normalmente, para dirigir el tráfico de un subdominio, se crea un registro en la zona alojada que tenga el mismo nombre que el dominio. Por ejemplo, para dirigir el tráfico de Internet de `acme.example.com` a un servidor web de su centro de datos, se crea un registro llamado `acme.example.com` en la zona alojada de `example.com`. Para obtener más información, consulte el tema [Uso de registros](#) y sus subtemas.

Creación una zona alojada para el subdominio y creación de registros en la nueva zona alojada

También puede crear una zona alojada para el subdominio. Usar una zona alojada independiente para dirigir el tráfico de Internet de un subdominio a veces recibe el nombre de “delegar la responsabilidad de un subdominio a una zona alojada” o “delegar un subdominio a otros

servidores de nombres”, o alguna combinación de términos similar. Aquí se ofrece información general de cómo funciona:

1. Cree una zona alojada que tiene el mismo nombre que el subdominio para el que desea enrutar el tráfico, como `acme.example.com`.
2. Cree registros en la nueva zona alojada, que definan cómo desea dirigir el tráfico para el subdominio (`acme.example.com`) y sus subdominios, como, por ejemplo, `backend.acme.example.com`.
3. Obtiene los servidores de nombres que asignó Route 53 a la nueva zona alojada cuando la creó.
4. Creas un registro NS nuevo en la zona alojada del dominio (`example.com`). El nombre del registro NS debe ser el nombre del subdominio (`acme.example.com`) y debe especificar los cuatro servidores de nombres que obtuvo en el paso 3 como valores de registro.

Cuando se usa una zona alojada independiente para dirigir el tráfico de un subdominio, se pueden utilizar permisos de IAM para restringir el acceso a la zona alojada del subdominio. Si tiene varios subdominios administrados por diferentes grupos, la creación de una zona alojada para cada subdominio puede reducir significativamente el número de personas que deben tener acceso a los registros de la zona alojada del dominio.

Para implementar este proceso de delegación, necesita los siguientes permisos de IAM. Para obtener más información sobre las políticas de IAM de Route 53, consulte [Identity and Access Management en Amazon Route 53](#):

Cuenta principal (es propietaria de `example.com`)

El usuario o rol necesita permisos para modificar los registros en la zona alojada del dominio principal:

Cuenta secundaria (crea `acme.example.com`)

El usuario o rol necesita permisos para crear y administrar la zona alojada del subdominio:

El uso de una zona alojada de un subdominio también le permite utilizar servicios DNS diferentes para el dominio y el subdominio. Para obtener más información, consulte [Uso de Amazon Route 53 como el servicio DNS de subdominios sin migrar el dominio principal](#).

Esta configuración tiene un pequeño impacto sobre el desempeño para la primera consulta de DNS de cada servicio de resolución de nombres DNS. El servicio de resolución debe obtener información de la zona alojada del dominio raíz y, a continuación, obtener información de la zona alojada para el subdominio. Después de la primera consulta de DNS a un subdominio, el servicio

de resolución de nombres almacena la información en caché y no necesita volver a obtenerla hasta que transcurra el tiempo de vida (TTL) y otro cliente solicite el subdominio a ese servicio de resolución. Para obtener más información, consulte [TTL \(segundos\)](#) en la sección [Valores que hay que especificar al crear o editar los registros de Amazon Route 53](#).

Temas

- [Creación de otra zona alojada para dirigir el tráfico para un subdominio](#)
- [Direccionamiento del tráfico para niveles adicionales de subdominios](#)

Creación de otra zona alojada para dirigir el tráfico para un subdominio

Una forma de dirigir el tráfico de un subdominio es crear una zona alojada para el subdominio y, a continuación, crear registros para el subdominio en la nueva zona alojada. (La opción más habitual es crear registros para el subdominio en la zona alojada del dominio).

Note

Este procedimiento muestra cómo delegar un subdominio a Route 53. También puede delegar un subdominio a otros servicios de DNS mediante la creación de registros NS que, en su lugar, apunten a los servidores de nombres de esos servicios.

A continuación se ofrece información general sobre el proceso:

1. Creación de una zona alojada para el subdominio. Para obtener más información, consulte [Creación de una nueva zona alojada para un subdominio](#).
2. Adición de registros a la zona alojada para el subdominio. Si la zona alojada del dominio contiene algún registro que pertenece a la zona alojada del subdominio, duplique esos registros en la zona alojada del subdominio. Para obtener más información, consulte [Creación de registros en la zona alojada para el subdominio](#)
3. Cree un registro NS para el subdominio en la zona alojada del dominio que delegue la responsabilidad sobre el subdominio a los servidores de nombres en la nueva zona alojada. Si la zona alojada del dominio contiene algún registro que pertenece a la zona alojada del subdominio, elimine los registros de la zona alojada del dominio. (Creó copias en la zona alojada del subdominio en el paso 2). Para obtener más información, consulte [Actualización de la zona alojada para el dominio](#).

Creación de una nueva zona alojada para un subdominio

Para crear una zona alojada para un subdominio con la consola de Route 53, siga estos pasos.

Para crear una zona alojada para un subdominio (consola)

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/route53/>
2. Si no conoce Route 53, elija Get started (Introducción).

Si ya trabaja con Route 53, seleccione Hosted zones (Zonas alojadas) en el panel de navegación.

3. Elija Create hosted zone (Crear zona alojada).
4. En el panel de la derecha, escriba el nombre del subdominio (por ejemplo, acme.example.com). Si lo desea, también puede escribir un comentario.

Para obtener información sobre cómo especificar caracteres distintos de a-z, 0-9 y - (guion), y cómo especificar nombres de dominio internacionalizados, consulte [Formato de nombres de dominio DNS](#).

5. En Type (Tipo), acepte el valor predeterminado de Public hosted zone (Zona alojada pública).
6. En la parte inferior del panel derecho, elija Create hosted zone (Crear zona alojada).

Creación de registros en la zona alojada para el subdominio

Para definir cómo quiere que dirija el tráfico Route 53 para el subdominio (acme.example.com) y sus subdominios (backend.acme.example.com), puede crear registros en la zona alojada para el subdominio.

Tenga en cuenta lo siguiente acerca de la creación de registros en la zona alojada del subdominio:

- No cree registros de servidor de nombres (NS) o de inicio de autoridad (SOA) adicionales en la zona alojada para el subdominio y no elimine los registros SOA y NS existentes.
- Cree todos los registros del subdominio en la zona alojada del subdominio. Por ejemplo, si tiene zonas alojadas para example.com y para el dominio acme.example.com, cree todos los registros para el subdominio acme.example.com en la zona alojada de acme.example.com. Entre estos se incluyen registros como backend.acme.example.com y beta.backend.acme.example.com.
- Si la zona alojada del dominio (example.com) ya contiene algún registro que pertenece a la zona alojada del subdominio (acme.example.com), duplique esos registros en la zona alojada del

subdominio. En el último paso del proceso, eliminará los registros duplicados de la zona alojada del dominio.

 Important

Si tiene algunos registros del subdominio tanto en la zona alojada del dominio como en la zona alojada del subdominio, el funcionamiento de DNS será incoherente. El funcionamiento dependerá de los servidores de nombres que un servicio de resolución de nombres DNS haya almacenado en caché, de los servidores de nombres de la zona alojada del dominio (example.com) o de los servidores de nombres de la zona alojada del subdominio (acme.example.com). En algunos casos, Route 53 devolverá NXDOMAIN (dominio inexistente) cuando el registro existe, pero no en la zona alojada a la que los servicios de resolución de nombres DNS envían la consulta.

Para obtener más información, consulte [Uso de registros](#).

Actualización de la zona alojada para el dominio

Al crear una zona alojada, Route 53 asigna automáticamente un conjunto de cuatro servidores a la zona. El registro NS de una zona alojada identifica los servidores de nombres que responden a las consulta de DNS del dominio o subdominio. Para comenzar a utilizar los registros de la zona alojada del subdominio para dirigir el tráfico de Internet, debe crear un nuevo registro NS en la zona alojada del dominio (example.com) y asignarle el nombre del subdominio (acme.example.com). Para el valor del registro NS, debe especificar los nombres de los servidores de nombres de la zona alojada del subdominio.

Esto es lo que ocurre cuando Route 53 recibe una consulta de DNS de un servicio de resolución de nombres DNS para el subdominio acme.example.com o uno de sus subdominios:

1. Route 53 busca en la zona alojada del dominio (example.com) y encuentra el registro NS para el subdominio (acme.example.com).
2. Route 53 obtiene los servidores de nombres del registro NS de acme.example.com de la zona alojada del dominio, example.com, y devuelve esos servidores de nombres al servicio de resolución de nombres DNS.
3. El servicio de resolución de nombres vuelve a enviar la consulta para acme.example.com a los servidores de nombres para la zona alojada acme.example.com.
4. Route 53 responde a la consulta mediante un registro en la zona alojada acme.example.com.

Para configurar Route 53 de forma que dirija el tráfico del subdominio utilizando la zona alojada del subdominio y que elimine los registros duplicados de la zona alojada del dominio, siga el procedimiento que se indica a continuación:

Para configurar Route 53 de modo que use la zona alojada del subdominio (consola)

1. En la consola de Route 53, obtenga los servidores de nombres de la zona alojada para el subdominio:
 - a. En el panel de navegación, elija Zonas alojadas.
 - b. En la página Hosted zones (Zonas alojadas), seleccione el nombre de la zona alojada para el subdominio.
 - c. En el panel de la derecha, copie los nombres de los cuatro servidores que aparecen en Name servers (Servidores de nombres) en la sección Hosted zones details (Detalles de zonas alojadas).
2. Elija el nombre de la zona alojada correspondiente al dominio (example.com), no para el subdominio.
3. Elija Crear registro.
4. Elija Simple routing (Enrutamiento sencillo) y Next (Siguiente).
5. Elija Define simple record (Definir registro simple).
6. Especifique los siguientes valores:

Name

Introduzca el nombre del subdominio (por ejemplo, `acme.example.com`). Debe coincidir exactamente con el nombre de la zona alojada del subdominio que creó.

Valor/ruta de destino del tráfico

Elija IP address (Dirección IP) u otro valor en función del tipo de registro y pegue los nombres de los servidores de nombres que haya copiado en el paso 1.

Tipo de registro

Elija NS — Servidores de nombres de una zona alojada.

TTL (Seconds)

Cambie a un valor más común de un registro NS, como, por ejemplo, 172 800 segundos.

7. Elija Define simple record (Definir registro simple) y, a continuación, Create records (Crear registros).
8. Si la zona alojada del dominio contiene algún registro que ha vuelto a crear en la zona alojada del subdominio, elimine esos registros de la zona alojada del dominio. Para obtener más información, consulte [Eliminar registros](#).

Cuando haya terminado, todos los registros del subdominio deberían estar en la zona alojada del subdominio.

Direccionamiento del tráfico para niveles adicionales de subdominios

Puede dirigir el tráfico a un subdominio de un subdominio, como backend.acme.example.com, de la misma manera que dirige el tráfico a un subdominio, como acme.example.com. Puede crear registros en la zona alojada para el dominio o crear una zona alojada para el subdominio de nivel inferior y, a continuación, crear registros en esa nueva zona alojada.

Si decide crear una zona alojada independiente para el subdominio de nivel inferior, cree el registro de NS para el subdominio de nivel inferior en la zona alojada del subdominio que se encuentre un nivel más cerca del nombre de dominio. Esto ayuda a garantizar que el tráfico se dirija correctamente a los recursos. Por ejemplo, suponga que desea dirigir el tráfico para los siguientes subdominios:

- subdomain1.example.com
- subdomain2.subdomain1.example.com

Para utilizar otra zona alojada para dirigir el tráfico de subdomain2.subdomain1.example.com, debe hacer lo siguiente:

1. Cree una zona alojada denominada subdomain2.subdomain1.example.com.
2. Cree registros en la zona alojada denominada subdomain2.subdomain1.example.com. Para obtener más información, consulte [Creación de registros en la zona alojada para el subdominio](#).
3. Copie los nombres de los servidores de nombres para la zona alojada subdomain2.subdomain1.example.com.
4. En la zona alojada subdomain1.example.com, cree un registro NS llamado subdomain2.subdomain1.example.com y pegue los nombres de los servidores de nombres para la zona alojada subdomain2.subdomain1.example.com.

Además, elimine los registros duplicados de `subdomain1.example.com`. Para obtener más información, consulte [Actualización de la zona alojada para el dominio](#).

Después de crear este registro NS, Route 53 comienza a utilizar la zona alojada `subdomain2.subdomain1.example.com` para dirigir el tráfico para el subdominio `subdomain2.subdomain1.example.com`.

Uso de zonas alojadas

Una zona alojada es un contenedor de registros y los registros contienen información sobre cómo desea direccionar el tráfico hacia un dominio específico (como `example.com`) y sus subdominios (como `acme.example.com`, `zenith.example.com`). Una zona alojada y el dominio correspondiente tienen el mismo nombre. Existen dos tipos de zonas alojadas:

- Las zonas alojadas públicas contienen registros que especifican cómo desea direccionar el tráfico en Internet. Para obtener más información, consulte [Trabajar con zonas públicas alojadas](#).
- Las zonas alojadas privadas contienen registros que especifican cómo desea direccionar el tráfico en una VPC de Amazon. Para obtener más información, consulte [Uso de zonas alojadas privadas](#).

Trabajar con zonas públicas alojadas

Una zona alojada pública es un contenedor que incluye información sobre cómo desea direccionar el tráfico en Internet hacia un dominio específico (como `example.com`) y sus subdominios (como `acme.example.com`, `zenith.example.com`). Puede obtener una zona alojada pública de una de las dos formas siguientes:

- Al registrar un dominio con Route 53, creamos automáticamente una zona alojada.
- Al transferir el servicio DNS de un dominio existente a Route 53, comience con la creación de una zona alojada para el dominio. Para obtener más información, consulte [Establecer Amazon Route 53 como servicio DNS de un dominio existente](#).

En ambos casos, cree registros en la zona alojada para especificar cómo desea dirigir el tráfico del dominio y los subdominios. Por ejemplo, puede crear un registro para enrutar el tráfico de `www.example.com` a una CloudFront distribución o a un servidor web de su centro de datos. Para obtener más información acerca de los registros, consulte [Uso de registros](#).

En este tema se explica cómo utilizar la consola de Amazon Route 53 para crear, enumerar y eliminar las zonas alojadas públicas.

 Note

También puede usar una zona alojada privada de Route 53 para enrutar el tráfico dentro de una o varias VPCs que cree con el servicio Amazon VPC. Para obtener más información, consulte [Uso de zonas alojadas privadas](#).

Temas

- [Consideraciones sobre el uso de zonas alojadas públicas](#)
- [Crear una zona alojada pública](#)
- [Obtener los servidores de nombres para una zona alojada pública](#)
- [Enumeración de zonas alojadas públicas](#)
- [Visualización de métricas de consultas de DNS para una zona alojada pública](#)
- [Eliminación de una zona alojadas pública](#)
- [Comprobación de las respuestas de DNS de Route 53](#)
- [Configuración de servidores de nombres de etiqueta blanca](#)
- [Registros SOA y NS que crea Amazon Route 53 para una zona alojada pública](#)
- [Permite una recuperación acelerada para administrar los registros DNS públicos](#)

Consideraciones sobre el uso de zonas alojadas públicas

Tenga en cuenta las siguientes consideraciones al trabajar con zonas alojadas públicas:

Registros NS y SOA

Cuando crea una zona alojada, Amazon Route 53 genera automáticamente un registro del servidor de nombres (NS) y un registro de inicio de autoridad (SOA) para dicha zona. El registro NS identifica los cuatro servidores de nombres que se proporcionan al registrador o al servicio DNS para que las consultas de DNS se redirijan a los servidores de nombres de Route 53. Para obtener más información acerca de los registros NS y SOA, consulte [Registros SOA y NS que crea Amazon Route 53 para una zona alojada pública](#).

Varias zonas alojadas que tienen el mismo nombre

Puede crear más de una zona alojada que tenga el mismo nombre y agregar diferentes registros para cada zona alojada. Route 53 asigna cuatro servidores de nombres a cada zona alojada, diferentes para cada una de ellas. Al actualizar los registros del servidor de nombres de su registrador, asegúrese de utilizar los servidores de nombres de Route 53 para la zona alojada correcta (es decir, la que contiene los registros que desea que utilice Route 53 al responder a las consultas del dominio). Route 53 nunca devuelve valores de registros de otras zonas alojadas que tengan el mismo nombre.

Conjuntos de delegación reutilizables

De forma predeterminada, Route 53 asigna un conjunto único de cuatro servidores de nombres (conocido colectivamente como un conjunto de delegación) para cada zona alojada creada. Si desea crear un número elevado de zonas alojadas, puede crear un conjunto de delegación reutilizable mediante programación. (Los conjuntos de delegación reutilizables no están disponibles en la consola de Route 53). A continuación, puede crear zonas alojadas mediante programación y asignar el mismo conjunto de delegaciones reutilizable (los mismos cuatro servidores de nombres) a cada zona alojada.

Los conjuntos de delegación reutilizables simplifican la migración del servicio DNS a Route 53, ya que puede indicar a su registrador de nombres de dominio que use los mismos cuatro servidores de nombres para todos los dominios para los que desea usar Route 53 como el servicio DNS. Para obtener más información, consulte [CreateReusableDelegationSet](#) la referencia de la API de Amazon Route 53.

Crear una zona alojada pública

Una zona alojada pública es un contenedor que incluye información sobre cómo desea dirigir el tráfico en Internet hacia un dominio específico (como example.com) y sus subdominios (como acme.example.com, zenith.example.com). Después de crear una zona alojada, cree registros que especifiquen cómo desea dirigir el tráfico del dominio y los subdominios.

Restricciones

Tenga en cuenta las siguientes restricciones para crear zonas alojadas con Route 53.

- Puede crear una zona alojada solo para los dominios para los que tenga permiso para administrar. Por lo general, esto indicará que es el propietario del dominio, aunque también podría estar desarrollando una aplicación para el registrador del dominio.
- Solo puede crear zonas alojadas para dominios y subdominios. Route 53 no admite el alojamiento de dominios de nivel superior (TLD), como .com.

Para crear una zona alojada pública a través de la consola de Route 53

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. Si es la primera vez que utiliza Route 53, seleccione Get started (Introducción) en DNS management (Administración de DNS).

Si ya trabaja con Route 53, seleccione Hosted zones (Zonas alojadas) en el panel de navegación.

3. Elija Create hosted zone (Crear zona alojada).
4. En el panel Create Hosted Zone (Crear zona alojada) escriba el nombre del dominio cuyo tráfico desea dirigir. Si lo desea, también puede escribir un comentario.

Para obtener información sobre cómo especificar caracteres distintos de a-z, 0-9 y - (guion), y cómo especificar nombres de dominio internacionalizados, consulte [Formato de nombres de dominio DNS](#).

5. En Type acepte el valor predeterminado de Public Hosted Zone.
6. Elija Create (Crear).
7. Cree registros que especifiquen cómo desea dirigir el tráfico del dominio y los subdominios. Para obtener más información, consulte [Uso de registros](#).
8. Para utilizar los registros de la nueva zona alojada para dirigir el tráfico de su dominio, consulte el tema pertinente:
 - Si hace que Route 53 sea el servicio DNS de un dominio registrado en otro registrador de dominios, consulte [Establecer Amazon Route 53 como servicio DNS de un dominio existente](#).
 - Si el dominio está registrado en Route 53, consulte [Adición o modificación de servidores de nombres y registros de conexión de un dominio](#).

Obtener los servidores de nombres para una zona alojada pública

Obtendrá los servidores de los nombres de una zona alojada pública si quiere cambiar el servicio DNS del registro de su dominio. Para obtener información acerca de cómo cambiar el servicio DNS, consulte [Establecer Amazon Route 53 como servicio DNS de un dominio existente](#).

Note

Algunos registradores solo permiten especificar servidores de nombres a través de direcciones IP; no permiten especificar nombres de dominio completos. Si su registrador requiere el uso de direcciones IP, puede obtener las direcciones IP de sus servidores de nombres mediante la herramienta dig (para Mac, Unix o Linux) o la herramienta nslookup (para Windows). No solemos cambiar las direcciones IP de los servidores de nombres; si tenemos que cambiar las direcciones IP, se lo notificaremos por adelantado.

Para obtener los servidores de nombres de una zona alojada a través de la consola de Route 53

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, haga clic en Hosted zones (Zonas alojadas).
3. En la página Hosted zones (Zonas alojadas), elija el botón de radio (no el nombre) de la zona alojada y luego View details (Ver detalles).
4. En la página de detalles de la zona alojada, elija Hosted zone details (Detalles de la zona alojada).
5. Anote los nombres de los cuatro servidores que aparecen en Name servers (Servidores de nombres).

Enumeración de zonas alojadas públicas

Puede usar la consola de Amazon Route 53 para enumerar todas las zonas alojadas que creó con la AWS cuenta actual. Para obtener información sobre cómo enumerar las zonas alojadas mediante la API de Route 53, consulte [ListHostedZones](#) la referencia de la API de Amazon Route 53.

Para ver una lista de las zonas alojadas públicas asociadas a una AWS cuenta mediante la consola de Route 53

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Zonas alojadas. La página muestra una lista de las zonas alojadas que están asociadas a la AWS cuenta con la que ha iniciado sesión actualmente.
3. Para filtrar las zonas alojadas, utilice la barra de búsqueda situada en la parte superior de la tabla.

El comportamiento de búsqueda depende de si la zona alojada contiene hasta 2000 registros o más de 2000 registros:

Hasta 2000 zonas alojadas

- Para visualizar los registros que tengan valores específicos, haga clic en la barra de búsqueda, elija una propiedad en la lista desplegable e ingrese un valor. También puede ingresar un valor directamente en la barra de búsqueda y pulsar Entrar. Por ejemplo, para mostrar las zonas alojadas que tienen un nombre que comience por **abc**, ingrese ese valor en la barra de búsqueda y pulse Entrar.
- Para visualizar solo las zonas alojadas que tengan el mismo tipo de zona alojada, seleccione el tipo en la lista desplegable e ingrese el tipo.

Más de 2000 zonas alojadas

- Puede buscar propiedades basadas en el nombre de dominio exacto, todas las propiedades y el tipo.
- Busque con el nombre de dominio exacto para obtener resultados de búsqueda más rápidos.

Visualización de métricas de consultas de DNS para una zona alojada pública

Puede ver el número total de consultas de DNS a las que responde Route 53 para una zona alojada pública especificada o una combinación de zonas alojadas públicas. Las métricas aparecen en CloudWatch, lo que te permite ver un gráfico, elegir el período de tiempo que quieres ver y personalizar las métricas de muchas otras formas. También puede crear alarmas y configurar notificaciones para recibir una notificación cuando el número de consultas de DNS de un periodo de tiempo especificado quede por encima o por debajo de un nivel especificado.

 Note

Route 53 envía automáticamente el número de consultas de DNS a CloudWatch todas las zonas alojadas públicas, por lo que no es necesario configurar nada para poder ver las métricas de las consultas. No se aplican cargos por las métricas de consulta de DNS.

¿Qué consultas de DNS se cuentan?

Las métricas incluyen solo las consultas que los solucionadores de DNS reenvían a Route 53. Si un solucionador de DNS ya ha almacenado en caché la respuesta a una consulta (por ejemplo, la dirección IP de un balanceador de carga para `example.com`), el solucionador continuará devolviendo la respuesta almacenada en caché sin reenviar la consulta a Route 53 hasta que venza el TTL del registro correspondiente.

Dependiendo de la cantidad de las consultas de DNS que se envíen para un nombre de dominio (`example.com`) o nombre de subdominio (`www.example.com`), cuyos solucionadores están utilizando sus usuarios y el TTL para el registro, las métricas de consulta de DNS pueden contener información sobre una única consulta de cada varios miles de consultas que se enviaron a los solucionadores de DNS. Para obtener más información sobre cómo funciona DNS, consulte [Cómo dirige Amazon Route 53 el tráfico de su dominio](#).

¿Cuándo empiezan a aparecer las métricas de consultas de una zona alojada en CloudWatch?

Después de crear una zona alojada, transcurren hasta varias horas antes de que la zona alojada aparezca en CloudWatch. Además, debe enviar una consulta de DNS de un registro de la zona alojada para que haya datos que mostrar.

Las métricas solo están disponibles en EE. UU. Este (Norte de Virginia)

Para obtener métricas en la consola, debe especificar EE. UU. Este (Norte de Virginia) para la región. Para obtener métricas mediante la AWS CLI, debe dejar la AWS región sin especificar o especificarla `us-east-1` como región. Las métricas de Route 53 no están disponibles si elige otra región.

CloudWatch métrica y dimensión para las consultas de DNS

Para obtener información sobre la CloudWatch métrica y la dimensión de las consultas de DNS, consulte [Supervisión de zonas alojadas mediante Amazon CloudWatch](#). Para obtener información sobre CloudWatch las métricas, consulta [Uso de CloudWatch las métricas de Amazon](#) en la Guía del CloudWatch usuario de Amazon.

Obtención de datos más detallados sobre las consultas de DNS

Para obtener información más detallada acerca de cada consulta de DNS a la que responde Route 53, incluidos los siguientes valores, puede configurar el registro de consultas:

- Dominio o subdominio que se solicitó
- La fecha y la hora de la solicitud
- El tipo de registro de DNS (por ejemplo, A o AAAA)
- La ubicación periférica de Route 53 que ha respondido a la consulta de DNS
- El código de respuesta de DNS como, por ejemplo, `NoError` o `ServFail`

Para obtener más información, consulte [Registro de consultas de DNS públicas](#).

Cómo obtener métricas de consulta de DNS

Poco después de crear una zona alojada, Amazon Route 53 comienza a enviar métricas y dimensiones una vez por minuto a CloudWatch. Puede usar los siguientes procedimientos para ver las métricas en la CloudWatch consola o verlas mediante AWS Command Line Interface (AWS CLI).

Temas

- [Visualización de las métricas de consultas de DNS de una zona alojada pública en la CloudWatch consola](#)
- [Obtener métricas de consultas de DNS mediante AWS CLI](#)

Visualización de las métricas de consultas de DNS de una zona alojada pública en la CloudWatch consola

Para ver las métricas de consultas de DNS de las zonas alojadas públicas en la CloudWatch consola, lleve a cabo el siguiente procedimiento.

Para ver las métricas de consultas de DNS de una zona alojada pública en la CloudWatch consola

1. Inicie sesión en Consola de administración de AWS y abra la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, seleccione Métricas.

3. En la lista de AWS regiones de la esquina superior derecha de la consola, selecciona EE.UU. Este (Norte de Virginia). Las métricas de Route 53 no están disponibles si eliges otra AWS región.
4. En la pestaña All metrics, elija Route 53.
5. Elija Hosted Zone Metrics (Métricas de zona alojada).
6. Selecciona la casilla de verificación de una o más zonas alojadas que tengan el nombre de la métrica DNSQueries.
7. En la pestaña Graphed metrics (Métricas incluidas en el gráfico) cambie los valores aplicables para ver las métricas en el formato que desee.

En Estadística, elija Suma o SampleCount; ambas estadísticas muestran el mismo valor.

Obtener métricas de consultas de DNS mediante AWS CLI

Para obtener las métricas de consultas de DNS mediante el AWS CLI, utilice el [get-metric-data](#) comando. Tenga en cuenta lo siguiente:

- La mayoría de los valores del comando se especifican en un archivo JSON independiente. Para obtener más información, consulte [get-metric-data](#).
- El comando devuelve un valor para cada intervalo que especifique para Period en el archivo JSON. Period está en segundos, por lo que si especifica un periodo de tiempo de cinco minutos y especifica 60 para Period, obtendrá cinco valores. Si especifica un periodo de cinco minutos y especifica 300 en Period, obtendrá un valor.
- En el archivo JSON, puede especificar cualquier valor para Id.
- Deje la AWS región sin especificar o especifíquela us-east-1 como región. Las métricas de Route 53 no están disponibles si elige otra región. Para obtener más información, consulte [Configuración de la AWS CLI](#) en la Guía del AWS Command Line Interface usuario.

Este es el AWS CLI comando que se utiliza para obtener las métricas de las consultas de DNS correspondientes al período de cinco minutos comprendido entre las 4:01 y las 4:07 del 1 de mayo de 2019. El parámetro metric-data-queries hace referencia al archivo JSON de ejemplo que sigue al comando.

```
aws cloudwatch get-metric-data --metric-data-queries file:///./metric.json --start-time 2019-05-01T04:01:00Z --end-time 2019-05-01T04:07:00Z
```

A continuación se muestra el archivo JSON de ejemplo:

```
[
  {
    "Id": "my_dns_queries_id",
    "MetricStat": {
      "Metric": {
        "Namespace": "AWS/Route53",
        "MetricName": "DNSQueries",
        "Dimensions": [
          {
            "Name": "HostedZoneId",
            "Value": "Z1D633PJN98FT9"
          }
        ]
      },
      "Period": 60,
      "Stat": "Sum"
    },
    "ReturnData": true
  }
]
```

Esta es la salida de este comando. Tenga en cuenta lo siguiente:

- La hora de inicio y la hora de finalización del comando abarcan un periodo de tiempo de siete minutos, de 2019-05-01T04:01:00Z a 2019-05-01T04:07:00Z.
- Solo hay seis valores devueltos. No hay ningún valor para 2019-05-01T04:05:00Z porque no había consultas de DNS durante ese minuto.
- El valor de Period especificado en el archivo JSON es 60 (segundos), por lo que los valores se notifican en intervalos de un minuto.

```
{
  "MetricDataResults": [
    {
      "Id": "my_dns_queries_id",
      "StatusCode": "Complete",
      "Label": "DNSQueries",
      "Values": [
        101.0,
        115.0,
```

```
        103.0,  
        127.0,  
        111.0,  
        120.0  
    ],  
    "Timestamps": [  
        "2019-05-01T04:07:00Z",  
        "2019-05-01T04:06:00Z",  
        "2019-05-01T04:04:00Z",  
        "2019-05-01T04:03:00Z",  
        "2019-05-01T04:02:00Z",  
        "2019-05-01T04:01:00Z"  
    ]  
}  
]  
}
```

Eliminación de una zona alojadas pública

En esta sección, se explica cómo eliminar una zona alojada pública con la consola de Amazon Route 53.

Solamente puede eliminar una zona alojada si los únicos registros son los registros SOA y NS predeterminados. Si su zona alojada contiene otros registros, debe eliminarlos para poder eliminar su zona alojada. Esto le impide eliminar accidentalmente una zona alojada que siga conteniendo registros.

Temas

- [Cómo evitar que el tráfico se dirija a su dominio](#)
- [Eliminación de zonas alojadas públicas creadas por otro servicio](#)
- [Elimine una zona alojada pública mediante la consola de Route 53.](#)

Cómo evitar que el tráfico se dirija a su dominio

Si desea conservar el registro del dominio pero desea detener el enrutamiento del tráfico de Internet a su sitio web o aplicación web, le recomendamos que elimine registros en la zona alojada en lugar de eliminar la zona alojada.

Important

La eliminación de una zona alojada es una acción que no se puede deshacer. Debe crear una nueva zona alojada y actualizar los servidores de nombres de su registro de dominio, proceso que puede requerir hasta 48 horas en surtir efecto. Además, si elimina una zona alojada, alguien podría piratear el dominio y dirigir el tráfico a sus propios recursos utilizando su nombre de dominio.

Si ha delegado la responsabilidad de un subdominio a una zona alojada y desea eliminar la zona alojada secundaria, también debe actualizar la zona alojada principal eliminando el registro de NS que tiene el mismo nombre que la zona alojada secundaria. Por ejemplo, si desea eliminar la zona alojada `acme.example.com`, también debe eliminar el registro de NS `acme.example.com` en la zona alojada `example.com`. Se recomienda eliminar primero el registro de NS y esperar a que transcurra el tiempo del TTL en el registro de NS antes de eliminar la zona alojada secundaria. Esto garantiza que no se pueda piratear la zona alojada secundaria durante el período en el que los solucionadores de DNS todavía tengan los servidores de nombres para la zona alojada secundaria en caché.

Si desea evitar la tarifa mensual correspondiente a la zona alojada, puede transferir el servicio de DNS del dominio a un servicio de DNS gratuito. Cuando transfiere el servicio de DNS, debe actualizar los servidores de nombres del registro de dominio. Si el dominio está registrado en Route 53, consulte [Adición o modificación de servidores de nombres y registros de conexión de un dominio](#) para obtener información sobre cómo sustituir los servidores de nombres de Route 53 por los servidores de nombres del nuevo servicio DNS. Si el dominio está registrado en otro registrador, utilice el método proporcionado por el registrador para actualizar los servidores de nombres del registro de dominio. Para obtener más información, busque en Internet "servicio DNS gratis".

Eliminación de zonas alojadas públicas creadas por otro servicio

Si otro servicio ha creado una zona alojada, no puede eliminarla con la consola de Route 53. En su lugar, ha de utilizar el proceso correspondiente del otro servicio:

- **AWS Cloud Map**— Para eliminar una zona alojada que se AWS Cloud Map creó al crear un espacio de nombres DNS público, elimine el espacio de nombres. AWS Cloud Map elimina la zona alojada automáticamente. Para obtener más información, consulte [Eliminación de espacios de nombres](#) en la AWS Cloud Map Guía para desarrolladores de .
- **Descubrimiento de servicios de Amazon Elastic Container Service (Amazon ECS)**: para eliminar una zona alojada pública que Amazon ECS creó al crear un servicio mediante la detección de

servicios, elimine los servicios de Amazon ECS que utilizan el espacio de nombres y elimine el espacio de nombres. Para obtener más información, consulte [Eliminación de un servicio](#) en la Guía para desarrolladores de Amazon Elastic Container Service.

Elimine una zona alojada pública mediante la consola de Route 53.

Para utilizar la consola de Route 53 para eliminar una zona alojada pública, realice el siguiente procedimiento.

Elimine una zona alojada pública mediante la consola de Route 53.

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Hosted zones (Zonas alojadas) y elija el enlace resaltado de la zona alojada que quiera eliminar.
3. Confirme que la zona alojada que desea eliminar solo contiene un registro NS y SOA. Si contiene registros adicionales, elimínelos: También tendrá que desactivar la firma de DNSSEC:

 Note

Si intenta eliminar la zona alojada sin cumplir estos requisitos, Route 53 arrojará un error:

- Si la firma de DNSSEC está activada: la zona alojada especificada contiene claves de firma de claves de DNSSEC y, por lo tanto, no se puede eliminar.
 - Si existen otros conjuntos de registros de recursos (distintos de los registros SOA y NS predeterminados): la zona alojada especificada contiene conjuntos de registros de recursos no obligatorios y, por lo tanto, no se puede eliminar.
-
- En la lista Records (Registros) de la página de detalles de la zona alojada, si la lista de registros incluye registros cuyo valor para la columna Type (Tipo) es distinto de NS o SOA, elija la fila y, a continuación, elija Delete (Eliminar).

Para seleccionar varios registros consecutivos, elija la primera fila, mantenga presionada la tecla Mayús y elija la última fila. Para seleccionar varios registros no consecutivos, elija la primera fila, mantenga presionada la tecla Ctrl y elija las filas restantes.

 Note

Si ha creado cualquier registro NS para subdominios en la zona alojada, elimine también esos registros.

4. Regrese a la página Hosted zones (Zonas alojadas) y elija la fila de la zona alojada que desea eliminar.
5. Elija Eliminar.
6. Escriba la clave de confirmación y elija Delete (Eliminar).
7. Si desea hacer que el dominio no esté disponible en Internet, le recomendamos que transfiera el servicio DNS a un servicio DNS gratuito y, a continuación, eliminar la zona alojada de Route 53. Esto evita que las futuras consultas DNS puedan dirigirse erróneamente.

Si el dominio está registrado en Route 53, consulte [Adición o modificación de servidores de nombres y registros de conexión de un dominio](#) para obtener información sobre cómo sustituir los servidores de nombres de Route 53 por los servidores de nombres del nuevo servicio DNS. Si el dominio está registrado en otro registrador, utilice el método proporcionado por el registrador para cambiar servidores de nombres en el dominio.

 Note

Si desea eliminar una zona alojada para un subdominio (acme.example.com), no es necesario cambiar servidores de nombres del dominio (example.com).

Comprobación de las respuestas de DNS de Route 53

Si ha creado una zona alojada de Amazon Route 53 para su dominio, puede utilizar la herramienta de comprobación de DNS de la consola para ver cómo responderá Route 53 a las consultas de DNS si configura su dominio para utilizar Route 53 como servicio DNS. Para los registros de geolocalización, geoproximidad y latencia, también puede simular las consultas desde una dirección IP concreta de un and/or cliente de resolución de DNS para averiguar qué respuesta devolvería Route 53.

 Important

La herramienta no envía consultas al sistema de nombres de dominio, solo responde en función de la configuración de los registros de la zona alojada. La herramienta devuelve la misma información independientemente de si la zona alojada se está utilizando actualmente para dirigir el tráfico del dominio.

La herramienta de comprobación de DNS funciona solo para zonas alojadas públicas.

 Note

La herramienta de comprobación de DNS muestra información similar a la que cabría esperar de la sección de respuestas del comando `dig`. Por lo tanto, si consulta los servidores de nombres de un subdominio que apuntan a los servidores de nombres principales, no se mostrará esta información.

Temas

- [Uso de la herramienta de comprobación para ver cómo responde Amazon Route 53 a consultas de DNS](#)
- [Uso de la herramienta de comprobación para simular consultas desde direcciones IP específicas \(solo para registros de geolocalización y latencia\)](#)

Uso de la herramienta de comprobación para ver cómo responde Amazon Route 53 a consultas de DNS

Puede utilizar la herramienta para ver qué respuesta devuelve Amazon Route 53 a una consulta de DNS para un registro.

Para usar la herramienta de comprobación y ver cómo responde Route 53 a consultas de DNS

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/route53/>
2. En el panel de navegación, elija Hosted Zones.
3. En la página Hosted Zones, elija el nombre de una zona alojada nueva. La consola muestra la lista de registros de dicha zona alojada.

4. Para ir directamente a la página Check response from Route 53 (Verificar respuesta de Route 53), elija Test record (Registro de prueba).
5. Especifique los siguientes valores:
 - El nombre del registro, excepto el nombre de la zona alojada. Por ejemplo, para comprobar `www.example.com`, ingrese `www`. Para comprobar `example.com`, deje el campo Record name (Nombre de registro) en blanco.
 - El tipo del registro que desea comprobar, como A o CNAME.
6. Elija Get Response.
7. La sección Response returned by Route 53 incluye los siguientes valores:

Código de respuesta de DNS

Un código que indica si la consulta era válida o no. El código de respuesta más habitual es NOERROR, para indicar que la consulta era válida. Si la respuesta no es válida, Route 53 devuelve un código de respuesta que explica el motivo. Para obtener una lista de posibles códigos de respuesta, consulte [DNS RCODES](#) en el sitio web de IANA.

Protocolo

El protocolo que Amazon Route 53 utilizó para responder a la consulta, UDP o TCP.

Respuesta devuelta por Route 53

El valor que devolvería Route 53 a una aplicación web. Puede ser uno de los siguientes:

- Para los registros sin alias, la respuesta contiene el valor o los valores del registro.
- Para varios registros que tengan el mismo nombre y tipo, que incluyan ponderación, geolocalización, latencia y conmutación por error, la respuesta contiene el valor del registro adecuado, en función de la solicitud.
- En el caso de los registros de alias que hacen referencia a AWS recursos distintos de otro registro, la respuesta contiene una dirección IP o un nombre de dominio para el AWS recurso, según el tipo de recurso.
- Para registros de alias que hacen referencia a otros registros, la respuesta contiene el valor o los valores del registro al que se hace referencia.

Uso de la herramienta de comprobación para simular consultas desde direcciones IP específicas (solo para registros de geolocalización y latencia)

Si ha creado registros de latencia o de geolocalización, puede utilizar la herramienta de comprobación para simular consultas desde la dirección IP para un solucionador de DNS y un cliente.

Para utilizar la herramienta de comprobación para simular consultas desde direcciones IP específicas

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Hosted Zones.
3. En la página Hosted Zones, elija el nombre de una zona alojada nueva. La consola muestra la lista de registros de dicha zona alojada.
4. Para ir directamente a la página Check response from Route 53, elija Test record set.

Para ir a la página Check response from Route 53 (Comprobar respuesta de Route 53) de un registro específico, seleccione la casilla para ese registro y elija Test record set (Probar conjunto de registros).

5. Si elige Test record set (Probar conjunto de registros) sin seleccionar antes un registro, especifique los siguientes valores:
 - El nombre del registro, excepto el nombre de la zona alojada. Por ejemplo, para comprobar `www.example.com`, ingrese `www`. Para comprobar `example.com`, deje el campo Record name (Nombre de registro) en blanco.
 - El tipo del registro que desea comprobar, como A o CNAME.
6. Especifique los valores aplicables:

Dirección IP de solucionador

Especifique una IPv6 dirección IPv4 o para simular la ubicación del solucionador de DNS que utiliza un cliente para realizar las solicitudes. Esto resulta útil para comprobar los registros de latencia y geolocalización. Si omite este valor, la herramienta utilizará la dirección IP de un solucionador de DNS de la región AWS EE.UU. Este (Virginia del Norte) (us-east-1).

IP de subred del cliente EDNS0

Si el solucionador admite EDNS0, escriba la IP de subred del cliente para una dirección IP en la ubicación geográfica correspondiente, por ejemplo, 192.0.2.0 o 2001:db8:85a3::8a2e:370:7334.

Máscara de subred

Si especifica una dirección IP para EDNS0 client subnet IP, puede especificar el número de bits de la dirección IP que desea que la herramienta de comprobación incluya en la consulta de DNS. Por ejemplo, si especifica 192.0.2.44 para EDNS0 client subnet IP y 24 para Subnet mask, la herramienta de comprobación simulará una consulta desde 192.0.2.0/24. El valor predeterminado es de 24 bits para IPv4 las direcciones y 64 bits para las direcciones. IPv6

7. Elija Get Response.
8. La sección Response returned by Route 53 incluye los siguientes valores:

Consulta de DNS enviada a Route 53

La consulta, en [formato BIND](#), que la herramienta de comprobación envió a Route 53. Este es el mismo formato que usaría una aplicación web para enviar una consulta. Los tres valores suelen ser el nombre del registro, IN (es decir, Internet) y el tipo de registro.

Código de respuesta de DNS

Un código que indica si la consulta era válida o no. El código de respuesta más habitual es NOERROR, para indicar que la consulta era válida. Si la respuesta no es válida, Route 53 devuelve un código de respuesta que explica el motivo. Para obtener una lista de posibles códigos de respuesta, consulte [DNS RCODES](#) en el sitio web de IANA.

Protocolo

El protocolo que Amazon Route 53 utilizó para responder a la consulta, UDP o TCP.

Respuesta devuelta por Route 53

El valor que devolvería Route 53 a una aplicación web. Puede ser uno de los siguientes:

- Para los registros sin alias, la respuesta contiene el valor o los valores del registro.
- Para varios registros que tengan el mismo nombre y tipo, que incluyan ponderación, geolocalización, latencia y conmutación por error, la respuesta contiene el valor del registro adecuado, en función de la solicitud.

- En el caso de los registros de alias que hacen referencia a AWS recursos distintos de otro registro, la respuesta contiene una dirección IP o un nombre de dominio para el AWS recurso, según el tipo de recurso.
- Para registros de alias que hacen referencia a otros registros, la respuesta contiene el valor o los valores del registro al que se hace referencia.

Configuración de servidores de nombres de etiqueta blanca

Cada zona alojada de Amazon Route 53 se asocia a cuatro servidores de nombres, conocidos colectivamente como conjunto de delegación. El nombre predeterminado de los servidores de nombres es similar a ns-2048.awsdns-64.com. Si desea que el nombre de dominio de sus servidores de nombres sea el mismo que el nombre de dominio de la zona alojada, por ejemplo, ns1.example.com, puede configurar servidores de nombres de etiqueta blanca, también conocidos como servidores de nombres personalizados o servidores de nombres privados.

Los siguientes pasos explican cómo configurar un conjunto de cuatro servidores de nombres de etiqueta blanca que puede reutilizar para varios dominios. Por ejemplo, suponga que posee los dominios example.com, example.org y example.net. Con este procedimiento, puede configurar servidores de nombres de etiqueta blanca para example.com y reutilizarlos con example.org y example.net.

Temas

- [Paso 1: Crear un conjunto de delegación reutilizable de Route 53](#)
- [Paso 2: Crear o volver a crear zonas alojadas de Amazon Route 53 y cambiar el TTL de los registros SOA y NS](#)
- [Paso 3: Volver a crear los registros para las zonas alojadas](#)
- [Paso 4: Obtener direcciones IP](#)
- [Paso 5: Crear registros para servidores de nombres de etiqueta blanca](#)
- [Paso 6: Actualizar los registros SOA y NS](#)
- [Paso 7: Crear registros de adherencia y cambiar los servidores de nombres del registrador](#)
- [Paso 8: Monitorizar el tráfico para el sitio web o aplicación](#)
- [Paso 9: TTLs Vuelva a sus valores originales](#)
- [Paso 10: Ponerse en contacto con los servicios DNS recursivos \(opcional\)](#)

Paso 1: Crear un conjunto de delegación reutilizable de Route 53

Los servidores de nombres de etiqueta blanca están asociados a un conjunto de delegación de Route 53 reutilizable. Puede usar servidores de nombres de marca blanca para una zona alojada solo si la zona alojada y el conjunto de delegación reutilizable los creó la misma AWS cuenta.

Para crear un conjunto de delegación reutilizable, puede usar la API de Route 53, la AWS CLI o una de las AWS SDKs. Para obtener más información, consulte la siguiente documentación sobre :

- API de Route 53: consulte [CreateReusableDelegationSet](#) la referencia de la API de Amazon Route 53
- AWS CLI: consulte [create-reusable-delegation-set](#) en la referencia de AWS CLI comandos
- AWS SDKs Consulte la documentación del SDK correspondiente en la página de [AWS documentación](#)

Paso 2: Crear o volver a crear zonas alojadas de Amazon Route 53 y cambiar el TTL de los registros SOA y NS

Cree o vuelva a crear las zonas alojadas de Amazon Route 53:

- Si no utiliza Route 53 como servicio DNS para los dominios en los que desea utilizar servidores de nombres de etiqueta blanca: cree las zonas alojadas y especifique el conjunto de delegación reutilizable que creó en el paso anterior con cada zona alojada. Para obtener más información, consulte [CreateHostedZone](#) la referencia de la API de Amazon Route 53.
- Si está utilizando Route 53 como servicio DNS para los dominios en los que desea utilizar servidores de nombres de marca blanca: debe volver a crear las zonas alojadas en las que desea utilizar servidores de nombres de marca blanca y especificar el conjunto de delegación reutilizable que creó en el paso anterior para cada zona alojada.

Important

No puede cambiar los servidores de nombres que están asociados a una zona alojada existente. Puede asociar un conjunto de delegación reutilizable a una zona alojada solo cuando crea esta.

Al crear las zonas alojadas y antes de intentar acceder a los recursos de los dominios correspondientes, cambie los siguientes valores de TTL para cada zona alojada:

- Cambie el valor del TTL para el registro NS para la zona alojada a 60 segundos o menos.
- Cambie el valor del TTL mínimo para el registro de SOA para la zona alojada a 60 segundos o menos. Este es el último valor del registro de SOA.

Si por error proporciona a su registrador direcciones IP incorrectas para sus servidores de nombres de etiqueta blanca, su sitio web dejará de estar disponible y permanecerá así durante el período que dure el TTL después de corregir el problema. Al configurar un valor de TTL bajo, reduce el tiempo que su sitio web no está disponible.

Para obtener más información sobre la creación de zonas alojadas y la especificación de un conjunto de delegación reutilizable para los servidores de nombres de las zonas alojadas, consulte [CreateHostedZone](#) la referencia de la API de Amazon Route 53.

Paso 3: Volver a crear los registros para las zonas alojadas

Cree registros en las zonas alojadas que creó en el paso 2:

- Si está migrando un servicio DNS para sus dominios a Amazon Route 53: es posible que pueda crear registros importando información sobre los registros existentes. Para obtener más información, consulte [Creación de registros mediante la importación de un archivo de zona](#).
- Si está sustituyendo las zonas alojadas existentes para utilizar servidores de nombres de etiqueta blanca: en las nuevas zonas alojadas, vuelva a crear los registros que aparecen en las zonas alojadas actuales. Route 53 no proporciona ningún método de exportación de registros desde una zona alojada, pero algunos proveedores externos sí lo hacen. A continuación, puede utilizar la característica de importación de Route 53 para importar registros sin alias cuya política de direccionamiento sea simple. No hay forma de exportar y reimportar registros de alias o registros cuya política de direccionamiento sea distinta de la simple.

Para obtener información sobre la creación de registros mediante la API de Route 53, consulte [CreateHostedZone](#) la referencia de la API de Amazon Route 53. Para obtener información sobre cómo crear registros mediante la consola de Route 53, consulte [Uso de registros](#).

Paso 4: Obtener direcciones IP

Obtenga las IPv6 direcciones IPv4 y las direcciones de los servidores de nombres del conjunto de delegación reutilizable y complete la siguiente tabla.

Nombre de un servidor de nombres en el conjunto de delegación reutilizable (ejemplo: ns-2048.awsdns-64.com)	IPv4 y IPv6 direcciones	Nombre que desea asignar al servidor de nombres de etiqueta blanca (por ejemplo: ns1.example.com)
	IPv4:	
	IPv6:	
	IPv4:	
	IPv6:	
	IPv4:	
	IPv6:	
	IPv4:	
	IPv6:	

Por ejemplo, suponga que los cuatro servidores de nombres de su conjunto de delegación reutilizable son:

- ns-2048.awsdns-64.com
- ns-2049.awsdns-65.net
- ns-2050.awsdns-66.org
- ns-2051.awsdns-67.co.uk

Estos son los comandos de Linux y Windows que podría ejecutar a fin de obtener las direcciones IP para los primeros de los cuatro servidores de nombres:

comandos dig para Linux

```
% dig A ns-2048.awsdns-64.com +short
192.0.2.117
```

```
% dig AAAA ns-2048.awsdns-64.com +short  
2001:db8:85a3::8a2e:370:7334
```

comando nslookup para Windows

```
c:\> nslookup ns-2048.awsdns-64.com  
Non-authoritative answer:  
Name:      ns-2048.awsdns-64.com  
Addresses:  2001:db8:85a3::8a2e:370:7334  
            192.0.2.117
```

Paso 5: Crear registros para servidores de nombres de etiqueta blanca

En la zona alojada que tenga el mismo nombre (como `example.com`) que el nombre de dominio de los servidores de nombres de etiqueta blanca (como `ns1.example.com`), cree ocho registros:

- Un registro A para cada servidor de nombres de etiqueta blanca
- Un registro AAAA para cada servidor de nombres de etiqueta blanca

Important

Si utiliza los mismos servidores de nombres de etiqueta blanca para dos o más zonas alojadas, no ejecute este paso para las demás zonas alojadas.

Para cada registro, especifique los valores siguientes. Consulte la tabla que rellenó en el paso anterior:

Política de direccionamiento

Especifique Simple routing (Enrutamiento simple).

Nombre del registro

Nombre que desea asignar a uno de sus servidores de nombres de etiqueta blanca; por ejemplo, `ns1.example.com`. Para el prefijo (`ns1` en este ejemplo), puede utilizar cualquier valor aceptable para un nombre de dominio.

Valor/ruta de destino del tráfico

La IPv6 dirección IPv4 o la dirección de uno de los servidores de nombres de Route 53 del conjunto de delegación reutilizable.

Important

Si se equivocó al especificar las direcciones IP al crear los registros para sus servidores de nombres de etiqueta blanca, su sitio o aplicación web no estarán disponibles en Internet al realizar los pasos siguientes. Aunque corrija inmediatamente las direcciones IP, su sitio o aplicación web no estarán disponibles durante el tiempo que dure el TTL.

Tipo de registro

Especifique A cuando cree registros para las IPv4 direcciones.

Especifique AAAA al crear registros para las IPv6 direcciones.

TTL (segundos)

Este valor es la cantidad de tiempo que los solucionadores de DNS almacenan en caché la información de este registro antes de transmitir otra consulta de DNS a Route 53. Le recomendamos que especifique un valor inicial de 60 segundos o menos, para que pueda recuperarse rápidamente si especifica valores incorrectos en estos registros accidentalmente.

Paso 6: Actualizar los registros SOA y NS

Actualice los registros SOA y NS en las zonas alojadas para las que desee utilizar servidores de nombres de etiqueta blanca. Realice los Pasos 6 a 8 para una zona alojada y el correspondiente dominio cada vez. Después, repita para otra zona alojada y dominio.

Important

Comience por la zona alojada de Amazon Route 53 que tenga el mismo nombre de dominio (como example.com) que los servidores de nombres de etiqueta blanca (como ns1.example.com).

1. Actualice el registro de SOA reemplazando el nombre del servidor de nombres de Route 53 por el nombre de uno de los servidores de nombres de etiqueta blanca

Ejemplo

Reemplazar el nombre del servidor de nombres de Route 53:

ns-2048.awsdns-64.net. hostmaster.example.com. 1 7200 900 1209600 60

por el nombre de uno de los servidores de nombres de etiqueta blanca:

ns1.example.com. hostmaster.example.com. 1 7200 900 1209600 60

Note

Ha cambiado el último valor, el tiempo mínimo de vida (TTL), en [Paso 2: Crear o volver a crear zonas alojadas de Amazon Route 53 y cambiar el TTL de los registros SOA y NS.](#)

Para obtener información sobre cómo actualizar registros mediante la consola de Route 53, consulte [Editar registros](#).

2. En el registro NS, anote los nombres de los servidores de nombres actuales para el dominio, para que pueda volver a estos servidores de nombres si fuera necesario.
3. Actualizar el registro NS. Cambie el nombre de los servidores de nombres de Route 53 por los nombres de sus cuatro servidores de nombres de etiqueta blanca; por ejemplo, ns1.example.com, ns2.example.com, ns3.example.com y ns4.example.com.

Paso 7: Crear registros de adherencia y cambiar los servidores de nombres del registrador

Utilice el método proporcionado por el registrador para crear registros de adherencia y cambiar los servidores de nombres del registrador:

1. Agregar registros de adherencia:
 - Si está actualizando el dominio que tiene el mismo nombre de dominio que los servidores de nombres de etiqueta blanca: Cree cuatro registros de adherencia para que los nombres y direcciones IP coincidan con los valores que ha obtenido en el paso 4. Incluya IPv4 tanto la dirección como la IPv6 dirección de un servidor de nombres de marca blanca en el registro adhesivo correspondiente, por ejemplo:

ns1.example.com: direcciones IP = 192.0.2.117 y 2001:db8:85a3::8a2e:370:7334

Los registradores utilizan una terminología variada para los registros de adherencia. Podría hacerse referencia a esto como registro de nuevos servidores de nombres o algo similar.

- Si está actualizando otro dominio: en el caso de que Route 53 sea su servicio DNS, primero debe completar el paso indicado en la viñeta anterior y crear los registros de adherencia que coincidan con el nombre de dominio. A continuación, vaya al paso 2 en este procedimiento.
2. Cambie los servidores de nombres del dominio por los nombres de los servidores de nombres de etiqueta blanca.

Si utiliza Amazon Route 53 como servicio DNS, consulte [Adición o modificación de servidores de nombres y registros de conexión de un dominio](#).

Paso 8: Monitorizar el tráfico para el sitio web o aplicación

Supervise el tráfico para el sitio web o aplicación para los que ha creado registros de adherencia y ha cambiado los servidores de nombres en el paso 7:

- Si el tráfico se detiene: utilice el método proporcionado por el registrador para devolver los servidores de nombres del dominio a los servidores de nombres de Route 53 anteriores. Se trata de los servidores de nombres que anotó en el paso 6b. A continuación, determine qué ha fallado.
- Si el tráfico no se ve afectado: repita los pasos 6 a 8 para el resto de las zonas alojadas con las que desea utilizar los mismos servidores de nombres de etiqueta blanca.

Paso 9: TTLs Vuelva a sus valores originales

Para todas las zonas alojadas que están utilizando ahora servidores de nombres de etiqueta blanca, cambie los siguientes valores:

- Cambie el TTL para el registro NS de la zona alojada a un valor más habitual; por ejemplo, 172800 segundos (dos días).
- Cambie el TTL mínimo para el registro de SOA de la zona alojada a un valor más normal; por ejemplo, 900 segundos. Este es el último valor del registro de SOA.

Paso 10: Ponerse en contacto con los servicios DNS recursivos (opcional)

Opcional Si utiliza el enrutamiento de geolocalización de Amazon Route 53, póngase en contacto con los servicios de DNS recursivo que admiten la `edns-client-subnet` extensión de EDNS0 y asígneles los nombres de sus servidores de nombres de marca blanca. De este modo, se garantiza que estos servicios de DNS seguirán dirigiendo consultas de DNS a la ubicación óptima de Route 53 en función de la ubicación geográfica aproximada de la que provino la consulta.

Registros SOA y NS que crea Amazon Route 53 para una zona alojada pública

Para cada zona alojada pública que se crea, Amazon Route 53 genera automáticamente un registro de servidor de nombres (NS) y un registro de inicio autoridad (SOA). Apenas necesita cambiar estos registros.

Temas

- [El registro de servidor de nombres \(NS\)](#)
- [El registro de inicio de autoridad \(SOA\)](#)

El registro de servidor de nombres (NS)

Amazon Route 53 crea automáticamente un registro de servidor de nombres (NS) que tiene el mismo nombre que la zona alojada. Enumera los cuatro servidores de nombres que son los autorizados para su zona alojada. Excepto en raras circunstancias, le recomendamos que no añada, cambie o elimine servidores de nombres en este registro.

Los ejemplos siguientes muestran el formato para los nombres de servidores de nombres de Route 53 (son solo ejemplos; no los utilice cuando actualice los registros de servidor de nombres de su registrador):

- ns-2048.awsdns-64.com
- ns-2049.awsdns-65.net
- ns-2050.awsdns-66.org
- ns-2051.awsdns-67.co.uk

Para obtener la lista de los servidores de nombres para su zona alojada:

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/route53/>

2. En el panel de navegación, haga clic en Hosted zones (Zonas alojadas).
3. En la página Hosted zones (Zonas alojadas), elija el botón de radio (no el nombre) de la zona alojada y luego View details (Ver detalles).
4. En la página de detalles de la zona alojada, elija Hosted zone details (Detalles de la zona alojada).
5. Anote los nombres de los cuatro servidores que aparecen en Name servers (Servidores de nombres).

Para obtener información acerca de cómo migrar el servicio DNS de otro proveedor de servicios DNS a Route 53, consulte [Establecer Amazon Route 53 como servicio DNS de un dominio existente](#).

El registro de inicio de autoridad (SOA)

El registro de inicio de autoridad (SOA) identifica la información de DNS básica sobre el dominio, por ejemplo:

```
ns-2048.awsdns-64.net. hostmaster.example.com. 1 7200 900 1209600 86400
```

Un registro de SOA incluye los siguientes elementos:

- El servidor de nombres de Route 53 que creó el registro de SOA; por ejemplo, `ns-2048.awsdns-64.net`.
- La dirección de correo electrónico del administrador. El símbolo @ se sustituye por un punto; por ejemplo, `hostmaster.example.com`. El valor predeterminado es una dirección de correo electrónico `amazon.com` que no se supervisa.
- Un número de serie que dispone de la opción de incremento siempre que se actualiza un registro en la zona alojada. Route 53 no incrementa el número de forma automática. (Los servicios DNS usan que admiten DNS secundario usan el número de serie). En este ejemplo, el valor es 1.
- El tiempo de actualización (en segundos) que los servidores DNS secundarios esperan antes de consultar el registro de SOA del servidor DNS primario y comprobar si hay cambios. En este ejemplo, el valor es 7200.
- El intervalo de reintento (en segundos) que un servidor secundario espera antes de reintentar una transferencia de zona errónea. Normalmente, el tiempo de reintento es inferior al de actualización. En este ejemplo, el valor es 900 (15 minutos).
- El tiempo en segundos durante el cual un servidor secundario seguirá intentando completar una transferencia de zona. Si este tiempo finaliza antes de efectuar una transferencia de zona correcta,

el servidor secundario dejará de responder a las consultas, ya que considera sus datos demasiado antiguos para ser de confianza. En este ejemplo el valor es 1209600 (dos semanas).

- El tiempo mínimo de vida (TTL). Este valor permite definir el período de tiempo durante el que los solucionadores recursivos deben almacenar en caché las siguientes respuestas de Route 53:

NXDOMAIN

No hay ningún registro de ningún tipo con el nombre especificado en la consulta DNS; por ejemplo, ejemplo.com. Tampoco hay registros que sean elementos secundarios del nombre especificado en la consulta DNS; por ejemplo, zenith.ejemplo.com.

NODATA

Hay al menos un registro con el nombre especificado en la consulta DNS, pero ninguno de esos registros tiene el tipo especificado en la consulta DNS (por ejemplo, A).

Cuando un solucionador DNS almacena en caché una respuesta NXDOMAIN o NODATA, esto se denomina almacenamiento en caché negativo.

La duración del almacenamiento en caché negativo es el valor más bajo de los siguientes valores:

- Este valor: el TTL mínimo del registro de SOA. En el ejemplo el valor es 86400 (un día).
- Valor de TTL para el registro de SOA. El valor de predeterminado es de 900 segundos. Para obtener más información acerca de cómo cambiar este valor, consulte [Editar registros](#).

Si Route 53 responde a las consulta de DNS con una respuesta NXDOMAIN o NODATA (una respuesta negativa), se le cobrará la tarifa de las consultas estándar. (Vea “Consultas” en [Precios de Amazon Route 53](#)). Si le preocupa el coste de las respuestas negativas, una opción es cambiar el TTL del registro de SOA y el TTL mínimo del registro de SOA (este valor o ambos). Tenga en cuenta que aumentarlas TTLs, que se aplican a las respuestas negativas en toda la zona alojada, puede tener efectos tanto positivos como negativos:

- Los solucionadores DNS de Internet almacenan en caché la inexistencia de registros durante períodos más largos, lo que reduce el número de consultas que se reenvían a Route 53. Esto reduce los gastos de Route 53 por las consulta de DNS.
- Sin embargo, si alguna vez elimina por error un registro válido y posteriormente lo vuelve a crear, los solucionadores DNS almacenarán en caché la respuesta negativa (este registro no existe) durante un período más largo. Esto aumentará el tiempo que los clientes o usuarios no pueden acceder al recurso correspondiente; por ejemplo, un servidor web de acme.ejemplo.com.

Para encontrar sus registros SOA en Route 53

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Zonas alojadas.
3. Seleccione el nombre vinculado del dominio para el que desea ver los registros.
4. En la sección Records (Registros) puede ver todos los registros enumerados y también puede filtrar registros para encontrar su valor SOA.

Permite una recuperación acelerada para administrar los registros DNS públicos

La recuperación acelerada de Route 53 para administrar registros DNS públicos está diseñada para alcanzar un objetivo de tiempo de recuperación (RTO) de 60 minutos en caso de que el servicio no esté disponible en la región de EE. UU. Este (Virginia del Norte). Si está activado en una zona alojada pública de Route 53, podrá volver a realizar cambios en los registros de DNS de la zona alojada pública en aproximadamente 60 minutos después de AWS detectar que las operaciones en la región de EE. UU. Este (Virginia del Norte) están alteradas.

Important

La recuperación acelerada solo está disponible para las zonas de alojamiento público. No se admiten las zonas alojadas privadas.

Note

La resolución de consultas de DNS desde el plano de datos de Route 53 sigue funcionando con normalidad durante el deterioro del servicio regional. Consulte [Resiliencia en Route 53](#) para comprender mejor las operaciones del plano de datos en comparación con las del plano de control.

Temas

- [Cómo funciona la recuperación acelerada de los registros DNS públicos](#)
- [Volver a enviar los cambios de DNS tras la conmutación por error](#)
- [Vuelva a la región EE.UU. Este \(Virginia del Norte\)](#)

- [Consideraciones adicionales](#)
- [¿Cómo habilitar la recuperación acelerada para administrar los registros DNS públicos](#)

Cómo funciona la recuperación acelerada de los registros DNS públicos

Cuando la recuperación acelerada esté habilitada, Route 53 conservará una copia de la zona alojada pública en la región EE.UU. Oeste (Oregón). Si los servicios de la región de EE. UU. Este (Virginia del Norte) dejan de estar disponibles durante un período prolongado, Route 53 ejecutará la conmutación por error en 60 minutos y redirigirá automáticamente las operaciones del plano de control de las zonas alojadas públicamente habilitadas para la recuperación acelerada a la región de EE. UU. Oeste (Oregón). A continuación, puede seguir realizando cambios en el DNS mediante programación mediante la CLI, el SDK y la API. Tenga en cuenta que estará disponible un conjunto limitado de métodos de API durante la conmutación por error. Consulte la sección «Consideraciones adicionales» para obtener más información. Cuando la región se recupere, la Ruta 53 ejecutará el procedimiento de recuperación por recuperación y redirigirá automáticamente las operaciones del avión de control a la región Este de EE. UU. (Virginia del Norte).

Note

Antes de que se produzca algún problema en la región EE.UU. Este (Virginia del Norte), primero debe activar la recuperación acelerada para administrar los registros DNS públicos en su zona de alojamiento público. Esto se puede hacer a través de la consola, la CLI, el SDK o la API (consulte la sección titulada [Cómo habilitar la recuperación acelerada para administrar registros DNS públicos](#) en esta página a continuación). No puede habilitar la recuperación acelerada para administrar los registros DNS públicos después de que se produzca una conmutación por error.

Volver a enviar los cambios de DNS tras la conmutación por error

En condiciones normales, los cambios en las zonas de alojamiento público que tengan habilitada la recuperación acelerada serán aceptados en la región EE.UU. Este (Virginia del Norte) y, a continuación, se replicarán correctamente en la región EE.UU. Oeste (Oregón). Sin embargo, cuando se produce una interrupción del servicio en la región EE.UU. Este (Norte de Virginia), es posible que algunos cambios sean aceptados por la región EE.UU. Este (Virginia Norte), pero no replicables en la región EE.UU. Oeste (Oregón). Estos cambios durante el vuelo se denominan «cambios temporales». Una vez finalizada la conmutación por error, Route 53 recomienda volver a enviar los

cambios pendientes antes de reanudar los flujos de trabajo de DNS. Puede lograrlo mediante la API o mediante AWS CloudFormation los métodos que se describen a continuación.

Uso de la API para realizar un seguimiento de los cambios en el DNS y enviarlos

Si usa la API, la AWS CLI o AWS SDKs la administración de registros de DNS de Route 53, necesitará usar la [ChangeResourceRecordSets API](#) y la [GetChange API](#) para enviar y realizar un seguimiento de los cambios de DNS, respectivamente.

Cuando usa la ChangeResourceRecordSets API para realizar cambios en el DNS, Route 53 devuelve un identificador (ID) para el cambio realizado (consulte [ChangeInfo](#) los detalles del objeto de respuesta al cambio). Puede proporcionar este ID en una solicitud posterior a la GetChange API y observar el estado del cambio. Los cambios de DNS con el estado INSYNC se han replicado en la región EE.UU. Oeste (Oregón) y se han propagado a todos los servidores DNS de Route 53. No es necesario realizar ninguna otra acción en relación con estos cambios antes o después de una conmutación por error. Sin embargo, si el cambio se produce en la región EE. UU. Este (Virginia del Norte), GetChange puede volver a estar PENDIENTE, lo que indica que es posible que el cambio no se haya replicado en la región EE. UU. Oeste (Oregón). Si ese es el caso, cuando se complete la conmutación por error, GetChange volverá NoSuchChange, lo que indica que Route 53 no ha podido replicar este cambio de DNS. Por lo tanto, después de la conmutación por error, puede ignorar estos cambios de DNS inactivos y volver a enviarlos como nuevos cambios de DNS. Sabrá que el proceso de conmutación por error se ha completado cuando Route 53 publique un mensaje en el AWS Health Dashboard.

Se utiliza AWS CloudFormation para realizar un seguimiento de los cambios y enviarlos

AWS CloudFormation Realiza un seguimiento automático del estado de replicación de los cambios de DNS mediante la GetChange API y solo completa una actualización una vez que los cambios de DNS se confirman como INSYNC. Si la utilizas CloudFormation para gestionar los registros de DNS y la región EE.UU. Este (Virginia del Norte) deja de estar disponible, las acciones que utilices no se CloudFormation completarán correctamente durante el período de no disponibilidad. Sin embargo, solo tiene que volver a intentar las mismas acciones para poder volver a enviar los cambios de DNS, una vez que CloudFormation se complete el proceso de conmutación por error de Route 53.

Vuelva a la región EE.UU. Este (Virginia del Norte)

Una vez que la región se recupere, la Ruta 53 suspenderá las operaciones del avión de control de su zona de acogida pública con destino a la región de EE. UU. Este (Virginia del Norte). Durante la recuperación, no tendrá que volver a enviar los cambios de DNS, ya que no se introducirán cambios innecesarios durante este proceso.

Consideraciones adicionales

Hay algunas consideraciones adicionales que debes tener en cuenta en relación con la función de recuperación acelerada:

1. No podrá crear nuevas zonas alojadas, eliminar las zonas alojadas existentes, habilitar la firma de DNSSEC ni deshabilitar la firma de DNSSEC durante la conmutación por error.
2. AWS PrivateLink las conexiones no funcionarán después de una conmutación por error, pero volverán a funcionar después de una conmutación por recuperación a la región EE.UU. Este (Norte de Virginia).
3. CloudFront Por el momento, no se admiten [planes de tarifa fija](#).
4. Las zonas alojadas con la recuperación acelerada habilitada no se pueden eliminar. Debe deshabilitar la recuperación acelerada antes de intentar eliminar la zona alojada.
5. Durante la conmutación por error, los siguientes métodos de API seguirán siendo compatibles en las zonas alojadas públicas con la recuperación acelerada habilitada. Sin embargo, los demás métodos de la API de Route 53 no funcionarán hasta que se produzca una conmutación por recuperación.
 - `ChangeResourceRecordSets`
 - `GetChange`
 - `GetGeoLocation`
 - `GetHostedZone`
 - `GetHostedZoneCount`
 - `GetHostedZoneLimit`
 - `GetReusableDelegationSet`
 - `GetReusableDelegationSetLimit`
 - `ListGeoLocations`
 - `ListHostedZones`
 - `ListHostedZonesByName`
 - `ListResourceRecordSets`
 - `ListReusableDelegationSets`

¿Cómo habilitar la recuperación acelerada para administrar los registros DNS públicos

Puede habilitar la recuperación acelerada para administrar los registros DNS públicos mediante la consola, la API, la CLI o el SDK de Route 53. El tiempo necesario para habilitar la recuperación acelerada dependerá del tamaño de la zona alojada pública y de otros factores. Debe planificar el proceso de habilitación de la recuperación acelerada para que tarde varias horas. Puede comprobar el estado del proceso de activación en la pestaña de recuperación acelerada de su zona alojada pública o mediante la `GetHostedZone` API. A medida que finalice el proceso, habrá un breve período de tiempo que durará varios minutos y en el que no se aceptarán los cambios de DNS. Una vez completados, los cambios de DNS pueden continuar con normalidad.

Para habilitar y deshabilitar la recuperación acelerada mediante la consola Route 53

1. Abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Zonas alojadas.
3. Elija la zona alojada pública en la que desee habilitar la recuperación acelerada.
4. En la pestaña Recuperación acelerada, seleccione Activar.
5. Seleccione Save changes (Guardar cambios).
6. Supervise el estado de la zona alojada. El estado muestra Habilitar la recuperación acelerada durante la configuración y cambia a Habilitado cuando se completa.

Puede deshabilitar la recuperación acelerada siguiendo los mismos pasos anteriores, pero en su lugar seleccionando Desactivar.

Ejemplo de CLI para habilitar

```
aws route53 update-hosted-zone-features --enable-accelerated-recovery --hosted-zone-id Z123456789
```

Ejemplo de CLI para deshabilitar

```
aws route53 update-hosted-zone-features --no-enable-accelerated-recovery --hosted-zone-id Z123456789
```

Uso de zonas alojadas privadas

Una zona alojada privada es un contenedor que contiene información sobre cómo desea que Amazon Route 53 responda a las consultas de DNS de un dominio y sus subdominios dentro de uno

o varios VPCs que cree con el servicio Amazon VPC. A continuación, se explica cómo funcionan las zonas alojadas privadas:

1. Se crea una zona alojada privada, como `example.com`, y se especifica la VPC que se desea asociar a la zona alojada. Después de crear la zona alojada, puede VPCs asociar más a ella.
2. Usted crea registros en la zona alojada que determinan cómo responde Route 53 a las consultas de DNS para su dominio y subdominios dentro y entre sus VPCs dominios. Por ejemplo, supongamos que tiene un servidor de base de datos que se ejecuta en una EC2 instancia de la VPC que ha asociado a su zona alojada privada. Usted crea un registro A o AAAA, como `db.example.com`, y especifica la dirección IP del servidor de base de datos.

Para obtener más información acerca de los registros, consulte [Uso de registros](#). Para obtener información acerca de los requisitos de Amazon VPC para usar zonas alojadas privadas, consulte [Uso de zonas alojadas privadas](#) en la Guía del usuario de Amazon VPC.

3. Cuando una aplicación envía una consulta de DNS para `db.example.com`, Route 53 devuelve la dirección IP correspondiente. Para obtener una respuesta de una zona alojada privada, también debes ejecutar una EC2 instancia en una de las asociadas VPCs (o tener un punto final de entrada de una configuración híbrida). Si intentas consultar una zona alojada privada desde fuera de la configuración VPCs o de la configuración híbrida, la consulta se resolverá de forma recursiva en Internet.
4. La aplicación utiliza la dirección IP que ha obtenido de Route 53 para establecer una conexión con el servidor de base de datos.

Al crear una zona alojada privada, se utilizan los siguientes servidores de nombres:

- `ns-0.awsdns-00.com`
- `ns-512.awsdns-00.net`
- `ns-1024.awsdns-00.org`
- `ns-1536.awsdns-00.co.uk`

Estos servidores de nombres se usan porque el protocolo DNS requiere que cada zona alojada tenga un conjunto de registros NS. Estos servidores de nombres están reservados y las zonas alojadas públicas de Route 53 nunca los utilizan. Solo puede consultar esas zonas a través de VPC Resolver en una VPC que se haya asociado a la zona alojada mediante un punto final de entrada conectado al VPCs especificado en la zona alojada privada.

Si bien los servidores de nombres están visibles en Internet, VPC Resolver no se conecta a las direcciones de los servidores de nombres. Además, la información de la zona alojada privada no se devuelve si consulta directamente los servidores de nombres a través de Internet. En cambio, el solucionador de VPC detecta que las consultas se encuentran dentro de un espacio de nombres privado basado en las asociaciones de VPC a zonas alojadas y utiliza conectividad privada y directa para llegar a los servidores DNS privados.

Note

Si lo desea, puede cambiar el conjunto de registros NS en una zona alojada privada y la resolución de DNS privada seguirá funcionando. No lo recomendamos, pero si elige hacerlo, debe usar nombres de dominio reservados que no sean usados por los servidores DNS públicos.

Si desea dirigir el tráfico de su dominio en Internet, utilice una zona alojada pública de Route 53. Para obtener más información, consulte [Trabajar con zonas públicas alojadas](#).

Temas

- [Consideraciones sobre el uso de una zona alojada privada](#)
- [Creación de una zona alojada privada](#)
- [Descripción de zonas alojadas privadas](#)
- [Asociarse más a una zona VPCs alojada privada](#)
- [Asociar una Amazon VPC y una zona alojada privada que haya creado con cuentas diferentes AWS](#)
- [Desasociarse de una zona VPCs alojada privada](#)
- [Eliminar una zona alojada privada](#)
- [Permisos de VPC](#)

Consideraciones sobre el uso de una zona alojada privada

Al utilizar zonas alojadas privadas, tenga en cuenta las siguientes consideraciones.

- [Amazon VPC settings](#)
- [Route 53 health checks](#)
- [Supported routing policies for records in a private hosted zone](#)

- [Split-view DNS](#)
- [Public and private hosted zones that have overlapping namespaces](#)
- [Private hosted zones that have overlapping namespaces](#)
- [Private hosted zones and Route 53 VPC Resolver rules](#)
- [Delegating responsibility for a subdomain](#)
- [Custom DNS servers](#)
- [Required IAM permissions](#)

Configuración de Amazon VPC

Para utilizar las zonas alojadas privadas, debe definir la siguiente configuración de Amazon VPC en `true`:

- `enableDnsHostnames`
- `enableDnsSupport`

Para obtener más información, consulte [Ver y actualizar los atributos de DNS de su VPC](#) en la Guía del usuario de Amazon VPC.

Controles de estado de Route 53

En una zona alojada privada, solo puede asociar comprobaciones de estado de Route 53 con registros de conmutación por error, de respuestas con varios valores, ponderados, de latencia, de geolocalización y de geoproximidad. Para obtener información acerca de cómo asociar las comprobaciones de estado a registros de conmutación por error, consulte [Configuración de la conmutación por error en una zona alojada privada](#).

Políticas de direccionamiento admitidas para registros de una zona alojada privada

Puede utilizar las siguientes políticas de direccionamiento al crear registros de una zona alojada privada:

- [Direccionamiento simple](#)
- [Enrutado de conmutación por error](#)
- [Direccionamiento de respuesta con varios valores](#)
- [Direccionamiento ponderado](#)
- [Enrutado basado en latencia](#)
- [Enrutado de geolocalización](#)
- [Enrutamiento por geoproximidad](#)

No se admite la creación de registros en una zona alojada privada mediante otras políticas de direccionamiento.

DNS de vista dividida

Puede usar Route 53 para configurar split-view DNS, también conocido como split-horizon DNS. En el DNS de vista dividida, se utiliza el mismo nombre de dominio (example.com) para usos internos (accounting.example.com) y externos, tales como su sitio web público (www.example.com). Es posible que también desee utilizar el mismo nombre de subdominio de forma interna y externa, pero distribuir contenido distinto o requerir una autenticación diferente para los usuarios internos y externos.

Para configurar DNS de vista dividida, siga estos pasos:

1. Cree zonas alojadas públicas y privadas que tengan el mismo nombre. (El DNS de vista dividida sigue funcionando si utiliza otro servicio DNS para la zona alojada pública).
2. Asocia uno o más Amazon VPCs a la zona alojada privada. El solucionador de VPC de Route 53 usa la zona alojada privada para enrutar las consultas de DNS en la zona especificada. VPCs
3. Cree registros en cada zona alojada. Los registros de la zona alojada pública controlan cómo se enruta el tráfico de Internet y los registros de la zona alojada privada controlan cómo se enruta el tráfico en Amazon. VPCs

Si necesita realizar la resolución de nombres de sus cargas de trabajo de VPC y locales, puede usar Route 53 VPC Resolver. Para obtener más información, consulte [¿Qué es el solucionador de VPC Route 53?](#).

Zonas alojadas públicas y privadas que tienen espacios de nombres que se superponen

Si tienes zonas alojadas públicas y privadas con espacios de nombres superpuestos, como example.com y accounting.example.com, VPC Resolver direcciona el tráfico en función de la coincidencia más específica. Cuando los usuarios inician sesión en una EC2 instancia de una Amazon VPC que usted ha asociado a la zona alojada privada, así es como Route 53 VPC Resolver gestiona las consultas de DNS:

1. El solucionador de VPC evalúa si el nombre de la zona alojada privada coincide con el nombre de dominio de la solicitud, como accounting.example.com. Una coincidencia se define como cualquiera de las siguientes:
 - Una coincidencia idéntica
 - El nombre de la zona alojada privada es un elemento principal del nombre de dominio de la solicitud. Por ejemplo, suponga que el nombre de dominio de la solicitud es el siguiente:

seattle.accounting.example.com

Las siguientes zonas alojadas coinciden porque son elementos principales de seattle.accounting.example.com:

- accounting.example.com
- example.com

Si no hay ninguna zona alojada privada que coincida, el Resolver de VPC reenvía la solicitud a un solucionador de DNS público y la solicitud se resuelve como una consulta de DNS normal.

2. Si hay un nombre de zona alojada privada que coincida con el nombre de dominio de la solicitud, en la zona alojada se busca un registro que coincida con el nombre de dominio y tipo de DNS de la solicitud, como un registro A para accounting.example.com.

Note

Si hay una zona alojada privada coincidente, pero no hay ningún registro que coincida con el nombre de dominio y el tipo de la solicitud, VPC Resolver no reenvía la solicitud a un solucionador de DNS público. En su lugar, devuelve NXDOMAIN (dominio no existente) al cliente.

Zonas alojadas privadas que tienen espacios de nombres que se superponen

Si tienes dos o más zonas alojadas privadas que tienen espacios de nombres superpuestos, como example.com y accounting.example.com, VPC Resolver direcciona el tráfico en función de la coincidencia más específica.

Note

Si tiene una zona alojada privada (example.com) y una regla de resolución de VPC de Route 53 que enruta el tráfico a su red para el mismo nombre de dominio, la regla de resolución de VPC tiene prioridad. Consulte [Private hosted zones and Route 53 VPC Resolver rules](#).

Cuando los usuarios inician sesión en una EC2 instancia de una Amazon VPC que has asociado a todas las zonas alojadas privadas, así es como VPC Resolver gestiona las consultas de DNS:

1. El solucionador de VPC evalúa si el nombre de dominio de la solicitud, como `accounting.example.com`, coincide con el nombre de una de las zonas alojadas privadas.
2. Si no hay ninguna zona alojada que coincida exactamente con el nombre de dominio de la solicitud, el Resolver de VPC busca una zona alojada que tenga un nombre que sea el principal del nombre de dominio de la solicitud. Por ejemplo, suponga que el nombre de dominio de la solicitud es el siguiente:

`seattle.accounting.example.com`

Las siguientes zonas alojadas coinciden porque son elementos principales de `seattle.accounting.example.com`:

- `accounting.example.com`
- `example.com`

VPC Resolver elige `accounting.example.com` porque es más específico que `example.com`.

3. El solucionador de VPC busca en la zona `accounting.example.com` alojada un registro que coincida con el nombre de dominio y el tipo de DNS de la solicitud, como un registro A de `seattle.accounting.example.com`.

Si no hay ningún registro que coincida con el nombre de dominio y el tipo de la solicitud, VPC Resolver devuelve NXDOMAIN (dominio inexistente) al cliente.

Zonas alojadas privadas y reglas de resolución de VPC de Route 53

Si tiene una zona alojada privada (`example.com`) y una regla de resolución de VPC que enruta el tráfico a su red para el mismo nombre de dominio, la regla de resolución de VPC tiene prioridad.

Supongamos que tiene la siguiente configuración:

- Tiene una zona alojada privada llamada `example.com` y la asocia a una VPC.
- Cree una regla de resolución de VPC de Route 53 que reenvíe el tráfico de `example.com` a su red y asocie la regla a la misma VPC.

En esta configuración, la regla de resolución de VPC tiene prioridad sobre la zona alojada privada. Las consultas DNS se reenvían a la red en lugar de resolverse en función de los registros de la zona alojada privada.

Delegación de la responsabilidad de un subdominio

Ahora puede crear registros NS en una zona alojada privada para delegar la responsabilidad sobre un subdominio. Para obtener más información, consulte [Tutorial sobre las reglas de delegación de Resolver](#).

Servidores DNS personalizados

Si ha configurado servidores DNS personalizados en las EC2 instancias de Amazon de su VPC, debe configurar esos servidores DNS para que enruten sus consultas de DNS privadas a la dirección IP de los servidores DNS proporcionados por Amazon para su VPC. Esta dirección IP es la dirección IP en la base del rango de red de VPC “más dos”. Por ejemplo, si el rango de CIDR de la VPC es 10.0.0.0/16, la dirección IP del servidor DNS es 10.0.0.2.

Si quieres enrutar las consultas de DNS entre VPCs y tu red, puedes usar VPC Resolver. Para obtener más información, consulte [¿Qué es el solucionador de VPC Route 53?](#).

Permisos de IAM necesarios

Para crear zonas alojadas privadas, debes conceder permisos de IAM para EC2 las acciones de Amazon además de los permisos para las acciones de Route 53. Para obtener más información, consulte [Acciones, recursos y claves de condición para Amazon Route 53](#) en la Referencia de autorizaciones de servicio.

Creación de una zona alojada privada

Una zona alojada privada es un contenedor de registros de un dominio que se aloja en una o más nubes privadas virtuales de Amazon (VPCs). Usted crea una zona alojada para un dominio (como example.com) y, a continuación, crea registros para indicar a Amazon Route 53 cómo desea que se redirija el tráfico de ese dominio dentro y entre sus dominios. VPCs

Important

Al crear una zona alojada privada, debe asociar una VPC con la zona alojada y la VPC que especifique debe haberse creado utilizando la misma cuenta que utiliza para crear la zona alojada. Tras crear la zona alojada, puede asociarle más, incluida la VPCs que haya creado VPCs con otra AWS cuenta.

Para asociar lo VPCs que creó con una cuenta a una zona alojada privada que creó con una cuenta diferente, debe autorizar la asociación y, a continuación, crearla mediante

programación. Para obtener más información, consulte [Asociar una Amazon VPC y una zona alojada privada que haya creado con cuentas diferentes AWS](#).

Para obtener información sobre la creación de una zona alojada privada mediante la API de Route 53, consulte la [Referencia de la API de Amazon Route 53](#).

Para crear una zona alojada privada a través de la consola de Route 53

1. Por cada VPC que desee asociar a la zona alojada de Route 53, cambie las siguientes opciones de VPC a true:

- enableDnsHostnames
- enableDnsSupport

A fin de obtener más información, consulte [Actualización de soporte de DNS para su VPC](#) en la guía del usuario de Amazon VPC.

2. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/route53/>
3. Si no conoce Route 53, elija Get started (Introducción).

Si ya trabaja con Route 53, seleccione Hosted zones (Zonas alojadas) en el panel de navegación.

4. Elija Create hosted zone (Crear zona alojada).
5. En el panel Create private hosted zone (Crear zona alojada privada), ingrese un nombre de dominio y, si lo desea, un comentario.

Para obtener información sobre cómo especificar caracteres distintos de a-z, 0-9 y - (guion), y cómo especificar nombres de dominio internacionalizados, consulte [Formato de nombres de dominio DNS](#).

6. En la lista Type (Tipo), elija Private hosted zone (Zona alojada privada).
7. En la lista VPC ID, elija la VPC que desea asociar con la zona alojada.

 Note

Si la consola muestra el siguiente mensaje, significa que está intentando asociar una zona alojada que utiliza el mismo espacio de nombres que el de otra zona alojada dentro de la misma VPC:

“Un dominio en conflicto ya está asociado a la VPC o al conjunto de delegación indicados”.

Por ejemplo, si las zonas alojadas A y B utilizan el mismo nombres de dominio, como `example.com`, no puede asociar ambas zonas alojadas con la misma VPC.

8. Elija Create hosted zone (Crear zona alojada).

Descripción de zonas alojadas privadas

Puede usar la consola de Amazon Route 53 para enumerar todas las zonas alojadas que creó con la AWS cuenta actual. Para obtener información sobre cómo enumerar las zonas alojadas mediante la API de Route 53, consulte [ListHostedZones](#) la referencia de la API de Amazon Route 53.

Para ver una lista de las zonas alojadas asociadas a una AWS cuenta

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Zonas alojadas.

La página Zonas alojadas muestra automáticamente una lista de todas las zonas alojadas que se crearon con la AWS cuenta corriente. La columna Type indica si una zona alojada es privada o pública. Elija el encabezado de columna para agrupar todas las zonas alojadas privadas y públicas.

Asociarse más a una zona VPCs alojada privada

Puede utilizar la consola de Amazon Route 53 para VPCs asociar más a una zona alojada privada si ha creado la zona alojada y la ha VPCs utilizado la misma AWS cuenta.

⚠ Important

Si desea asociar los VPCs que creó con una cuenta con una zona alojada privada que creó con una cuenta diferente, primero debe autorizar la asociación. Además, no puede utilizar la AWS consola para autorizar la asociación ni para asociarla a los VPCs zona alojada. Para obtener más información, consulte [Asociar una Amazon VPC y una zona alojada privada que haya creado con cuentas diferentes AWS](#).

Para obtener información sobre cómo asociar más VPCs a una zona alojada privada mediante la API de Route 53, consulte [Associate VPCWith HostedZone](#) en la referencia de la API de Amazon Route 53.

Para asociarse adicionalmente VPCs a una zona alojada privada mediante la consola de Route 53

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Zonas alojadas.
3. Seleccione el botón de radio de la zona alojada privada a la que quieras asociarte más VPCs .
4. Seleccione Editar.
5. Elija Add VPC (Agregar VPC).
6. Elija la región y el ID de la VPC; que desea asociar con la zona alojada.
7. Para VPCs asociar más a esta zona alojada, repita los pasos 5 y 6.
8. Seleccione Save changes (Guardar cambios).

Asociar una Amazon VPC y una zona alojada privada que haya creado con cuentas diferentes AWS

Si desea asociar una VPC que creó con una AWS cuenta a una zona alojada privada que creó con una cuenta diferente, lleve a cabo el siguiente procedimiento:

Para asociar una Amazon VPC y una zona alojada privada que haya creado con cuentas diferentes AWS

1. Con la cuenta que ha creado la zona alojada, autorice la asociación de la VPC con la zona alojada privada mediante uno de los siguientes métodos:

- AWS CLI— Consulte [create-vpc-association-authorization](#) en la Referencia de AWS CLI comandos
- AWS SDK o AWS Tools for Windows PowerShell: consulte la documentación correspondiente en la página de [AWS documentación](#)
- API de Amazon Route 53: consulte [Crear VPCAssociation autorización](#) en la referencia de la API de Amazon Route 53

Tenga en cuenta lo siguiente:

- Si desea asociar varias de las VPCs que creó con una cuenta a una zona alojada que creó con una cuenta diferente, debe enviar una solicitud de autorización para cada VPC.
 - Al autorizar la asociación, debe especificar el ID de la zona alojada, por lo que la zona alojada privada ya debe existir.
 - No puede utilizar la consola de Route 53 para autorizar la asociación de una VPC con una zona alojada privada o para realizar la asociación.
2. Con la cuenta que ha creado la VPC, asocie la VPC con la zona alojada. Al igual que al autorizar la asociación, puede utilizar el AWS SDK, las herramientas para Windows PowerShell, la API de Route 53 o la AWS CLI API de Route 53. Si usas la API, usa la VPCWith HostedZone acción [Asociar](#).
 3. Recomendado: elimine la autorización para asociar la VPC a la zona alojada. La eliminación de la autorización no afecta a la asociación, solo le impide volver a asociar la VPC con la zona alojada en el futuro. Si desea volver a asociar la VPC con la zona alojada, repita los pasos 1 y 2 de este procedimiento.

 Important

ListHostedZonesByVPC devuelve las zonas alojadas con una VPC y la GetHostedZone API devuelve las VPCs asociadas a la zona alojada. APIs Solo consideran la asociación de la zona alojada a la VPC creada por la AssociateVPCWithHostedZone API o cuando se crea la zona alojada privada. Si desea obtener una lista completa de las asociaciones de zonas alojadas a una VPC, llame también. [ListProfileResourceAssociations](#)

 Note

Para conocer el número máximo de autorizaciones que puede crear, consulte [Cuotas de entidades](#).

Desasociarse de una zona VPCs alojada privada

Puede usar la consola de Amazon Route 53 para desvincularse VPCs de una zona alojada privada. Esto hace que Route 53 detenga el tráfico de enrutamiento utilizando registros en la zona alojada para las consultas de DNS que se originan en la VPC. Por ejemplo, si la zona alojada example.com está asociada a una VPC y desasocia la zona alojada de dicha VPC, Route 53 deja de resolver las consultas de DNS para example.com o cualquiera de los demás registros de la zona alojada example.com.

 Note

No puede desasociar la última VPC de una zona alojada privada. Si desea desasociar esa VPC, primero debe asociar otra VPC a la zona alojada.

Para desasociarse VPCs de una zona alojada privada

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Zonas alojadas.
3. Elija el botón de radio de la zona alojada privada de la que desee desvincular una o más VPCs .
4. Seleccione Editar.
5. Elija Remove VPC (Eliminar VPC) junto a la VPC que desea desvincular de esta zona alojada.
6. Seleccione Save changes (Guardar cambios).

Eliminar una zona alojada privada

En esta sección, se explica cómo eliminar una zona alojada privada con la consola de Amazon Route 53.

Puede eliminar una zona alojada privada solo si los únicos registros son los registros SOA y NS predeterminados. Si su zona alojada contiene otros registros, debe eliminarlos para poder eliminar su zona alojada. Esto le impide eliminar accidentalmente una zona alojada que siga conteniendo registros.

Temas

- [Eliminar zonas alojadas privadas creadas por otro servicio](#)
- [Uso de la consola de Route 53 para eliminar una zona alojada privada](#)

Eliminar zonas alojadas privadas creadas por otro servicio

Si otro servicio ha creado una zona alojada privada, no puede eliminarla con la consola de Route 53. En su lugar, ha de utilizar el proceso correspondiente del otro servicio:

- AWS Cloud Map— Para eliminar una zona alojada que se AWS Cloud Map creó al crear un espacio de nombres DNS privado, elimine el espacio de nombres. AWS Cloud Map elimina la zona alojada automáticamente. Para obtener más información, consulte [Eliminación de espacios de nombres](#) en la Guía para desarrolladores de AWS Cloud Map .
- Descubrimiento de servicios de Amazon Elastic Container Service (Amazon ECS): para eliminar una zona alojada privada que Amazon ECS creó al crear un servicio mediante la detección de servicios, elimine los servicios de Amazon ECS que utilizan el espacio de nombres y elimine el espacio de nombres. Para obtener más información, consulte [Eliminación de un servicio](#) en la Guía para desarrolladores de Amazon Elastic Container Service.

Uso de la consola de Route 53 para eliminar una zona alojada privada

Para utilizar la consola de Route 53 para eliminar una zona alojada privada, realice el siguiente procedimiento.

Para eliminar una zona alojada privada a través de la consola de Route 53

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. Confirme que la zona alojada que desea eliminar solo contiene un registro NS y SOA. Si contiene registros adicionales, elimínelos:
 - a. Elija el nombre de la zona alojada que desea eliminar.

- b. En la página Record (Registro), si la lista de registros incluye registros cuyo valor para la columna Type (Tipo) es distinto de NS o SOA, elija la fila y, a continuación, elija Delete (Eliminar).

Para seleccionar varios registros s consecutivos, elija la primera fila, mantenga presionada la tecla Mayús y elija la última fila. Para seleccionar varios registros no consecutivos, elija la primera fila, mantenga presionada la tecla Ctrl y elija las filas restantes.

3. En la página Hosted Zones (Zonas alojadas), elija la fila de la zona alojada que desea eliminar.
4. Elija Eliminar.
5. Escriba la clave de confirmación y elija Delete (Eliminar).

Permisos de VPC

[Los permisos de VPC utilizan una condición de política de administración de identidad y acceso \(IAM\) que le permite establecer permisos granulares para VPCs cuando utilice Associate VPCWith HostedZone, Disassociation, Create VPCAssociation Authorization VPCFromHostedZone, Delete VPCAssociation Authorization y VPC. CreateHostedZoneListHostedZonesBy APIs](#)

Con la condición de política de IAM `route53:VPCs`, puedes conceder derechos administrativos detallados a otros usuarios. AWS Esto le permite conceder a alguien permisos para asociar la zona alojada, desasociar la zona alojada, crear una autorización de asociación de VPC, eliminar una autorización de asociación de VPC, crear una zona alojada o enumerar zonas alojadas para lo siguiente:

- Una sola VPC.
- Cualquiera VPCs dentro de la misma región.
- Múltiple VPCs.

Para obtener más información sobre los permisos de VPC, consulte [Uso de condiciones de las políticas de IAM para control de acceso preciso](#).

Para obtener información sobre cómo autenticar a AWS los usuarios, consulte [Autenticación con identidades](#) y aprenda a controlar el acceso a los recursos de Route 53, consulte [Control de acceso](#).

Migración de una zona alojada a otra cuenta de AWS

Cuando quiera migrar una zona alojada a una Cuenta de AWS diferente, siga los pasos a continuación.

Estos pasos son los más adecuados para las zonas alojadas con cambios de registro poco frecuentes. En el caso de las zonas alojadas con actualizaciones de registro frecuentes, tenga en cuenta lo siguiente:

- No actualice ningún registro de recursos durante la migración.
- Publique los cambios en los registros de recursos tanto en las zonas alojadas antiguas como en las nuevas una vez transferida la delegación.

Requisitos previos

Instala o actualiza la de AWS CLI:

Para obtener información sobre cómo descargar, instalar y configurar la AWS CLI, consulte la [Guía del usuario de la AWS Command Line Interface](#).

Note

Configure la CLI de forma que pueda usarla cuando utilice tanto la cuenta que ha creado la zona alojada como la cuenta a la que está migrando dicha zona. Para obtener más información, consulte [Configure](#) (Configurar) en la Guía del usuario de AWS Command Line Interface.

Si ya está utilizando la AWS CLI, le recomendamos que actualice a la versión más reciente de esta para que los comandos de la CLI admitan las últimas características de Route 53.

Temas

- [Paso 1: prepare todo para la migración](#)
- [Paso 2: Crear la zona alojada nueva](#)
- [Paso 3 \(opcional\): migre las comprobaciones de estado](#)
- [Paso 4: migre los registros de la zona alojada anterior a la nueva zona alojada](#)
- [Paso 5: Comparar los registros de la zona alojada nueva con los de la antigua](#)

- [Paso 6: Actualizar el registro de dominio para que utilice los servidores de nombres de la zona alojada nueva](#)
- [Paso 7: volver a cambiar el TTL del registro NS a un valor más alto](#)
- [Paso 8: vuelva a activar la firma de DNSSEC y establezca la cadena de confianza \(si es necesario\)](#)
- [Paso 9: Eliminar la zona alojada antigua \(opcional\)](#)

Paso 1: prepare todo para la migración

Los pasos de preparación ayudan a minimizar los riesgos asociados a la migración de una zona alojada.

1. Controle la disponibilidad de zonas

Puede supervisar la zona para comprobar la disponibilidad de sus nombres de dominio. Esto puede ayudar a solucionar cualquier problema que pueda provocar la reversión de la migración. Puede supervisar los nombres de dominio con mayor volumen de tráfico por medio de CloudWatch o el registro de consultas. Para obtener más información sobre la configuración del registro de consultas, consulte [Monitoreo de Amazon Route 53](#).

La supervisión se puede realizar a través de un script de shell o mediante un servicio de terceros. Sin embargo, no debería ser la única señal para determinar si se requiere una reversión, ya que es posible que también reciba comentarios de sus clientes debido a que un dominio no está disponible.

2. Reduzca la configuración del TTL

La opción TTL (tiempo de vida) de un registro especifica el tiempo que quiere que los solucionadores de DNS tengan en caché el registro y se use la información de la memoria caché. Cuando el TTL vence, un solucionador envía otra consulta al proveedor de servicios DNS para que un dominio obtenga la información más reciente.

Normalmente, la configuración de TTL para el registro NS es de 172 800 segundos o dos días. El registro NS muestra una lista de los servidores de nombres que el sistema de nombres de dominio (DNS) puede utilizar para obtener información acerca de cómo dirigir el tráfico para su dominio. Si reduce el TTL del registro NS, tanto en su proveedor de servicios DNS actual como en Route 53, se reducirá el tiempo de inactividad de su dominio si descubre un problema mientras realiza la migración de DNS a Route 53. Si no reduce el TTL, su dominio podría no estar disponible en Internet durante un máximo de dos días si algo va mal.

Cómo reducir el TTL

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. Seleccione Zonas alojadas en el panel de navegación.
3. Elija el nombre de la zona alojada.
4. Seleccione el registro NS y, en el panel Detalles del registro, seleccione Editar registro.
5. Cambie el valor de TTL (Seconds) (Segundos). Le recomendamos que especifique un valor entre 60 segundos y 900 segundos (15 minutos).
6. Seleccione Save.

3. Elimine el registro de DS de la zona principal (si DNSSEC está configurado)

Si ha configurado DNSSEC para su dominio, quite el registro de Delegation Signer (DS) de la zona principal antes de migrar el dominio a Route 53.

Si la zona principal está alojada a través de Route 53, consulte [Eliminar claves públicas de un dominio](#) para obtener más información. Si la zona principal está alojada a través de otro registrador, comuníquese con este para eliminar el registro DS.

Actualmente, Route 53 no admite la migración de la configuración de DNSSEC. Por lo tanto, deberá desactivar la validación de DNSSEC realizada en su dominio antes de la migración. Para ello, elimine el registro DS de la zona principal. Tras la migración, podrá volver a activar la validación de DNSSEC, para lo que deberá configurar DNSSEC en la nueva zona alojada y añadir el registro DS correspondiente a la zona principal.

4. Asegúrese de que no haya otras operaciones en curso que dependan de la zona alojada que se está migrando

Algunas operaciones dependen de la resolución del DNS en la zona alojada que se está migrando; por ejemplo, el proceso de renovación del certificado TLS/SSL puede requerir cambios en el registro de DNS y el proveedor intentará resolver el registro de DNS como el método de validación. Antes de hacer la migración, debe asegurarse de que no se esté llevando a cabo ninguna otra operación para evitar que la migración de la zona alojada se vea afectada de forma inesperada.

Paso 2: Crear la zona alojada nueva

Cree la zona alojada nueva en la cuenta a la que desea migrar la zona alojada.

Seleccione la pestaña correspondiente para ver las instrucciones de la AWS CLI o la consola.

- [CLI](#)
- [Consola](#)

CLI

Escriba el siguiente comando:

```
aws route53 create-hosted-zone \
    --name $hosted_zone_name \
    --caller-reference $unique_string
```

Para obtener más información, consulte [create-hosted-zone](#).

Console

Para crear la zona alojada nueva utilizando otra cuenta

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.

Inicie sesión con las credenciales de la cuenta a la que desea migrar la zona alojada.

2. Cree una zona alojada. Para obtener más información, consulte [Crear una zona alojada pública](#).
3. Anote el ID de la zona alojada. En algunos casos, necesitará esta información más adelante durante el proceso.
4. Cierre la sesión en la consola de Route 53.

Reduzca también el TTL de NS en la nueva zona, de forma similar al ajuste para reducir el TTL como preparación en el paso 1.

Paso 3 (opcional): migre las comprobaciones de estado

Puede asociar los registros de DNS de la nueva cuenta con las comprobaciones de estado de Route 53 de la cuenta desde la que está realizando la migración. Para migrar una comprobación de estado de Route 53, debe crear nuevas comprobaciones de estado en la cuenta nueva con

la misma configuración que las existentes. Para obtener más información, consulte [Creación de comprobaciones de estado de Amazon Route 53](#).

Paso 4: migre los registros de la zona alojada anterior a la nueva zona alojada

Para migrar los registros de una Cuenta de AWS a otra, puede utilizar la consola o la AWS CLI.

Console

Si su zona contiene solo unos pocos registros, puede utilizar la consola de Route 53 para enumerar los registros de la zona anterior, anotarlos y crearlos en la nueva zona. Si migró la comprobación de estado en [Paso 3 \(opcional\): migre las comprobaciones de estado](#), cuando cree los registros en la nueva zona alojada, deberá especificar el nuevo identificador de comprobación de estado. Para obtener más información, consulte los temas siguientes:

- [Descripción de registros](#)
- [Creación de registros con la consola de Amazon Route 53](#)
- [Configuración de la recuperación ante errores a nivel de DNS](#)

También debe reducir el TTL de NS en la nueva zona, de forma similar a la configuración para reducir el TTL en el paso 1.

CLI

Si su zona contiene una gran cantidad de registros, puede exportar los registros que quiere migrar a un archivo, editar el archivo y, a continuación, utilizar el archivo editado para crear los registros en la zona alojada nueva. El siguiente procedimiento utiliza comandos de la CLI de AWS, aunque también hay herramientas de terceros disponibles para este fin.

1. Ejecuta el siguiente comando:

```
aws route53 list-resource-record-sets --hosted-zone-id hosted-zone-id > path-to-output-file
```

Tenga en cuenta lo siguiente:

- En *hosted-zone-id*, especifique el ID de la zona alojada anterior que contiene los registros que desea migrar.

- En *path-to-output-file*, especifique la ruta del directorio y el nombre del archivo en el que desea guardar la salida.
- El carácter > envía la salida al archivo especificado.
- La AWS CLI se encarga automáticamente de la paginación de las zonas alojadas que contienen más de 100 registros. Para obtener más información, consulte [Uso de las opciones de paginación de la interfaz de línea de comandos de AWS](#) en la Guía del usuario de AWS Command Line Interface.

Si utiliza otro método de programación para crear una lista de los registros, como uno de los AWS SDK, puede conseguir un máximo de 100 registros por página de resultados. Si la zona alojada contiene más de 100 registros, debe enviar varias solicitudes para conseguir todos los registros.

Haga una copia de esta salida. Después de crear los registros en la zona alojada nueva, le recomendamos que ejecute en esta el comando AWS CLI de la `list-resource-record-sets` y que compare las dos salidas para asegurarse de que se han creado todos los registros.

2. Edite los registros que quiera migrar.

Edite el archivo exportado para poder usarlo con el comando `change-resource-record-sets`. Para efectuar estos cambios, puede usar la función de búsqueda y sustitución en un editor de texto.

Note

En los pasos siguientes se describe la edición manual mediante un editor de texto. Los usuarios avanzados pueden automatizar estas transformaciones con herramientas programáticas como jq, Python u otros lenguajes de secuencias de comandos.

Abra una copia del archivo que creó en el paso 1 de este procedimiento que contenga los registros que desee migrar y realice los siguientes cambios:

- Sustituya el elemento `ResourceRecordSets` de la parte superior del archivo por el elemento `Changes`.

- Opcional: agregue un elemento `Comment`.
- Elimine las líneas relacionadas con los registros `SOA` y `NS` del nombre de la zona alojada. La zona alojada nueva ya tiene esos registros.
- Para cada registro, añada un elemento `Action` y `ResourceRecordSets`, y añada corchetes de apertura y cierre (`{ }`) según sea necesario para que el código JSON sea válido.

 Note

Puede utilizar un validador JSON para verificar que todas las llaves y corchetes están en los lugares correctos. Para encontrar un validador de JSON en línea, busque «validador de JSON» en su navegador.

- Si la zona alojada contiene algún alias que hace referencia a otros registros de la misma zona alojada, realice los siguientes cambios:
 - Cambie el ID de la zona alojada por el ID de la zona alojada nueva.

 Important

Si el registro de alias apunta a otro recurso, como un equilibrador de carga, no cambie el ID de zona alojada al ID de zona alojada del dominio. Si cambia el ID de zona alojada por accidente, revierta el ID de zona alojada al ID de zona alojada del recurso en sí, no al ID de zona alojada del dominio. Ese ID de la zona alojada del recurso se puede encontrar en la consola de AWS donde se creó el recurso.

- Mueva los registros de alias a la parte inferior del archivo. Route 53 debe crear el registro al que hace referencia un registro de alias antes de crear el propio registro de alias.

 Important

Si uno o varios registros de alias hacen referencia a otros registros de alias, los registros que son el destino del alias deben aparecer en el archivo antes que los registros de alias que hacen de referencia a ellos. Por ejemplo, si `alias.example.com` es el destino de alias para

`alias.alias.example.com`, `alias.example.com` debe aparecer primero en el archivo.

- Elimine los registros de alias que dirijan el tráfico a una instancia de políticas de tráfico. Anote los registros para que pueda volver a crearlos más adelante.
- Si migró las comprobaciones de estado en [Paso 3 \(opcional\): migre las comprobaciones de estado](#), cambie los registros para asociarlos a los ID de las comprobaciones de estado recién creados.

En el siguiente ejemplo se muestra la versión editada de los registros de una zona alojada para `example.com`. El texto en cursiva y en color rojo es nuevo:

```
{
  "Comment": "string",
  "Changes": [
    {
      "Action": "CREATE",
      "ResourceRecordSet": {
        "ResourceRecords": [
          {
            "Value": "192.0.2.4"
          },
          {
            "Value": "192.0.2.5"
          },
          {
            "Value": "192.0.2.6"
          }
        ],
        "Type": "A",
        "Name": "route53documentation.com.",
        "TTL": 300
      }
    },
    {
      "Action": "CREATE",
      "ResourceRecordSet": {
        "AliasTarget": {
          "HostedZoneId": "Z3BJ6K6RIION7M",
          "EvaluateTargetHealth": false,
          "DNSName": "s3-website-us-west-2.amazonaws.com."
        }
      }
    }
  ]
}
```

```
    },  
    "Type": "A",  
    "Name": "www.route53documentation.com."  
  }  
]  
}
```

3. Divida los archivos grandes en archivos más pequeños.

Si tiene una gran cantidad de registros o registros con muchos valores (por ejemplo, una gran cantidad de direcciones IP), es posible que tenga que dividir el archivo en archivos más pequeños. Los valores máximos son:

- Cada archivo puede contener un máximo de 1 000 registros.
- La longitud combinada máxima de los valores de todos los elementos `Value` es de 32 000 bytes.

4. Cree registros en la zona alojada nueva.

Ingresa la siguiente CLI:

```
aws route53 change-resource-record-sets \  
    --hosted-zone-id new-hosted-zone-id \  
    --change-batch file://path-to-file-that-contains-records
```

Especifique los siguientes valores:

- En *new-hosted-zone-id*, especifique el ID de la zona alojada nueva.
- En *path-to-file-that-contains-records*, especifique la ruta del directorio y el nombre del archivo que editó en los pasos anteriores.

Si ha eliminado registros de alias que dirigen el tráfico a una instancia de políticas de tráfico, vuelva a crearlos mediante la consola de Route 53. Para obtener más información, consulte [Creación de registros con la consola de Amazon Route 53](#).

Paso 5: Comparar los registros de la zona alojada nueva con los de la antigua

Para confirmar que haya creado correctamente todos los registros en la zona alojada nueva, ingrese el siguiente comando de la CLI para obtener una lista de los registros que contiene la zona alojada nueva y compare la salida con la lista de registros de la zona alojada antigua.

```
aws route53 list-resource-record-sets \  
    --hosted-zone-id new-hosted-zone-id \  
    --output json > path-to-output-file
```

Especifique los siguientes valores:

- En *new-hosted-zone-id*, especifique el ID de la zona alojada nueva.
- En *path-to-output-file*, especifique la ruta del directorio y el nombre del archivo en el que desea guardar la salida. Utilice un nombre de archivo diferente al que ha utilizado en el paso 4.

El carácter > envía la salida al archivo especificado.

Compare la salida con la salida del paso 4. Aparte de los valores de los registros SOA y NS y de los cambios que haya hecho en el paso 4 (como los ID de la zona alojada o los nombres de dominio diferentes), las dos salidas deberían ser idénticas.

Si los registros de la zona alojada nueva no coinciden con los registros de la antigua, opte por alguna de estas posibilidades:

- Realice pequeñas correcciones mediante la consola de Route 53. Para obtener más información, consulte [Editar registros](#).
- Elimine todos los registros, excepto los registros SOA y NS, de la zona alojada nueva y repita el procedimiento del paso 4.

Paso 6: Actualizar el registro de dominio para que utilice los servidores de nombres de la zona alojada nueva

Cuando termine de migrar los registros a la zona alojada nueva, cambie los servidores de nombres del registro de dominio para utilizar los servidores de nombres de la zona alojada nueva. Para obtener más información, consulte Establecimiento de Amazon Route 53 como el servicio DNS de un dominio existente.

Si está utilizando la zona alojada, por ejemplo, si los usuarios utilizan el nombre de dominio para navegar a un sitio web u obtener acceso a una aplicación web, debe seguir supervisando el tráfico y la disponibilidad de la zona alojada, incluido el tráfico del sitio web o la aplicación, el correo electrónico, etc.

- Si el tráfico se reduce o se detiene: cambie el servicio de nombres del registro de dominio por los servidores de nombres anteriores de la zona alojada anterior. A continuación, determine qué ha fallado.
- Si el tráfico no se ve afectado: continúe con el próximo paso.

Paso 7: volver a cambiar el TTL del registro NS a un valor más alto

En la zona alojada nueva, cambie el TTL del registro NS a un valor más normal como, por ejemplo, 172 800 segundos (dos días). Esto mejorará la latencia de los usuarios, ya que no tendrán que esperar tan a menudo para que los solucionadores de DNS envíen una consulta para obtener los servidores de nombres de su dominio.

Cómo cambiar el TTL:

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. Seleccione Zonas alojadas en el panel de navegación.
3. Elija el nombre de la zona alojada.
4. Seleccione el registro NS y, en el panel Detalles del registro, seleccione Editar registro.
5. Cambie el valor de TTL (segundos) por el número de segundos en que desea que los solucionadores de DNS almacenen en caché los nombres de los servidores de nombres de su dominio. Le recomendamos un valor de 172 800 segundos.
6. Seleccione Save.

Paso 8: vuelva a activar la firma de DNSSEC y establezca la cadena de confianza (si es necesario)

Para volver a habilitar la firma de DNSSEC, siga estos dos pasos:

1. Habilite la firma de DNSSEC para Route 53 y solicite que Route 53 cree una clave de firma de claves (KSK) basada en una clave administrada por el cliente en AWS Key Management Service.

2. Cree una cadena de confianza para la zona alojada. Para ello, agregue un registro de firmante de delegación (DS) a la zona principal, de modo que las respuestas de DNS se puedan autenticar con firmas criptográficas de confianza.

Para obtener instrucciones, consulte [Activar la firma de DNSSEC y establecer una cadena de confianza](#).

Paso 9: Eliminar la zona alojada antigua (opcional)

Cuando esté seguro de que ya no necesita la zona alojada antigua, puede eliminarla si lo desea. Para obtener instrucciones, consulte [Eliminación de una zona alojadas pública](#).

Important

No elimine la antigua zona alojada o ningún registro de dicha zona durante al menos 48 horas después de actualizar el registro de dominio para que use servidores de nombres de la nueva zona alojada. Si elimina la antigua zona alojada antes de que los solucionadores de DNS dejen de utilizar los registros de dicha zona, puede que su dominio deje de estar disponible en Internet hasta que los solucionadores comiencen a usar la nueva zona alojada.

Uso de registros

Después de crear una zona alojada para su dominio, como example.com, puede crear registros para indicar al sistema de nombres de dominio (DNS) cómo desea redirigir el tráfico para ese dominio.

Por ejemplo, puede crear registros para que el DNS haga lo siguiente:

- Redirigir el tráfico de Internet de example.com a la dirección IP de un host de su centro de datos.
- Redirigir el correo electrónico de ese dominio (ichiro@example.com) a un servidor de correo (mail.example.com).
- Redirigir el tráfico para un subdominio llamado operations.tokyo.example.com a la dirección IP de un host diferente.

Cada registro incluye el nombre de un dominio o un subdominio, un tipo de registro (por ejemplo, un registro con tipo de correo electrónico redirigido MX) y otros datos del tipo de registro (para los registros MX, el nombre de host de uno o varios servidores de correo electrónico y una prioridad

para cada servidor). Para obtener más información acerca de los distintos tipos de registros, consulte [Tipos de registros de DNS admitidos](#).

El nombre de cada registro de una zona alojada debe terminar con el nombre de la zona alojada. Por ejemplo, la zona alojada example.com puede contener registros de www.example.com y subdominios accounting.tokyo.example.com, pero no registros para un subdominio www.example.ca.

Note

Para crear registros para las configuraciones de enrutamiento complejas, también puede utilizar el editor visual de Flujo de tráfico y guardar la configuración como una política de tráfico. A continuación, puede asociar la política de tráfico con uno o varios nombres de dominio (como example.com) o nombres de subdominio (como www.example.com) en la misma zona alojada o en varias zonas hospedadas. Además, puede revertir las actualizaciones si la nueva configuración no tiene el desempeño previsto. Para obtener más información, consulte [Uso de flujo de tráfico para dirigir el tráfico DNS](#).

Amazon Route 53 no cobra por los registros que agregue a una zona alojada. Para obtener más información acerca del número máximo de registros que puede crear en una zona alojada, consulte [Cuotas](#).

Temas

- [Elección de una política de enrutado](#)
- [Elección entre registros de alias y sin alias](#)
- [Tipos de registros de DNS admitidos](#)
- [Creación de registros con la consola de Amazon Route 53](#)
- [Permisos del conjunto de registros de recursos](#)
- [Valores que hay que especificar al crear o editar los registros de Amazon Route 53](#)
- [Creación de registros mediante la importación de un archivo de zona](#)
- [Editar registros](#)
- [Eliminar registros](#)
- [Descripción de registros](#)

Elección de una política de enrutado

Al crear un registro, puede seleccionar una política de direccionamiento, que determina cómo Amazon Route 53 responde a las consultas:

- Política de direccionamiento simple: se utiliza para un único recurso que realiza una función determinada para su dominio; por ejemplo, un servidor web que ofrece contenido para el sitio web example.com. Puede usar el enrutamiento simple para crear registros en una zona alojada privada.
- Política de direccionamiento de conmutación por error: se utiliza si desea configurar la conmutación por error activa-pasiva. Puede usar el enrutamiento de conmutación por error para crear registros en una zona alojada privada.
- Política de direccionamiento de geolocalización: se utiliza si desea dirigir el tráfico en función de la ubicación de los usuarios. Puede usar el enrutamiento por geolocalización para crear registros en una zona alojada privada.
- Política de enrutamiento de geoproximidad: se utiliza si desea dirigir el tráfico en función de la ubicación de los recursos y, opcionalmente, desviar el tráfico desde los recursos de una ubicación a los de otra. Puede usar el enrutamiento por geoproximidad para crear registros en una zona alojada privada.
- Política de enrutamiento de latencia: utilícela cuando tenga varios recursos Regiones de AWS y desee enrutar el tráfico a la región que proporciona la mejor latencia. Puede usar el enrutamiento de latencia para crear registros en una zona alojada privada.
- Política de direccionamiento basada en IP: se usa cuando se quiere enrutar el tráfico en función de la ubicación de los usuarios, y tener las direcciones IP de las que se origina el tráfico.
- Política de direccionamiento de respuesta con varios valores: se utiliza si desea que Route 53 responda a consultas de DNS con hasta ocho registros de estado seleccionados al azar. Puede usar el enrutamiento de respuesta multivalor para crear registros en una zona alojada privada.
- Política de direccionamiento ponderada: se utiliza para dirigir el tráfico a varios recursos en las proporciones que especifique. Puede usar el enrutamiento ponderado para crear registros en una zona alojada privada.

Temas

- [Direccionamiento simple](#)
- [Enrutado de conmutación por error](#)
- [Enrutado de geolocalización](#)

- [Enrutamiento por geoproximidad](#)
- [Enrutado basado en latencia](#)
- [Direccionamiento basado en IP](#)
- [Direccionamiento de respuesta con varios valores](#)
- [Direccionamiento ponderado](#)
- [Cómo Amazon Route 53 utiliza EDNS0 para calcular la ubicación de un usuario](#)

Direccionamiento simple

El direccionamiento simple le permite configurar registros DNS estándar, sin direccionamiento de Route 53 especial, como ponderado o de latencia. Con el direccionamiento simple, el tráfico se dirige normalmente a un único recurso, como un servidor web de su sitio web.

Puede utilizar una política de enrutamiento sencillo para los registros de una zona alojada privada.

Si elige la política de direccionamiento simple en la consola de Route 53, no puede crear varios registros que tengan el mismo nombre y tipo, pero puede especificar varios valores en el mismo registro, como varias direcciones IP. (Si elige la política de enrutamiento simple para un registro de alias, puede especificar solo un AWS recurso o un registro en la zona alojada actual). Si especifica varios valores en un registro, Route 53 devuelve todos los valores al servicio de resolución de nombres recursivo en orden aleatorio y el servicio devuelve los valores al cliente (como un navegador web) que envió la consulta de DNS. A continuación, el cliente elige un valor y vuelve a enviar la consulta. Con una política de enrutamiento sencillo, si bien puede especificar varias direcciones IP, no se puede comprobar el estado de estas direcciones.

Para obtener información acerca de los valores que especifica cuando se utiliza la política de direccionamiento simple para crear registros, consulte los siguientes temas:

- [Valores específicos para registros simples](#)
- [Valores específicos para registros de alias simples](#)
- [Valores comunes a todas las políticas de enrutamiento](#)
- [Valores comunes de registros de alias para todas las políticas de enrutamiento](#)

Enrutado de conmutación por error

El direccionamiento de conmutación por error permite redirigir el tráfico a un recurso cuando este está en buen estado o a uno diferente cuando el primer recurso no está en buen estado. Los

registros primarios y secundarios pueden dirigir el tráfico a cualquier elemento desde un bucket de Amazon S3 configurado como un sitio web a un árbol complejo de registros. Para obtener más información, consulte [Conmutación por error activa-pasiva](#).

Puede utilizar una política de enrutamiento de conmutación por error para los registros de una zona alojada privada.

Para obtener información acerca de los valores que especifica cuando se utiliza la política de direccionamiento de conmutación por error para crear registros, consulte los siguientes temas:

- [Valores específicos de registros de conmutación por error](#)
- [Valores específicos de registros de alias de conmutación por error](#)
- [Valores comunes a todas las políticas de enrutamiento](#)
- [Valores comunes de registros de alias para todas las políticas de enrutamiento](#)

Enrutado de geolocalización

El direccionamiento de geolocalización permite elegir los recursos que dan servicio al tráfico en función de la ubicación geográfica de los usuarios, es decir, la procedencia de las consultas de DNS. Por ejemplo, es posible que desee que todas las consultas de Europa se envíen a un balanceador de cargas ELB en la región de Fráncfort.

Cuando usa el direccionamiento de geolocalización, puede localizar su contenido y presentar todo su sitio web o parte de este en el idioma de sus usuarios. También puede utilizar el direccionamiento de geolocalización para restringir la distribución de contenido solo a los lugares para los que tiene derechos de distribución. Otro posible uso es equilibrar la carga entre los puntos finales de forma predecible, de easy-to-manage modo que la ubicación de cada usuario se dirija de forma coherente al mismo punto final.

Puede especificar ubicaciones geográficas por continente, por país o por estado en Estados Unidos. Si crea registros independientes para superponer regiones geográficas (por ejemplo, un registro para América del Norte y otro para Canadá), la región geográfica más pequeña recibirá la mayor prioridad. De esta manera, puede redirigir algunas consultas de un continente a un recurso y las consultas de países seleccionados de dicho continente a otro recurso. (Para ver una lista de los países de cada continente, consulte [Ubicación](#)).

La geolocalización funciona mediante el mapeo de direcciones IP a ubicaciones. No obstante, algunas direcciones IP no se mapean a ubicaciones geográficas por lo que, aunque cree conjuntos

de registros de geolocalización que abarquen los siete continentes, Amazon Route 53 recibirá algunas consultas de DNS de ubicaciones que no puede identificar. Puede crear un registro predeterminado que administre tanto las consultas de direcciones IP no mapeadas a ninguna ubicación como las que procedan de ubicaciones para las que no haya creado registros de geolocalización. Si no crea un registro predeterminado, Route 53 devuelve un mensaje de tipo “sin respuesta” a las consultas de esas ubicaciones.

Se puede utilizar el enrutamiento de geolocalización para los registros de zonas alojadas privadas y públicas.

Para obtener más información, consulte [Cómo Amazon Route 53 utiliza EDNS0 para calcular la ubicación de un usuario](#).

Para obtener información acerca de los valores que especifica cuando se utiliza la política de direccionamiento de geolocalización para crear registros, consulte los siguientes temas:

- [Valores específicos de registros de geolocalización](#)
- [Valores específicos de registros de alias de geolocalización](#)
- [Valores comunes a todas las políticas de enrutamiento](#)
- [Valores comunes de registros de alias para todas las políticas de enrutamiento](#)

Enrutado de geolocalización en zonas alojadas privadas

En el caso de las zonas alojadas privadas, Route 53 responde a las consultas de DNS en función Región de AWS de la VPC de la que se originó la consulta. Para ver la lista Regiones de AWS, consulta [Regiones y zonas](#) en la guía del EC2 usuario de Amazon.

Si la consulta de DNS se origina en una parte en las instalaciones de una red híbrida, se considerará que se originó en la Región de AWS en la que se encuentra la VPC.

Si incluye comprobaciones de estado, puede crear registros predeterminados para:

- Direcciones IP que no están asignadas a ubicaciones geográficas.
- Consultas de DNS que provienen de ubicaciones para las que no ha creado registros de geolocalización.

Si el registro de geolocalización de la región de la consulta de DNS no está en buen estado, se devolverá el registro predeterminado (si está en buen estado).

En la configuración de ejemplo de la siguiente figura, las consultas de DNS procedentes de un Región de AWS us-east-1 (Virginia) se enrutarán al punto final 1.1.1.1.

Quick create record [Info](#) [Switch to wizard](#)

▼ Record 1 [Delete](#)

Record name [Info](#) .demo.com

Record type [Info](#)

Keep blank to create a record for the root domain.

Value [Info](#) ☒ Alias

Enter multiple values on separate lines.

TTL (seconds) [Info](#)

Recommended values: 60 to 172800 (two days)

Routing policy [Info](#)

Location

Health check ID - optional [Info](#)

Enrutamiento por geoproximidad

El direccionamiento de geoproximidad permite a Amazon Route 53 dirigir el tráfico a sus recursos en función de la ubicación geográfica de sus usuarios y recursos. Enruta el tráfico al recurso más cercano disponible. También puede optar por enrutar más o menos tráfico a un determinado recurso especificando un valor, conocido como sesgo. Un sesgo expande o reduce el tamaño de la región geográfica desde la que se direcciona el tráfico a un recurso.

Puede crear reglas de geoproximidad para sus recursos y especificar uno de los siguientes valores para cada regla:

- Si utiliza AWS recursos, especifique el grupo de zonas locales Región de AWS o el grupo de zonas en el que creó el recurso.
- Si utiliza recursos que no son AWS recursos, especifique la latitud y la longitud del recurso.

Para usar las Zonas AWS Locales, primero debe habilitarlas. Para obtener más información, consulte la sección [Introducción al uso de zonas locales](#), en la AWS Guía del usuario de zonas locales.

Para obtener más información sobre las diferencias entre las Zonas Locales Regiones de AWS y las Zonas, consulta [Regiones y Zonas](#) en la Guía del EC2 usuario de Amazon.

Para cambiar opcionalmente el tamaño de la región geográfica en la que Route 53 dirige el tráfico a un recurso, especifique el valor aplicable para el sesgo:

- Para ampliar el tamaño de la región geográfica en la que Route 53 dirige el tráfico a un recurso, especifique un número entero positivo de 1 a 99 para el sesgo. Route 53 reduce el tamaño de las regiones adyacentes.
- Para contraer el tamaño de la región geográfica en la que Route 53 dirige el tráfico a un recurso, especifique un sesgo negativo de -1 a -99. Route 53 expande el tamaño de las regiones adyacentes.

 Note

Estamos actualizando la consola de Flujo de tráfico para Route 53. Durante el periodo de transición, puede seguir utilizando la consola anterior.

Seleccione la pestaña de la consola que esté utilizando.

- [Nueva consola](#)
- [Consola antigua](#)

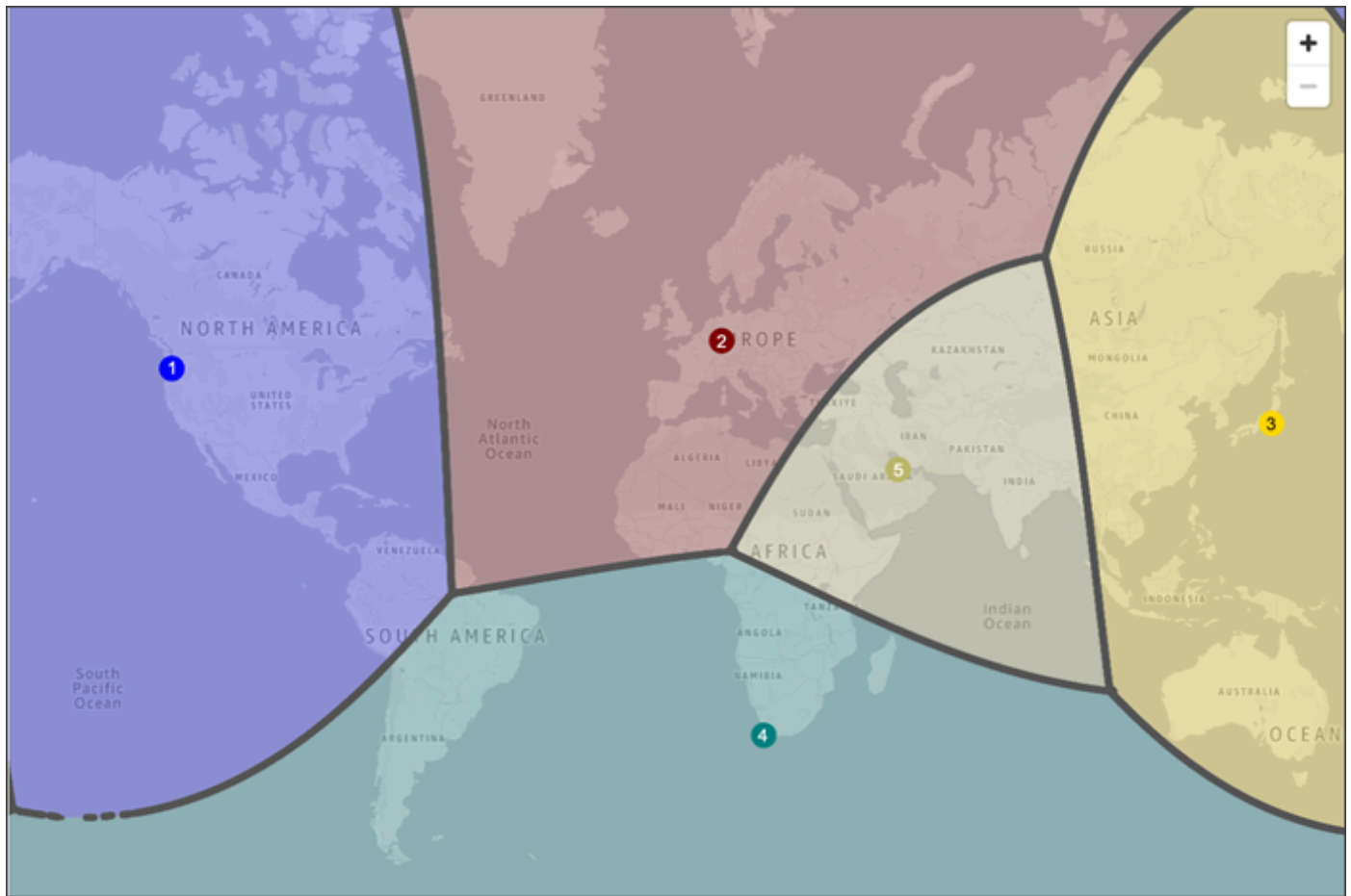
New console

El siguiente mapa muestra cuatro Regiones de AWS (numeradas del 1 al 5):

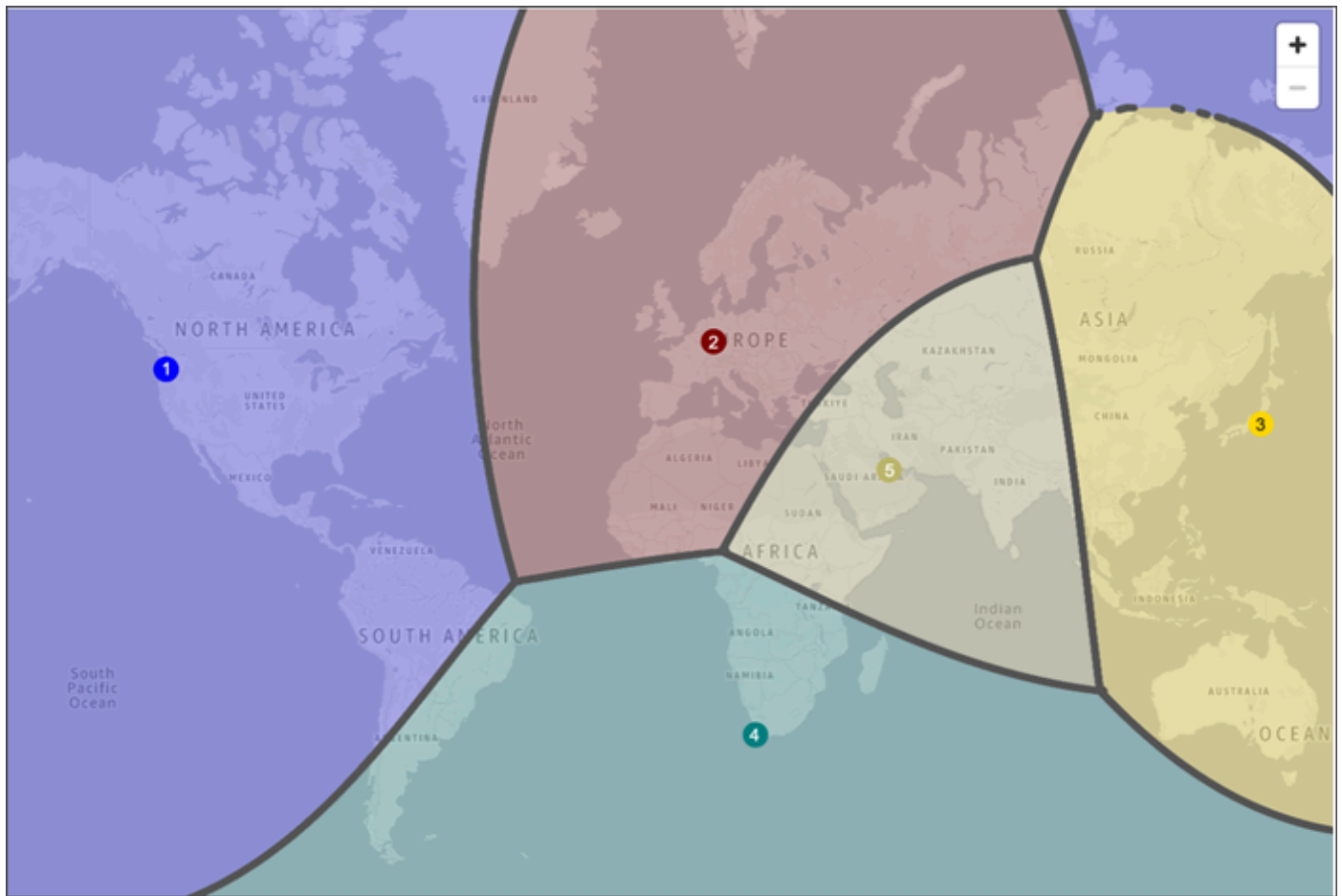
1. Oeste de EE. UU. (Oregón)
2. Europa (Fráncfort)
3. Asia-Pacífico (Tokio)
4. África (Ciudad del Cabo)
5. Middle East (Bahrain)

 Note

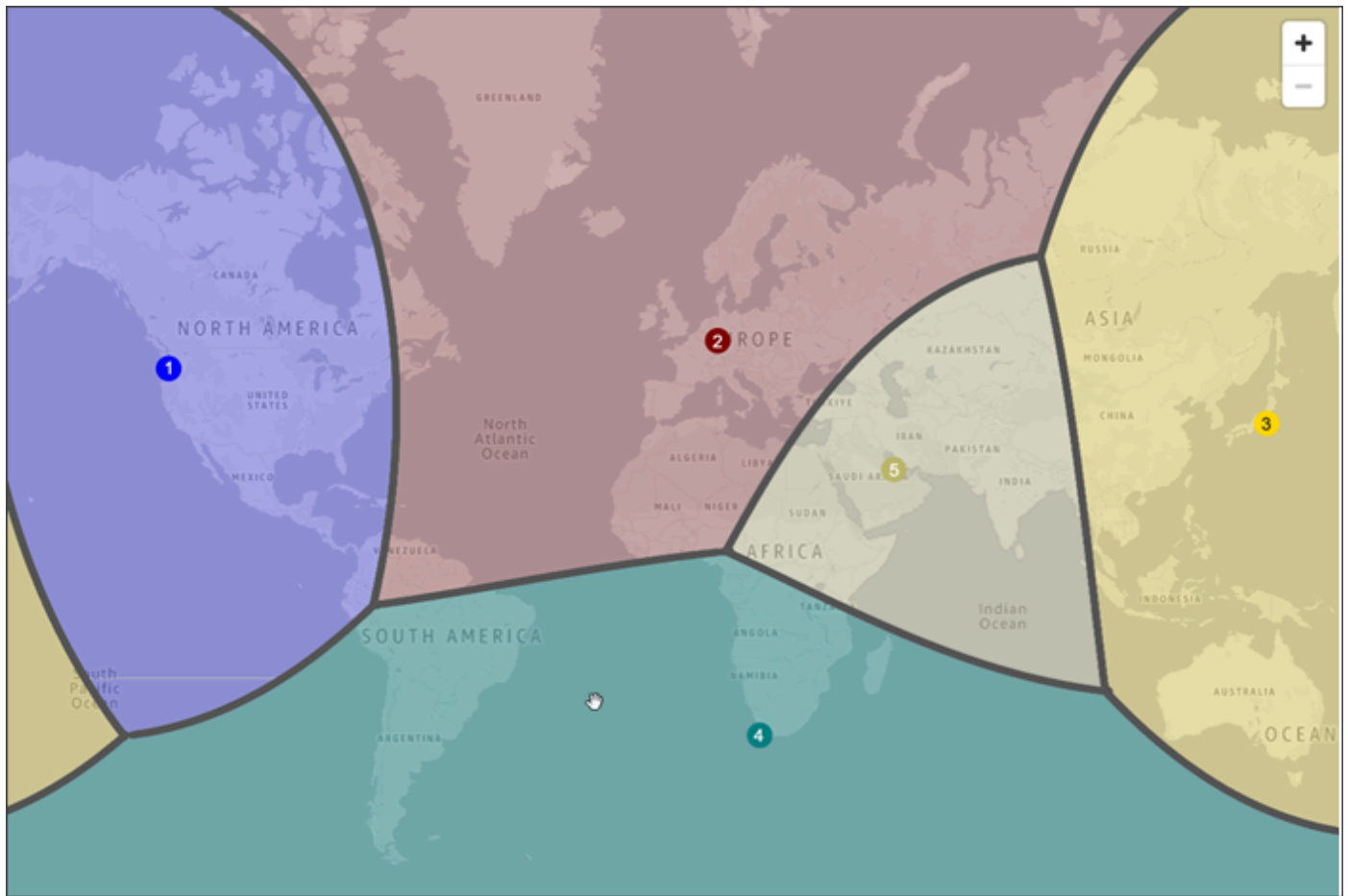
Los mapas solo están disponibles con el Flujo de tráfico.



En el siguiente mapa se muestra lo que sucede si agrega un sesgo de +25 para la región Oeste de EE. UU. (Oregón) (número 1 en el mapa). El tráfico se enruta al recurso de esa región desde una parte mayor de Norteamérica que antes y desde toda Sudamérica.



En el siguiente mapa se muestra lo que sucede si cambia el sesgo a -25 para la región Oeste de EE. UU. (Oregón). El tráfico se enruta al recurso de esa región desde partes más pequeñas de Norteamérica y Sudamérica que antes, y se dirige más tráfico a los recursos de las regiones 2, 3 y 4 adyacentes.

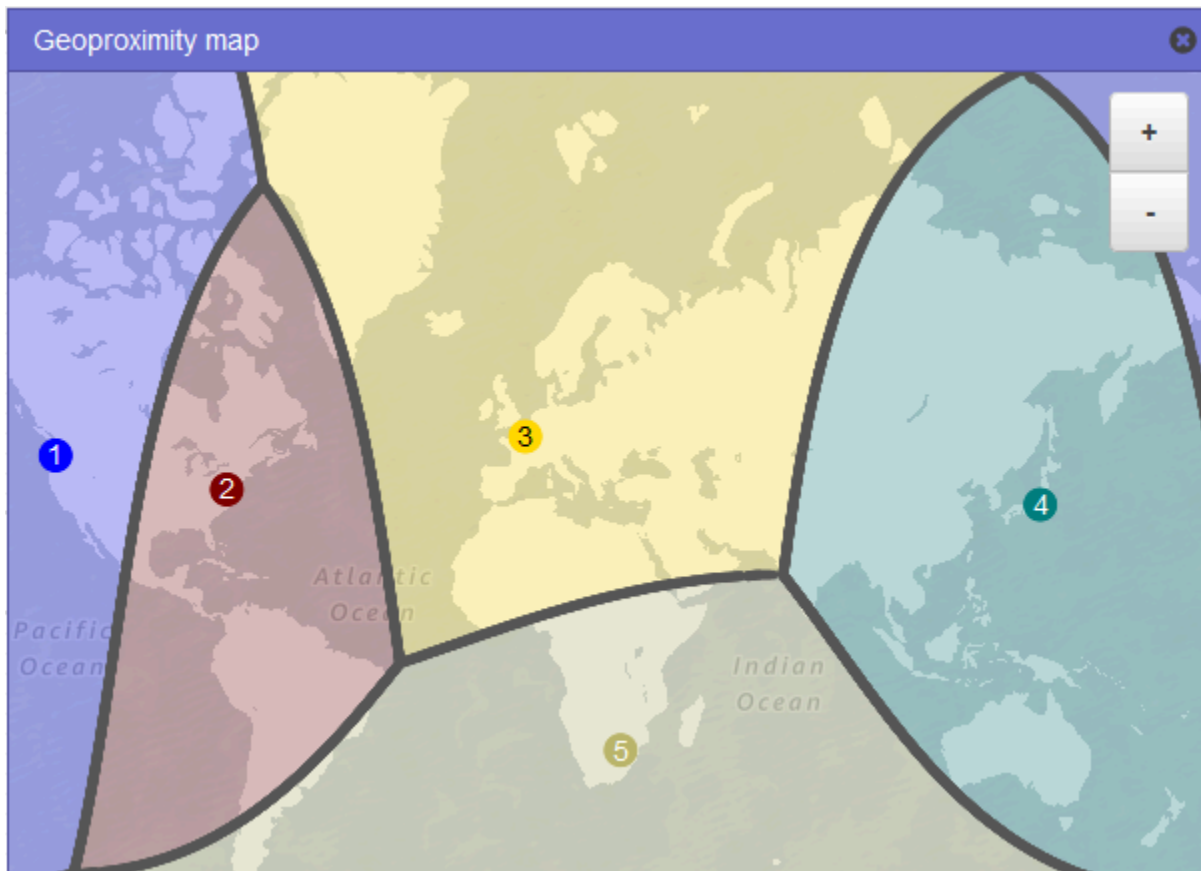


Old console

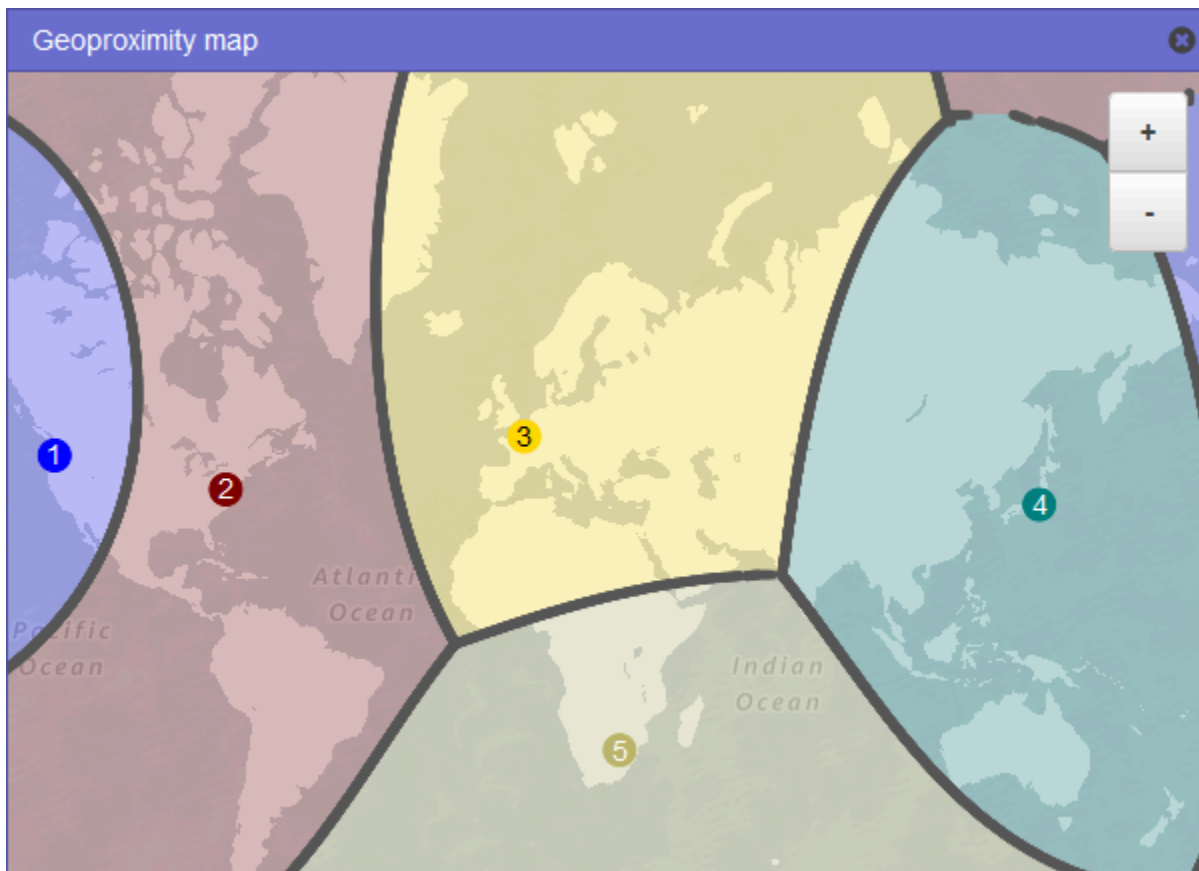
El siguiente mapa muestra cuatro Regiones de AWS (numerados del 1 al 4) y una ubicación en Johannesburg (Sudáfrica) que se especifica por latitud y longitud (5).

Note

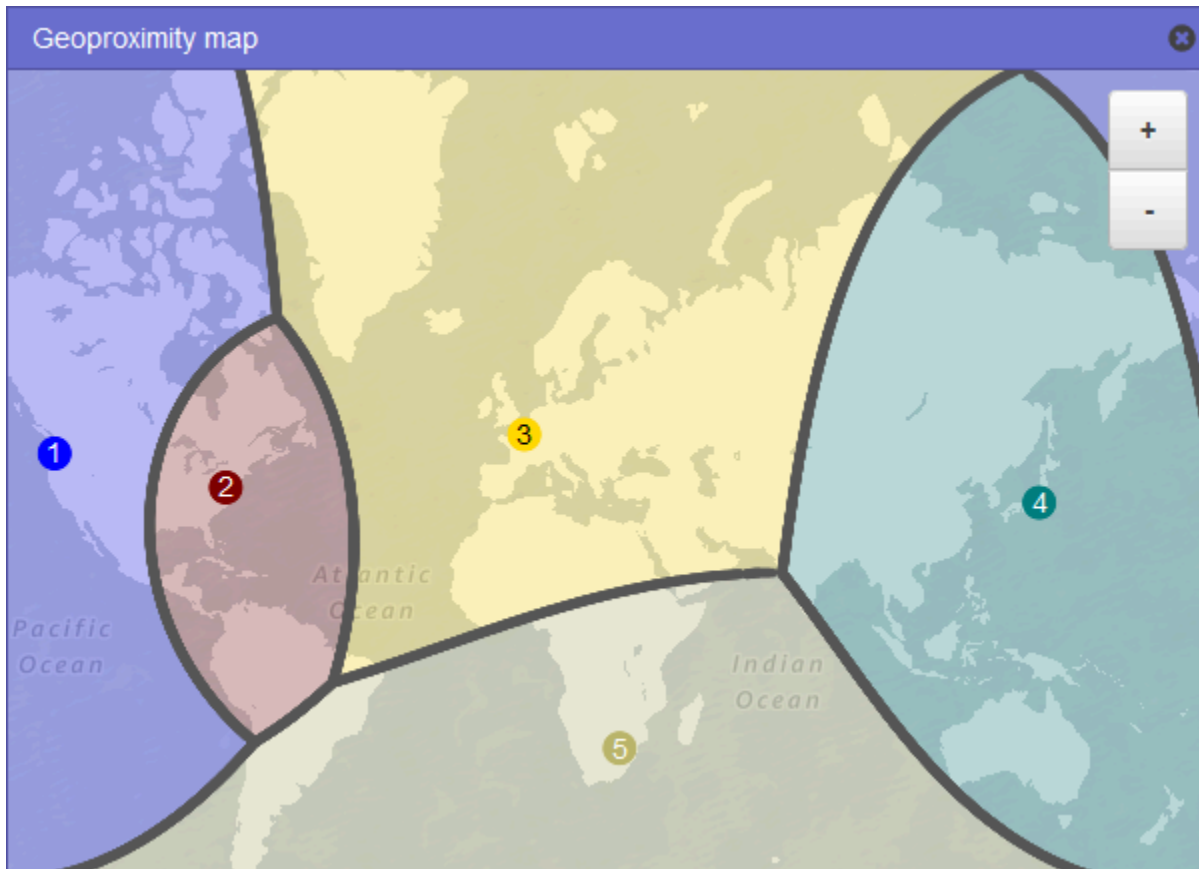
Los mapas solo están disponibles con el Flujo de tráfico.



El siguiente mapa muestra lo que sucede si agrega un sesgo de +25 para la región Este de EE. UU. (Norte de Virginia) (número 2 en el mapa). El tráfico se direcciona al recurso de esa región desde una parte mayor de Norteamérica que antes y desde toda Sudamérica.



El siguiente mapa muestra lo que sucede si cambia el sesgo a -25 para la región Este de EE. UU. (Norte de Virginia). El tráfico se direcciona al recurso de esa región desde partes más pequeñas de América del Norte y del Sur que antes, y más tráfico se direcciona a los recursos de las regiones adyacentes 1, 3 y 5.



El efecto de cambiar el sesgo de sus recursos depende de una serie de factores, entre los que se incluyen los siguientes:

- El número de recursos de los que dispone.
- Lo cercanos que están los recursos entre sí.
- El número de usuarios que haya cerca de la zona fronteriza entre regiones geográficas. Por ejemplo, supongamos que tiene recursos en Regiones de AWS EE.UU. Este (Norte de Virginia) y EE.UU. Oeste (Oregón), y tiene muchos usuarios en Dallas, Austin y San Antonio, Texas (EE. UU.). Esas ciudades están aproximadamente a la misma distancia entre sus recursos, por lo que un pequeño cambio en el sesgo podría provocar un gran cambio en el tráfico de los recursos de una Región de AWS a otra.

Le recomendamos que cambie el sesgo en incrementos pequeños para evitar desbordar los recursos debido a una oscilación no prevista en el tráfico.

Para obtener más información, consulte [Cómo Amazon Route 53 utiliza EDNS0 para calcular la ubicación de un usuario.](#)

Cómo utiliza Amazon Route 53 el sesgo para dirigir el tráfico

Esta es la fórmula que Amazon Route 53 utiliza para determinar cómo dirigir el tráfico:

Sesgo

$$\text{Biased distance} = \text{actual distance} * [1 - (\text{bias}/100)]$$

Cuando el valor del sesgo es positivo, Route 53 trata la fuente de una consulta de DNS y el recurso que especifique en un registro de geoproximidad (como una EC2 instancia de un registro Región de AWS) como si estuvieran más cerca de lo que realmente están. Suponga, por ejemplo, que tiene los siguientes registros de geoproximidad:

- Un registro para el servidor web A, que tiene un sesgo positivo de 50.
- Un registro para el servidor web B, que no tiene sesgos.

Cuando un registro de geoproximidad tiene un sesgo positivo de 50, Route 53 recorta a la mitad la distancia entre el origen de una consulta y el recurso para el registro. A continuación, Route 53 calcula qué recurso está más cerca del origen de la consulta. Supongamos que un servidor web A está a 150 kilómetros del origen de la consulta y que el servidor web B está a 100 kilómetros de dicho origen. Si ningún registro tiene un sesgo, Route 53 dirigirá la consulta al servidor web B porque está más cerca. No obstante, dado que el registro del servidor web A tiene un sesgo positivo de 50, Route 53 considera al servidor web A como si estuviera a 75 kilómetros del origen de la consulta. Como resultado, Route 53 dirige la consulta al servidor web A.

Este es el cálculo de un sesgo positivo de 50:

```
Bias = 50
Biased distance = actual distance * [1 - (bias/100)]

Biased distance = 150 kilometers * [1 - (50/100)]
Biased distance = 150 kilometers * (1 - .50)
Biased distance = 150 kilometers * (.50)
Biased distance = 75 kilometers
```

Enrutado basado en latencia

Si la aplicación está alojada en varios Regiones de AWS servidores, puede mejorar el rendimiento de los usuarios atendiendo sus solicitudes desde el Región de AWS que ofrezca la latencia más baja.

 Note

Los datos sobre la latencia entre los usuarios y sus recursos se basan totalmente en el tráfico entre los usuarios y los centros de datos de AWS . Si no utilizas los recursos en una Región de AWS, la latencia real entre tus usuarios y tus recursos puede variar considerablemente de los datos de AWS latencia. Esto es así aunque sus recursos se encuentren en la misma ciudad que una región de Región de AWS.

Para utilizar el enrutamiento basado en la latencia, debe crear registros de latencia para los recursos en varias Regiones de AWS. Cuando recibe una consulta de DNS para su dominio o subdominio (ejemplo.com o acme.ejemplo.com), Route 53 determina para qué Regiones de AWS usted ha creado registros de latencia, decide qué región ofrece a los usuarios la menor latencia y, finalmente, selecciona un registro de latencia para dicha región. Route 53 responde con el valor del registro seleccionado, como la dirección IP de un servidor web.

Por ejemplo, suponga que tiene balanceadores de carga de ELB en la región EE. UU. Oeste (Oregón) y en la región Asia-Pacífico (Singapur). Crea un registro de latencia para cada equilibrador de carga. Esto es lo que ocurre cuando un usuario en Londres escribe el nombre de su dominio en un navegador:

1. DNS dirige la consulta a un servidor de nombres de Route 53.
2. Route 53 consulta los datos sobre latencia entre Londres y la región de Singapur, y entre Londres y la región de Oregón.
3. Si la latencia es menor entre las regiones de Londres y Oregón, Route 53 responde a la consulta con la dirección IP del equilibrador de carga de Oregón. Si la latencia es menor entre las regiones de Londres y Singapur, Route 53 responde a la consulta con la dirección IP del equilibrador de carga de Singapur.

La latencia entre hosts en Internet puede cambiar con el tiempo como consecuencia de los cambios en la conectividad de la red y el direccionamiento. El enrutamiento basado en la latencia se fundamenta en mediciones de latencia realizadas durante un periodo, y estas mediciones reflejan estos cambios. Una solicitud que se direccionó a la región de Oregón esta semana puede enrutarse a la región de Singapur la próxima semana.

 Note

Cuando un navegador u otro visor utiliza un solucionador de DNS que admite la edns-client-subnet extensión EDNS0, el solucionador de DNS envía a Route 53 una versión truncada de la dirección IP del usuario. Si configura el direccionamiento basado en la latencia, Route 53 considera este valor al dirigir el tráfico a sus recursos. Para obtener más información, consulte [Cómo Amazon Route 53 utiliza EDNS0 para calcular la ubicación de un usuario](#).

Puede utilizar una política de enrutamiento de latencia para los registros de una zona alojada privada.

Para obtener información acerca de los valores que especifica cuando se utiliza la política de direccionamiento de latencia para crear registros, consulte los siguientes temas:

- [Valores específicos de registros de latencia](#)
- [Valores específicos de registros de alias de latencia](#)
- [Valores comunes a todas las políticas de enrutamiento](#)
- [Valores comunes de registros de alias para todas las políticas de enrutamiento](#)

Enrutado basado en latencia en zonas alojadas privadas

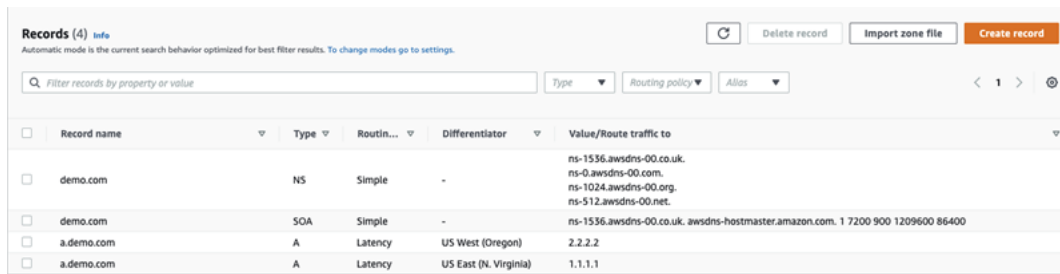
En el caso de las zonas alojadas privadas, Route 53 responde a las consultas de DNS con un punto final que se encuentra en el mismo Región de AWS punto final de la VPC Región de AWS de la que se originó la consulta o que está más cerca de ella.

 Note

Si se reenvía un punto de conexión saliente a un punto de conexión entrante, el registro se resolverá en función de dónde se encuentre el punto de conexión entrante, no el punto de conexión saliente.

Si incluye comprobaciones de estado y el registro con la latencia más baja hasta el origen de la consulta no está en buen estado, se devuelve un punto de conexión en buen estado con la siguiente latencia más baja.

En la configuración de ejemplo de la siguiente figura, las consultas de DNS procedentes de un Región de AWS us-east-1, o el más cercano a él, se enrutarán al punto final 1.1.1.1. Las consultas de DNS de us-west-2, o las más cercanas a esa región, se enrutarán al punto de conexión 2.2.2.2.



The screenshot shows the Amazon Route 53 console interface. At the top, there are buttons for 'Delete record', 'Import zone file', and 'Create record'. Below these is a search bar and filters for 'Type', 'Routing policy', and 'Alias'. The main table displays the following records:

Record name	Type	Routing...	Differentiator	Value/Route traffic to
demo.com	NS	Simple	-	ns-1536.awsdns-00.co.uk, ns-0.awsdns-00.com, ns-1024.awsdns-00.org, ns-512.awsdns-00.net
demo.com	SOA	Simple	-	ns-1536.awsdns-00.co.uk, awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400
a.demo.com	A	Latency	US West (Oregon)	2.2.2.2
a.demo.com	A	Latency	US East (N. Virginia)	1.1.1.1

Direccionamiento basado en IP

Con el enrutamiento basado en IP en Amazon Route 53, puede ajustar su enrutamiento DNS usando lo que sabe acerca de su red, aplicaciones y clientes para tomar las mejores decisiones de enrutamiento DNS para sus usuarios finales. El enrutamiento basado en IP le brinda un control detallado para optimizar el rendimiento o reducir los costos de la red al cargar sus datos a Route 53 en forma de mapeos. user-IP-to-endpoint

El enrutamiento basado en la geolocalización y la latencia se basa en los datos que Route 53 recopila y mantiene actualizados. Este enfoque funciona bien para la mayoría de los clientes, pero el enrutamiento basado en IP le ofrece la capacidad adicional de optimizar el enrutamiento en función del conocimiento específico de su base de clientes. Por ejemplo, un proveedor de contenidos global de video puede querer enrutar a los usuarios finales de un determinado proveedor de servicio de Internet (ISP).

Algunos casos de usos comunes para el enrutamiento basado en IP son los siguientes:

- Desea dirigir a los usuarios finales desde determinados puntos finales a puntos finales específicos ISPs para poder optimizar los costos o el rendimiento del tránsito de la red.
- Desea agregar anulaciones a los tipos de enrutamiento de Route 53 existentes, como el enrutamiento de geolocalización basado en su conocimiento de las ubicaciones físicas de sus clientes.

Administrar los rangos de IP y asociarlos a un conjunto de registros de recursos () RRSet

Para IPv4, puede usar bloques CIDR de entre 1 y 24 bits de longitud, ambos inclusive, mientras que para IPv6, puede usar bloques CIDR de entre 1 y 48 bits de longitud, ambos inclusive. Para definir un bloque de CIDR de cero bits (0.0.0.0/0 o ::/0), utilice la ubicación predeterminada ("").

Para consultas DNS con un CIDR más largo que el especificado en la colección CIDR, Route 53 las asociará con el CIDR más corto. Por ejemplo, si especificas 2001:0DB8: :/32 como bloque CIDR de tu colección CIDR y una consulta se origina en DB8 2001:0:0000:1234: :/48, coincidirá. Si, por otro lado, especifica 2001:0DB8: 0000:1234: :/48 en su colección CIDR y una consulta se origina en 2001:0DB8: :/32, no coincidirá y Route 53 responderá con el registro de la ubicación predeterminada («*»).

Puede agrupar conjuntos de bloques CIDR (o rangos de IP) en ubicaciones CIDR, que a su vez se agrupan en entidades reutilizables llamadas colecciones CIDR:

Bloque CIDR

Un rango de IP en notación CIDR, por ejemplo, 192.0.2.0/24 o 2001:: :/32. DB8

Ubicación CIDR

Una lista con nombre de bloques CIDR. Por ejemplo, example-isp-seattle = [192.0.2.0/24, 203.0.113.0/22, 198.51.100.0/24, 2001: :/32]. DB8 Los bloques de una lista de localización CIDR no tienen por qué ser adyacentes o del mismo rango.

Una única ubicación puede tener IPv6 bloques IPv4 y, y esta ubicación se puede asociar a los conjuntos de registros A y AAAA, respectivamente.

El nombre de la ubicación suele ser un lugar por convención, pero puede ser cualquier cadena, por ejemplo Compañía-A.

Colección CIDR

Una colección de ubicaciones con nombre. Por ejemplo, mycollection = [example-isp-seattle, example-isp-tokyo].

Los conjuntos de registros de recursos de enrutamiento basados en IP hacen referencia a una ubicación en una colección, y todos los conjuntos de registros de recursos para el mismo nombre y tipo de conjunto de registros deben hacer referencia a la misma colección. Por ejemplo, si crea sitios web en dos regiones y desea dirigir las consultas de DNS desde dos ubicaciones CIDR diferentes a un sitio web específico en función de las direcciones IP de origen, entonces ambas ubicaciones deben figurar en la misma colección CIDR.

No puede utilizar una política de enrutamiento basado en IP para los registros de una zona alojada privada.

Para obtener información sobre los valores que se especifican cuando se usa la política de enrutamiento basada en IP para crear registros, consulte los siguientes temas:

- [Valores específicos para los registros basados en IP](#)
- [Valores específicos para los registros de alias basados en IP](#)
- [Valores comunes a todas las políticas de enrutamiento](#)
- [Valores comunes de registros de alias para todas las políticas de enrutamiento](#)

Temas

- [Creación de una colección de CIDR con ubicaciones y bloques CIDR](#)
- [Trabajo con ubicaciones y bloques CIDR](#)
- [Eliminar una colección CIDR](#)
- [Mover una geolocalización a un enrutamiento basado en IP](#)

Creación de una colección de CIDR con ubicaciones y bloques CIDR

Para empezar, cree una colección de CIDR y agregue a ella bloques y ubicaciones CIDR.

Para crear una colección de CIDR mediante la consola de Route 53

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija IP-based routing (Enrutamiento basado en IP) y, luego, CIDR collections (Recopilaciones de CIDR).
3. Seleccione Create CIDR collection (Crear una colección de CIDR).
4. En el panel Create CIDR collection en Details (Detalles), ingrese un nombre para la colección.
5. Elija Create collection (Crear colección) para crear una colección vacía.

-o bien-

En la sección Crear ubicaciones del CIDR, introduzca un nombre para la ubicación del CIDR en el cuadro de Ubicación del CIDR. El nombre de la ubicación puede ser cualquier cadena identificativa, por ejemplo **company 1**, o bien **Seattle**. No tiene por qué ser una ubicación geográfica real.

 Important

El nombre de la ubicación del CIDR tiene una longitud máxima de 16 caracteres.

Introduzca los bloques del CIDR en el cuadro Bloques del CIDR, uno por línea. Pueden ser IPv6 direcciones IPv4 o direcciones comprendidas entre /0 y /24 y entre /0 IPv4 y /48. IPv6

- Una vez ingresados los bloques CIDR, elija Create CIDR collection, o bien Add another location (Agregar otra ubicación) ingresando ubicaciones y bloque CIDR. Puede introducir varias ubicaciones CIDR por colección.
- Una vez ingresadas las ubicaciones CIDR, seleccione Create CIDR collection.

Trabajo con ubicaciones y bloques CIDR

Para trabajar con ubicaciones CIDR mediante la consola de Route 53

- Inicie sesión en la consola de Route Consola de administración de AWS 53 y ábrala en. <https://console.aws.amazon.com/route53/>
- En el panel de navegación, seleccione Enrutamiento basado en IP, Recopilaciones de CIDR y, a continuación, en la sección Recopilaciones de CIDR, haga clic en un enlace a una recopilación de CIDR en la lista Nombre de la recopilación.

En la página CIDR locations (Ubicaciones CIDR), puede crear una ubicación CIDR, eliminarla o editar una ubicación y sus bloques.

- Para crear una ubicación, seleccione Create CIDR location (Crear ubicación CIDR).
- En el panel Create CIDR location, ingrese un nombre para la ubicación, los bloques CIDR asociados con la ubicación y, luego, seleccione Create (Crear).
- Para ver una ubicación CIDR y los bloques que contiene, elija el botón de opción situado junto a una ubicación para mostrar su nombre y los bloques CIDR en el panel de ubicación.

En este panel, también puede elegir Editar para actualizar el nombre de la ubicación o sus bloques CIDR. Cuando haya terminado de editar, elija Save (Guardar).

- Para eliminar una ubicación CIDR y los bloques de su interior, seleccione el botón de opción situado junto a la ubicación que desea eliminar y, a continuación, seleccione Delete (Borrar).

Para confirmar la eliminación, escriba el nombre de la ubicación en el campo de entrada de texto y elija Delete de nuevo.

 Important

No se puede deshacer la eliminación de una ubicación CIDR. Si tiene algún registro DNS asociado a la ubicación, es posible que no se pueda acceder a su dominio.

Eliminar una colección CIDR

Para eliminar una colección CIDR, sus ubicaciones y bloques mediante la consola de Route 53

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija IP-based routing (Enrutamiento basado en IP) y, luego, CIDR collections (Recopilaciones de CIDR).
3. En la sección CIDR collections, haga clic en el nombre vinculado de la colección que desea eliminar.
4. En la página CIDR locations (Ubicaciones CIDR), seleccione cada ubicación de una en una, elija Delete (Eliminar), ingrese su nombre en el cuadro de diálogo y luego elija Delete. Debe eliminar cada ubicación asociada a una colección CIDR para poder eliminar la colección.
5. Una vez finalizada la eliminación de cada ubicación CIDR, en la página CIDR locations, elija el botón de opción junto a la colección que desea eliminar y, a continuación, elija Delete.

Mover una geolocalización a un enrutamiento basado en IP

Si usa políticas de enrutamiento de geolocalización o geoproximidad, y ve constantemente clientes específicos enrutados a un punto de conexión que no es óptimo basado en su ubicación física o topología de red, puede orientar mejor los rangos de IP pública de estos clientes mediante el enrutamiento basado en IP.

La siguiente tabla contiene un ejemplo de configuración de geolocalización para un enrutamiento de geolocalización existente que afinaremos para los rangos IP de California.

Nombre del conjunto de registros	Política de enrutamiento y origen	Dirección IP del punto de conexión de la aplicación
example.com	Enrutamiento de geolocalización (EE. UU.)	198.51.100.1
example.com	Enrutamiento de geolocalización (UE)	198.51.100.2

Para anular los rangos de IP de California para ir a un nuevo punto de conexión de la aplicación, primero vuelva a crear el enrutamiento de geolocalización bajo un nuevo nombre de conjunto de registros.

Nombre del conjunto de registros	Política de enrutamiento y origen	Dirección IP del punto de conexión de la aplicación
geo.ejemplo.com	Enrutamiento de geolocalización (EE.UU.)	198.51.100.1
geo.ejemplo.com	Enrutamiento de geolocalización (UE)	198.51.100.2

Luego, cree registros de enrutamiento basados en IP y un registro por defecto que apunte a su conjunto de registros de enrutamiento de geolocalización recientemente recreado.

Nombre del conjunto de registros	Política de enrutamiento y origen	Dirección IP del punto de conexión de la aplicación
example.com	Enrutamiento basado en IP (predeterminado)	Registro de alias del punto de conexión de la aplicación geo.example.com que desea que sea el predeterminado.

Nombre del conjunto de registros	Política de enrutamiento y origen	Dirección IP del punto de conexión de la aplicación
		Por ejemplo, 198.51.100.1 .
example.com	Enrutamiento basado en IP (rangos IP de California)	198.51.100.3

Direccionamiento de respuesta con varios valores

El direccionamiento de respuesta con varios valores permite configurar Amazon Route 53 para devolver varios valores, como direcciones IP a los servidores web, en respuesta a las consultas de DNS. Puede especificar varios valores para casi cualquier registro, pero este direccionamiento también permite verificar el estado de cada recurso, por lo que Route 53 devuelve los valores únicamente para los recursos en buen estado. No es sustituto de un balanceador de carga, pero la capacidad de devolver varias direcciones IP (cuyo estado sea comprobable) constituye una forma de usar el DNS para mejorar la disponibilidad y el equilibrio de la carga.

Para dirigir el tráfico de forma aproximativa aleatoriamente a varios recursos, como servidores web, cree un registro de respuesta con varios valores para cada recurso y, de manera opcional, asocie una comprobación de estado de Route 53 a cada registro. Route 53 responde a las consultas de DNS con hasta ocho registros en buen estado y da diferentes respuestas a distintos solucionadores de DNS. Si un servidor web deja de estar disponible después de que un solucionador almacene una respuesta en memoria caché, el software de cliente puede intentar utilizar otra dirección IP en la respuesta.

Tenga en cuenta lo siguiente:

- Si asocia una comprobación de estado a un registro de respuesta con varios valores, Route 53 responde a las consultas de DNS con la correspondiente dirección IP solo si se verifica que está en buen estado.
- Si no asocia ninguna comprobación de estado a un registro de respuesta con varios valores, Route 53 siempre considera que el registro está en buen estado.
- Si tiene ocho registros o menos en buen estado, Route 53 responde a todas las consultas de DNS con todos los registros en buen estado.

- Cuando todos los registros están en mal estado, Route 53 responde a las consultas de DNS con hasta ocho registros en mal estado.

Puede utilizar una política de enrutamiento de respuesta con varios valores para los registros de una zona alojada privada.

Para obtener más información acerca de los valores que especifica cuando se utiliza la política de enrutamiento de respuesta multivalor para crear registros, consulte [Valores específicos de registros de respuesta de varios valores](#) y [Valores comunes a todas las políticas de enrutamiento](#).

Direccionamiento ponderado

El direccionamiento ponderado permite asociar varios recursos a un solo nombre de dominio (example.com) o nombre de subdominio (acme.example.com) y elegir cuánto tráfico se redirige a cada recurso. Esto puede resultar útil para distintos fines, entre otros, equilibrar la carga y probar nuevas versiones de software.

Para configurar el direccionamiento ponderado, debe crear registros que tengan el mismo nombre y tipo para cada uno de sus recursos. Asigne a cada registro un peso relativo que se corresponda con la cantidad de tráfico que desea enviar a cada recurso. Amazon Route 53 envía el tráfico a un recurso en función del peso que se asigna al registro, como una proporción del peso total de todos los registros del grupo:

$$\frac{\text{Weight for a specified record}}{\text{Sum of the weights for all records}}$$

Por ejemplo, si desea enviar una pequeña parte del tráfico a un recurso y el resto a otro recurso, puede especificar pesos de 1 y 255. El recurso con un peso de 1 se lleva una fracción de 1/256 del tráfico ($1/(1+255)$), y el otro recurso, 255/256 ($255/(1+255)$). Para modificar gradualmente el equilibrio puede cambiar los pesos. Si desea detener el envío de tráfico a un recurso, puede cambiar por 0 el peso de ese registro.

Para obtener información acerca de los valores que especifica cuando se utiliza la política de direccionamiento ponderado para crear registros, consulte los siguientes temas:

- [Valores específicos de registros ponderados](#)
- [Valores específicos de registros de alias ponderados](#)
- [Valores comunes a todas las políticas de enrutamiento](#)
- [Valores comunes de registros de alias para todas las políticas de enrutamiento](#)

Puede utilizar una política de enrutamiento ponderado para los registros de una zona alojada privada.

Comprobaciones de estado y enrutamiento ponderado

Si agrega comprobaciones de estado a todos los registros de un grupo de registros ponderados, pero asigna ponderaciones distintas de cero a algunos registros y ponderaciones cero a otros, las comprobaciones de estado funcionan igual que si todos los registros tuvieran ponderaciones distintas de cero con las excepciones siguientes:

- Route 53 tiene en cuenta inicialmente solo los registros con ponderación distinta de cero, si los hubiera.
- Si todos los registros con una ponderación mayor que 0 tienen un estado incorrecto, Route 53 tiene en cuenta los registros con ponderación cero.

En la siguiente tabla, se detalla el comportamiento cuando el registro de ponderación 0 incluye una comprobación de estado:

	Registro 1	Registro 2	Registro 3
Peso	1	1	0
¿Incluye comprobación de estado?	Sí	Sí	Sí
Health check status (Estado de la comprobación de estado)	Mal estado	Mal estado	Buen estado
¿Consulta de DNS respondida?	No	No	Sí
	Mal estado	Mal estado	Mal estado

	Registro 1	Registro 2	Registro 3
Health check status (Estado de la comprobación de estado)			
¿Consulta de DNS respondida?	Sí	Sí	No
Health check status (Estado de la comprobación de estado)	Mal estado	Buen estado	Mal estado
¿Consulta de DNS respondida?	No	Sí	No
Health check status (Estado de la comprobación de estado)	Buen estado	Buen estado	Mal estado
¿Consulta de DNS respondida?	Sí	Sí	No
Health check status (Estado de la comprobación de estado)	Buen estado	Buen estado	Buen estado
¿Consulta de DNS respondida?	Sí	Sí	No

En la siguiente tabla, se detalla el comportamiento cuando el registro de ponderación 0 no incluye una comprobación de estado:

	Registro 1	Registro 2	Registro 3
Peso	1	1	0
¿Incluye comprobación de estado?	Sí	Sí	No
Health check status (Estado de la comprobación de estado)	Buen estado	Buen estado	N/A
¿Consulta de DNS respondida?	Sí	Sí	No
Health check status (Estado de la comprobación de estado)	Mal estado	Mal estado	N/A
¿Consulta de DNS respondida?	No	No	Sí
Health check status (Estado de la comprobación de estado)	Mal estado	Buen estado	N/A
¿Consulta de DNS respondida?	No	Sí	No

Cómo Amazon Route 53 utiliza EDNS0 para calcular la ubicación de un usuario

Para mejorar la precisión de la geolocalización, la geoproximidad, el enrutamiento basado en IP y la latencia, Amazon Route 53 admite la `edns-client-subnet` extensión de EDNS0. (EDNS0 agrega varias extensiones opcionales al protocolo de DNS). Route 53 `edns-client-subnet` solo se puede usar cuando los resolutores de DNS lo admiten:

- Cuando un navegador u otro visor usa una resolución de DNS que no es compatible `edns-client-subnet`, Route 53 usa la dirección IP de origen de la resolución de DNS para aproximar la ubicación del usuario y responde a las consultas de geolocalización con el registro DNS de la ubicación de la resolución.
- Cuando un navegador u otro visor utiliza un solucionador de DNS compatible `edns-client-subnet`, el solucionador de DNS envía a Route 53 una versión truncada de la dirección IP del usuario. Route 53 determina la ubicación del usuario a través de la dirección IP truncada, en lugar de hacerlo mediante la dirección IP de origen del solucionador de DNS; este método suele proporcionar una estimación más precisa de la ubicación del usuario. Después, Route 53 responde a las consultas de geolocalización con el registro de DNS de la ubicación del usuario.
- EDNS0 no se aplica a zonas alojadas privadas. En el caso de las zonas alojadas privadas, Route 53 utiliza los datos de los solucionadores de VPC en la Región de AWS que se encuentra la zona alojada privada para tomar decisiones de geolocalización y enrutamiento de latencia.

[Para obtener más información `edns-client-subnet`, consulte el RFC de la subred del cliente de EDNS y la subred del cliente en las solicitudes de DNS.](#)

Elección entre registros de alias y sin alias

Los registros de alias de Amazon Route 53 proporcionan una extensión específica de Route 53 para la funcionalidad de DNS. Los registros de alias le permiten enrutar el tráfico a AWS los recursos seleccionados, incluidas, entre otras, las CloudFront distribuciones y los buckets de Amazon S3. También le permiten dirigir el tráfico de un registro de una zona alojada a otro registro.

A diferencia de un registro CNAME, puede crear un registro de alias en el nodo superior de un espacio de nombres de DNS, también conocido como vértice de zona. Por ejemplo, si registra el nombre DNS `example.com`, el vértice de zona será `example.com`. No puede crear un registro CNAME para `example.com`, aunque sí puede crear un registro de alias para `example.com` que dirige el tráfico a `www.example.com` (siempre que el tipo de registro para `www.example.com` no sea el tipo CNAME).

Cuando Route 53 recibe una consulta de DNS para un registro de alias, Route 53 responde con el valor aplicable de dicho recurso:

- Una API regional personalizada o una optimizada para periferia de Amazon API Gateway: Route 53 responde con una o varias direcciones IP para la API.
- Un punto de conexión de interfaz de Amazon VPC: Route 53 responde con una o varias direcciones IP para el punto de conexión de interfaz.
- Una CloudFront distribución: Route 53 responde con una o más direcciones IP para los servidores CloudFront perimetrales que pueden ofrecer su contenido.
- Servicio de App Runner: Route 53 responde con una o varias direcciones IP.
- Un entorno de Elastic Beanstalk: Route 53 responde con una o varias direcciones IP para el entorno.
- Un balanceador de carga de ELB: Route 53 responde con una o varias direcciones IP para el balanceador de carga. Esto incluye el equilibrador de carga de aplicación, el equilibrador de carga clásico y el equilibrador de carga de red.
- Un AWS Global Accelerator acelerador: Route 53 responde con las direcciones IP del acelerador.
- Un OpenSearch servicio: Route 53 responde con una o más direcciones IP para el dominio personalizado del OpenSearch servicio.
- Un bucket de Amazon S3 configurado como sitio web estático: Route 53 responde con una dirección IP para el bucket de Amazon S3.
- Otro registro de Route 53 del mismo tipo de la misma zona alojada: Route 53 responde como si la consulta fuera para el registro al que hace referencia el registro de alias (consulte [Comparación de los registros de alias y CNAME](#)).
- AWS AppSync nombre de dominio: Route 53 responde con una o más direcciones IP para el punto final de la interfaz.

Para obtener más información, consulte [Enrutar el tráfico de Internet a sus AWS recursos](#).

Cuando usa un registro de alias para enrutar el tráfico a un AWS recurso, Route 53 reconoce automáticamente los cambios en el recurso. Por ejemplo, suponga que un registro de alias para example.com apunta a un balanceador de carga de ELB en lb1-1234.us-east-2.elb.amazonaws.com. Si la dirección IP del balanceador de carga cambia, Route 53 se inicia automáticamente para responder a las consultas de DNS utilizando la nueva dirección IP.

Si un registro de alias apunta a un AWS recurso, no puede establecer el tiempo de vida (TTL); Route 53 usa el TTL predeterminado para el recurso. Si un registro de alias apunta a otro registro de la misma zona alojada, Route 53 utiliza el TTL del registro al que apunta el registro de alias. Para obtener más información sobre el valor TTL actual para ELB, vaya a [Request routing](#) en la Guía del usuario de Elastic Load Balancing y busque «ttl».

Para obtener información sobre cómo crear registros mediante la consola de Route 53, consulte [Creación de registros con la consola de Amazon Route 53](#). Para obtener información acerca de los valores que especifique para registros de alias, consulte el tema correspondiente en [Valores que hay que especificar al crear o editar los registros de Amazon Route 53](#):

- [Valores específicos para registros de alias simples](#)
- [Valores específicos de registros de alias ponderados](#)
- [Valores específicos de registros de alias de latencia](#)
- [Valores específicos de registros de alias de conmutación por error](#)
- [Valores específicos de registros de alias de geolocalización](#)
- [Valores específicos de registros de alias de geoproximidad](#)
- [Valores comunes de registros de alias para todas las políticas de enrutamiento](#)

Comparación de los registros de alias y CNAME

Los registros de alias se parecen a los registros CNAME, pero hay algunas diferencias importantes. La siguiente lista compara los registros de alias y los registros CNAME.

Recursos a los que puede redirigir consultas

Registros de alias

Un registro de alias solo puede redirigir las consultas a AWS los recursos seleccionados, incluidos, entre otros, los siguientes:

- Buckets de Amazon S3
- CloudFront distribuciones
- Otro registro de la misma zona alojada de Route 53

Por ejemplo, puede crear un registro de alias denominado `acme.example.com` que redirija las consultas a un bucket de Amazon S3 que también se denomine `acme.example.com`. También

puede crear un registro de alias de `acme.example.com` que redirija las consultas a un registro denominado `zenith.example.com` de la zona alojada de `example.com`.

Registros CNAME

Un registro CNAME puede redirigir las consultas de DNS a cualquier registro de DNS. Por ejemplo, puede crear un registro CNAME que redirija las consultas de `acme.example.com` a `zenith.example.com` o a `acme.example.org`. No tiene que utilizar Route 53 como servicio de DNS para el dominio al que está redirigiendo las consultas.

Crear registros que tengan el mismo nombre que el dominio (registros en el vértice de zona)

Registros de alias

En la mayoría de las configuraciones, puede crear un registro de alias que tenga el mismo nombre que la zona alojada (vértice de zona). La única excepción se da cuando desea redirigir consultas desde el vértice de zona (como `example.com`) a un registro de la misma zona alojada que tiene un tipo de CNAME (como `zenith.example.com`). El registro de alias debe tener el mismo tipo que el registro al que está redirigiendo el tráfico y no es posible crear un registro CNAME para el vértice de zona (ni siquiera para un registro de alias).

Registros CNAME

No se puede crear un registro CNAME que tenga el mismo nombre que la zona alojada (vértice de zona). Esto es válido tanto para las zonas hospedadas de nombres de dominio (`example.com`) como para las zonas hospedadas de subdominios (`zenith.example.com`).

Precios para consultas de DNS

Registros de alias

Route 53 no cobra por las consultas de alias a AWS los recursos. Para obtener más información, consulte [Precios de Amazon Route 53](#).

Registros CNAME

Route 53 cobra por las consultas CNAME.

Note

Si crea un registro CNAME que redirige al nombre de otro registro en una zona alojada de Route 53 (la misma zona alojada u otra), cada consulta de DNS se carga como dos consultas:

- Route 53 responde a la primera consulta de DNS con el nombre del registro al que desea redirigir.

- A continuación, el solucionador de DNS debe enviar otra consulta para el registro en la primera respuesta para obtener información sobre dónde dirigir el tráfico, por ejemplo, la dirección IP de un servidor web.
- Si el registro CNAME redirige al nombre de un registro alojado con otro servicio de DNS, Route 53 carga una consulta. El otro servicio de DNS podría cargar la segunda consulta.

Tipo de registro especificado en la consulta de DNS

Registros de alias

Route 53 responde a una consulta de DNS solo cuando el nombre del registro de alias (como `acme.example.com`) y el tipo del registro de alias (como A o AAAA) coinciden con el nombre y el tipo de la consulta de DNS.

Registros CNAME

Un registro CNAME redirige las consultas de DNS para un nombre de registro independientemente del tipo de registro especificado en la consulta de DNS, como A o AAAA.

Cómo se enumeran los registros en las consultas de `dig` o `nslookup`

Registros de alias

En la respuesta a una consulta de `dig` o `nslookup`, se muestra un registro de alias como el tipo de registro que especificó al crear el registro, como A o AAAA. (El tipo de registro que especifique para un registro de alias depende del recurso al que esté dirigiendo el tráfico. Por ejemplo, para dirigir tráfico a un bucket de S3, especifique A en el tipo). La propiedad `alias` solo está visible en la consola de Route 53 o en la respuesta a una solicitud programática, como un `list-resource-record-sets` comando AWS CLI.

Registros CNAME

Un registro CNAME aparece como registro CNAME en respuesta a consultas `dig` o `nslookup`.

Tipos de registros de DNS admitidos

Amazon Route 53 admite los tipos de registros de DNS que se indican en esta sección. Cada tipo de registro incluye también un ejemplo de cómo formatear el elemento `Value` cuando tenga acceso a Route 53 mediante la API.

 Note

Para los tipos de registros que incluyen un nombre de dominio, especifique un nombre de dominio completo (por ejemplo, `www.example.com`). El punto final es opcional; Route 53 presupone que el nombre de dominio es completo. Esto significa que Route 53 trata a `www.example.com` (sin punto final) y `www.example.com.` (con punto final) de idéntica forma.

Route 53 proporciona una extensión a la funcionalidad DNS conocida como registros de alias. De forma parecida a los registros CNAME, los registros de alias le permiten dirigir el tráfico a recursos de AWS seleccionados, como, por ejemplo, distribuciones de CloudFront o buckets de Amazon S3. Para obtener más información, incluida una comparación de registros CNAME y alias, consulte [Elección entre registros de alias y sin alias](#).

Temas

- [Un tipo de registro](#)
- [Tipo de registro AAAA](#)
- [Tipo de registro de CAA](#)
- [Tipo de registro CNAME](#)
- [Tipo de registro DS](#)
- [Tipo de registro HTTPS](#)
- [Tipo de registro MX](#)
- [Tipo de registro NAPTR](#)
- [Tipo de registro NS](#)
- [Tipo de registro PTR](#)
- [Tipo de registro SOA](#)
- [Tipo de registro SPF](#)
- [Tipo de registro SRV](#)
- [Registro de tipo SSHFP](#)
- [Registro de tipo SVCB](#)
- [Registro de tipo TLSA](#)
- [Tipo de registro TXT](#)

Un tipo de registro

Utilice un registro A para enrutar el tráfico a un recurso, por ejemplo un servidor web, mediante una dirección IPv4 en notación decimal con puntos.

Ejemplo de la consola de Amazon Route 53

```
192.0.2.1
```

Ejemplo de la API de Route

```
<Value>192.0.2.1</Value>
```

Tipo de registro AAAA

Utilice un registro AAAA para enrutar el tráfico a un recurso, como un servidor web, mediante una dirección IPv6 en formato hexadecimal separada con el carácter de dos puntos.

Ejemplo de la consola de Amazon Route 53

```
2001:0db8:85a3:0:0:8a2e:0370:7334
```

Ejemplo de la API de Route

```
<Value>2001:0db8:85a3:0:0:8a2e:0370:7334</Value>
```

Tipo de registro de CAA

Un registro de CAA especifica qué entidades de certificación (CA) están autorizadas a emitir certificados para un dominio o subdominio. La creación de un registro de CAA ayuda a evitar que una CA errónea emita certificados para sus dominios. Un registro de CAA no es un sustituto de los requisitos de seguridad que especifica su entidad de certificación como, por ejemplo, la necesidad de validar que usted es el propietario de un dominio.

Puede utilizar los registros CAA para especificar lo siguiente:

- Qué autoridades de certificación (CA, Certificate Authority) pueden emitir certificados SSL/TLS, si procede.

- La dirección de correo electrónico o URL con la que hay que contactar en caso de que una CA emita un certificado para el dominio o subdominio.

Cuando añade un registro de CAA a su zona alojada, debe especificar tres valores separados por espacios:

```
flags tag "value"
```

Tenga en cuenta lo siguiente en relación con el formato de los registros CAA:

- El valor de `tag` solo puede contener los caracteres A-Z, a-z y 0-9.
- Encuadre siempre `value` entre comillas ("").
- Algunas CA permiten o requieren valores adicionales para `value`. Especifique valores adicionales como pares nombre-valor y sepárelos con punto y coma (;), por ejemplo:

```
0 issue "ca.example.net; account=123456"
```

- En caso de que una CA reciba una solicitud de certificado para un subdominio (como `www.example.com`) y si no existe registro de CAA del subdominio, la CA enviará una consulta de DNS para un registro de CAA para el dominio principal (como `example.com`). Si existe un registro de dominio principal y si la solicitud de certificado es válida, la CA genera el certificado para el subdominio.
- Le recomendamos que consulte a su CA para determinar qué valores especificar para un registro de CAA.
- No se puede crear un registro de CAA y un registro CNAME que tengan el mismo nombre, ya que el DNS no permite utilizar el mismo nombre para un registro CNAME y cualquier otro tipo de registro.

Temas

- [Autorización a una CA a emitir un certificado para un dominio o subdominio](#)
- [Autorización a una CA a emitir un certificado comodín para un dominio o subdominio](#)
- [Evitar que cualquier CA emita un certificado para un dominio o un subdominio](#)
- [Solicitar que cualquier CA se ponga en contacto con usted si la CA recibe una solicitud de certificado no válida](#)
- [Uso de otra opción compatible con la CA](#)
- [Ejemplos](#)

Autorización a una CA a emitir un certificado para un dominio o subdominio

Para autorizar a una CA a emitir un certificado para un dominio o un subdominio, cree un registro que tenga el mismo nombre que el dominio o subdominio y especifique la siguiente configuración:

- marcadores – `0`
- etiqueta – `issue`
- valor: el código de la CA a la que autoriza a emitir un certificado para el dominio o subdominio

Por ejemplo, suponga que desea autorizar `ca.example.net` para que emita un certificado para `example.com`. Puede crear un registro de CAA para `example.com` con la siguiente configuración:

```
0 issue "ca.example.net"
```

Para obtener información sobre cómo autorizar AWS Certificate Manager para emitir un certificado, consulte [Configuración de un registro de CAA](#) en la Guía del usuario de AWS Certificate Manager.

Autorización a una CA a emitir un certificado comodín para un dominio o subdominio

Para autorizar a una CA a emitir un certificado comodín para un dominio o subdominio, cree un registro que tenga el mismo nombre que el dominio o subdominio y especifique la siguiente configuración: Un certificado comodín se aplica al dominio o subdominio y a todos sus subdominios.

- marcadores – `0`
- etiqueta – `issuewild`
- valor: el código de la CA a la que autoriza a emitir un certificado para un dominio o subdominio y sus subdominios

Por ejemplo, suponga que desea autorizar a `ca.example.net` a emitir un certificado comodín para `example.com`, que se aplica a `example.com` y todos sus subdominios. Puede crear un registro de CAA para `example.com` con la siguiente configuración:

```
0 issuewild "ca.example.net"
```

Cuando quiera autorizar a una CA a emitir un certificado comodín para un dominio o subdominio, cree un registro que tenga el mismo nombre que el dominio o subdominio y especifique la siguiente configuración: Un certificado comodín se aplica al dominio o subdominio y a todos sus subdominios.

Evitar que cualquier CA emita un certificado para un dominio o un subdominio

Para evitar que cualquier CA emita un certificado para un dominio o un subdominio, cree un registro que tenga el mismo nombre que el dominio o subdominio y especifique la siguiente configuración:

- marcadores – `0`
- etiqueta – `issue`
- valor – `""`

Por ejemplo, suponga que no desea que ninguna CA emita un certificado para `example.com`. Puede crear un registro de CAA para `example.com` con la siguiente configuración:

```
0 issue ""
```

Si no quiere que ninguna CA emita un certificado para `example.com` o sus subdominios, debe crear un registro de CAA para `example.com` con la siguiente configuración:

```
0 issuewild ""
```

Note

Si crea un registro de CAA para `example.com` y especifica los dos valores siguientes, una CA que utiliza el valor `ca.example.net` puede emitir el certificado para `example.com`:

```
0 issue ""  
0 issue "ca.example.net"
```

Solicitar que cualquier CA se ponga en contacto con usted si la CA recibe una solicitud de certificado no válida

Si desea que toda CA que reciba una solicitud no válida de certificado se ponga en contacto con usted, especifique la siguiente configuración:

- marcadores – `0`
- etiqueta – `iodef`
- valor: la dirección URL o la dirección de correo electrónico a la que desea que la CA envíe una notificación si recibe una solicitud no válida de certificado. Use el formato aplicable:

```
"mailto:email-address"
```

```
"http://URL"
```

```
"https://URL"
```

Por ejemplo, si desea que toda CA que recibe una solicitud no válida de certificado envíe un correo electrónico a `admin@example.com`, cree un registro de CAA con la siguiente configuración:

```
0 iodef "mailto:admin@example.com"
```

Uso de otra opción compatible con la CA

Si la CA admite una característica que no está definida en RFC para registros de CAA, especifique la siguiente configuración:

- **marcadores:** 128 (este valor impide que la CA emita un certificado si esta no es compatible con la característica especificada).
- **etiqueta:** la etiqueta que la CA tiene permiso para utilizar
- **valor:** el valor que corresponde al valor de etiqueta

Por ejemplo, suponga que la CA admita el envío de un mensaje de texto si recibe una solicitud de certificado no válida. (No somos conscientes de que haya ninguna CA que admita esta opción). La configuración del registro podría ser la siguiente:

```
128 exampletag "15555551212"
```

Ejemplos

Ejemplo de la consola de Route

```
0 issue "ca.example.net"  
0 iodef "mailto:admin@example.com"
```

Ejemplo de la API de Route

```
<ResourceRecord>  
  <Value>0 issue "ca.example.net"</Value>
```

```
<Value>0 iodef "mailto:admin@example.com"</Value>
</ResourceRecord>
```

Tipo de registro CNAME

Un registro CNAME asigna consultas DNS para el nombre del registro actual, como `acme.example.com`, a otro dominio (`example.com` o `example.net`) o subdominio (`acme.example.com` o `zenith.example.org`).

Important

El protocolo DNS no permite crear un registro CNAME para el nodo superior de un espacio de nombres de DNS, también conocido como ápex de zona. Por ejemplo, si registra el nombre DNS `example.com`, el vértice de zona será `example.com`. No puede crear un registro CNAME para `ejemplo.com`, pero puede crear registros CNAME para `www.ejemplo.com`, `nuevoproducto.ejemplo.com`, etcétera.

Además, si crea un registro CNAME para un subdominio, no puede crear ningún otro registro para ese subdominio. Por ejemplo, si crea un CNAME para `www.example.com`, no puede crear ningún otro registro para el que el valor del campo Name (Nombre) sea `www.example.com`.

Amazon Route 53 admite también registros de alias, que le permiten dirigir las consultas a recursos de AWS seleccionados, como distribuciones de CloudFront y buckets de Amazon S3. Los alias son similares en cierto sentido al tipo de registro CNAME; sin embargo, puede crear un alias para el ápex de zona. Para obtener más información, consulte [Elección entre registros de alias y sin alias](#).

Ejemplo de la consola de Route

```
hostname.example.com
```

Ejemplo de la API de Route

```
<Value>hostname.example.com</Value>
```

Tipo de registro DS

Un registro de firmante de delegación (DS) hace referencia a una clave de zona para una zona de subdominio delegada. Puede crear un registro DS cuando establezca una cadena de confianza al

configurar la firma DNSSEC. Para obtener más información sobre la configuración de DNSSEC en Route 53, consulte [Configuración de la firma de DNSSEC en Amazon Route 53](#).

Los tres primeros valores son números decimales que representan la etiqueta de clave, el algoritmo y el tipo de resumen. El cuarto valor es el resumen de la clave de zona. Para obtener más información acerca del formato del registro DS, consulte [RFC 4034](#).

Ejemplo de la consola de Route

```
123 4 5 1234567890abcdef1234567890absdef
```

Ejemplo de la API de Route

```
<Value>123 4 5 1234567890abcdef1234567890absdef</Value>
```

Tipo de registro HTTPS

Un registro de recursos HTTPS es un tipo de registro de DNS de Service Binding (SVCB) que proporciona información de configuración adicional, lo que permite al cliente conectarse de forma fácil y segura a un servicio con un protocolo HTTP. La información de configuración se proporciona en parámetros que permiten la conexión en una consulta de DNS, en lugar de necesitar varias consultas de DNS.

El formato de los registros de recursos HTTPS es:

```
SvcPriority TargetName SvcParams(optional)
```

Los siguientes parámetros están descritos en la [sección 9.1 del RFC 9460](#).

SvcPriority

Un número entero que representa la prioridad. La prioridad 0 significa modo de alias y, por lo general, está destinada para la creación de alias en el vértice de zona. Este valor es un número entero del 0 al 32 767 para Route 53, de los cuales 1 a 32 767 son registros de modo de servicio. Cuanto menor sea la prioridad, mayor será la preferencia.

TargetName

El nombre de dominio del alias objetivo (para el modo de alias) o del punto de conexión alternativo (para ServiceMode).

SvcParams (opcional)

Una lista separada por espacios en blanco en la que cada parámetro consta de un par clave=valor o de una clave independiente. En caso de haber más de un valor, se presentan en forma de lista separada por comas. A continuación se detallan los SvcParams definidos:

- `1:alpn`: identificadores de protocolos de negociación de protocolo de capa de aplicación. El valor predeterminado es HTTP/1.1, h2 es HTTP/2 sobre TLS y h3 es HTTP/3 (HTTP sobre el protocolo QUIC).
- `2:no-default-alpn`: el valor predeterminado no es compatible y debe proporcionar un parámetro alpn.
- `3:port`: el punto de conexión alternativo o el puerto en el que se puede acceder al servicio.
- `4:ipv4hint`: sugerencias de la dirección IPv4.
- `5:ech`: saludo del cliente cifrado.
- `6:ipv6hint`: sugerencias de la dirección IPv6.
- `7:dohpath`: plantilla de DNS sobre HTTPS.
- `8:ohhttp`: el servicio opera con un objetivo Oblivious HTTP.

Ejemplo de la consola de Amazon Route 53 para el modo de alias

```
0 example.com
```

Ejemplo de la consola de Amazon Route 53 para el modo de servicio

```
16 example.com alpn="h2,h3" port=808
```

Ejemplo de la API de Amazon Route 53 para el modo de alias

```
<Value>0 example.com</Value>
```

Ejemplo de la API de Amazon Route 53 para el modo de servicio

```
<Value>16 example.com alpn="h2,h3" port=808</Value>
```

Para obtener más información, consulte el [RFC 9460, Service Binding and Parameter Specification via the DNS \(SVCB and HTTPS Resource Records\)](#).

 Note

Route 53 no admite el formato de presentación arbitrario de clave desconocida keyNNNNN.

Tipo de registro MX

Un registro MX especifica los nombres de los servidores de correo y, si tiene dos o más servidores de este tipo, el orden de prioridad. Cada valor de un registro MX contiene dos valores, que son la prioridad y el nombre del dominio.

Prioridad

Un número entero que representa la prioridad de un servidor de correo electrónico. Si especifica un único servidor, la prioridad puede ser cualquier número entero comprendido entre 0 y 65535. Si especifica varios servidores, el valor que especifique para la prioridad indica el primer servidor de correo electrónico al que se debe enviar el correo electrónico, el segundo y así sucesivamente. El servidor que tenga el valor más bajo para la prioridad será el prioritario. Por ejemplo, si tiene dos servidores de correo electrónico y especifica los valores de 10 y 20 para la prioridad, el correo electrónico siempre se envía al servidor con la prioridad de 10 a menos que no esté disponible. Si especifica los valores de 10 y 10, el correo electrónico se redirige a los dos servidores aproximadamente en partes iguales.

Nombre del dominio

El nombre del dominio del servidor de correo electrónico. Especifique el nombre (por ejemplo, mail.example.com) de un registro A o AAAA. En [RFC 2181, Clarifications to the DNS Specification](#), la sección 10.3 prohíbe especificar el nombre de un registro CNAME para valor del nombre de dominio. (Cuando la especificación RFC habla de “alias”, se refiere a un registro CNAME, no a un registro de alias de Route 53).

Ejemplo de la consola de Amazon Route 53

```
10 mail.example.com
```

Ejemplo de la API de Route

```
<Value>10 mail.example.com</Value>
```

Tipo de registro NAPTR

Un NAPTR (Name Authority Pointer, Señalizador de autoridad de asignación de nombres) es un tipo de registro que usan las aplicaciones DDDS (Dynamic Delegation Discovery System, Sistema de detección de delegación dinámica) para convertir un valor en otro o para sustituir un valor por otro. Por ejemplo, un uso habitual es convertir los números de teléfono en URI de SIP.

El elemento `Value` de un registro NAPTR consta de seis valores separados por espacios:

Order

Cuando especifica más de un registro, el orden en que desea que la aplicación DDDS evalúe los registros. Valores válidos: 0 - 65535.

Preference

Cuando especifica dos o más registros que tienen el mismo valor de Order, el orden preferido en el que desea que se evalúen esos registros. Por ejemplo, si dos registros tienen un valor de Order de 1, la primera aplicación DDDS evalúa el registro que tiene el valor de Preference menor. Valores válidos: 0 - 65535.

Indicadores

Un valor específico de las aplicaciones DDDS. Los valores definidos actualmente en [RFC 3404](#) son las letras mayúsculas y minúsculas "A", "P", "S" y "U" y la cadena vacía, "". Incluya los valores de Flags entre comillas.

Servicio

Un valor específico de las aplicaciones DDDS. Incluya los valores de Service entre comillas.

Para obtener más información, consulte los RFC correspondientes:

- Aplicación DDDS URI: <https://tools.ietf.org/html/rfc3404#section-4.4>
- Aplicación DDDS S-NAPTR: <https://tools.ietf.org/html/rfc3958#section-6.5>
- Aplicación DDDS U-NAPTR: <https://tools.ietf.org/html/rfc4848#section-4.5>

Regexp

Una expresión regular que la aplicación DDDS utiliza para convertir un valor de entrada en un valor de salida. Por ejemplo, un sistema de telefonía por IP podría utilizar una expresión regular para convertir un número de teléfono introducido por un usuario en un URI de SIP.

Incluya los valores de Regexp entre comillas. Especifique un valor para Regexp o un valor para Replacement, pero no ambos.

Las expresiones regulares pueden incluir cualquiera de los siguientes caracteres ASCII imprimibles:

- a-z
- 0-9
- - (guion)
- (espacio)
- ! # \$ % & ' () * + , - / : ; < = > ? @ [] ^ _ ` { | } ~ .
- " (comillas). Para incluir un carácter de comillas literal en una cadena, incluya un carácter \ delante: \".
- \ (barra diagonal invertida). Para incluir una barra diagonal invertida en una cadena, incluya un carácter \ delante: \\.

Especifique el resto de los valores, como los nombres de dominio internacionalizados, en formato octal.

Para ver la sintaxis de Regexp, consulte [RFC 3402, sección 3.2, Substitution Expression Syntax](#)

Reemplazo

El nombre de dominio completo (FQDN) del siguiente nombre de dominio para el que desea que la aplicación DDDS envíe una consulta DNS. La aplicación DDDS sustituye el valor de entrada por el valor que especifique para Replacement, si especifica alguno. Especifique un valor para Regexp o un valor para Replacement, pero no ambos. Si especifica un valor para Regexp, especifique un punto (.) para Replacement (Sustituto).

El nombre de dominio puede incluir a-z, 0-9 y - (guion).

Para obtener más información acerca de las aplicaciones DDDS y los registros NAPTR, consulte los siguientes RFC:

- [RFC 3401](#)
- [RFC 3402](#)
- [RFC 3403](#)

- [RFC 3404](#)

Ejemplo de la consola de Amazon Route 53

```
100 50 "u" "E2U+sip" "!^(\\"+441632960083)$!sip:\\1@example.com!" .
100 51 "u" "E2U+h323" "!^(\\"+441632960083$!h323:operator@example.com!" .
100 52 "u" "E2U+email:mailto" "!^.*$!mailto:info@example.com!" .
```

Ejemplo de la API de Route

```
<ResourceRecord>
  <Value>100 50 "u" "E2U+sip" "!^(\\"+441632960083)$!sip:\\1@example.com!" .</Value>
  <Value>100 51 "u" "E2U+h323" "!^(\\"+441632960083$!h323:operator@example.com!" .</
Value>
  <Value>100 52 "u" "E2U+email:mailto" "!^.*$!mailto:info@example.com!" .</Value>
</ResourceRecord>
```

Tipo de registro NS

Un registro NS identifica los servidores de nombres de la zona alojada. Tenga en cuenta lo siguiente:

- El uso más común de un registro NS es controlar cómo se enruta el tráfico de Internet para un dominio. Para utilizar los registros de una zona alojada para enrutar el tráfico de un dominio, actualice la configuración del registro de dominio para utilizar los cuatro servidores de nombres en el registro NS predeterminado. (Este es el registro NS que tiene el mismo nombre que la zona alojada).
- Puede crear una zona alojada independiente para un subdominio (acme.example.com) y utilizarla para enrutar el tráfico de Internet del subdominio y de los subdominios de este (subdominio.acme.example.com). Para establecer esta configuración, conocida como “delegar la responsabilidad de un subdominio a una zona alojada”, se crea otro registro NS en la zona alojada para el dominio raíz (example.com). Para obtener más información, consulte [Direccionamiento del tráfico de subdominios](#).
- También se utilizan registros NS para configurar servidores de nombres de etiqueta blanca. Para obtener más información, consulte [Configuración de servidores de nombres de etiqueta blanca](#).
- Otro uso de un registro NS es para las zonas alojadas privadas, cuando se crea una regla de delegación para delegar la autoridad sobre un subdominio al solucionador en las instalaciones. Debe crear este registro NS antes de crear una regla de delegación. Para obtener más

información, consulte [Cómo reenvían los puntos de conexión de Resolver las consultas de DNS de su red a su red VPCs](#).

Para obtener más información acerca de los registros NS, consulte [Registros SOA y NS que crea Amazon Route 53 para una zona alojada pública](#).

Ejemplo de la consola de Amazon Route 53

```
ns-1.example.com
```

Ejemplo de la API de Route

```
<Value>ns-1.example.com</Value>
```

Tipo de registro PTR

Un registro PTR asigna una dirección IP al nombre de dominio correspondiente.

Ejemplo de la consola de Amazon Route 53

```
hostname.example.com
```

Ejemplo de la API de Route

```
<Value>hostname.example.com</Value>
```

Tipo de registro SOA

Un registro de inicio de autoridad (SOA) proporciona información sobre un dominio y la zona alojada de Amazon Route 53 correspondiente. Para obtener información sobre los campos de un registro SOA, consulte [Registros SOA y NS que crea Amazon Route 53 para una zona alojada pública](#).

Ejemplo de la consola de Route

```
ns-2048.awsdns-64.net hostmaster.awsdns.com 1 1 1 1 60
```

Ejemplo de la API de Route

```
<Value>ns-2048.awsdns-64.net hostmaster.awsdns.com 1 1 1 1 60</Value>
```

Tipo de registro SPF

Los registros SPF se usaban anteriormente para verificar la identidad del remitente de mensajes de correo electrónico. Sin embargo, ya no se recomienda crear registros para los que el tipo de registro sea SPF. El RFC 7208, Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, versión 1, se ha actualizado y ahora indica, "...su existencia y el mecanismo definido en [RFC4408] han producido algunos problemas de interoperabilidad. Por lo tanto, su uso ya no es adecuado para SPF, versión 1; las implementaciones no van a utilizarlo". En RFC 7208, consulte la sección 14.1, [The SPF DNS Record Type](#).

En lugar de un registro SPF, le recomendamos que cree un registro TXT que contenga el valor correspondiente. Para obtener más información sobre valores válidos, consulte el artículo de Wikipedia [Sender Policy Framework](#).

Ejemplo de la consola de Amazon Route 53

```
"v=spf1 ip4:192.168.0.1/16 -all"
```

Ejemplo de la API de Route

```
<Value>"v=spf1 ip4:192.168.0.1/16 -all"</Value>
```

Tipo de registro SRV

El elemento `Value` de un registro SRV consta de cuatro valores separados por espacios. Los tres primeros valores son números decimales que representan la prioridad, el peso y el puerto. El cuarto valor es un nombre de dominio. Los registros SRV se utilizan para acceder a servicios, como un servicio de correo electrónico o comunicaciones. Para obtener información sobre el formato del registro SRV, consulte la documentación del servicio al que desee conectarse.

Ejemplo de la consola de Amazon Route 53

```
10 5 80 hostname.example.com
```

Ejemplo de la API de Route

```
<Value>10 5 80 hostname.example.com</Value>
```

Registro de tipo SSHFP

Los registros de huellas dactilares de Secure Shell (SSHFP) identifican las claves SSH asociadas al nombre de dominio. Los registros de SSHFP deben estar protegidos con DNSSEC para poder establecer una cadena de confianza. Para obtener más información acerca de DNSSEC, consulte [Configuración de la firma de DNSSEC en Amazon Route 53](#).

El formato de los registros de recursos SSHFP es:

[Key Algorithm] [Hash Type] Fingerprint

Los siguientes parámetros están definidos en el [RFC 4255](#).

Algoritmo clave

Tipo de algoritmo:

- 0: reservado y no utilizado.
- 1: RSA: el algoritmo Rivest-Shamir-Adleman es uno de los primeros criptosistemas de clave pública y todavía se utiliza para la transmisión segura de datos.
- 2: DSA: el algoritmo de firma digital es un estándar federal de procesamiento de información para firmas digitales. El DSA se basa en la exponenciación modular y en los modelos matemáticos de logaritmos discretos.
- 3: ECDSA: el algoritmo de firma digital de curva elíptica es una variante del DSA que utiliza criptografía de curva elíptica.
- 4: Ed25519: el algoritmo Ed25519 es el esquema de firma EdDSA que utiliza SHA-512 (SHA-2) y Curve25519.
- 6: Ed448: Ed448 es el esquema de firma EdDSA que utiliza SHAKE256 y Curve448.

Tipo de hash

Algoritmo utilizado para crear el hash de clave pública:

- 0: reservado y no utilizado.
- 1: SHA-1
- 2: SHA-256

Huella digital

Representación hexadecimal del hash.

Ejemplo de la consola de Amazon Route 53

```
1 1 09F6A01D2175742B257C6B98B7C72C44C4040683
```

Ejemplo de la API de Route

```
<Value>1 1 09F6A01D2175742B257C6B98B7C72C44C4040683</Value>
```

Para obtener más información, consulte el [RFC 4255: Using DNS to Securely Publish Secure Shell \(SSH\) Key Fingerprints](#).

Registro de tipo SVCB

Los registros SVCB se utilizan para proporcionar información de configuración para acceder a los puntos de conexión de los servicios. El SVCB es un registro de DNS genérico y se puede utilizar para negociar los parámetros de una variedad de protocolos de aplicación.

El formato de los registros de recursos SVCB es:

`SvcPriority TargetName SvcParams(optional)`

Los siguientes parámetros están descritos en la [sección 2.3 del RFC 9460](#).

SvcPriority

Un número entero que representa la prioridad. La prioridad 0 significa modo de alias y, por lo general, está destinada para la creación de alias en el vértice de zona. Cuanto menor sea la prioridad, mayor será la preferencia.

TargetName

El nombre de dominio del alias objetivo (para el modo de alias) o del punto de conexión alternativo (para ServiceMode).

SvcParams (opcional)

Una lista separada por espacios en blanco en la que cada parámetro consta de un par clave=valor o de una clave independiente. En caso de haber más de un valor, se presentan en forma de lista separada por comas. Este valor es un número entero del 0 al 32 767 para Route 53, de los cuales 1 a 32 767 son registros de modo de servicio. A continuación se detallan los SvcParams definidos:

- `1:alpn`: identificadores de protocolos de negociación de protocolo de capa de aplicación. El valor predeterminado es HTTP/1.1, h2 es HTTP/2 sobre TLS y h3 es HTTP/3 (HTTP sobre el protocolo QUIC).
- `2:no-default-alpn`: el valor predeterminado no es compatible y debe proporcionar un parámetro `alpn`.
- `3:port`: el puerto del punto de conexión alternativo desde el que se puede acceder al servicio.
- `4:ipv4hint`: sugerencias de la dirección IPv4.
- `5:ech`: saludo del cliente cifrado.
- `6:ipv6hint`: sugerencias de la dirección IPv6.
- `7:dohpath`: plantilla de DNS sobre HTTPS.
- `8:ohhttp`: el servicio opera con un objetivo Oblivious HTTP.

Ejemplo de la consola de Amazon Route 53 para el modo de alias

```
0 example.com
```

Ejemplo de la consola de Amazon Route 53 para el modo de servicio

```
16 example.com alpn="h2,h3" port=808
```

Ejemplo de la API de Amazon Route 53 para el modo de alias

```
<Value>0 example.com</Value>
```

Ejemplo de la API de Amazon Route 53 para el modo de servicio

```
<Value>16 example.com alpn="h2,h3" port=808</Value>
```

Para obtener más información, consulte el [RFC 9460, Service Binding and Parameter Specification via the DNS \(SVCB and HTTPS Resource Records\)](#).

Note

Route 53 no admite el formato de presentación arbitrario de clave desconocida `keyNNNNN`.

Registro de tipo TLSA

Los registros TLSA se utilizan para usar la autenticación de entidades con nombre basada en DNS (DANE). Los registros TLSA asocian un certificado o clave pública a un punto de conexión de seguridad de la capa de transporte (TLS), y los clientes pueden validar el certificado o la clave pública mediante un registro TLSA firmado con DNSSEC.

Solo se puede confiar en los registros de TLSA si DNSSEC está habilitado en su dominio. Para obtener más información acerca de DNSSEC, consulte [Configuración de la firma de DNSSEC en Amazon Route 53](#).

El formato de los registros de recursos TLSA es:

[Certificate usage] Selector [Matching type] [Certificate association data]

Los siguientes parámetros están especificados en la [sección 3 del RFC 6698](#).

Uso de certificados

Especifica la asociación proporcionada que se utilizará para que coincida con el certificado presentado en el establecimiento de comunicación TLS:

- 0: Restricción de CA: el certificado o la clave pública debe encontrarse en alguna de las rutas de certificación de la infraestructura de la clave pública (PKIX) del certificado de entidad final proporcionado por el servidor en TLS. Esta restricción limita qué CA pueden utilizarse para emitir certificados para un servicio especificado.
- 1: Restricción de certificado de servicio: especifica un certificado de entidad final (o la clave pública) que debe coincidir con el certificado de entidad final proporcionado por el servidor en TLS. Esta certificación limita qué certificado de entidad final puede usar un servicio específico en un host.
- 2: Una afirmación de anclaje de veracidad: especifica un certificado (o la clave pública) que debe usarse como el «anclaje de veracidad» al validar el certificado de entidad final emitido por el servidor en TLS. Permite al administrador de dominios especificar un anclaje de veracidad.
- 3: Certificación emitida por dominio: especifica un certificado (o la clave pública) que debe coincidir con el certificado de entidad final proporcionado por el servidor en TLS. Esta certificación permite al administrador de dominios emitir certificados para un dominio sin la participación de una CA externa. No es necesario que este certificado pase la validación de PKIX.

Selector

Especifica qué parte del certificado presentado por el servidor en el establecimiento de comunicación coincide con el valor de la asociación:

- 0: Debe coincidir todo el certificado.
- 1: La clave pública del sujeto, o la estructura binaria codificada en DER, debe coincidir.

Tipo coincidente

Especifica la presentación (según lo determinado por el campo Selector) de la coincidencia del certificado:

- 0: Coincidencia exacta del contenido.
- 1: hash SHA-256.
- 2: hash SHA-512.

Datos de asociación del certificado

Los datos que se van a comparar en función de la configuración de los demás campos.

Ejemplo de la consola de Amazon Route 53

```
0 0 1 d2abde240d7cd3ee6b4b28c54df034b97983a1d16e8a410e4561cb106618e971
```

Ejemplo de la API de Route

```
<Value>0 0 1 d2abde240d7cd3ee6b4b28c54df034b97983a1d16e8a410e4561cb106618e971</Value>
```

Para obtener más información, consulte el [RFC 6698, The DNS-Based Authentication of Named Entities \(DANE\) Transport Layer Security \(TLS\) Protocol: TLSA](#).

Tipo de registro TXT

Un registro TXT contiene una o varias cadenas que se encierran entre comillas dobles ("). Al utilizar la [política de direccionamiento](#) sencilla, incluye todos los valores de un dominio (example.com) o subdominio (www.example.com) en el mismo registro TXT.

Temas

- [Introducción de valores de registro TXT](#)
- [Caracteres especiales en un valor de registro TXT](#)

- [Mayúsculas y minúsculas en un valor de registro TXT](#)
- [Ejemplos](#)

Introducción de valores de registro TXT

Una única cadena puede incluir hasta 255 caracteres, entre las que se incluyen las siguientes:

- a-z
- A-Z
- 0-9
- Espacio
- - (guion)
- !"#\$%&'()*+,-/:;<=>?@[\\]^_`{|}~.

Si necesita introducir un valor de más de 255 caracteres, divida el valor en cadenas de 255 caracteres o menos e incluya cada cadena entre comillas dobles ("). En la consola, enumere todas las cadenas de la misma línea:

```
"String 1" "String 2" "String 3"
```

En la API, incluya todas las cadenas en el mismo elemento Value:

```
<Value>"String 1" "String 2" "String 3"</Value>
```

La longitud máxima de un valor en un registro TXT es de 4000 caracteres.

Para ingresar más de un valor TXT, ingrese un valor por fila.

Caracteres especiales en un valor de registro TXT

Si su registro TXT contiene alguno de los siguientes caracteres, debe especificar los caracteres usando códigos de escape en el formato *\código octal de tres dígitos*:

- Caracteres de 000 a 040 octales (de 0 a 32 decimales, de 0x20 a 0x00 hexadecimales)
- Caracteres de 177 a 377 octales (de 127 a 255 decimales, de 0x7F a 0xFF hexadecimales)

Por ejemplo, si el valor de su registro TXT es "exämple.com", especifique "ex\344mple.com".

Para consultar un mapeo entre caracteres ASCII y códigos octales, busque en Internet «códigos octales ASCII». Una referencia útil es [ASCII Code - The extended ASCII table](#).

Para incluir una comilla (") en una cadena, ponga una contrabarra (\) delante de esta: \".

Mayúsculas y minúsculas en un valor de registro TXT

Se distingue entre mayúsculas y minúsculas, por lo que "Ab" y "aB" son valores diferentes.

Ejemplos

Ejemplo de la consola de Amazon Route 53

Ponga cada valor en una línea independiente:

```
"This string includes \"quotation marks\"."
"The last character in this string is an accented e specified in octal format: \351"
"v=spf1 ip4:192.168.0.1/16 -all"
```

Ejemplo de la API de Route

Ponga cada valor en un elemento Value independiente:

```
<Value>"This string includes \"quotation marks\"."</Value>
<Value>"The last character in this string is an accented e specified in octal format:
\351"</Value>
<Value>"v=spf1 ip4:192.168.0.1/16 -all"</Value>
```

Creación de registros con la consola de Amazon Route 53

En el siguiente procedimiento se explica cómo crear registros mediante la consola de Amazon Route 53. Para obtener información sobre cómo crear registros mediante la API de Route 53, consulte la referencia [ChangeResourceRecordSets](#) de la API de Amazon Route 53.

Note

Para crear registros para las configuraciones de enrutamiento complejas, también puede utilizar el editor visual de Flujo de tráfico y guardar la configuración como una política de tráfico. A continuación, puede asociar la política de tráfico con uno o varios nombres de dominio (como example.com) o nombres de subdominio (como www.example.com) en la misma zona alojada o en varias zonas hospedadas. Además, puede revertir las

actualizaciones si la nueva configuración no tiene el desempeño previsto. Para obtener más información, consulte [Uso de flujo de tráfico para dirigir el tráfico DNS](#).

Creación de un registro mediante la consola de Route 53

1. Si no está creando un registro de alias, vaya al paso 2.

Vaya también al paso 2 si va a crear un registro de alias que dirija el tráfico de DNS a un AWS recurso que no sea un balanceador de cargas ELB u otro registro de Route 53.

Si va a crear un registro de alias que redirija el tráfico a un balanceador de carga de ELB, y si creó la zona alojada y el balanceador de carga con cuentas diferentes, siga el procedimiento [Obtener el nombre del DNS para un balanceador de carga ELB](#) para obtener el nombre DNS del balanceador de carga.

2. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/route53/>
3. En el panel de navegación, elija Zonas alojadas.
4. Si ya tiene una zona alojada para su dominio, vaya al paso 5. De lo contrario, realice el procedimiento correspondiente para crear una zona alojada:
 - Para enrutar el tráfico de Internet a sus recursos, como los buckets de Amazon S3 o EC2 las instancias de Amazon, consulte [Crear una zona alojada pública](#).
 - Para direccionar el tráfico de la VPC, consulte [Creación de una zona alojada privada](#).
5. En la página Zonas alojadas, elija el nombre de la zona alojada en la que desea crear registros.
6. Elija Crear registro.
7. Elija y defina la política de direccionamiento y los valores aplicables. Para obtener más información, consulte el tema para el tipo de registro que desea crear:
 - [Valores comunes a todas las políticas de enrutamiento](#)
 - [Valores comunes de registros de alias para todas las políticas de enrutamiento](#)
 - [Valores específicos para registros simples](#)
 - [Valores específicos para registros de alias simples](#)
 - [Valores específicos de registros de conmutación por error](#)
 - [Valores específicos de registros de alias de conmutación por error](#)
 - [Valores específicos de registros de geolocalización](#)

- [Valores específicos de registros de alias de geolocalización](#)
- [Valores específicos de registros de geoproximidad](#)
- [Valores específicos de registros de alias de geoproximidad](#)
- [Valores específicos de registros de latencia](#)
- [Valores específicos de registros de alias de latencia](#)
- [Valores específicos para los registros basados en IP](#)
- [Valores específicos para los registros de alias basados en IP](#)
- [Valores específicos de registros de respuesta de varios valores](#)
- [Valores específicos de registros ponderados](#)
- [Valores específicos de registros de alias ponderados](#)

8. Elija Crear registros.

 Note

Los nuevos registros tardan un tiempo en propagarse a los servidores DNS de Route 53. Actualmente, la única forma de comprobar que los cambios se han propagado es mediante la acción de la [GetChangeAPI](#). Por lo general, los cambios se propagan a todos los servidores de Route 53 en un plazo de 60 segundos.

9. Si está creando varios registros, repita los pasos 7 a 8.

Obtener el nombre del DNS para un balanceador de carga ELB

1. Inicie sesión Consola de administración de AWS con la AWS cuenta que se utilizó para crear el Classic, Application o Network Load Balancer para el que desee crear un registro de alias.
2. Abra la EC2 consola de Amazon en <https://console.aws.amazon.com/ec2/>.
3. En el panel de navegación, seleccione Equilibradores de carga.
4. En la lista de balanceadores de carga, seleccione uno para el que desea crear un registro de alias.
5. En la pestaña Description, obtenga el valor de DNS name.
6. Si desea crear registros de alias para otros balanceadores de carga de ELB, repita los pasos 4 y 5.
7. Cierre sesión en Consola de administración de AWS.

8. Consola de administración de AWS Vuelva a iniciar sesión con la AWS cuenta que utilizó para crear la zona alojada de Route 53.
9. Volver al paso 3 del procedimiento [Creación de registros con la consola de Amazon Route 53](#).

Permisos del conjunto de registros de recursos

Los permisos del conjunto de registros de recursos utilizan las condiciones de la política de administración de identidad y acceso (IAM) para poder establecer permisos detallados para las acciones en la consola de Route 53 o para usar la [ChangeResourceRecordSets](#) API.

Un conjunto de registros de recursos se define como varios registros de recursos con el mismo nombre y tipo (y clase, aunque para la mayoría de los propósitos la clase siempre es IN o Internet), pero con datos diferentes. Por ejemplo, si elige el enrutamiento de geolocalización, puede tener varios registros A o AAAA que apunten a diferentes puntos de conexión para el mismo dominio. Todos estos registros A o AAAA se combinan para formar un conjunto de registros de recursos. Para obtener más información acerca de la terminología de DNS, consulte [RFC 7719](#).

Con las condiciones de la política de IAM

`route53:ChangeResourceRecordSetsNormalizedRecordNames`, `route53:ChangeResourceRecordSetsActions`, puede conceder derechos administrativos detallados a otros AWS usuarios de cualquier otra AWS cuenta. Esto le permite conceder permisos a alguien para:

- Un único conjunto de registros de recursos.
- Todos los conjuntos de registros de recursos de un tipo de registro de DNS específico.
- Conjuntos de registros de recursos en los que los nombres contienen una cadena específica.
- Realice alguna o todas las `CREATE` | `UPSERT` | `DELETE` acciones cuando utilice la [ChangeResourceRecordSets](#) API o la consola de Route 53.

También puede crear permisos de acceso que combinen cualquiera de las condiciones de la política de Route 53. Por ejemplo, puede conceder permisos a alguien para modificar los datos del registro A de `marketing-example.com`, pero no permitir que ese usuario elimine ningún registro.

Para obtener más información sobre los permisos de conjuntos de registros de recursos y ejemplos de cómo utilizarlos, consulte [Uso de condiciones de las políticas de IAM para control de acceso preciso](#).

Para obtener información sobre cómo autenticar a AWS los usuarios, consulte [Autenticación con identidades](#) y aprenda a controlar el acceso a los recursos de Route 53, consulte [Control de acceso](#).

Valores que hay que especificar al crear o editar los registros de Amazon Route 53.

Cuando crea registros con la consola de Amazon Route 53, los valores que especifique dependen de la política de enrutamiento que desee usar y de si va a crear registros de alias, que enrutan el tráfico a AWS los recursos.

Registros de alias que redirigen el tráfico a determinados AWS recursos para los que se especifica el recurso de destino (por ejemplo, ELB, CloudFront distribución, bucket de Amazon S3). Si lo desea, también puede asociar las comprobaciones de estado y configurar la evaluación del estado de destino. En los siguientes temas, se proporciona información detallada sobre los valores necesarios para cada política de enrutamiento y tipo de registro, lo que lo ayuda a configurar los registros de Route 53 de manera eficaz.

Temas

- [Valores comunes a todas las políticas de enrutamiento](#)
- [Valores comunes de registros de alias para todas las políticas de enrutamiento](#)
- [Valores específicos para registros simples](#)
- [Valores específicos para registros de alias simples](#)
- [Valores específicos de registros de conmutación por error](#)
- [Valores específicos de registros de alias de conmutación por error](#)
- [Valores específicos de registros de geolocalización](#)
- [Valores específicos de registros de alias de geolocalización](#)
- [Valores específicos de registros de geoproximidad](#)
- [Valores específicos de registros de alias de geoproximidad](#)
- [Valores específicos de registros de latencia](#)
- [Valores específicos de registros de alias de latencia](#)
- [Valores específicos para los registros basados en IP](#)
- [Valores específicos para los registros de alias basados en IP](#)
- [Valores específicos de registros de respuesta de varios valores](#)
- [Valores específicos de registros ponderados](#)

- [Valores específicos de registros de alias ponderados](#)

Valores comunes a todas las políticas de enrutamiento

Estos son los valores comunes que puede especificar al crear o editar registros de Amazon Route 53. Todas las políticas de enrutamiento utilizan estos valores.

Temas

- [Nombre del registro](#)
- [Valor/ruta de destino del tráfico](#)
- [TTL \(segundos\)](#)

Nombre del registro

Escriba el nombre del dominio o subdominio para el que desea dirigir el tráfico. El valor predeterminado es el nombre de la zona alojada.

Note

Si crea un registro con el mismo nombre que el de la zona alojada, no escriba un valor (por ejemplo, un símbolo @) en el campo Name (Nombre).

Registros CNAME

Si crea un registro con el valor CNAME (CNAME) para Record type (Tipo de registro), el nombre del registro no puede ser el mismo que el de la zona alojada.

Caracteres especiales

Para obtener información sobre cómo especificar caracteres distintos de a-z, 0-9 y - (guion), y cómo especificar nombres de dominio internacionalizados, consulte [Formato de nombres de dominio DNS](#).

Caracteres comodín

Puede usar un asterisco (*) en el nombre. DNS trata el asterisco como comodín o como el carácter ASCII (42) *, en función de dónde aparece en el nombre. Para obtener más información, consulte [Uso de un asterisco \(*\) en nombres de zonas alojadas y registros](#).

 Important

No puede usar el carácter comodín * para los conjuntos de registros de recursos con el tipo NS.

Valor/ruta de destino del tráfico

Elija IP address or another value depending on the record type (Dirección IP u otro valor en función del tipo de registro). Ingrese un valor que sea adecuado para el valor de Record type (Tipo de registro). Para todos los tipos excepto CNAME, puede escribir más de un valor. Escriba cada valor en una línea independiente.

A: dirección IPv4

Una dirección IP con el formato IPv4, por ejemplo, 192.0.2.235.

AAAA: dirección IPv6

Una dirección IP con el formato IPv6, por ejemplo, 2001:0db8:85a3:0:0:8a2e:0370:7334.

CAA: autorización de la entidad de certificación

Tres valores separados por espacios que controlan qué autoridades de certificación están autorizadas para emitir certificados (normales o comodín) para el dominio o subdominio especificado en Record name (Nombre del registro). Puede utilizar los registros CAA para especificar lo siguiente:

- Qué autoridades de certificación (CA, Certificate Authority) pueden emitir certificados SSL/TLS, si procede.
- La dirección de correo electrónico o URL con la que hay que contactar en caso de que una CA emita un certificado para el dominio o subdominio.

CNAME: nombre canónico

El nombre de dominio completo (por ejemplo, `www.example.com`) que desea que Route 53 devuelva como respuesta a las consultas de DNS para este registro. El punto final es opcional; Route 53 presupone que el nombre de dominio es completo. Esto significa que Route 53 trata a `www.example.com` (sin punto final) y `www.example.com.` (con punto final) de idéntica forma.

MX: intercambio de correo

Una prioridad y un nombre de dominio que especifican un servidor de correo, por ejemplo, 10 mailserver.ejemplo.com. El punto final se trata como opcional.

NAPTR: señalizador de autoridad de asignación de nombres

Seis valores separados por espacios que las aplicaciones DDDS (Dynamic Delegation Discovery System, Sistema de detección de delegación dinámica) usan para convertir un valor en otro o para reemplazar un valor por otro. Para obtener más información, consulte [Tipo de registro NAPTR](#).

PTR: puntero

El nombre de dominio que desea que Route 53 devuelva.

NS: servidor de nombres

El nombre de dominio de un servidor de nombres, por ejemplo, ns1.ejemplo.com.

Note

Puede especificar un registro NS con solo una política de enrutamiento simple.

SPF: marco de políticas de remitente

Un registro SPF envuelto en comillas, por ejemplo, "v=spf1 ip4:192.168.0.1/16-all". El uso de registros SPF no es recomendado. Para obtener más información, consulte [Tipos de registros de DNS admitidos](#).

SRV: localizador de servicios

Un registro SRV. Los registros SRV se utilizan para acceder a servicios, como un servicio de correo electrónico o comunicaciones. Para obtener información sobre el formato del registro SRV, consulte la documentación del servicio al que desee conectarse. El punto final se trata como opcional.

El formato de un registro SRV es el siguiente:

[prioridad] [ponderación] [puerto] [nombre del host de servidor]

Por ejemplo:

1 10 5269 xmpp-servidor.ejemplo.com.

TXT: texto

Un registro de texto. Entrecomille el texto; por ejemplo, "Entrada de texto de ejemplo".

TTL (segundos)

El tiempo, en segundos, en que desea que los solucionadores recursivos de DNS almacenen en caché información sobre este registro. Si especifica un valor más largo (por ejemplo, 172 800 segundos o dos días), se reduce el número de llamadas que los solucionadores recursivos de DNS deben realizar a Route 53 para obtener la información más reciente de este registro. Esto reduce la latencia y la factura del servicio Route 53. Para obtener más información, consulte [Cómo dirige Amazon Route 53 el tráfico de su dominio](#).

Sin embargo, si especifica un valor más largo para TTL, los cambios realizados en el registro (por ejemplo, una nueva dirección IP) tardarán más tiempo en surtir efecto, ya que los solucionadores recursivos usan los valores de la memoria caché durante periodos más largos antes de solicitar la información más reciente a Route 53. Si está cambiando la configuración de un dominio o subdominio que ya está en uso, le recomendamos que inicialmente especifique un valor más corto, por ejemplo, 300 segundos y que aumente el valor después de confirmar que la configuración nueva es correcta.

Si asocia este registro a una comprobación de estado, es recomendable que especifique un TTL de 60 segundos o menos para que los clientes respondan rápidamente a los cambios de estado.

Valores comunes de registros de alias para todas las políticas de enrutamiento

Estos son los valores de alias comunes que puede especificar al crear o editar registros de Amazon Route 53. Todas las políticas de enrutamiento utilizan estos valores.

Temas

- [Nombre del registro](#)
- [Valor/ruta de destino del tráfico](#)

Nombre del registro

Escriba el nombre del dominio o subdominio para el que desea dirigir el tráfico. El valor predeterminado es el nombre de la zona alojada.

Note

Si crea un registro con el mismo nombre que el de la zona alojada, no escriba un valor (por ejemplo, un símbolo @) en el campo Name (Nombre).

Registros CNAME

Si crea un registro con el valor CNAME para Type (Tipo), el nombre del registro no puede ser el mismo que el de la zona alojada.

Alias para distribuciones de CloudFront y buckets de Amazon S3

El valor que especifique depende parcialmente del recurso de AWS al que dirige el tráfico:

- Distribución de CloudFront: la distribución debe incluir un nombre de dominio alternativo que coincida con el nombre del registro. Por ejemplo, si el nombre del registro es `acme.ejemplo.com`, la distribución de CloudFront debe incluir `acme.ejemplo.com` como uno de los nombres de dominio alternativos. Para obtener más información, consulte [Uso de nombres de dominio alternativos \(CNAME\)](#) en la Guía para desarrolladores de Amazon CloudFront.
- Bucket de Amazon S3: el nombre del registro debe coincidir con el nombre del bucket de Amazon S3. Por ejemplo, si el nombre del bucket es `acme.ejemplo.com`, el nombre de este registro también debe ser `acme.ejemplo.com`.

Además, debe configurar el bucket para el hospedaje de sitio web. Para obtener más información, consulte [Configuración de un bucket para un alojamiento de sitio web](#) en la Guía del usuario de Amazon Simple Storage Service.

Caracteres especiales

Para obtener información sobre cómo especificar caracteres distintos de a-z, 0-9 y - (guion), y cómo especificar nombres de dominio internacionalizados, consulte [Formato de nombres de dominio DNS](#).

Caracteres comodín

Puede usar un asterisco (*) en el nombre. DNS trata el asterisco como comodín o como el carácter ASCII (42) *, en función de dónde aparece en el nombre. Para obtener más información, consulte [Uso de un asterisco \(*\) en nombres de zonas alojadas y registros](#).

Valor/ruta de destino del tráfico

El valor que elija en la lista o que escriba en el campo depende del recurso de AWS al que esté intentando redirigir el tráfico.

Para obtener más información sobre cómo configurar Route 53 para dirigir tráfico a recursos específicos de AWS, consulte [Enrutar el tráfico de Internet a sus AWS recursos](#).

Important

Si utiliza la misma cuenta de AWS para crear la zona alojada y el recurso al que está dirigiendo el tráfico, y si el recurso no aparece en la lista Endpoint (Punto de conexión), verifique lo siguiente:

- Confirme que ha elegido un valor admitido para Record type (Tipo de registro). Los valores admitidos son específicos del recurso al que restá redirigiendo el tráfico. Por ejemplo, para dirigir el tráfico a un bucket de S3, debe elegir A — IPv4 address (A: dirección IPv4) para Record type (Tipo de registro).
- Confirme que la cuenta tiene los permisos de IAM necesarios para enumerar los recursos aplicables. Por ejemplo, para que las distribuciones de CloudFront aparezcan en la lista Punto de conexión, la cuenta debe tener permiso para realizar la siguiente acción: `cloudfront:ListDistributions`.

Para ver una política de IAM de ejemplo, consulte [Permisos necesarios para usar la consola de Amazon Route 53](#).

Si ha utilizado cuentas de AWS distintas para crear la zona alojada y el recurso, la lista Endpoint (Punto de conexión) no muestra el recurso. Consulte la siguiente documentación sobre su tipo de recurso para determinar el valor que debe ingresar en Punto de conexión.

API regionales personalizadas y API optimizadas para bordes de API Gateway

En el caso de las API regionales personalizadas y las API optimizadas para bordes de API Gateway, realice una de las siguientes operaciones:

- Si ha usado la misma cuenta para crear la zona alojada de Route 53 y la API: elija Punto de conexión y luego una API de la lista. Si tiene muchas API, puede escribir los primeros caracteres del punto de conexión de la API para filtrar la lista.

Note

El nombre del registro debe coincidir con un nombre de dominio personalizado para su API, como api.ejemplo.com.

- Si ha usado cuentas diferentes para crear la zona alojada de Route 53 y la API: ingrese el punto de conexión de API de la API, como, por ejemplo, api.example.com.

Si ha usado una cuenta de AWS para crear la zona alojada actual y otra cuenta para crear una API, esta última no aparecerá en la lista Endpoints (Puntos de enlace) en API Gateway APIs (API de API Gateway).

Si ha usado una cuenta para crear la zona alojada actual, y una o varias cuentas diferentes para crear todas las API, en la lista Endpoints (Puntos de conexión) se muestra No targets available (Sin destinos disponibles) en API Gateway APIs (API de API Gateway). Para obtener más información, consulte [Enrutamiento del tráfico a una API de Amazon API Gateway mediante su nombre de dominio](#).

Distribuciones de CloudFront

En el caso de las distribuciones de CloudFront, realice una de las siguientes operaciones:

- Si ha usado la misma cuenta para crear la zona alojada de Route 53 y la distribución de CloudFront: elija Punto de conexión y luego una distribución de la lista. Si tiene muchas distribuciones, puede escribir los primeros caracteres del nombre de dominio de la distribución para filtrar la lista.

Si la distribución no aparece en la lista, tenga en cuenta lo siguiente:

- El nombre de este registro debe coincidir con un nombre de dominio alternativo de la distribución.
- Si acaba de agregar un nombre de dominio alternativo a la distribución, es posible que la propagación de los cambios a todas las ubicaciones de borde de CloudFront tarde unos 15 minutos. Hasta que no se hayan propagado los cambios, Route 53 no puede saber nada del nuevo nombre de dominio alternativo.
- Si ha usado cuentas diferentes para crear la zona alojada de Route 53 y la distribución: ingrese el nombre de dominio de CloudFront de la distribución, como, por ejemplo, d111111abcdef8.cloudfront.net.

Si ha usado una cuenta de AWS para crear la zona alojada actual y otra para crear una distribución, esta última no aparecerá en la lista Endpoints (Puntos de enlace).

Si ha usado una cuenta para crear la zona alojada actual, y una o varias cuentas diferentes para crear todas las distribuciones, en la lista Endpoints (Puntos de enlace) se muestra No targets available (Sin destinos disponibles) en CloudFront distributions (Distribuciones de CloudFront).

 Important

No dirija consultas a una distribución de CloudFront que no se haya propagado a todas las ubicaciones de borde. De lo contrario, los usuarios no podrán obtener acceso al contenido aplicable.

La distribución de CloudFront debe incluir un nombre de dominio alternativo que coincida con el nombre del registro. Por ejemplo, si el nombre del registro es acme.ejemplo.com, la distribución de CloudFront debe incluir acme.ejemplo.com como uno de los nombres de dominio alternativos. Para obtener más información, consulte [Uso de nombres de dominio alternativos \(CNAME\)](#) en la Guía para desarrolladores de Amazon CloudFront.

Si se habilita IPv6 para la distribución, cree dos registros, uno con el valor A — IPv4 address (A: dirección IPv4) para Record type (Tipo de registro) y otro con el valor AAAA — IPv6 address (AAAA: dirección IPv6). Para obtener más información, consulte [Enrutar el tráfico a una CloudFront distribución de Amazon mediante tu nombre de dominio](#).

Servicio de App Runner

En el caso del servicio de App Runner, realice una de las siguientes operaciones:

- Si ha usado la misma cuenta para crear la zona alojada de Route 53 y el servicio de App Runner: seleccione la Región de AWS y, a continuación, seleccione el nombre de dominio del entorno al que quiere enrutar el tráfico de la lista.
- Si ha usado cuentas diferentes para crear la zona alojada de Route 53 y App Runner: ingrese el nombre de dominio personalizado. Para obtener más información, consulte [Managing custom domain names for App Runner](#) (Administración de nombres de dominio personalizados para App Runner).

Si ha usado una cuenta de AWS para crear la zona alojada actual y otra para crear un servicio de App Runner, este último no aparecerá en la lista Puntos de conexión.

Para obtener más información, consulte [Configuración de Amazon Route 53 para dirigir el tráfico a un servicio de App Runner](#).

Entornos de Elastic Beanstalk que tienen subdominios regionalizados

Si el nombre de dominio del entorno de Elastic Beanstalk incluye la región en la que implementó el entorno, puede crear un registro de alias que dirija el tráfico al entorno. Por ejemplo, el nombre de dominio `my-environment.us-west-2.elasticbeanstalk.com` es un nombre de dominio regionalizado.

Important

Para los entornos creados antes de principios de 2016, el nombre de dominio no incluye la región. Para dirigir el tráfico a estos entornos, debe crear un registro CNAME en lugar de un registro de alias. Tenga en cuenta que no puede crear un registro CNAME para el nombre de dominio raíz. Por ejemplo, si su nombre de dominio es `example.com`, puede crear un registro que dirija el tráfico de `acme.example.com` a su entorno de Elastic Beanstalk, pero no puede crear un registro que dirija el tráfico de `example.com` a su entorno de Elastic Beanstalk.

Para los entornos de Elastic Beanstalk que tienen subdominios regionalizados, realice una de las siguientes acciones:

- Si ha usado la misma cuenta para crear la zona alojada de Route 53 y el entorno de Elastic Beanstalk: elija Punto de conexión y luego un entorno de la lista. Si tiene muchos entornos, puede escribir los primeros caracteres del atributo CNAME del entorno para filtrar la lista.
- Si ha usado cuentas diferentes para crear la zona alojada de Route 53 y el entorno de Elastic Beanstalk: ingrese el atributo CNAME del entorno de Elastic Beanstalk.

Para obtener más información, consulte [Enrutar el tráfico a un AWS Elastic Beanstalk entorno](#).

Balanceadores de carga de ELB

Para los equilibradores de carga de ELB, realice una de las siguientes operaciones:

- Si ha usado la misma cuenta para crear la zona alojada de Route 53 y el equilibrador de carga: elija Punto de conexión y luego un equilibrador de carga de la lista. Si tiene muchos equilibradores de carga, puede escribir los primeros caracteres del nombre DNS para filtrar la lista.
- Si ha usado cuentas distintas para crear la zona alojada de Route 53 y el balanceador de carga: ingrese el valor que obtuvo en el procedimiento [Obtener el nombre del DNS para un balanceador de carga ELB](#).

Si ha usado una cuenta de AWS para crear la zona alojada actual y otra cuenta para crear un balanceador de carga, este último no aparecerá en la lista Endpoints (Puntos de enlace).

Si ha usado una cuenta para crear la zona alojada actual, y una o varias cuentas diferentes para crear todos los equilibradores de carga, en la lista Endpoints (Puntos de conexión) se muestra No targets available (Sin destinos disponibles) en Elastic Load Balancers (Elastic Load Balancers).

La consola agrega dualstack. para la aplicación y el balanceador de carga clásico desde una cuenta diferente. Cuando un cliente, como un navegador web, solicita la dirección IP del nombre de dominio (ejemplo.com) o nombre de subdominio (www.ejemplo.com), puede solicitar una dirección IPv4 (registro A), una dirección IPv6 (registro AAAA) o tanto las direcciones IPv4 como IPv6 (en solicitudes independientes). La designación dualstack. permite a Route 53 responder con la dirección IP adecuada del balanceador de carga en función del formato de dirección IP que ha solicitado el cliente.

Para obtener más información, consulte [Direccionamiento del tráfico a un balanceador de carga ELB](#).

AWSAceleradores de Global Accelerator

Para los aceleradores de AWS Global Accelerator, ingrese el nombre de DNS del acelerador. Puede ingresar el nombre de DNS de un acelerador que creó utilizando la cuenta actual de AWS o mediante una cuenta de AWS distinta.

Buckets de Amazon S3

Para los buckets de Amazon S3 configurados en los puntos de enlace de sitio web, realice una de las siguientes acciones:

- Si ha usado la misma cuenta para crear la zona alojada de Route 53 y el bucket de Amazon S3: elija Punto de conexión y luego un bucket de la lista. Si tiene muchos buckets, puede escribir los primeros caracteres del nombre DNS para filtrar la lista.

El valor de Punto de conexión cambia al punto de conexión del sitio web de Amazon S3 para el bucket.

- Si ha usado cuentas diferentes para crear la zona alojada de Route 53 y el bucket de Amazon S3: ingrese el nombre de la región en la que ha creado el bucket de S3. Use el valor que aparece en la columna punto de conexión del sitio web de la tabla [Punto de conexión de sitio web de Amazon S3](#) en Referencia general de Amazon Web Services.

Si ha usado cuentas de AWS distintas de la actual para crear los buckets de Amazon S3, el bucket no figurará en la lista Endpoints (Puntos de enlace).

Debe configurar el bucket para el hospedaje de sitio web. Para obtener más información, consulte [Configuración de un bucket para un alojamiento de sitio web](#) en la Guía del usuario de Amazon Simple Storage Service.

El nombre del registro debe coincidir con el nombre del bucket de Amazon S3. Por ejemplo, si el nombre del bucket de Amazon S3 es `acme.example.com`, el nombre de este registro también debe ser `acme.example.com`.

En un grupo de registros de alias ponderados, alias de latencia, alias de conmutación por error o alias de geolocalización, solo puede crear un registro que dirija las consultas a un bucket de Amazon S3, porque el nombre del registro debe coincidir con el nombre del bucket, y los nombres de bucket deben ser únicos de forma global.

Amazon OpenSearch Service

En el caso del servicio de OpenSearch, realice una de las siguientes operaciones:

- Dominio personalizado de OpenSearch Service: el nombre del registro debe coincidir con el dominio personalizado. Por ejemplo, si el nombre del dominio personalizado es test.example.com, el nombre de este registro también debe ser test.example.com.
- Si ha usado la misma cuenta para crear la zona alojada de Route 53 y el dominio de OpenSearch Service: seleccione la Región de AWS y luego el nombre del dominio.
- Si ha usado cuentas diferentes para crear la zona alojada de Route 53 y el dominio de OpenSearch Service: ingrese el nombre de dominio personalizado. Para obtener más información, consulte [Create a custom endpoint](#).

Si ha usado una cuenta de AWS para crear la zona alojada actual y otra cuenta para crear un dominio de OpenSearch Service, este último no aparecerá en la lista Puntos de conexión.

Si ha usado una cuenta para crear la zona alojada actual y una o varias cuentas diferentes para crear todos los dominios de OpenSearch Service, en la lista Puntos de conexión se muestra Sin destinos disponibles en OpenSearch Service.

Para obtener más información, consulte [Configuración de Amazon Route 53 para enrutar el tráfico a un punto final OpenSearch de dominio de Amazon Service](#).

Puntos de enlace de interfaz de Amazon VPC

Para los puntos de interfaz de Amazon VPC, realice una de las siguientes opciones:

- Si ha usado la misma cuenta para crear la zona alojada de Route 53 y el punto de conexión de interfaz: elija Punto de conexión y luego un punto de conexión de interfaz de la lista. Si tiene muchos puntos de conexión de interfaz, puede escribir los primeros caracteres del nombre de host DNS para filtrar la lista.
- Si ha usado cuentas diferentes para crear la zona alojada de Route 53 y el punto de conexión de interfaz: ingrese el nombre de host DNS para el punto de conexión de interfaz, como, por ejemplo, vpce-123456789abcdef01-example-us-east-1a.elasticloadbalancing.us-east-1.vpce.amazonaws.com.

Si ha usado una cuenta de AWS para crear la zona alojada actual y otra cuenta para crear un punto de conexión de interfaz, este último no aparecerá en la lista Punto de conexión en Punto de conexión de VPC.

Si ha usado una cuenta para crear la zona alojada actual, y una o varias cuentas diferentes para crear todos los puntos de conexión de interfaz, en la lista Endpoint (Punto de conexión) se muestra No targets available (Sin destinos disponibles) en VPC Endpoints (Puntos de conexión de VPC).

Para obtener más información, consulte [Enrutamiento del tráfico a un punto de conexión de interfaz de Amazon Virtual Private Cloud mediante el nombre de dominio](#).

Registros de esta zona alojada

Para los registros de esta zona alojada, elija Endpoint (Punto de conexión) y luego el registro correspondiente. Si tiene muchos registros, puede escribir los primeros caracteres del nombre para filtrar la lista.

Si en la zona alojada se incluyen solo los registros de NS y SOA predeterminados, en la lista Endpoints (Puntos de conexión) se muestra No targets available (Sin destinos disponibles).

Note

Si va a crear un registro de alias con el mismo nombre que la zona alojada (lo que se conoce como ápex de zona), no podrá elegir un registro en el que el valor de Record type (Tipo de registro) sea CNAME (CNAME). Esto se debe a que el registro de alias debe tener el mismo tipo que el registro al que está redirigiendo el tráfico y no es posible crear un registro CNAME para el ápex de zona (ni siquiera para un registro de alias).

Valores específicos para registros simples

Cuando se crean registros simples, hay que especificar los siguientes valores.

Temas

- [Política de direccionamiento](#)
- [Nombre del registro](#)
- [Valor/ruta de destino del tráfico](#)
- [Tipo de registro](#)
- [TTL \(segundos\)](#)

Política de direccionamiento

Elija Direccionamiento simple.

Nombre del registro

Escriba el nombre del dominio o subdominio para el que desea dirigir el tráfico. El valor predeterminado es el nombre de la zona alojada.

Note

Si crea un registro con el mismo nombre que el de la zona alojada, no escriba un valor (por ejemplo, un símbolo @) en el campo Name (Nombre).

Para obtener más información acerca de nombres de registro, consulte [Nombre del registro](#).

Valor/ruta de destino del tráfico

Elija IP address or another value depending on the record type (Dirección IP u otro valor en función del tipo de registro). Ingrese un valor que sea adecuado para el valor de Record type (Tipo de registro). Para todos los tipos excepto CNAME, puede escribir más de un valor. Escriba cada valor en una línea independiente.

Puede dirigir el tráfico a, o especificar los siguientes valores:

- A: dirección IPv

- AAAA: dirección IPv
- CAA: autorización de la entidad de certificación
- CNAME: nombre canónico
- MX: intercambio de correo
- NAPTR: señalizador de autoridad de asignación de nombres
- NS: servidor de nombres

El nombre de dominio de un servidor de nombres, por ejemplo, ns1.ejemplo.com.

 Note

Puede especificar un registro NS con solo una política de enrutamiento simple.

- PTR: puntero
- SPF: marco de políticas de remitente
- SRV: localizador de servicios
- TXT: texto

Para más información acerca de los valores anteriores, consulte los [valores comunes del valor/ruta de destino del tráfico](#).

Tipo de registro

El tipo de registro de DNS. Para obtener más información, consulte [Tipos de registros de DNS admitidos](#).

Seleccione el valor de Record type (Tipo de registro) en función de cómo desee que Route 53 responda a las consultas de DNS.

TTL (segundos)

El tiempo, en segundos, en que desea que los solucionadores recursivos de DNS almacenen en caché información sobre este registro. Si especifica un valor más largo (por ejemplo, 172 800 segundos o dos días), se reduce el número de llamadas que los solucionadores recursivos de DNS deben realizar a Route 53 para obtener la información más reciente de este registro. Esto reduce la latencia y la factura del servicio Route 53. Para obtener más información, consulte [Cómo dirige Amazon Route 53 el tráfico de su dominio](#).

Sin embargo, si especifica un valor más largo para TTL, los cambios realizados en el registro (por ejemplo, una nueva dirección IP) tardarán más tiempo en surtir efecto, ya que los solucionadores recursivos usan los valores de la memoria caché durante periodos más largos antes de solicitar la información más reciente a Route 53. Si está cambiando la configuración de un dominio o subdominio que ya está en uso, le recomendamos que inicialmente especifique un valor más corto, por ejemplo, 300 segundos y que aumente el valor después de confirmar que la configuración nueva es correcta.

Valores específicos para registros de alias simples

Cuando se crean registros de alias, hay que especificar los siguientes valores. Para obtener más información, consulte [Elección entre registros de alias y sin alias](#).

Note

Si utiliza Route 53 en AWS GovCloud (US) Region, esta característica tiene algunas restricciones. Para obtener más información, consulte la [Página de Amazon Route 53](#) en la Guía del usuario de AWS GovCloud (US).

Temas

- [Política de direccionamiento](#)
- [Nombre del registro](#)
- [Valor/ruta de destino del tráfico](#)
- [Tipo de registro](#)
- [Evaluate target health](#)

Política de direccionamiento

Elija Direccionamiento simple.

Nombre del registro

Escriba el nombre del dominio o subdominio para el que desea dirigir el tráfico. El valor predeterminado es el nombre de la zona alojada.

Note

Si crea un registro con el mismo nombre que el de la zona alojada, no escriba un valor (por ejemplo, un símbolo @) en el campo Name (Nombre).

Para obtener más información acerca de nombres de registro, consulte [Nombre del registro](#).

Valor/ruta de destino del tráfico

El valor que elija en la lista o que escriba en el campo depende del recurso de AWS al que esté intentando redirigir el tráfico.

Para obtener información sobre los recursos de AWS con los que puede tratar, consulte los [valores comunes de los registros de alias de valor/ruta de destino del tráfico](#).

Para obtener más información sobre cómo configurar Route 53 para dirigir tráfico a recursos específicos de AWS, consulte [Enrutar el tráfico de Internet a sus AWS recursos](#).

Tipo de registro

El tipo de registro de DNS. Para obtener más información, consulte [Tipos de registros de DNS admitidos](#).

Seleccione el valor aplicable en función del recurso de AWS al que dirige el tráfico:

API regionales personalizadas o API optimizadas para bordes de API Gateway

Seleccione A — IPv4 address (A: dirección IPv4).

Puntos de conexión de interfaz de Amazon VPC

Seleccione A — IPv4 address (A: dirección IPv4).

Distribución de CloudFront

Seleccione A — IPv4 address (A: dirección IPv4).

Si se habilita IPv6 para la distribución cree dos registros, uno con el valor A — IPv4 address (A: dirección IPv4) para Type (Tipo) y otro con el valor AAAA — IPv6 address (AAAA: dirección IPv6).

Servicio de App Runner

Seleccione A — IPv4 address (A: dirección IPv4).

Entorno de Elastic Beanstalk con subdominios regionalizados

Seleccione A — IPv4 address (A: dirección IPv4).

Balanceador de carga de ELB

Seleccione A — IPv4 address (A: dirección IPv4) o AAAA — IPv6 address (AAAA: dirección IPv6).

Bucket de Amazon S3

Seleccione A — IPv4 address (A: dirección IPv4).

OpenSearch Service

Seleccione A — IPv4 address (A: dirección IPv4) o AAAA — IPv6 address (AAAA: dirección IPv6).

Otro registro en esta zona alojada

Seleccione el tipo de registro para el que va a crear el alias. Se admiten todos los tipos, excepto NS y SOA.

Note

Si va a crear un registro de alias con el mismo nombre que la zona alojada (lo que se conoce como ápex de zona), no podrá dirigir el tráfico a un registro en el que el valor de Type (Tipo) sea CNAME. Esto se debe a que el registro de alias debe tener el mismo tipo que el registro al que está redirigiendo el tráfico y no es posible crear un registro CNAME para el ápex de zona (ni siquiera para un registro de alias).

Evaluate target health

Cuando el valor de Política de enrutamiento es Sencillo, puede elegir los valores No o el valor predeterminado Sí, porque Evaluar estado del destino no tiene ningún efecto para el enrutamiento Sencillo. Si solo tiene un registro que tiene un nombre y un tipo determinados, Route 53 responde las consultas de DNS utilizando los valores de ese registro, independientemente de si el recurso está o no en buen estado.

Para otras políticas de enrutamiento, Evaluar estado del destino determina si Route 53 comprueba el estado del recurso al que hace referencia el registro de alias:

- Servicios en los que Evaluar estado del destino proporciona beneficios operativos: en el caso de los equilibradores de carga (ELB) y los entornos de AWS Elastic Beanstalk con equilibradores de carga, establecer la opción Evaluar estado del destino en Sí permite a Route 53 enrutar el tráfico y alejarlo de los recursos insalubres.
- Servicios de alta disponibilidad: en el caso de servicios como los buckets de Amazon S3, los puntos de conexión de la interfaz de VPC, Amazon API Gateway, AWS Global Accelerator, Amazon OpenSearch Service y Amazon VPC Lattice, Evaluar estado del destino no ofrece ningún

beneficio operativo porque estos servicios están diseñados para una alta disponibilidad. Para situaciones de conmutación por error con estos servicios, utilice en su lugar las [comprobaciones de estado de Route 53](#).

Para obtener información detallada sobre cómo funciona Evaluar estado del destino con diferentes servicios de AWS, consulte la documentación de [EvaluateTargetHealth](#) en la referencia de la API.

Valores específicos de registros de conmutación por error

Cuando se crean registros de conmutación por error, hay que especificar los siguientes valores.

Note

Para obtener información sobre cómo crear registros de conmutación por error en una zona alojada privada, consulte [Configuración de la conmutación por error en una zona alojada privada](#).

Temas

- [Política de direccionamiento](#)
- [Nombre del registro](#)
- [Tipo de registro](#)
- [TTL \(segundos\)](#)
- [Valor/ruta de destino del tráfico](#)
- [Tipo de registro de conmutación por error](#)
- [Comprobación de estado](#)
- [ID de registro](#)

Política de direccionamiento

Elija Failover (Conmutación por error).

Nombre del registro

Escriba el nombre del dominio o subdominio para el que desea dirigir el tráfico. El valor predeterminado es el nombre de la zona alojada.

Note

Si crea un registro con el mismo nombre que el de la zona alojada, no ingrese un valor (por ejemplo, un símbolo @) en el campo Record name (Nombre del registro).

Escriba el mismo nombre para los dos registros del grupo de registros de conmutación por error.

Para obtener más información acerca de nombres de registro, consulte [Nombre del registro](#).

Tipo de registro

El tipo de registro de DNS. Para obtener más información, consulte [Tipos de registros de DNS admitidos](#).

Seleccione el mismo valor para los registros de conmutación por error principales y secundarios.

TTL (segundos)

El tiempo, en segundos, en que desea que los solucionadores recursivos de DNS almacenen en caché información sobre este registro. Si especifica un valor más largo (por ejemplo, 172 800 segundos o dos días), se reduce el número de llamadas que los solucionadores recursivos de DNS deben realizar a Route 53 para obtener la información más reciente de este registro. Esto reduce la latencia y la factura del servicio Route 53. Para obtener más información, consulte [Cómo dirige Amazon Route 53 el tráfico de su dominio](#).

Sin embargo, si especifica un valor más largo para TTL, los cambios realizados en el registro (por ejemplo, una nueva dirección IP) tardarán más tiempo en surtir efecto, ya que los solucionadores recursivos usan los valores de la memoria caché durante periodos más largos antes de solicitar la información más reciente a Route 53. Si está cambiando la configuración de un dominio o subdominio que ya está en uso, le recomendamos que inicialmente especifique un valor más corto, por ejemplo, 300 segundos y que aumente el valor después de confirmar que la configuración nueva es correcta.

Si asocia este registro a una comprobación de estado, es recomendable que especifique un TTL de 60 segundos o menos para que los clientes respondan rápidamente a los cambios de estado.

Valor/ruta de destino del tráfico

Elija IP address or another value depending on the record type (Dirección IP u otro valor en función del tipo de registro). Ingrese un valor que sea adecuado para el valor de Record type (Tipo de registro). Para todos los tipos excepto CNAME, puede escribir más de un valor. Escriba cada valor en una línea independiente.

Puede dirigir el tráfico a, o especificar los siguientes valores:

- A: dirección IPv
- AAAA: dirección IPv

- CAA: autorización de la entidad de certificación
- CNAME: nombre canónico
- MX: intercambio de correo
- NAPTR: señalizador de autoridad de asignación de nombres
- PTR: puntero
- SPF: marco de políticas de remitente
- SRV: localizador de servicios
- TXT: texto

Para más información acerca de los valores anteriores, consulte los [valores comunes del valor/ruta de destino del tráfico](#).

Tipo de registro de conmutación por error

Elija el valor aplicable para este registro. Para que la conmutación por error funcione correctamente, debe crear un registro de conmutación por error principal y uno secundario.

No puede crear registros sin conmutación por error que tengan los mismos valores de Record name (Nombre del registro) y Record type (Tipo de registro) que los registros de conmutación por error.

Comprobación de estado

Si desea que Route 53 verifique el estado de un punto de conexión dado y que solamente responda a las consultas de DNS utilizando este registro cuando el punto de conexión esté en buen estado, seleccione una comprobación de estado.

Route 53 no verifica el estado del punto de conexión especificado en el registro; por ejemplo, el punto de conexión que especifica la dirección IP en el campo Valor. Cuando se selecciona una comprobación de estado para un registro, Route 53 verifica el estado del punto de conexión especificado. Para obtener información sobre cómo Route 53 determina si un punto de conexión tiene un estado correcto, consulte [Cómo determina Amazon Route 53 si la comprobación de estado es correcta](#).

La asociación de una comprobación de estado a un conjunto de registros de recursos solo es útil cuando Route 53 elige entre dos o más registros para responder a una consulta de DNS y desea que Route 53 base la elección parcialmente en el estado de la comprobación de estado. Use las comprobaciones de estado solamente en las siguientes configuraciones:

- Va a comprobar el estado de todos los registros de un grupo de registros que tienen el mismo nombre, tipo y política de enrutamiento (como los registros de conmutación por error o ponderados) y especifica los identificadores de comprobación de estado de todos los registros. Si en la comprobación de estado de un registro se especifica un punto de conexión que no está en buen estado, Route 53 deja de responder a las consultas mediante el valor de dicho registro.
- Seleccione Yes (Sí) en Evaluate Target Health (Evaluar el estado del destino) para un registro de alias o los registros de un grupo de alias de conmutación por error, alias de geolocalización, alias de latencia, alias basado en IP o registro de alias ponderado. Si los registros de alias hacen referencia a registros que no son alias en la misma zona alojada, también debe especificar comprobaciones de estado para estos últimos. Si asocia una comprobación de estado a un registro de alias y también selecciona Yes para Evaluate Target Health, ambos deben evaluarse como verdaderos. Para obtener más información, consulte [¿Qué sucede cuando se asocia una comprobación de estado a un registro de alias?](#).

Si en las comprobaciones de estado se especifica el punto de conexión solo por nombre de dominio, es recomendable crear una comprobación de estado independiente para cada punto de conexión. Por ejemplo, cree una comprobación de estado para cada servidor HTTP que sirva contenido de `www.ejemplo.com`. Para el valor de Domain Name (Nombre de dominio), especifique el nombre de dominio del servidor (por ejemplo, `us-east-2-www.example.com`), no el nombre de los registros (`example.com`).

Important

En esta configuración, si crea una comprobación de estado cuyo valor de Domain name (Nombre de dominio) coincide con el nombre de los registros y a continuación la asocia con estos, los resultados de la comprobación serán impredecibles.

ID de registro

Escriba un valor que identifique de manera exclusiva los registros principal y secundario.

Valores específicos de registros de alias de conmutación por error

Cuando se crean registros de alias de conmutación por error, hay que especificar los siguientes valores.

Para obtener información, consulte los siguientes temas:

- Para obtener información sobre cómo crear registros de conmutación por error en una zona alojada privada, consulte [Configuración de la conmutación por error en una zona alojada privada](#).
- Para obtener información sobre los registros de alias, consulte [Elección entre registros de alias y sin alias](#).

Temas

- [Política de direccionamiento](#)
- [Nombre del registro](#)
- [Tipo de registro](#)
- [Valor/ruta de destino del tráfico](#)
- [Tipo de registro de conmutación por error](#)
- [Health check](#)
- [Evaluate target health](#)
- [ID de registro](#)

Política de direccionamiento

Elija Failover (Conmutación por error).

Nombre del registro

Escriba el nombre del dominio o subdominio para el que desea dirigir el tráfico. El valor predeterminado es el nombre de la zona alojada.

Note

Si crea un registro con el mismo nombre que el de la zona alojada, no ingrese un valor (por ejemplo, un símbolo @) en el campo Record name (Nombre del registro).

Escriba el mismo nombre para los dos registros del grupo de registros de conmutación por error.

Para obtener más información acerca de nombres de registro, consulte [Nombre del registro](#).

Tipo de registro

El tipo de registro de DNS. Para obtener más información, consulte [Tipos de registros de DNS admitidos](#).

Seleccione el valor aplicable en función del AWS recurso al que está enrutando el tráfico. Seleccione el mismo valor para los registros de conmutación por error principales y secundarios:

API regionales personalizadas o API optimizadas para bordes de API Gateway

Selecciona A — IPv4 dirección.

Puntos de conexión de interfaz de Amazon VPC

Seleccione A — IPv4 dirección.

CloudFront distribución

Seleccione A — IPv4 dirección.

Si IPv6 está habilitada para la distribución, cree dos registros, uno con el valor A (IPv4 dirección de tipo) y otro con el valor AAAA (IPv6 dirección).

Servicio de App Runner

Seleccione A — dirección IPv4

Entorno de Elastic Beanstalk con subdominios regionalizados

Seleccione A — IPv4 dirección

Balanceador de carga de ELB

Seleccione una IPv4 dirección O una dirección AAAA IPv6

Bucket de Amazon S3

Seleccione A — dirección IPv4

OpenSearch Servicio

Seleccione una IPv4 dirección o una dirección AAAA IPv6

Otro registro en esta zona alojada

Seleccione el tipo de registro para el que va a crear el alias. Se admiten todos los tipos, excepto NS y SOA.

Note

Si va a crear un registro de alias con el mismo nombre que la zona alojada (lo que se conoce como ápex de zona), no podrá dirigir el tráfico a un registro en el que el valor de Type (Tipo) sea CNAME. Esto se debe a que el registro de alias debe tener el mismo tipo que el registro al que está redirigiendo el tráfico y no es posible crear un registro CNAME para el ápex de zona (ni siquiera para un registro de alias).

Valor/ruta de destino del tráfico

El valor que elija de la lista o que escriba en el campo depende del AWS recurso al que dirija el tráfico.

Para obtener información sobre AWS los recursos a los que puede dirigirse, consulte [los valores comunes de los registros de alias a los que se dirige value/route el tráfico](#).

Para obtener más información sobre cómo configurar Route 53 para enrutar el tráfico a AWS recursos específicos, consulte [Enrutar el tráfico de Internet a sus AWS recursos](#).

Note

Cuando cree registros de conmutación por error principales y secundarios, tiene la opción de crear un registro de conmutación por error y un registro de alias de conmutación por error con los mismos valores para Name (Nombre) y Record type (Tipo de registro). Si combina registros de conmutación por error y de alias de conmutación por error, cualquiera de ellos puede ser el registro principal.

Tipo de registro de conmutación por error

Elija el valor aplicable para este registro. Para que la conmutación por error funcione correctamente, debe crear un registro de conmutación por error principal y uno secundario.

No puede crear registros sin conmutación por error que tengan los mismos valores de Record name (Nombre del registro) y Record type (Tipo de registro) que los registros de conmutación por error.

Health check

Si desea que Route 53 verifique el estado de un punto de conexión dado y que solamente responda a las consultas de DNS utilizando este registro cuando el punto de conexión esté en buen estado, seleccione una comprobación de estado.

Route 53 no verifica el estado del punto de conexión especificado en el registro; por ejemplo, el punto de conexión que especifica la dirección IP en el campo Valor. Cuando se selecciona una comprobación de estado para un registro, Route 53 verifica el estado del punto de conexión especificado. Para obtener información sobre cómo Route 53 determina si un punto de conexión tiene un estado correcto, consulte [Cómo determina Amazon Route 53 si la comprobación de estado es correcta](#).

La asociación de una comprobación de estado a un conjunto de registros de recursos solo es útil cuando Route 53 elige entre dos o más registros para responder a una consulta de DNS y desea que Route 53 base la elección parcialmente en el estado de la comprobación de estado. Use las comprobaciones de estado solamente en las siguientes configuraciones:

- Está comprobando el estado de todos los registros de un grupo de registros que tienen el mismo nombre, tipo y política de enrutamiento (como los registros de conmutación por error o ponderados) y especifica la comprobación IDs de estado de todos los registros. Si en la comprobación de estado de un registro se especifica un punto de conexión que no está en buen estado, Route 53 deja de responder a las consultas mediante el valor de dicho registro.
- Seleccione Yes (Sí) en Evaluate Target Health (Evaluar el estado del destino) para un registro de alias o los registros de un grupo de alias de conmutación por error, alias de geolocalización, alias de latencia, alias basado en IP o registro de alias ponderado. Si los registros de alias hacen referencia a registros que no son alias en la misma zona alojada, también debe especificar comprobaciones de estado para estos últimos. Si asocia una comprobación de estado a un registro de alias y también selecciona Yes para Evaluate Target Health, ambos deben evaluarse como verdaderos. Para obtener más información, consulte [¿Qué sucede cuando se asocia una comprobación de estado a un registro de alias?](#).

Si en las comprobaciones de estado se especifica el punto de conexión solo por nombre de dominio, es recomendable crear una comprobación de estado independiente para cada punto de conexión. Por ejemplo, cree una comprobación de estado para cada servidor HTTP que sirva contenido de

www.ejemplo.com. Para el valor de Domain Name (Nombre de dominio), especifique el nombre de dominio del servidor (por ejemplo, us-east-2-www.example.com), no el nombre de los registros (example.com).

 Important

En esta configuración, si crea una comprobación de estado cuyo valor de Domain name (Nombre de dominio) coincide con el nombre de los registros y a continuación la asocia con estos, los resultados de la comprobación serán impredecibles.

Evaluate target health

Seleccione Sí, si desea que Route 53 determine si debe responder a las consultas de DNS mediante este registro al verificar el estado del recurso especificado mediante Punto de conexión.

Tenga en cuenta lo siguiente:

API Gateway personalizado, regional APIs y optimizado para entornos periféricos APIs

No existen requisitos especiales para establecer Evaluar estado del destino en Sí cuando el punto de conexión es una API regional personalizada o una API optimizada para periféricas de API Gateway.

CloudFront distribuciones

No puede establecer Evaluar el estado del objetivo en Sí cuando el punto final es una CloudFront distribución.

Entornos de Elastic Beanstalk que tienen subdominios regionalizados

Si especifica un entorno de Elastic Beanstalk en Endpoint y el entorno contiene un balanceador de cargas ELB, ELB direcciona las consultas únicamente a las instancias de Amazon en EC2 buen estado que estén registradas en el balanceador de cargas. (Un entorno contiene automáticamente un balanceador de cargas ELB si incluye más de una EC2 instancia de Amazon). Si estableces Evaluar el estado del objetivo en Sí y ninguna EC2 instancia de Amazon está en buen estado o el propio balanceador de carga está en mal estado, Route 53 redirige las consultas a otros recursos disponibles que estén en buen estado, si los hay.

Si el entorno contiene una sola EC2 instancia de Amazon, no hay requisitos especiales.

Balanceadores de carga de ELB

El comportamiento de la comprobación de estado depende del tipo de balanceador de carga:

- Balanceadores de carga clásicos: si especificas un balanceador de carga clásico de ELB en Endpoint, ELB dirige las consultas solo a las instancias de EC2 Amazon en buen estado que estén registradas en el balanceador de cargas. Si estableces Evaluar el estado del objetivo en Sí y ninguna EC2 instancia está en buen estado o el propio balanceador de carga no está en buen estado, Route 53 redirige las consultas a otros recursos.
- Balanceadores de carga de red y aplicaciones: si especifica un balanceador de carga de red o aplicaciones ELB, y establece Evaluate Target health (Evaluar estado del destino) en Yes (Sí), Route 53 dirige consultas al balanceador de carga en función del estado de los grupos de destino asociados al balanceador de carga:
 - Para que se considere que una aplicación o un equilibrador de carga de red está en buen estado, cada grupo de destinos que contenga destinos debe tener al menos un destino en buen estado. Si cualquier grupo de destinos contiene únicamente destinos en mal estado, se considera que el balanceador de carga está en mal estado y Route 53 envía las consultas a otros recursos.
 - Un grupo de destinos que no tiene destinos registrados se considera que no está en buen estado.

Note

Al crear un balanceador de cargas, se configuran los ajustes para las comprobaciones de estado de ELB; no son comprobaciones de estado de Route 53, pero realizan una función similar. No cree comprobaciones de estado de Route 53 para las EC2 instancias que registre en un balanceador de cargas de ELB.

Buckets de S3

No existen requisitos especiales para establecer Evaluar estado del destino en Sí cuando el punto de conexión es un bucket de S3.

Puntos de enlace de interfaz de Amazon VPC

No existen requisitos especiales para establecer Evaluar estado del destino en Sí cuando el punto de conexión es uno de interfaz de Amazon VPC.

Otros registros de la misma zona alojada

Si el AWS recurso que especifica en Endpoint es un registro o un grupo de registros (por ejemplo, un grupo de registros ponderados) pero no es otro registro de alias, le recomendamos que asocie una comprobación de estado a todos los registros del punto final. Para obtener más información, consulte [¿Qué sucede cuando se omiten las comprobaciones de estado?](#).

ID de registro

Escriba un valor que identifique de manera exclusiva los registros principal y secundario.

Valores específicos de registros de geolocalización

Cuando se crean registros de geolocalización, hay que especificar los siguientes valores.

Temas

- [Política de direccionamiento](#)
- [Nombre del registro](#)
- [Tipo de registro](#)
- [TTL \(segundos\)](#)
- [Valor/ruta de destino del tráfico](#)
- [Ubicación](#)
- [Estados de Estados Unidos](#)
- [Comprobación de estado](#)
- [ID de registro](#)

Política de direccionamiento

Elija Geolocation (Geolocalización).

Nombre del registro

Escriba el nombre del dominio o subdominio para el que desea dirigir el tráfico. El valor predeterminado es el nombre de la zona alojada.

Note

Si crea un registro con el mismo nombre que el de la zona alojada, no escriba un valor (por ejemplo, un símbolo @) en el campo Name (Nombre).

Escriba el mismo nombre para todos los registros del grupo de registros de geolocalización.

Para obtener más información acerca de nombres de registro, consulte [Nombre del registro](#).

Tipo de registro

El tipo de registro de DNS. Para obtener más información, consulte [Tipos de registros de DNS admitidos](#).

Seleccione el mismo valor para todos los registros del grupo de registros de geolocalización.

TTL (segundos)

El tiempo, en segundos, en que desea que los solucionadores recursivos de DNS almacenen en caché información sobre este registro. Si especifica un valor más largo (por ejemplo, 172 800 segundos o dos días), se reduce el número de llamadas que los solucionadores recursivos de DNS deben realizar a Route 53 para obtener la información más reciente de este registro. Esto reduce la latencia y la factura del servicio Route 53. Para obtener más información, consulte [Cómo dirige Amazon Route 53 el tráfico de su dominio](#).

Sin embargo, si especifica un valor más largo para TTL, los cambios realizados en el registro (por ejemplo, una nueva dirección IP) tardarán más tiempo en surtir efecto, ya que los solucionadores recursivos usan los valores de la memoria caché durante periodos más largos antes de solicitar la información más reciente a Route 53. Si está cambiando la configuración de un dominio o subdominio que ya está en uso, le recomendamos que inicialmente especifique un valor más corto, por ejemplo, 300 segundos y que aumente el valor después de confirmar que la configuración nueva es correcta.

Si asocia este registro a una comprobación de estado, es recomendable que especifique un TTL de 60 segundos o menos para que los clientes respondan rápidamente a los cambios de estado.

Valor/ruta de destino del tráfico

Elija IP address or another value depending on the record type (Dirección IP u otro valor en función del tipo de registro). Ingrese un valor que sea adecuado para el valor de Record type (Tipo de registro). Para todos los tipos excepto CNAME, puede escribir más de un valor. Escriba cada valor en una línea independiente.

Puede dirigir el tráfico a, o especificar los siguientes valores:

- A: dirección IPv
- AAAA: dirección IPv
- CAA: autorización de la entidad de certificación
- CNAME: nombre canónico
- MX: intercambio de correo
- NAPTR: señalizador de autoridad de asignación de nombres
- PTR: puntero

- SPF: marco de políticas de remitente
- SRV: localizador de servicios
- TXT: texto

Para más información acerca de los valores anteriores, consulte los [valores comunes de valor/ruta de destino del tráfico](#).

Ubicación

Cuando configure Route 53 para que responda a las consultas de DNS según la ubicación de origen de estas, seleccione el continente o el país para el que quiere que Route 53 responda con la configuración de este registro. Si quiere que Route 53 responda a las consultas de DNS para estados individuales de Estados Unidos, seleccione United States (Estados Unidos) de la lista Location (Ubicación) y luego el estado en el grupo Sublocation (Sublocalización).

Para una zona alojada privada, seleccione el continente, el país o la subdivisión más cercana a la Región de AWS en que se encuentra su recurso. Por ejemplo, si el recurso se encuentra en us-east-1, puede especificar Norteamérica, Estados Unidos o Virginia.

Important

Es recomendable crear un registro de geolocalización con el valor Default (Predeterminada) para Location (Ubicación). Esto cubre las ubicaciones geográficas para las que no se hayan creado registros y las direcciones IP para las que Route 53 no puede identificar la ubicación.

No puede crear registros sin geolocalización que tengan los mismos valores de Record name (Nombre del registro) y Record type (Tipo de registro) que los registros de geolocalización.

Para obtener más información, consulte [Enrutado de geolocalización](#).

Estos son los países que Amazon Route 53 asocia con cada continente. Los códigos de país son de ISO 3166. Para obtener más información, consulte el artículo de Wikipedia [ISO 3166-1 alpha-2](#):

África (AF)

AO, BF, BI, BJ, BW, CD, CF, CG, CI, CM, CV, DJ, DZ, EG, ER, ET, GA, GH, GM, GN, GQ, GW, KE, KM, LR, LS, LY, MA, MG, ML, MR, MU, MW, MZ, NA, NE, NG, RE, RW, SC, SD, SH, SL, SN, SO, SS, ST, SZ, TD, TG, TN, TZ, UG, YT, ZA, ZM, ZW

Antártida (AN)

AQ, GS, TF

Asia (AS)

AE, AF, AM, AZ, BD, BH, BN, BT, CC, CN, GE, HK, ID, IL, IN, IO, IQ, IR, JO, JP, KG, KH, KP, KR, KW, KZ, LA, LB, LK, MM, MN, MO, MV, MY, NP, OM, PH, PK, PS, QA, SA, SG, SY, TH, TJ, TM, TW, UZ, VN, YE

Europa (EU)

AD, AL, AT, AX, BA, BE, BG, BY, CH, CY, CZ, DE, DK, EE, ES, FI, FO, FR, GB, GG, GI, GR, HR, HU, IE, IM, IS, IT, JE, LI, LT, LU, LV, MC, MD, ME, MK, MT, NL, NO, PL, PT, RO, RS, RU, SE, SI, SJ, SK, SM, TR, UA, VA, XK

Note

Algunos proveedores consideran que TR está en Asia, y esto se verá reflejado en las direcciones IP.

América del Norte (NA)

AG, AI, AW, BB, BL, BM, BQ, BS, BZ, CA, CR, CU, CW, DM, DO, GD, GL, GP, GT, HN, HT, JM, KN, KY, LC, MF, MQ, MS, MX, NI, PA, PM, PR, SV, SX, TC, TT, US, VC, VG, VI

Oceanía (OC)

AS, AU, CK, FJ, FM, GU, KI, MH, MP, NC, NF, NR, NU, NZ, PF, PG, PN, PW, SB, TK, TL, TO, TV, UM, VU, WF, WS

América del Sur (SA)

AR, BO, BR, CL, CO, EC, FK, GF, GY, PE, PY, SR, UY, VE

Note

Route 53 no admite la creación de registros de geolocalización para los siguientes países: Isla Bouvet (BV), Isla de Navidad (CX), Sáhara Occidental (EH) e Islas Heard y McDonald (HM). No hay datos disponibles sobre las direcciones IP de estos países.

Estados de Estados Unidos

Cuando configure Route 53 para que responda a las consultas de DNS según el estado de Estados Unidos de origen de las consultas, seleccione el estado de la lista U.S. states (Estados de Estados Unidos). En la lista Location (Ubicación), los territorios de Estados Unidos (por ejemplo, Puerto Rico) figuran como países.

Important

Algunas direcciones IP están asociadas con Estados Unidos, pero no con un estado individual. Si crea registros para todos los estados de Estados Unidos, es recomendable que también cree un registro para Estados Unidos con objeto de dirigir las consultas de estas direcciones IP no asociadas. Si no crea un registro para Estados Unidos, Route 53 responde a las consultas de DNS procedentes de las direcciones IP de Estados Unidos no asociadas con la configuración del registro de geolocalización predeterminado (si ha creado uno) o con una respuesta “sin respuesta”.

Comprobación de estado

Si desea que Route 53 verifique el estado de un punto de conexión dado y que solamente responda a las consultas de DNS utilizando este registro cuando el punto de conexión esté en buen estado, seleccione una comprobación de estado.

Route 53 no verifica el estado del punto de conexión especificado en el registro; por ejemplo, el punto de conexión que especifica la dirección IP en el campo Valor. Cuando se selecciona una comprobación de estado para un registro, Route 53 verifica el estado del punto de conexión especificado. Para obtener información sobre cómo Route 53 determina si un punto de conexión tiene un estado correcto, consulte [Cómo determina Amazon Route 53 si la comprobación de estado es correcta](#).

La asociación de una comprobación de estado a un conjunto de registros de recursos solo es útil cuando Route 53 elige entre dos o más registros para responder a una consulta de DNS y desea que Route 53 base la elección parcialmente en el estado de la comprobación de estado. Use las comprobaciones de estado solamente en las siguientes configuraciones:

- Va a comprobar el estado de todos los registros de un grupo de registros que tienen el mismo nombre, tipo y política de enrutamiento (como los registros de conmutación por error o ponderados) y especifica los identificadores de comprobación de estado de todos los registros. Si

en la comprobación de estado de un registro se especifica un punto de conexión que no está en buen estado, Route 53 deja de responder a las consultas mediante el valor de dicho registro.

- Seleccione Yes (Sí) en Evaluate Target Health (Evaluar el estado del destino) para un registro de alias o los registros de un grupo de alias de conmutación por error, alias de geolocalización, alias de latencia, alias basado en IP o registro de alias ponderado. Si los registros de alias hacen referencia a registros que no son alias en la misma zona alojada, también debe especificar comprobaciones de estado para estos últimos. Si asocia una comprobación de estado a un registro de alias y también selecciona Yes para Evaluate Target Health, ambos deben evaluarse como verdaderos. Para obtener más información, consulte [¿Qué sucede cuando se asocia una comprobación de estado a un registro de alias?](#).

Si en las comprobaciones de estado se especifica el punto de conexión solo por nombre de dominio, es recomendable crear una comprobación de estado independiente para cada punto de conexión. Por ejemplo, cree una comprobación de estado para cada servidor HTTP que sirva contenido de `www.ejemplo.com`. Para el valor de Domain Name (Nombre de dominio), especifique el nombre de dominio del servidor (por ejemplo, `us-east-2-www.example.com`), no el nombre de los registros (`example.com`).

 Important

En esta configuración, si crea una comprobación de estado cuyo valor de Domain name (Nombre de dominio) coincide con el nombre de los registros y a continuación la asocia con estos, los resultados de la comprobación serán impredecibles.

En el caso de los registros de geolocalización, si un punto de conexión no está en buen estado, Route 53 busca un registro para la región geográfica asociada de mayor tamaño. Por ejemplo, supongamos que tiene registros para un estado en Estados Unidos, para Estados Unidos, para América del Norte y para todas las ubicaciones (Location (Ubicación) es Default (Predeterminada)). Si el punto de conexión del registro de estado no está en buen estado, Route 53 verifica los registros para Estados Unidos, para América del Norte y para todas las ubicaciones, en ese orden, hasta que encuentre un registro con un punto de conexión en buen estado. Si ninguno de los registros está en buen estado, incluido el registro de todas las ubicaciones, Route 53 responde a la consulta de DNS utilizando el valor del registro de la región geográfica más pequeña.

ID de registro

Escriba un valor que identifique de manera exclusiva este registro en el grupo de registros de geolocalización.

Valores específicos de registros de alias de geolocalización

Cuando se crean registros de alias de geolocalización, hay que especificar los siguientes valores.

Para obtener más información, consulte [Elección entre registros de alias y sin alias](#).

Temas

- [Política de direccionamiento](#)
- [Nombre del registro](#)
- [Tipo de registro](#)
- [Valor/ruta de destino del tráfico](#)
- [Ubicación](#)
- [Estados de Estados Unidos](#)
- [Chequeo de salud](#)
- [Evaluate target health](#)
- [ID de registro](#)

Política de direccionamiento

Elija Geolocation (Geolocalización).

Nombre del registro

Escriba el nombre del dominio o subdominio para el que desea dirigir el tráfico. El valor predeterminado es el nombre de la zona alojada.

Note

Si crea un registro con el mismo nombre que el de la zona alojada, no ingrese un valor (por ejemplo, un símbolo @) en el campo Record name (Nombre del registro).

Escriba el mismo nombre para todos los registros del grupo de registros de geolocalización.

Para obtener más información acerca de nombres de registro, consulte [Nombre del registro](#).

Tipo de registro

El tipo de registro de DNS. Para obtener más información, consulte [Tipos de registros de DNS admitidos](#).

Seleccione el valor aplicable en función del AWS recurso al que está enrutando el tráfico. Seleccione el mismo valor para todos los registros del grupo de registros de geolocalización:

API regionales personalizadas o API optimizadas para bordes de API Gateway

Selecciona A — IPv4 dirección.

Puntos de conexión de interfaz de Amazon VPC

Seleccione A — IPv4 dirección.

CloudFront distribución

Seleccione A — IPv4 dirección.

Si IPv6 está habilitada para la distribución, cree dos registros, uno con el valor A (IPv4 dirección para el tipo) y otro con el valor AAAA (IPv6 dirección).

Servicio de App Runner

Seleccione A — dirección IPv4

Entorno de Elastic Beanstalk con subdominios regionalizados

Seleccione A — IPv4 dirección

Balanceador de carga de ELB

Seleccione la IPv4 dirección A o la dirección AAAA IPv6

Bucket de Amazon S3

Seleccione A — dirección IPv4

OpenSearch Servicio

Seleccione una IPv4 dirección o una dirección AAAA IPv6

Otro registro en esta zona alojada

Seleccione el tipo de registro para el que va a crear el alias. Se admiten todos los tipos, excepto NS y SOA.

 Note

Si va a crear un registro de alias con el mismo nombre que la zona alojada (lo que se conoce como ápex de zona), no podrá dirigir el tráfico a un registro en el que el valor de Type (Tipo) sea CNAME. Esto se debe a que el registro de alias debe tener el mismo tipo que el registro al que está redirigiendo el tráfico y no es posible crear un registro CNAME para el ápex de zona (ni siquiera para un registro de alias).

Valor/ruta de destino del tráfico

El valor que elija de la lista o que escriba en el campo depende del AWS recurso al que dirija el tráfico.

Para obtener información sobre AWS los recursos a los que puede dirigirse, consulte [Valor/ruta de destino del tráfico](#).

Para obtener más información sobre cómo configurar Route 53 para enrutar el tráfico a AWS recursos específicos, consulte [Enrutar el tráfico de Internet a sus AWS recursos](#).

Ubicación

Cuando configure Route 53 para que responda a las consultas de DNS según la ubicación de origen de estas, seleccione el continente o el país para el que quiere que Route 53 responda con la configuración de este registro. Si quiere que Route 53 responda a las consultas de DNS para estados individuales de Estados Unidos, seleccione United States (Estados Unidos) de la lista Location (Ubicación) y luego el estado en la lista U.S. states (Estados de Estados Unidos).

Para una zona alojada privada, seleccione el continente, país o subdivisión más cercano al lugar en el Región de AWS que se encuentra su recurso. Por ejemplo, si el recurso se encuentra en us-east-1, puede especificar Norteamérica, Estados Unidos o Virginia.

 Important

Es recomendable crear un registro de geolocalización con el valor Default (Predeterminada) para Location (Ubicación). Esto cubre las ubicaciones geográficas para las que no se hayan creado registros y las direcciones IP para las que Route 53 no puede identificar la ubicación.

No puede crear registros sin geolocalización que tengan los mismos valores de Record name (Nombre del registro) y Record type (Tipo de registro) que los registros de geolocalización.

Para obtener más información, consulte [Enrutado de geolocalización](#).

Estos son los países que Amazon Route 53 asocia con cada continente. Los códigos de país son de ISO 3166. Para obtener más información, consulte el artículo de Wikipedia [ISO 3166-1 alpha-2](#):

África (AF)

AO, BF, BI, BJ, BW, CD, CF, CG, CI, CM, CV, DJ, DZ, EG, ER, ET, GA, GH, GM, GN, GQ, GW, KE, KM, LR, LS, LY, MA, MG, ML, MR, MU, MW, MZ, NA, NE, NG, RE, RW, SC, SD, SH, SL, SN, SO, SS, ST, SZ, TD, TG, TN, TZ, UG, YT, ZA, ZM, ZW

Antártida (AN)

AQ, GS, TF

Asia (AS)

AE, AF, AM, AZ, BD, BH, BN, BT, CC, CN, GE, HK, ID, IL, IN, IO, IQ, IR, JO, JP, KG, KH, KP, KR, KW, KZ, LA, LB, LK, MM, MN, MO, MV, MY, NP, OM, PH, PK, PS, QA, SA, SG, SY, TH, TJ, TM, TW, UZ, VN, YE

Europa (UE)

AD, AL, AT, AX, BA, BE, BG, BY, CH, CY, CZ, DE, DK, EE, ES, FI, FO, FR, GB, GG, GI, GR, HR, HU, IE, IM, IS, IT, JE, LI, LT, LU, LV, MC, MD, ME, MK, MT, NL, NO, PL, PT, RO, RS, RU, SE, SI, SJ, SK, SM, TR, UA, VA, XK

Note

Algunos proveedores consideran que TR está en Asia, y esto se verá reflejado en las direcciones IP.

América del Norte (NA)

AG, AI, AW, BB, BL, BM, BQ, BS, BZ, CA, CR, CU, CW, DM, DO, GD, GL, GP, GT, HN, HT, JM, KN, KY, LC, MF, MQ, MS, MX, NI, PA, PM, PR, SV, SX, TC, TT, US, VC, VG, VI

Oceanía (OC)

AS, AU, CK, FJ, FM, GU, KI, MH, MP, NC, NF, NR, NU, NZ, PF, PG, PN, PW, SB, TK, TL, TO, TV, UM, VU, WF, WS

América del Sur (SA)

AR, BO, BR, CL, CO, EC, FK, GF, GY, PE, PY, SR, UY, VE

Note

Route 53 no permite crear registros de geolocalización para los siguientes países: Isla Bouvet (BV), Isla de Navidad (CX), Sáhara Occidental (EH) e Isla e Islas Heard McDonald (HM). No hay datos disponibles sobre las direcciones IP de estos países.

Estados de Estados Unidos

Cuando configure Route 53 para que responda a las consultas de DNS según el estado de Estados Unidos de origen de las consultas, seleccione el estado de la lista U.S. states (Estados de Estados Unidos). En la lista Location (Ubicación), los territorios de Estados Unidos (por ejemplo, Puerto Rico) figuran como países.

Important

Algunas direcciones IP están asociadas con Estados Unidos, pero no con un estado individual. Si crea registros para todos los estados de Estados Unidos, es recomendable que también cree un registro para Estados Unidos con objeto de dirigir las consultas de estas direcciones IP no asociadas. Si no crea un registro para Estados Unidos, Route 53 responde a las consultas de DNS procedentes de las direcciones IP de Estados Unidos no asociadas con la configuración del registro de geolocalización predeterminado (si ha creado uno) o con una respuesta “sin respuesta”.

Chequeo de salud

Si desea que Route 53 verifique el estado de un punto de conexión dado y que solamente responda a las consultas de DNS utilizando este registro cuando el punto de conexión esté en buen estado, seleccione una comprobación de estado.

Route 53 no verifica el estado del punto de conexión especificado en el registro; por ejemplo, el punto de conexión que especifica la dirección IP en el campo Valor. Cuando se selecciona una comprobación de estado para un registro, Route 53 verifica el estado del punto de conexión especificado. Para obtener información sobre cómo Route 53 determina si un punto de conexión tiene un estado correcto, consulte [Cómo determina Amazon Route 53 si la comprobación de estado es correcta](#).

La asociación de una comprobación de estado a un conjunto de registros de recursos solo es útil cuando Route 53 elige entre dos o más registros para responder a una consulta de DNS y desea que Route 53 base la elección parcialmente en el estado de la comprobación de estado. Use las comprobaciones de estado solamente en las siguientes configuraciones:

- Está comprobando el estado de todos los registros de un grupo de registros que tienen el mismo nombre, tipo y política de enrutamiento (como los registros de conmutación por error o ponderados) y especifica la comprobación IDs de estado de todos los registros. Si en la comprobación de estado de un registro se especifica un punto de conexión que no está en buen estado, Route 53 deja de responder a las consultas mediante el valor de dicho registro.
- Seleccione Yes (Sí) en Evaluate Target Health (Evaluar el estado del destino) para un registro de alias o los registros de un grupo de alias de conmutación por error, alias de geolocalización, alias de latencia, alias basado en IP o registro de alias ponderado. Si los registros de alias hacen referencia a registros que no son alias en la misma zona alojada, también debe especificar comprobaciones de estado para estos últimos. Si asocia una comprobación de estado a un registro de alias y también selecciona Yes para Evaluate Target Health, ambos deben evaluarse como verdaderos. Para obtener más información, consulte [¿Qué sucede cuando se asocia una comprobación de estado a un registro de alias?](#).

Si en las comprobaciones de estado se especifica el punto de conexión solo por nombre de dominio, es recomendable crear una comprobación de estado independiente para cada punto de conexión. Por ejemplo, cree una comprobación de estado para cada servidor HTTP que sirva contenido de `www.ejemplo.com`. Para el valor de Domain name (Nombre de dominio), especifique el nombre de dominio del servidor (por ejemplo, `us-east-2-www.example.com`), no el nombre de los registros (`example.com`).

 Important

En esta configuración, si crea una comprobación de estado cuyo valor de Domain name coincide con el nombre de los registros y luego la asocia con estos, los resultados de la comprobación serán impredecibles.

En el caso de los registros de geolocalización, si un punto de conexión no está en buen estado, Route 53 busca un registro para la región geográfica asociada de mayor tamaño. Por ejemplo, supongamos que tiene registros para un estado en Estados Unidos, para Estados Unidos, para América del Norte y para todas las ubicaciones (Location (Ubicación) es Default (Predeterminada)). Si el punto de conexión del registro de estado no está en buen estado, Route 53 verifica los registros para Estados Unidos, para América del Norte y para todas las ubicaciones, en ese orden, hasta que encuentre un registro con un punto de conexión en buen estado. Si ninguno de los registros está en buen estado, incluido el registro de todas las ubicaciones, Route 53 responde a la consulta de DNS utilizando el valor del registro de la región geográfica más pequeña.

Evaluate target health

Seleccione Sí, si desea que Route 53 determine si debe responder a las consultas de DNS mediante este registro al verificar el estado del recurso especificado mediante Punto de conexión.

Tenga en cuenta lo siguiente:

API Gateway personalizado, regional APIs y optimizado para entornos periféricos APIs

No existen requisitos especiales para establecer Evaluate target health (Evaluar estado del destino) en Yes (Sí) cuando el punto de conexión es una API regional personalizada o una API optimizada para bordes de API Gateway.

CloudFront distribuciones

No puede establecer Evaluar el estado del objetivo en Sí cuando el punto final es una CloudFront distribución.

Entornos de Elastic Beanstalk que tienen subdominios regionalizados

Si especifica un entorno de Elastic Beanstalk en Endpoint y el entorno contiene un balanceador de cargas ELB, ELB direcciona las consultas únicamente a las instancias de Amazon en EC2 buen estado que estén registradas en el balanceador de cargas. (Un entorno contiene automáticamente un balanceador de cargas ELB si incluye más de una EC2 instancia de

Amazon). Si estableces Evaluar el estado del objetivo en Sí y ninguna EC2 instancia de Amazon está en buen estado o el propio balanceador de carga no está en buen estado, Route 53 redirige las consultas a otros recursos disponibles que estén en buen estado, si los hay.

Si el entorno contiene una sola EC2 instancia de Amazon, no hay requisitos especiales.

Balanceadores de carga de ELB

El comportamiento de la comprobación de estado depende del tipo de balanceador de carga:

- **Classic Load Balancers:** si especificas un balanceador de carga clásico ELB en Endpoint, ELB dirige las consultas solo a las instancias de EC2 Amazon en buen estado que estén registradas en el balanceador de cargas. Si estableces Evaluar el estado del objetivo en Sí y ninguna EC2 instancia está en buen estado o el propio balanceador de carga no está en buen estado, Route 53 redirige las consultas a otros recursos.
- **Network Load Balancers y aplicaciones:** si especifica un Network Load Balancers o aplicaciones ELB, y establece Evaluate target health (Evaluar estado del destino) en Yes (Sí), Route 53 dirige consultas al balanceador de carga en función del estado de los grupos de destino asociados al balanceador de carga:
 - Para que se considere que un Application Load Balancer o un Network Load Balancer está en buen estado, cada grupo de destinos que contenga destinos debe contener al menos un destino en buen estado. Si cualquier grupo de destinos contiene únicamente destinos en mal estado, se considera que el balanceador de carga está en mal estado y Route 53 envía las consultas a otros recursos.
 - Un grupo de destinos que no tiene destinos registrados se considera que no está en buen estado.

Note

Al crear un balanceador de cargas, se configuran los ajustes para las comprobaciones de estado de ELB; no son comprobaciones de estado de Route 53, pero realizan una función similar. No cree comprobaciones de estado de Route 53 para las EC2 instancias que registre en un balanceador de cargas de ELB.

Buckets de S3

No existen requisitos especiales para establecer Evaluar estado del destino en Sí cuando el punto de conexión es un bucket de S3.

Puntos de enlace de interfaz de Amazon VPC

No existen requisitos especiales para establecer Evaluar estado del destino en Sí cuando el punto de conexión es uno de interfaz de Amazon VPC.

Otros registros de la misma zona alojada

Si el AWS recurso que especifica en Endpoint es un registro o un grupo de registros (por ejemplo, un grupo de registros ponderados) pero no es otro registro de alias, le recomendamos que asocie una comprobación de estado a todos los registros del punto final. Para obtener más información, consulte [¿Qué sucede cuando se omiten las comprobaciones de estado?](#).

ID de registro

Escriba un valor que identifique de manera exclusiva este registro en el grupo de registros de geolocalización.

Valores específicos de registros de geoproximidad

Cuando se crean registros de geoproximidad, debe especificar los siguientes valores.

Temas

- [Política de direccionamiento](#)
- [Nombre del registro](#)
- [Tipo de registro](#)
- [TTL \(segundos\)](#)
- [Valor/ruta de destino del tráfico](#)
- [Ubicación de puntos de conexión](#)
- [Sesgo](#)
- [Comprobación de estado](#)
- [ID de registro](#)

Política de direccionamiento

Elija Geoproximidad.

Nombre del registro

Escriba el nombre del dominio o subdominio para el que desea dirigir el tráfico. El valor predeterminado es el nombre de la zona alojada.

Note

Si crea un registro con el mismo nombre que el de la zona alojada, no escriba un valor (por ejemplo, un símbolo @) en el campo Name (Nombre).

Escriba el mismo nombre para todos los registros del grupo de registros de geoproximidad.

Para obtener más información acerca de nombres de registro, consulte [Nombre del registro](#).

Tipo de registro

El tipo de registro de DNS. Para obtener más información, consulte [Tipos de registros de DNS admitidos](#).

Seleccione el mismo valor para todos los registros del grupo de registros de geoproximidad.

TTL (segundos)

El tiempo, en segundos, en que desea que los solucionadores recursivos de DNS almacenen en caché información sobre este registro. Si especifica un valor más largo (por ejemplo, 172 800 segundos o dos días), se reduce el número de llamadas que los solucionadores recursivos de DNS deben realizar a Route 53 para obtener la información más reciente de este registro. Esto reduce la latencia y la factura del servicio Route 53. Para obtener más información, consulte [Cómo dirige Amazon Route 53 el tráfico de su dominio](#).

Sin embargo, si especifica un valor más largo para TTL, los cambios realizados en el registro (por ejemplo, una nueva dirección IP) tardarán más tiempo en surtir efecto, ya que los solucionadores recursivos usan los valores de la memoria caché durante periodos más largos antes de solicitar la información más reciente a Route 53. Si está cambiando la configuración de un dominio o subdominio que ya está en uso, le recomendamos que inicialmente especifique un valor más corto, por ejemplo, 300 segundos y que aumente el valor después de confirmar que la configuración nueva es correcta.

Si asocia este registro a una comprobación de estado, es recomendable que especifique un TTL de 60 segundos o menos para que los clientes respondan rápidamente a los cambios de estado.

Valor/ruta de destino del tráfico

Elija IP address or another value depending on the record type (Dirección IP u otro valor en función del tipo de registro). Ingrese un valor que sea adecuado para el valor de Record type (Tipo de registro). Para todos los tipos excepto CNAME, puede escribir más de un valor. Escriba cada valor en una línea independiente.

Puede dirigir el tráfico a, o especificar los siguientes valores:

- A: dirección IPv
- AAAA: dirección IPv
- CAA: autorización de la entidad de certificación
- CNAME: nombre canónico
- MX: intercambio de correo
- NAPTR: señalizador de autoridad de asignación de nombres
- PTR: puntero

- SPF: marco de políticas de remitente
- SRV: localizador de servicios
- TXT: texto

Para más información acerca de los valores anteriores, consulte los [valores comunes de valor/ruta de destino del tráfico](#).

Ubicación de puntos de conexión

Puede especificar la ubicación del punto de conexión del recurso mediante uno de los siguientes métodos:

Coordenadas personalizadas

Especifique la longitud y la latitud de un área geográfica.

Región de AWS

Elija una región disponible en la lista de Ubicaciones.

Para obtener más información acerca de las regiones, consulte [Infraestructura global de AWS](#).

Grupo de zona local de AWS

Elija un grupo de zonas locales disponible de la lista de Ubicaciones.

Para obtener más información acerca de las zonas locales, consulte [Zonas locales disponibles](#) en la Guía del usuario de zonas locales de AWS. Un grupo de zonas locales suele ser la zona local sin el carácter final. Por ejemplo, si la zona local es `us-east-1-bue-1a`, el grupo de zonas locales es `us-east-1-bue-1`.

También puede identificar el grupo de zonas locales de una zona local específica mediante el comando de la CLI [describe-availability-zones](#):

```
aws ec2 describe-availability-zones --region us-west-2 --all-availability-zones --query
"AvailabilityZones[?ZoneName=='us-west-2-den-1a']" | grep "GroupName"
```

Este comando devuelve `"GroupName": "us-west-2-den-1"` y se especifica que la zona local `us-west-2-den-1a` pertenece al grupo de zonas locales `us-west-2-den-1`.

No puede crear registros sin geoproximidad que tengan los mismos valores de Nombre del registro y Tipo de registro que los registros de geoproximidad.

Tampoco puede crear dos conjuntos de registros de recursos de geoproximidad que especifiquen la misma ubicación para el mismo nombre y tipo de registro.

Sesgo

Un sesgo expande o reduce el área geográfica desde la que Route 53 direcciona el tráfico a un recurso. Un sesgo positivo expande el área y un sesgo negativo la reduce. Para obtener más información, consulte [Cómo utiliza Amazon Route 53 el sesgo para dirigir el tráfico](#).

Comprobación de estado

Si desea que Route 53 verifique el estado de un punto de conexión dado y que solamente responda a las consultas de DNS utilizando este registro cuando el punto de conexión esté en buen estado, seleccione una comprobación de estado.

Route 53 no verifica el estado del punto de conexión especificado en el registro; por ejemplo, el punto de conexión que especifica la dirección IP en el campo Valor. Cuando se selecciona una comprobación de estado para un registro, Route 53 verifica el estado del punto de conexión especificado. Para obtener información sobre cómo Route 53 determina si un punto de conexión tiene un estado correcto, consulte [Cómo determina Amazon Route 53 si la comprobación de estado es correcta](#).

La asociación de una comprobación de estado a un conjunto de registros de recursos solo es útil cuando Route 53 elige entre dos o más registros para responder a una consulta de DNS y desea que Route 53 base la elección parcialmente en el estado de la comprobación de estado. Use las comprobaciones de estado solamente en las siguientes configuraciones:

- Va a comprobar el estado de todos los registros de un grupo de registros que tienen el mismo nombre, tipo y política de enrutamiento (como los registros de conmutación por error o ponderados) y especifica los identificadores de comprobación de estado de todos los registros. Si en la comprobación de estado de un registro se especifica un punto de conexión que no está en buen estado, Route 53 deja de responder a las consultas mediante el valor de dicho registro.
- Seleccione Sí en Evaluar el estado del destino para un registro de alias o los registros de un grupo de alias de conmutación por error, alias de geolocalización, alias de geoproximidad, alias de latencia, alias basado en IP o registro de alias ponderado. Si los registros de alias hacen referencia a registros que no son alias en la misma zona alojada, también debe especificar comprobaciones

de estado para estos últimos. Si asocia una comprobación de estado a un registro de alias y también selecciona Yes para Evaluate Target Health, ambos deben evaluarse como verdaderos. Para obtener más información, consulte [¿Qué sucede cuando se asocia una comprobación de estado a un registro de alias?](#).

Si en las comprobaciones de estado se especifica el punto de conexión solo por nombre de dominio, es recomendable crear una comprobación de estado independiente para cada punto de conexión. Por ejemplo, cree una comprobación de estado para cada servidor HTTP que sirva contenido de `www.ejemplo.com`. Para el valor de Domain Name (Nombre de dominio), especifique el nombre de dominio del servidor (por ejemplo, `us-east-2-www.example.com`), no el nombre de los registros (`example.com`).

 Important

En esta configuración, si crea una comprobación de estado cuyo valor de Domain name (Nombre de dominio) coincide con el nombre de los registros y a continuación la asocia con estos, los resultados de la comprobación serán impredecibles.

En el caso de los registros de geoproximidad, si un punto de conexión no está en buen estado, Route 53 busca el punto de conexión más cercano que todavía esté en buen estado.

ID de registro

Escriba un valor que identifique de manera exclusiva este registro en el grupo de registros de geoproximidad.

Valores específicos de registros de alias de geoproximidad

Cuando se crean registros de alias de geoproximidad, hay que especificar los siguientes valores.

Para obtener más información, consulte [Elección entre registros de alias y sin alias](#).

Temas

- [Política de direccionamiento](#)
- [Nombre del registro](#)
- [Tipo de registro](#)
- [Valor/ruta de destino del tráfico](#)
- [Ubicación de puntos de conexión](#)
- [Sesgo](#)
- [Health check](#)
- [Evaluate target health](#)
- [ID de registro](#)

Política de direccionamiento

Elija Geoproximidad.

Nombre del registro

Escriba el nombre del dominio o subdominio para el que desea dirigir el tráfico. El valor predeterminado es el nombre de la zona alojada.

Note

Si crea un registro con el mismo nombre que el de la zona alojada, no ingrese un valor (por ejemplo, un símbolo @) en el campo Record name (Nombre del registro).

Escriba el mismo nombre para todos los registros del grupo de registros de geoproximidad.

Para obtener más información acerca de nombres de registro, consulte [Nombre del registro](#).

Tipo de registro

El tipo de registro de DNS. Para obtener más información, consulte [Tipos de registros de DNS admitidos](#).

Seleccione el valor aplicable en función del AWS recurso al que está enrutando el tráfico. Seleccione el mismo valor para todos los registros del grupo de registros de geoproximidad:

API regionales personalizadas o API optimizadas para bordes de API Gateway

Selecciona A — IPv4 dirección.

Puntos de conexión de interfaz de Amazon VPC

Seleccione A — IPv4 dirección.

CloudFront distribución

Seleccione A — IPv4 dirección.

Si IPv6 está habilitada para la distribución, cree dos registros, uno con el valor A (IPv4 dirección de tipo) y otro con el valor AAAA (IPv6 dirección).

Servicio de App Runner

Seleccione A — dirección IPv4

Entorno de Elastic Beanstalk con subdominios regionalizados

Seleccione A — IPv4 dirección

Balanceador de carga de ELB

Seleccione la IPv4 dirección A o la dirección AAAA IPv6

Bucket de Amazon S3

Seleccione A — dirección IPv4

OpenSearch Servicio

Seleccione una IPv4 dirección o una dirección AAAA IPv6

Otro registro en esta zona alojada

Seleccione el tipo de registro para el que va a crear el alias. Se admiten todos los tipos, excepto NS y SOA.

 Note

Si va a crear un registro de alias con el mismo nombre que la zona alojada (lo que se conoce como ápex de zona), no podrá dirigir el tráfico a un registro en el que el valor de Type (Tipo) sea CNAME. Esto se debe a que el registro de alias debe tener el mismo tipo que el registro al que está redirigiendo el tráfico y no es posible crear un registro CNAME para el ápex de zona (ni siquiera para un registro de alias).

Valor/ruta de destino del tráfico

El valor que elija de la lista o que escriba en el campo depende del AWS recurso al que dirija el tráfico.

Para obtener información sobre AWS los recursos a los que puede dirigirse, consulte [Valor/ruta de destino del tráfico](#).

Para obtener más información sobre cómo configurar Route 53 para enrutar el tráfico a AWS recursos específicos, consulte [Enrutar el tráfico de Internet a sus AWS recursos](#).

Ubicación de puntos de conexión

Puede especificar la ubicación del punto de conexión del recurso mediante uno de los siguientes métodos:

Coordenadas personalizadas

Especifique la longitud y la latitud de un área geográfica.

Región de AWS

Elija una región disponible en la lista de Ubicaciones.

Para obtener más información acerca de las regiones, consulte [Infraestructura global de AWS](#).

AWS Grupo de zonas locales

Elija una región de zona local disponible de la lista de Ubicaciones.

Para obtener más información acerca de las zonas locales, consulte [Zonas locales disponibles](#) en la Guía del usuario de zonas locales de AWS . Un grupo de zonas locales suele ser la zona

local sin el carácter final. Por ejemplo, si la zona local es `us-east-1-bue-1a`, el grupo de zonas locales es `us-east-1-bue-1`.

También puede identificar el grupo de zonas locales de una zona local específica mediante el comando [describe-availability-zones](#) CLI:

```
aws ec2 describe-availability-zones --region us-west-2 --all-availability-zones --query "AvailabilityZones[?ZoneName=='us-west-2-den-1a']" | grep "GroupName"
```

Este comando devuelve `"GroupName": "us-west-2-den-1"` y se especifica que la zona local `us-west-2-den-1a` pertenece al grupo de zonas locales `us-west-2-den-1`.

No puede crear registros sin geoproximidad que tengan los mismos valores de Nombre del registro y Tipo de registro que los registros de geoproximidad.

Tampoco puede crear dos conjuntos de registros de recursos de geoproximidad que especifiquen la misma ubicación para el mismo nombre y tipo de registro.

Para obtener más información, consulte [available-local-zones.html](#)

Sesgo

Un sesgo expande o reduce el área geográfica desde la que Route 53 direcciona el tráfico a un recurso. Un sesgo positivo expande el área y un sesgo negativo la reduce. Para obtener más información, consulte [Cómo utiliza Amazon Route 53 el sesgo para dirigir el tráfico](#).

Health check

Si desea que Route 53 verifique el estado de un punto de conexión dado y que solamente responda a las consultas de DNS utilizando este registro cuando el punto de conexión esté en buen estado, seleccione una comprobación de estado.

Route 53 no verifica el estado del punto de conexión especificado en el registro; por ejemplo, el punto de conexión que especifica la dirección IP en el campo Valor. Cuando se selecciona una comprobación de estado para un registro, Route 53 verifica el estado del punto de conexión especificado. Para obtener información sobre cómo Route 53 determina si un punto de conexión tiene un estado correcto, consulte [Cómo determina Amazon Route 53 si la comprobación de estado es correcta](#).

La asociación de una comprobación de estado a un conjunto de registros de recursos solo es útil cuando Route 53 elige entre dos o más registros para responder a una consulta de DNS y desea

que Route 53 base la elección parcialmente en el estado de la comprobación de estado. Use las comprobaciones de estado solamente en las siguientes configuraciones:

- Está comprobando el estado de todos los registros de un grupo de registros que tienen el mismo nombre, tipo y política de enrutamiento (como los registros de conmutación por error o ponderados) y especifica la comprobación IDs de estado de todos los registros. Si en la comprobación de estado de un registro se especifica un punto de conexión que no está en buen estado, Route 53 deja de responder a las consultas mediante el valor de dicho registro.
- Seleccione Sí en Evaluar el estado del destino para un registro de alias o los registros de un grupo de alias de conmutación por error, alias de geolocalización, alias de geoproximidad, alias de latencia, alias basado en IP o registro de alias ponderado. Si los registros de alias hacen referencia a registros que no son alias en la misma zona alojada, también debe especificar comprobaciones de estado para estos últimos. Si asocia una comprobación de estado a un registro de alias y también selecciona Yes para Evaluate Target Health, ambos deben evaluarse como verdaderos. Para obtener más información, consulte [¿Qué sucede cuando se asocia una comprobación de estado a un registro de alias?](#).

Si en las comprobaciones de estado se especifica el punto de conexión solo por nombre de dominio, es recomendable crear una comprobación de estado independiente para cada punto de conexión. Por ejemplo, cree una comprobación de estado para cada servidor HTTP que sirva contenido de `www.ejemplo.com`. Para el valor de Domain name (Nombre de dominio), especifique el nombre de dominio del servidor (por ejemplo, `us-east-2-www.example.com`), no el nombre de los registros (`example.com`).

Important

En esta configuración, si crea una comprobación de estado cuyo valor de Domain name coincide con el nombre de los registros y luego la asocia con estos, los resultados de la comprobación serán impredecibles.

En el caso de los registros de geoproximidad, si un punto de conexión no está en buen estado, Route 53 busca el punto de conexión más cercano que todavía esté en buen estado.

Evaluate target health

Seleccione Sí, si desea que Route 53 determine si debe responder a las consultas de DNS mediante este registro al verificar el estado del recurso especificado mediante Punto de conexión.

Tenga en cuenta lo siguiente:

API Gateway personalizado, regional APIs y optimizado para entornos periféricos APIs

No existen requisitos especiales para establecer Evaluate target health (Evaluar estado del destino) en Yes (Sí) cuando el punto de conexión es una API regional personalizada o una API optimizada para bordes de API Gateway.

CloudFront distribuciones

No puede establecer Evaluar el estado del objetivo en Sí cuando el punto final es una CloudFront distribución.

Entornos de Elastic Beanstalk que tienen subdominios regionalizados

Si especifica un entorno de Elastic Beanstalk en Endpoint y el entorno contiene un balanceador de cargas ELB, ELB direcciona las consultas únicamente a las instancias de Amazon en EC2 buen estado que estén registradas en el balanceador de cargas. (Un entorno contiene automáticamente un balanceador de cargas ELB si incluye más de una EC2 instancia de Amazon). Si estableces Evaluar el estado del objetivo en Sí y ninguna EC2 instancia de Amazon está en buen estado o el propio balanceador de carga no está en buen estado, Route 53 redirige las consultas a otros recursos disponibles que estén en buen estado, si los hay.

Si el entorno contiene una sola EC2 instancia de Amazon, no hay requisitos especiales.

Balanceadores de carga de ELB

El comportamiento de la comprobación de estado depende del tipo de balanceador de carga:

- **Classic Load Balancers:** si especificas un balanceador de carga clásico ELB en Endpoint, ELB dirige las consultas solo a las instancias de EC2 Amazon en buen estado que estén registradas en el balanceador de cargas. Si estableces Evaluar el estado del objetivo en Sí y ninguna EC2 instancia está en buen estado o el propio balanceador de carga no está en buen estado, Route 53 redirige las consultas a otros recursos.
- **Network Load Balancers y aplicaciones:** si especifica un Network Load Balancers o aplicaciones ELB, y establece Evaluate target health (Evaluar estado del destino) en Yes (Sí), Route 53 dirige consultas al balanceador de carga en función del estado de los grupos de destino asociados al balanceador de carga:
 - Para que se considere que un Application Load Balancer o un Network Load Balancer está en buen estado, cada grupo de destinos que contenga destinos debe contener al menos un destino en buen estado. Si cualquier grupo de destinos contiene únicamente destinos en mal

estado, se considera que el balanceador de carga está en mal estado y Route 53 envía las consultas a otros recursos.

- Un grupo de destinos que no tiene destinos registrados se considera que no está en buen estado.

 Note

Al crear un balanceador de cargas, se configuran los ajustes para las comprobaciones de estado de ELB; no son comprobaciones de estado de Route 53, pero realizan una función similar. No cree comprobaciones de estado de Route 53 para las EC2 instancias que registre en un balanceador de cargas de ELB.

Buckets de S3

No existen requisitos especiales para establecer Evaluar estado del destino en Sí cuando el punto de conexión es un bucket de S3.

Puntos de enlace de interfaz de Amazon VPC

No existen requisitos especiales para establecer Evaluar estado del destino en Sí cuando el punto de conexión es uno de interfaz de Amazon VPC.

Otros registros de la misma zona alojada

Si el AWS recurso que especifica en Endpoint es un registro o un grupo de registros (por ejemplo, un grupo de registros ponderados) pero no es otro registro de alias, le recomendamos que asocie una comprobación de estado a todos los registros del punto final. Para obtener más información, consulte [¿Qué sucede cuando se omiten las comprobaciones de estado?](#).

ID de registro

Escriba un valor que identifique de manera exclusiva este registro en el grupo de registros de geoproximidad.

Valores específicos de registros de latencia

Cuando se crean registros de latencia, hay que especificar los siguientes valores.

Temas

- [Política de direccionamiento](#)
- [Nombre del registro](#)
- [Tipo de registro](#)
- [TTL \(segundos\)](#)
- [Valor/ruta de destino del tráfico](#)
- [Región](#)
- [Comprobación de estado](#)
- [ID de registro](#)

Política de direccionamiento

Elija Latency (Latencia).

Nombre del registro

Escriba el nombre del dominio o subdominio para el que desea dirigir el tráfico. El valor predeterminado es el nombre de la zona alojada.

Note

Si crea un registro con el mismo nombre que el de la zona alojada, no ingrese un valor (por ejemplo, un símbolo @) en el campo Record name (Nombre del registro).

Escriba el mismo nombre para todos los registros del grupo de registros de latencia.

Para obtener más información acerca de nombres de registro, consulte [Nombre del registro](#).

Tipo de registro

El tipo de registro de DNS. Para obtener más información, consulte [Tipos de registros de DNS admitidos](#).

Seleccione el valor de Type (Tipo) en función de cómo desee que Route 53 responda a las consultas de DNS.

Seleccione el mismo valor para todos los registros del grupo de registros de latencia.

TTL (segundos)

El tiempo, en segundos, que desea que los solucionadores recursivos de DNS almacenen en caché información sobre este registro. Si especifica un valor más largo (por ejemplo, 172 800 segundos o dos días), se reduce el número de llamadas que los solucionadores recursivos de DNS deben realizar a Route 53 para obtener la información más reciente de este registro. Esto reduce la latencia y la factura del servicio Route 53. Para obtener más información, consulte [Cómo dirige Amazon Route 53 el tráfico de su dominio](#).

Sin embargo, si especifica un valor más largo para TTL, los cambios realizados en el registro (por ejemplo, una nueva dirección IP) tardarán más tiempo en surtir efecto, ya que los solucionadores recursivos usan los valores de la memoria caché durante periodos más largos antes de solicitar la información más reciente a Route 53. Si está cambiando la configuración de un dominio o subdominio que ya está en uso, le recomendamos que inicialmente especifique un valor más corto, por ejemplo, 300 segundos y que aumente el valor después de confirmar que la configuración nueva es correcta.

Si asocia este registro a una comprobación de estado, es recomendable que especifique un TTL de 60 segundos o menos para que los clientes respondan rápidamente a los cambios de estado.

Valor/ruta de destino del tráfico

Elija IP address or another value depending on the record type (Dirección IP u otro valor en función del tipo de registro). Ingrese un valor que sea adecuado para el valor de Record type (Tipo de registro). Para todos los tipos excepto CNAME, puede escribir más de un valor. Escriba cada valor en una línea independiente.

Puede dirigir el tráfico a, o especificar los siguientes valores:

- A: dirección IPv
- AAAA: dirección IPv
- CAA: autorización de la entidad de certificación
- CNAME: nombre canónico
- MX: intercambio de correo

- NAPTR: señalizador de autoridad de asignación de nombres
- PTR: puntero
- SPF: marco de políticas de remitente
- SRV: localizador de servicios
- TXT: texto

Para más información acerca de los valores anteriores, consulte los [valores comunes del valor/ruta de destino del tráfico](#).

Región

Región de Amazon EC2 en la que reside el recurso especificado en este registro. Route 53 recomienda una región de Amazon EC2 en función de otros valores especificados. Esto también se aplica a las zonas alojadas privadas. Es recomendable que no cambie este valor.

Tenga en cuenta lo siguiente:

- Solo puede crear un registro de latencia para cada región de Amazon EC2.
- No es necesario crear registros de latencia para todas las regiones de Amazon EC2. Route 53 elige la región con la mejor latencia entre aquellas en las que creó registros de latencia.
- No puede crear registros sin latencia que tengan los mismos valores de Record name (Nombre del registro) y Record type (Tipo de registro) que los registros de latencia.
- Si crea un registro etiquetado con la región cn-north-1, Route 53 responderá siempre a las consultas procedentes de China utilizando este registro, independientemente de la latencia.

Para obtener más información acerca del uso de registros de latencia, consulte [Enrutado basado en latencia](#).

Comprobación de estado

Si desea que Route 53 verifique el estado de un punto de conexión dado y que solamente responda a las consultas de DNS utilizando este registro cuando el punto de conexión esté en buen estado, seleccione una comprobación de estado.

Route 53 no verifica el estado del punto de conexión especificado en el registro; por ejemplo, el punto de conexión que especifica la dirección IP en el campo Valor. Cuando se selecciona

una comprobación de estado para un registro, Route 53 verifica el estado del punto de conexión especificado. Para obtener información sobre cómo Route 53 determina si un punto de conexión tiene un estado correcto, consulte [Cómo determina Amazon Route 53 si la comprobación de estado es correcta](#).

La asociación de una comprobación de estado a un conjunto de registros de recursos solo es útil cuando Route 53 elige entre dos o más registros para responder a una consulta de DNS y desea que Route 53 base la elección parcialmente en el estado de la comprobación de estado. Use las comprobaciones de estado solamente en las siguientes configuraciones:

- Va a comprobar el estado de todos los registros de un grupo de registros que tienen el mismo nombre, tipo y política de enrutamiento (como los registros de conmutación por error o ponderados) y especifica los identificadores de comprobación de estado de todos los registros. Si en la comprobación de estado de un registro se especifica un punto de conexión que no está en buen estado, Route 53 deja de responder a las consultas mediante el valor de dicho registro.
- Seleccione Yes (Sí) en Evaluate Target Health (Evaluar el estado del destino) para un registro de alias o los registros de un grupo de alias de conmutación por error, alias de geolocalización, alias de latencia, alias basado en IP o registro de alias ponderado. Si los registros de alias hacen referencia a registros que no son alias en la misma zona alojada, también debe especificar comprobaciones de estado para estos últimos. Si asocia una comprobación de estado a un registro de alias y también selecciona Yes para Evaluate Target Health, ambos deben evaluarse como verdaderos. Para obtener más información, consulte [¿Qué sucede cuando se asocia una comprobación de estado a un registro de alias?](#).

Si en las comprobaciones de estado se especifica el punto de conexión solo por nombre de dominio, es recomendable crear una comprobación de estado independiente para cada punto de conexión. Por ejemplo, cree una comprobación de estado para cada servidor HTTP que sirva contenido de `www.ejemplo.com`. Para el valor de Domain name (Nombre de dominio), especifique el nombre de dominio del servidor (por ejemplo, `us-east-2-www.example.com`), no el nombre de los registros (`example.com`).

Important

En esta configuración, si crea una comprobación de estado cuyo valor de Domain name coincide con el nombre de los registros y luego la asocia con estos, los resultados de la comprobación serán impredecibles.

ID de registro

Escriba un valor que identifique de manera exclusiva este registro en el grupo de registros de latencia.

Valores específicos de registros de alias de latencia

Cuando crean registros de alias de latencia, hay que especificar los siguientes valores.

Para obtener más información, consulte [Elección entre registros de alias y sin alias](#).

Temas

- [Política de direccionamiento](#)
- [Nombre del registro](#)
- [Tipo de registro](#)
- [Valor/ruta de destino del tráfico](#)
- [Region](#)
- [Chequeo de salud](#)
- [Evaluate target health](#)
- [ID de registro](#)

Política de direccionamiento

Elija Latency (Latencia).

Nombre del registro

Escriba el nombre del dominio o subdominio para el que desea dirigir el tráfico. El valor predeterminado es el nombre de la zona alojada.

Note

Si crea un registro con el mismo nombre que el de la zona alojada, no ingrese un valor (por ejemplo, un símbolo @) en el campo Record name (Nombre del registro).

Escriba el mismo nombre para todos los registros del grupo de registros de latencia.

Para obtener más información acerca de nombres de registro, consulte [Nombre del registro](#)

Tipo de registro

El tipo de registro de DNS. Para obtener más información, consulte [Tipos de registros de DNS admitidos](#).

Seleccione el valor aplicable en función del AWS recurso al que está enrutando el tráfico:

API regionales personalizadas o API optimizadas para bordes de API Gateway

Selecciona A — IPv4 dirección.

Puntos de conexión de interfaz de Amazon VPC

Seleccione A — IPv4 dirección.

CloudFront distribución

Seleccione A — IPv4 dirección.

Si IPv6 está habilitada para la distribución, cree dos registros, uno con el valor A (IPv4 dirección para el tipo) y otro con el valor AAAA (IPv6 dirección).

Servicio de App Runner

Seleccione A — dirección IPv4

Entorno de Elastic Beanstalk con subdominios regionalizados

Seleccione A — IPv4 dirección

Balanceador de carga de ELB

Seleccione la IPv4 dirección A o la dirección AAAA IPv6

Bucket de Amazon S3

Seleccione A — dirección IPv4

OpenSearch Servicio

Seleccione una IPv4 dirección o una dirección AAAA IPv6

Otro registro en esta zona alojada

Seleccione el tipo de registro para el que va a crear el alias. Se admiten todos los tipos, excepto NS y SOA.

 Note

Si va a crear un registro de alias con el mismo nombre que la zona alojada (lo que se conoce como ápex de zona), no podrá dirigir el tráfico a un registro en el que el valor de Type (Tipo) sea CNAME. Esto se debe a que el registro de alias debe tener el mismo tipo

que el registro al que está redirigiendo el tráfico y no es posible crear un registro CNAME para el ápex de zona (ni siquiera para un registro de alias).

Seleccione el mismo valor para todos los registros del grupo de registros de latencia.

Valor/ruta de destino del tráfico

El valor que elija de la lista o que escriba en el campo depende del AWS recurso al que dirija el tráfico.

Para obtener información sobre AWS los recursos a los que puede dirigirse, consulte [los valores comunes de los registros de alias a los que se dirige value/route el tráfico](#).

Para obtener más información sobre cómo configurar Route 53 para enrutar el tráfico a AWS recursos específicos, consulte [Enrutar el tráfico de Internet a sus AWS recursos](#).

Region

La EC2 región de Amazon en la que reside el recurso que especificó en este registro. Route 53 recomienda una EC2 región Amazon en función de otros valores que haya especificado. Esto también se aplica a las zonas alojadas privadas. Es recomendable que no cambie este valor.

Tenga en cuenta lo siguiente:

- Solo puedes crear un registro de latencia para cada EC2 región de Amazon.
- No es necesario que crees registros de latencia para todas las EC2 regiones de Amazon. Route 53 elige la región con la mejor latencia entre aquellas en las que creó registros de latencia.
- No puede crear registros sin latencia que tengan los mismos valores de Record name (Nombre del registro) y Record type (Tipo de registro) que los registros de latencia.
- Si crea un registro etiquetado con la región cn-north-1, Route 53 responderá siempre a las consultas procedentes de China utilizando este registro, independientemente de la latencia.

Para obtener más información acerca del uso de registros de latencia, consulte [Enrutado basado en latencia](#).

Chequeo de salud

Si desea que Route 53 verifique el estado de un punto de conexión dado y que solamente responda a las consultas de DNS utilizando este registro cuando el punto de conexión esté en buen estado, seleccione una comprobación de estado.

Route 53 no verifica el estado del punto de conexión especificado en el registro; por ejemplo, el punto de conexión que especifica la dirección IP en el campo Valor. Cuando se selecciona una comprobación de estado para un registro, Route 53 verifica el estado del punto de conexión especificado. Para obtener información sobre cómo Route 53 determina si un punto de conexión tiene un estado correcto, consulte [Cómo determina Amazon Route 53 si la comprobación de estado es correcta](#).

La asociación de una comprobación de estado a un conjunto de registros de recursos solo es útil cuando Route 53 elige entre dos o más registros para responder a una consulta de DNS y desea que Route 53 base la elección parcialmente en el estado de la comprobación de estado. Use las comprobaciones de estado solamente en las siguientes configuraciones:

- Está comprobando el estado de todos los registros de un grupo de registros que tienen el mismo nombre, tipo y política de enrutamiento (como los registros de conmutación por error o ponderados) y especifica la comprobación IDs de estado de todos los registros. Si en la comprobación de estado de un registro se especifica un punto de conexión que no está en buen estado, Route 53 deja de responder a las consultas mediante el valor de dicho registro.
- Seleccione Yes (Sí) en Evaluate Target Health (Evaluar el estado del destino) para un registro de alias o los registros de un grupo de alias de conmutación por error, alias de geolocalización, alias de latencia, alias basado en IP o registro de alias ponderado. Si los registros de alias hacen referencia a registros que no son alias en la misma zona alojada, también debe especificar comprobaciones de estado para estos últimos. Si asocia una comprobación de estado a un registro de alias y también selecciona Yes para Evaluate Target Health, ambos deben evaluarse como verdaderos. Para obtener más información, consulte [¿Qué sucede cuando se asocia una comprobación de estado a un registro de alias?](#).

Si en las comprobaciones de estado se especifica el punto de conexión solo por nombre de dominio, es recomendable crear una comprobación de estado independiente para cada punto de conexión. Por ejemplo, cree una comprobación de estado para cada servidor HTTP que sirva contenido de `www.ejemplo.com`. Para el valor de Domain name (Nombre de dominio), especifique el nombre de dominio del servidor (por ejemplo, `us-east-2-www.example.com`), no el nombre de los registros (`example.com`).

 Important

En esta configuración, si crea una comprobación de estado cuyo valor de Domain name (Nombre de dominio) coincide con el nombre de los registros y a continuación la asocia con estos, los resultados de la comprobación serán impredecibles.

Evaluate target health

Seleccione Sí, si desea que Route 53 determine si debe responder a las consultas de DNS mediante este registro al verificar el estado del recurso especificado mediante Punto de conexión.

Tenga en cuenta lo siguiente:

API Gateway personalizado, regional APIs y optimizado para entornos periféricos APIs

No existen requisitos especiales para establecer Evaluar estado del destino en Sí cuando el punto de conexión es una API regional personalizada o una API optimizada para periféricas de API Gateway.

CloudFront distribuciones

No puede establecer Evaluate Target Health en Sí cuando el punto final es una CloudFront distribución.

Entornos de Elastic Beanstalk que tienen subdominios regionalizados

Si especifica un entorno de Elastic Beanstalk en Endpoint y el entorno contiene un balanceador de cargas ELB, ELB direcciona las consultas únicamente a las instancias de Amazon en EC2 buen estado que estén registradas en el balanceador de cargas. (Un entorno contiene automáticamente un balanceador de cargas ELB si incluye más de una EC2 instancia de Amazon). Si estableces Evaluar el estado del objetivo en Sí y ninguna EC2 instancia de Amazon está en buen estado o el propio balanceador de carga no está en buen estado, Route 53 redirige las consultas a otros recursos disponibles que estén en buen estado, si los hay.

Si el entorno contiene una sola EC2 instancia de Amazon, no hay requisitos especiales.

Balanceadores de carga de ELB

El comportamiento de la comprobación de estado depende del tipo de balanceador de carga:

- Classic Load Balancers: si especificas un balanceador de carga clásico ELB en Endpoint, ELB dirige las consultas solo a las instancias de EC2 Amazon en buen estado que estén registradas

en el balanceador de cargas. Si estableces Evaluar el estado del objetivo en Sí y ninguna EC2 instancia está en buen estado o el propio balanceador de carga no está en buen estado, Route 53 redirige las consultas a otros recursos.

- Network Load Balancers y aplicaciones: si especifica un Network Load Balancers o aplicaciones ELB, y establece Evaluate target health (Evaluar estado del destino) en Yes (Sí), Route 53 dirige consultas al balanceador de carga en función del estado de los grupos de destino asociados al balanceador de carga:
 - Para que se considere que un Application Load Balancer o un Network Load Balancer está en buen estado, cada grupo de destinos que contenga destinos debe contener al menos un destino en buen estado. Si cualquier grupo de destinos contiene únicamente destinos en mal estado, se considera que el balanceador de carga está en mal estado y Route 53 envía las consultas a otros recursos.
 - Un grupo de destinos que no tiene destinos registrados se considera que no está en buen estado.

 Note

Al crear un balanceador de cargas, se configuran los ajustes para las comprobaciones de estado de ELB; no son comprobaciones de estado de Route 53, pero realizan una función similar. No cree comprobaciones de estado de Route 53 para las EC2 instancias que registre en un balanceador de cargas de ELB.

Buckets de S3

No existen requisitos especiales para establecer Evaluar estado del destino en Sí cuando el punto de conexión es un bucket de S3.

Puntos de enlace de interfaz de Amazon VPC

No existen requisitos especiales para establecer Evaluar estado del destino en Sí cuando el punto de conexión es uno de interfaz de Amazon VPC.

Otros registros de la misma zona alojada

Si el AWS recurso que especifica en Endpoint es un registro o un grupo de registros (por ejemplo, un grupo de registros ponderados) pero no es otro registro de alias, le recomendamos que asocie una comprobación de estado a todos los registros del punto final. Para obtener más información, consulte [¿Qué sucede cuando se omiten las comprobaciones de estado?](#).

ID de registro

Escriba un valor que identifique de manera exclusiva este registro en el grupo de registros de latencia.

Valores específicos para los registros basados en IP

Cuando se crean registros basados en IP, se especifican los siguientes valores.

Note

Aunque la creación de registros basados en IP en una zona alojada privada está permitida, no es compatible.

Temas

- [Política de direccionamiento](#)
- [Nombre del registro](#)
- [Tipo de registro](#)
- [TTL \(segundos\)](#)
- [Valor/ruta de destino del tráfico](#)
- [Ubicación](#)
- [Comprobación de estado](#)
- [ID de registro](#)

Política de direccionamiento

Elija IP-based (Basado en IP).

Nombre del registro

Escriba el nombre del dominio o subdominio para el que desea dirigir el tráfico. El valor predeterminado es el nombre de la zona alojada.

Note

Si crea un registro con el mismo nombre que el de la zona alojada, no ingrese un valor (por ejemplo, un símbolo @) en el campo Record name (Nombre del registro).

Ingresa el mismo nombre para todos los registros en el grupo de registros basados en IP.

Registros CNAME

Si crea un registro con el valor CNAME (CNAME) para Record type (Tipo de registro), el nombre del registro no puede ser el mismo que el de la zona alojada.

Caracteres especiales

Para obtener información sobre cómo especificar caracteres distintos de a-z, 0-9 y - (guion), y cómo especificar nombres de dominio internacionalizados, consulte [Formato de nombres de dominio DNS](#).

Caracteres comodín

Puede usar un asterisco (*) en el nombre. DNS trata el asterisco como comodín o como el carácter ASCII (42) *, en función de dónde aparece en el nombre. Para obtener más información, consulte [Uso de un asterisco \(*\) en nombres de zonas alojadas y registros](#).

Tipo de registro

El tipo de registro de DNS. Para obtener más información, consulte [Tipos de registros de DNS admitidos](#).

Seleccione el valor de Type (Tipo) en función de cómo desee que Route 53 responda a las consultas de DNS.

Seleccione el mismo valor para todos los registros del grupo de registros basados en IP.

TTL (segundos)

El tiempo, en segundos, en que desea que los solucionadores recursivos de DNS almacenen en caché información sobre este registro. Si especifica un valor más largo (por ejemplo, 172 800 segundos o dos días), se reduce el número de llamadas que los solucionadores recursivos de DNS deben realizar a Route 53 para obtener la información más reciente de este registro. Esto reduce la latencia y la factura del servicio Route 53. Para obtener más información, consulte [Cómo dirige Amazon Route 53 el tráfico de su dominio](#).

Sin embargo, si especifica un valor más largo para TTL, los cambios realizados en el registro (por ejemplo, una nueva dirección IP) tardarán más tiempo en surtir efecto, ya que los solucionadores recursivos usan los valores de la memoria caché durante periodos más largos antes de solicitar la información más reciente a Route 53. Si está cambiando la configuración de un dominio o subdominio que ya está en uso, le recomendamos que inicialmente especifique un valor más corto,

por ejemplo, 300 segundos y que aumente el valor después de confirmar que la configuración nueva es correcta.

Si asocia este registro a una comprobación de estado, es recomendable que especifique un TTL de 60 segundos o menos para que los clientes respondan rápidamente a los cambios de estado.

Valor/ruta de destino del tráfico

Elija IP address or another value depending on the record type (Dirección IP u otro valor en función del tipo de registro). Ingrese un valor que sea adecuado para el valor de Record type (Tipo de registro). Para todos los tipos excepto CNAME, puede escribir más de un valor. Escriba cada valor en una línea independiente.

Puede dirigir el tráfico a, o especificar los siguientes valores:

- A: dirección IPv
- AAAA: dirección IPv
- CAA: autorización de la entidad de certificación
- CNAME: nombre canónico
- MX: intercambio de correo
- NAPTR: señalizador de autoridad de asignación de nombres
- PTR: puntero
- SPF: marco de políticas de remitente
- SRV: localizador de servicios
- TXT: texto

Para más información acerca de los valores anteriores, consulte los [Valor/ruta de destino del tráfico valores comunes del valor/ruta de destino del tráfico](#).

Ubicación

El nombre de la ubicación CIDR donde se encuentra el recurso especificado en este registro por los valores del bloque CIDR dentro de la ubicación CIDR.

Para más información acerca del uso de los registros basados en IP, consulte [Direccionamiento basado en IP](#).

Comprobación de estado

Si desea que Route 53 verifique el estado de un punto de conexión dado y que solamente responda a las consultas de DNS utilizando este registro cuando el punto de conexión esté en buen estado, seleccione una comprobación de estado.

Route 53 no verifica el estado del punto de conexión especificado en el registro; por ejemplo, el punto de conexión que especifica la dirección IP en el campo Valor. Cuando se selecciona una comprobación de estado para un registro, Route 53 verifica el estado del punto de conexión especificado. Para obtener información sobre cómo Route 53 determina si un punto de conexión tiene un estado correcto, consulte [Cómo determina Amazon Route 53 si la comprobación de estado es correcta](#).

La asociación de una comprobación de estado a un conjunto de registros de recursos solo es útil cuando Route 53 elige entre dos o más registros para responder a una consulta de DNS y desea que Route 53 base la elección parcialmente en el estado de la comprobación de estado. Use las comprobaciones de estado solamente en las siguientes configuraciones:

- Va a comprobar el estado de todos los registros de un grupo de registros que tienen el mismo nombre, tipo y política de enrutamiento (como los registros de conmutación por error o ponderados) y especifica los identificadores de comprobación de estado de todos los registros. Si en la comprobación de estado de un registro se especifica un punto de conexión que no está en buen estado, Route 53 deja de responder a las consultas mediante el valor de dicho registro.
- Seleccione Yes (Sí) en Evaluate Target Health (Evaluar el estado del destino) para un registro de alias o los registros de un grupo de alias de conmutación por error, alias de geolocalización, alias basado en IP, alias de latencia o registro de alias ponderado. Si los registros de alias hacen referencia a registros que no son alias en la misma zona alojada, también debe especificar comprobaciones de estado para estos últimos. Si asocia una comprobación de estado a un registro de alias y también selecciona Yes para Evaluate Target Health, ambos deben evaluarse como verdaderos. Para obtener más información, consulte [¿Qué sucede cuando se asocia una comprobación de estado a un registro de alias?](#).

Si en las comprobaciones de estado se especifica el punto de conexión solo por nombre de dominio, es recomendable crear una comprobación de estado independiente para cada punto de conexión. Por ejemplo, cree una comprobación de estado para cada servidor HTTP que sirva contenido de `www.ejemplo.com`. Para el valor de Domain name (Nombre de dominio), especifique el nombre de dominio del servidor (por ejemplo, `us-east-2-www.example.com`), no el nombre de los registros (`example.com`).

 Important

En esta configuración, si crea una comprobación de estado cuyo valor de Domain name coincide con el nombre de los registros y luego la asocia con estos, los resultados de la comprobación serán impredecibles.

ID de registro

Ingresa un valor que identifique de manera única este registro en el grupo de registros basados en IP.

Valores específicos para los registros de alias basados en IP

Cuando se crean registros de alias basados en IP, se especifican los siguientes valores.

Note

Aunque la creación de registros de alias basados en IP en una zona alojada privada está permitida, no es compatible.

Para obtener más información, consulte [Elección entre registros de alias y sin alias](#).

Temas

- [Política de direccionamiento](#)
- [Nombre del registro](#)
- [Tipo de registro](#)
- [Valor/ruta de destino del tráfico](#)
- [Ubicación](#)
- [Chequeo de salud](#)
- [Evaluate target health](#)
- [ID de registro](#)

Política de direccionamiento

Elija IP-based (Basado en IP).

Note

Aunque la creación de registros de alias basados en IP en una zona alojada privada está permitida, no es compatible.

Nombre del registro

Escriba el nombre del dominio o subdominio para el que desea dirigir el tráfico. El valor predeterminado es el nombre de la zona alojada.

 Note

Si crea un registro con el mismo nombre que el de la zona alojada, no ingrese un valor (por ejemplo, un símbolo @) en el campo Record name (Nombre del registro).

Ingresa el mismo nombre para todos los registros en el grupo de registros basados en IP.

Registros CNAME

Si crea un registro con el valor CNAME (CNAME) para Record type (Tipo de registro), el nombre del registro no puede ser el mismo que el de la zona alojada.

Alias para CloudFront distribuciones y buckets de Amazon S3

El valor que especifique depende en parte del AWS recurso al que dirija el tráfico:

- CloudFront distribución: la distribución debe incluir un nombre de dominio alternativo que coincida con el nombre del registro. Por ejemplo, si el nombre del registro es acme.ejemplo.com, la distribución de CloudFront debe incluir acme.ejemplo.com como uno de los nombres de dominio alternativos. Para obtener más información, consulte [Uso de nombres de dominio alternativos \(CNAMEs\)](#) en la Guía para CloudFront desarrolladores de Amazon.
- Bucket de Amazon S3: el nombre del registro debe coincidir con el nombre del bucket de Amazon S3. Por ejemplo, si el nombre del bucket es acme.ejemplo.com, el nombre de este registro también debe ser acme.ejemplo.com.

Además, debe configurar el bucket para el hospedaje de sitio web. Para obtener más información, consulte [Configuración de un bucket para un alojamiento de sitio web](#) en la Guía del usuario de Amazon Simple Storage Service.

Caracteres especiales

Para obtener información sobre cómo especificar caracteres distintos de a-z, 0-9 y - (guion), y cómo especificar nombres de dominio internacionalizados, consulte [Formato de nombres de dominio DNS](#).

Caracteres comodín

Puede usar un asterisco (*) en el nombre. DNS trata el asterisco como comodín o como el carácter ASCII (42) *, en función de dónde aparece en el nombre. Para obtener más información, consulte [Uso de un asterisco \(*\) en nombres de zonas alojadas y registros](#).

Tipo de registro

El tipo de registro de DNS. Para obtener más información, consulte [Tipos de registros de DNS admitidos](#).

Seleccione el valor aplicable en función del AWS recurso al que está enrutando el tráfico. Seleccione el mismo valor para todos los registros del grupo de registros basados en IP:

API regionales personalizadas o API optimizadas para bordes de API Gateway

Selecciona A — IPv4 dirección.

Puntos de conexión de interfaz de Amazon VPC

Seleccione A — IPv4 dirección.

CloudFront distribución

Seleccione A — IPv4 dirección.

Si IPv6 está habilitada para la distribución, cree dos registros, uno con el valor A (IPv4 dirección de tipo) y otro con el valor AAAA (IPv6 dirección).

Servicio de App Runner

Seleccione A — dirección IPv4

Entorno de Elastic Beanstalk con subdominios regionalizados

Seleccione A — IPv4 dirección

Balanceador de carga de ELB

Seleccione la IPv4 dirección A o la dirección AAAA IPv6

Bucket de Amazon S3

Seleccione A — dirección IPv4

OpenSearch Servicio

Seleccione una IPv4 dirección o una dirección AAAA IPv6

Otro registro en esta zona alojada

Seleccione el tipo de registro para el que va a crear el alias. Se admiten todos los tipos, excepto NS y SOA.

 Note

Si va a crear un registro de alias con el mismo nombre que la zona alojada (lo que se conoce como ápex de zona), no podrá dirigir el tráfico a un registro en el que el valor de Type (Tipo) sea CNAME. Esto se debe a que el registro de alias debe tener el mismo tipo que el registro al que está redirigiendo el tráfico y no es posible crear un registro CNAME para el ápex de zona (ni siquiera para un registro de alias).

Valor/ruta de destino del tráfico

El valor que elija de la lista o que escriba en el campo depende del AWS recurso al que dirija el tráfico.

Para obtener información sobre AWS los recursos a los que puede dirigirse, consulte [los valores comunes de los registros de alias a los que se dirige value/route el tráfico](#).

Para obtener más información sobre cómo configurar Route 53 para enrutar el tráfico a AWS recursos específicos, consulte [Enrutar el tráfico de Internet a sus AWS recursos](#).

Ubicación

Cuando configure Route 53 para que responda a las consultas DNS en función de la ubicación desde la que se originan las consultas, seleccione la ubicación CIDR para la que desea que Route 53 responda con la configuración de este registro.

 Important

Le recomendamos que cree un registro basado en la IP que tenga el valor Default (Predeterminado) para Location (Ubicación). Esto cubre las ubicaciones geográficas para las que no se hayan creado registros y las direcciones IP para las que Route 53 no puede identificar la ubicación.

No puede crear non-IP-based registros que tengan los mismos valores de nombre y tipo de registro que los registros basados en IP.

Para obtener más información, consulte [Direccionamiento basado en IP](#).

Chequeo de salud

Si desea que Route 53 verifique el estado de un punto de conexión dado y que solamente responda a las consultas de DNS utilizando este registro cuando el punto de conexión esté en buen estado, seleccione una comprobación de estado.

Route 53 no verifica el estado del punto de conexión especificado en el registro; por ejemplo, el punto de conexión que especifica la dirección IP en el campo Valor. Cuando se selecciona una comprobación de estado para un registro, Route 53 verifica el estado del punto de conexión especificado. Para obtener información sobre cómo Route 53 determina si un punto de conexión tiene un estado correcto, consulte [Cómo determina Amazon Route 53 si la comprobación de estado es correcta](#).

La asociación de una comprobación de estado a un conjunto de registros de recursos solo es útil cuando Route 53 elige entre dos o más registros para responder a una consulta de DNS y desea que Route 53 base la elección parcialmente en el estado de la comprobación de estado. Use las comprobaciones de estado solamente en las siguientes configuraciones:

- Está comprobando el estado de todos los registros de un grupo de registros que tienen el mismo nombre, tipo y política de enrutamiento (como los registros de conmutación por error o ponderados) y especifica la comprobación IDs de estado de todos los registros. Si en la comprobación de estado de un registro se especifica un punto de conexión que no está en buen estado, Route 53 deja de responder a las consultas mediante el valor de dicho registro.
- Seleccione Yes (Sí) en Evaluate Target Health (Evaluar el estado del destino) para un registro de alias o los registros de un grupo de alias de conmutación por error, alias de geolocalización, alias basado en IP, alias de latencia o registro de alias ponderado. Si los registros de alias hacen referencia a registros que no son alias en la misma zona alojada, también debe especificar comprobaciones de estado para estos últimos. Si asocia una comprobación de estado a un registro de alias y también selecciona Yes para Evaluate Target Health, ambos deben evaluarse como verdaderos. Para obtener más información, consulte [¿Qué sucede cuando se asocia una comprobación de estado a un registro de alias?](#).

Si en las comprobaciones de estado se especifica el punto de conexión solo por nombre de dominio, es recomendable crear una comprobación de estado independiente para cada punto de conexión. Por ejemplo, cree una comprobación de estado para cada servidor HTTP que sirva contenido de `www.ejemplo.com`. Para el valor de Domain name (Nombre de dominio), especifique el nombre de dominio del servidor (por ejemplo, `us-east-2-www.example.com`), no el nombre de los registros (`example.com`).

 Important

En esta configuración, si crea una comprobación de estado cuyo valor de Domain name coincide con el nombre de los registros y luego la asocia con estos, los resultados de la comprobación serán impredecibles.

En el caso de los registros de alias basados en IP, si un punto de conexión no está en buen estado, Route 53 busca un registro dentro de la ubicación asociada más grande. Por ejemplo, supongamos que tiene registros para un estado en Estados Unidos, para Estados Unidos, para América del Norte y para todas las ubicaciones (Location (Ubicación) es Default (Predeterminada)). Si el punto de conexión del registro de estado no está en buen estado, Route 53 verifica los registros para Estados Unidos, para América del Norte y para todas las ubicaciones, en ese orden, hasta que encuentre un registro con un punto de conexión en buen estado. Si ninguno de los registros está en buen estado, incluido el registro de todas las ubicaciones, Route 53 responde a la consulta de DNS utilizando el valor del registro de la región geográfica más pequeña.

Evaluate target health

Seleccione Sí, si desea que Route 53 determine si debe responder a las consultas de DNS mediante este registro al verificar el estado del recurso especificado mediante Punto de conexión.

Tenga en cuenta lo siguiente:

API Gateway personalizado, regional APIs y optimizado para entornos periféricos APIs

No existen requisitos especiales para establecer Evaluar estado del destino en Sí cuando el punto de conexión es una API regional personalizada o una API optimizada para periféricas de API Gateway.

CloudFront distribuciones

No puede establecer Evaluar el estado del objetivo en Sí cuando el punto final es una CloudFront distribución.

Entornos de Elastic Beanstalk que tienen subdominios regionalizados

Si especifica un entorno de Elastic Beanstalk en Endpoint y el entorno contiene un balanceador de cargas ELB, ELB direcciona las consultas únicamente a las instancias de Amazon en EC2 buen estado que estén registradas en el balanceador de cargas. (Un entorno contiene automáticamente un balanceador de cargas ELB si incluye más de una EC2 instancia de

Amazon). Si estableces Evaluar el estado del objetivo en Sí y ninguna EC2 instancia de Amazon está en buen estado o el propio balanceador de carga no está en buen estado, Route 53 redirige las consultas a otros recursos disponibles que estén en buen estado, si los hay.

Si el entorno contiene una sola EC2 instancia de Amazon, no hay requisitos especiales.

Balanceadores de carga de ELB

El comportamiento de la comprobación de estado depende del tipo de balanceador de carga:

- **Classic Load Balancers:** si especificas un balanceador de carga clásico ELB en Endpoint, ELB dirige las consultas solo a las instancias de EC2 Amazon en buen estado que estén registradas en el balanceador de cargas. Si estableces Evaluar el estado del objetivo en Sí y ninguna EC2 instancia está en buen estado o el propio balanceador de carga no está en buen estado, Route 53 redirige las consultas a otros recursos.
- **Network Load Balancers y aplicaciones:** si especifica un Network Load Balancers o aplicaciones ELB, y establece Evaluate target health (Evaluar estado del destino) en Yes (Sí), Route 53 dirige consultas al balanceador de carga en función del estado de los grupos de destino asociados al balanceador de carga:
 - Para que se considere que un Application Load Balancer o un Network Load Balancer está en buen estado, cada grupo de destinos que contenga destinos debe contener al menos un destino en buen estado. Si cualquier grupo de destinos contiene únicamente destinos en mal estado, se considera que el balanceador de carga está en mal estado y Route 53 envía las consultas a otros recursos.
 - Un grupo de destinos que no tiene destinos registrados se considera que no está en buen estado.

Note

Al crear un balanceador de cargas, se configuran los ajustes para las comprobaciones de estado de ELB; no son comprobaciones de estado de Route 53, pero realizan una función similar. No cree comprobaciones de estado de Route 53 para las EC2 instancias que registre en un balanceador de cargas de ELB.

Buckets de S3

No existen requisitos especiales para establecer Evaluar estado del destino en Sí cuando el punto de conexión es un bucket de S3.

Puntos de enlace de interfaz de Amazon VPC

No existen requisitos especiales para establecer Evaluar estado del destino en Sí cuando el punto de conexión es uno de interfaz de Amazon VPC.

Otros registros de la misma zona alojada

Si el AWS recurso que especifica en Endpoint es un registro o un grupo de registros (por ejemplo, un grupo de registros ponderados) pero no es otro registro de alias, le recomendamos que asocie una comprobación de estado a todos los registros del punto final. Para obtener más información, consulte [¿Qué sucede cuando se omiten las comprobaciones de estado?](#).

ID de registro

Ingresa un valor que identifique de manera única este registro en el grupo de registros basados en IP.

Valores específicos de registros de respuesta de varios valores

Cuando se crean registros de respuesta de varios valores, hay que especificar los siguientes valores.

Note

No se permite la creación de alias de respuesta de varios valores.

Temas

- [Política de direccionamiento](#)
- [Nombre del registro](#)
- [Tipo de registro](#)
- [TTL \(segundos\)](#)
- [Valor/ruta de destino del tráfico](#)
- [Comprobación de estado](#)
- [ID de registro](#)

Política de direccionamiento

Elija Multivalue answer (Respuesta con varios valores).

Nombre del registro

Escriba el nombre del dominio o subdominio para el que desea dirigir el tráfico. El valor predeterminado es el nombre de la zona alojada.

Note

Si crea un registro con el mismo nombre que el de la zona alojada, no ingrese un valor (por ejemplo, un símbolo @) en el campo Record name (Nombre del registro).

Escriba el mismo nombre para todos los registros del grupo de registros de varios valores.

Para obtener más información acerca de nombres de registro, consulte [Nombre del registro](#).

Tipo de registro

El tipo de registro de DNS. Para obtener más información, consulte [Tipos de registros de DNS admitidos](#).

Seleccione cualquier valor excepto NS o CNAME.

Seleccione el mismo valor para todos los registros del grupo de registros de respuesta con varios valores.

TTL (segundos)

El tiempo, en segundos, en que desea que los solucionadores recursivos de DNS almacenen en caché información sobre este registro. Si especifica un valor más largo (por ejemplo, 172 800 segundos o dos días), se reduce el número de llamadas que los solucionadores recursivos de DNS deben realizar a Route 53 para obtener la información más reciente de este registro. Esto reduce la latencia y la factura del servicio Route 53. Para obtener más información, consulte [Cómo dirige Amazon Route 53 el tráfico de su dominio](#).

Sin embargo, si especifica un valor más largo para TTL, los cambios realizados en el registro (por ejemplo, una nueva dirección IP) tardarán más tiempo en surtir efecto, ya que los solucionadores recursivos usan los valores de la memoria caché durante periodos más largos antes de solicitar la información más reciente a Route 53. Si está cambiando la configuración de un dominio o subdominio que ya está en uso, le recomendamos que inicialmente especifique un valor más corto, por ejemplo, 300 segundos y que aumente el valor después de confirmar que la configuración nueva es correcta.

Si asocia este registro a una comprobación de estado, es recomendable que especifique un TTL de 60 segundos o menos para que los clientes respondan rápidamente a los cambios de estado.

Note

Si crea dos o más registros de respuesta con varios valores que tienen el mismo nombre y el mismo tipo, está usando la consola y especifica valores distintos para TTL, Route 53 cambia el valor de TTL de todos los registros al último valor especificado.

Valor/ruta de destino del tráfico

Elija IP address or another value depending on the record type (Dirección IP u otro valor en función del tipo de registro). Ingrese un valor que sea adecuado para el valor de Record type (Tipo de registro). Si escribe más de un valor, escriba cada uno en una línea independiente.

Puede dirigir el tráfico a, o especificar los siguientes valores:

- A: dirección IPv
- AAAA: dirección IPv
- CAA: autorización de la entidad de certificación
- MX: intercambio de correo
- NAPTR: señalizador de autoridad de asignación de nombres
- PTR: puntero
- SPF: marco de políticas de remitente
- SRV: localizador de servicios
- TXT: texto

Para más información acerca de los valores anteriores, consulte los [valores comunes del valor/ruta de destino del tráfico](#).

Comprobación de estado

Si desea que Route 53 verifique el estado de un punto de conexión dado y que solamente responda a las consultas de DNS utilizando este registro cuando el punto de conexión esté en buen estado, seleccione una comprobación de estado.

Route 53 no verifica el estado del punto de conexión especificado en el registro; por ejemplo, el punto de conexión que especifica la dirección IP en el campo Valor. Cuando se selecciona una comprobación de estado para un registro, Route 53 verifica el estado del punto de conexión especificado. Para obtener información sobre cómo Route 53 determina si un punto de conexión tiene un estado correcto, consulte [Cómo determina Amazon Route 53 si la comprobación de estado es correcta](#).

La asociación de una comprobación de estado a un conjunto de registros de recursos solo es útil cuando Route 53 elige entre dos o más registros para responder a una consulta de DNS y desea

que Route 53 base la elección parcialmente en el estado de la comprobación de estado. Use las comprobaciones de estado solamente en las siguientes configuraciones:

- Va a comprobar el estado de todos los registros de un grupo de registros que tienen el mismo nombre, tipo y política de enrutamiento (como los registros de conmutación por error o ponderados) y especifica los identificadores de comprobación de estado de todos los registros. Si en la comprobación de estado de un registro se especifica un punto de conexión que no está en buen estado, Route 53 deja de responder a las consultas mediante el valor de dicho registro.
- Ha seleccionado Yes (Sí) para Evaluate target health (Evaluar estado del destino) para un registro de alias o para los registros de un grupo de registros de alias de conmutación por error, alias de geolocalización, alias de latencia o alias ponderado. Si los registros de alias hacen referencia a registros que no son alias en la misma zona alojada, también debe especificar comprobaciones de estado para estos últimos. Si asocia una comprobación de estado a un registro de alias y también selecciona Yes para Evaluate Target Health, ambos deben evaluarse como verdaderos. Para obtener más información, consulte [¿Qué sucede cuando se asocia una comprobación de estado a un registro de alias?](#).

Si en las comprobaciones de estado se especifica el punto de conexión solo por nombre de dominio, es recomendable crear una comprobación de estado independiente para cada punto de conexión. Por ejemplo, cree una comprobación de estado para cada servidor HTTP que sirva contenido de `www.ejemplo.com`. Para el valor de Domain name (Nombre de dominio), especifique el nombre de dominio del servidor (por ejemplo, `us-east-2-www.example.com`), no el nombre de los registros (`example.com`).

Important

En esta configuración, si crea una comprobación de estado cuyo valor de Domain name coincide con el nombre de los registros y luego la asocia con estos, los resultados de la comprobación serán impredecibles.

ID de registro

Escriba un valor que identifique de manera exclusiva este registro en el grupo de registros de respuesta con varios valores.

Valores específicos de registros ponderados

Cuando se crean registros ponderados, hay que especificar los siguientes valores.

Temas

- [Política de direccionamiento](#)
- [Nombre del registro](#)
- [Tipo de registro](#)
- [TTL \(segundos\)](#)
- [Valor/ruta de destino del tráfico](#)
- [Peso](#)
- [Comprobación de estado](#)
- [ID de registro](#)

Política de direccionamiento

Seleccione Weighted (Ponderado).

Nombre del registro

Escriba el nombre del dominio o subdominio para el que desea dirigir el tráfico. El valor predeterminado es el nombre de la zona alojada.

Note

Si crea un registro con el mismo nombre que el de la zona alojada, no ingrese un valor (por ejemplo, un símbolo @) en el campo Record name (Nombre del registro).

Escriba el mismo nombre para todos los registros del grupo de registros ponderados.

Para obtener más información acerca de nombres de registro, consulte [Nombre del registro](#).

Tipo de registro

El tipo de registro de DNS. Para obtener más información, consulte [Tipos de registros de DNS admitidos](#).

Seleccione el mismo valor para todos los registros del grupo de registros ponderados.

TTL (segundos)

El tiempo, en segundos, en que desea que los solucionadores recursivos de DNS almacenen en caché información sobre este registro. Si especifica un valor más largo (por ejemplo, 172 800 segundos o dos días), se reduce el número de llamadas que los solucionadores recursivos de DNS deben realizar a Route 53 para obtener la información más reciente de este registro. Esto reduce la latencia y la factura del servicio Route 53. Para obtener más información, consulte [Cómo dirige Amazon Route 53 el tráfico de su dominio](#).

Sin embargo, si especifica un valor más largo para TTL, los cambios realizados en el registro (por ejemplo, una nueva dirección IP) tardarán más tiempo en surtir efecto, ya que los solucionadores recursivos usan los valores de la memoria caché durante periodos más largos antes de solicitar la información más reciente a Route 53. Si está cambiando la configuración de un dominio o subdominio que ya está en uso, le recomendamos que inicialmente especifique un valor más corto, por ejemplo, 300 segundos y que aumente el valor después de confirmar que la configuración nueva es correcta.

Si asocia este registro a una comprobación de estado, es recomendable que especifique un TTL de 60 segundos o menos para que los clientes respondan rápidamente a los cambios de estado.

Debe especificar el mismo valor de TTL para todos los registros de este grupo de registros ponderados.

Note

Si crea dos o más registros ponderados que tienen el mismo nombre y el mismo tipo, y especifica valores distintos para TTL (TTL), Route 53 cambia el valor de TTL (TTL) de todos los registros al último valor especificado.

Si un grupo de registros ponderados incluye uno o más registros de alias ponderados que dirigen tráfico a un balanceador de carga de ELB, es recomendable especificar un TTL de 60 segundos para todos los registros ponderados sin alias que tengan el mismo nombre y tipo. Los valores distintos de 60 segundos (el TTL de los equilibradores de carga) cambiarán el efecto de los valores que especifique para Weight (Ponderación).

Valor/ruta de destino del tráfico

Elija IP address or another value depending on the record type (Dirección IP u otro valor en función del tipo de registro). Ingrese un valor que sea adecuado para el valor de Record type (Tipo de

registro). Para todos los tipos excepto CNAME, puede escribir más de un valor. Escriba cada valor en una línea independiente.

Puede dirigir el tráfico a, o especificar los siguientes valores:

- A: dirección IPv
- AAAA: dirección IPv
- CAA: autorización de la entidad de certificación
- CNAME: nombre canónico
- MX: intercambio de correo
- NAPTR: señalizador de autoridad de asignación de nombres
- PTR: puntero
- SPF: marco de políticas de remitente
- SRV: localizador de servicios
- TXT: texto

Para más información acerca de los valores anteriores, consulte los [valores comunes del valor/ruta de destino del tráfico](#).

Peso

Un valor que determina la proporción de consultas de DNS a las que Route 53 responde usando el registro actual. Route 53 calcula la suma de las ponderaciones de los registros que tienen la misma combinación de nombre y tipo de DNS. Route 53 luego responde a las consultas en función de la proporción de la ponderación del recurso con el total.

No puede crear registros sin ponderación que tengan los mismos valores de Record name (Nombre del registro) y Record type (Tipo de registro) que los registros ponderados.

Escriba un número entero entre 0 y 255. Para deshabilitar el direccionamiento a un recurso, establezca Weight (Ponderación) en 0. Si establece Weight (Ponderación) en 0 para todos los registros del grupo, el tráfico se dirige a todos los recursos con una probabilidad equivalente. De este modo, se asegurará de que no desactivará por error el enrutamiento de un grupo de registros ponderados.

El efecto de establecer Weight (Ponderación) en 0 es diferente cuando se asocian comprobaciones de estado a los registros ponderados. Para obtener más información, consulte [Cómo elige Amazon Route 53 registros cuando está configurado la comprobación de estado](#).

Comprobación de estado

Si desea que Route 53 verifique el estado de un punto de conexión dado y que solamente responda a las consultas de DNS utilizando este registro cuando el punto de conexión esté en buen estado, seleccione una comprobación de estado.

Route 53 no verifica el estado del punto de conexión especificado en el registro; por ejemplo, el punto de conexión que especifica la dirección IP en el campo Valor. Cuando se selecciona una comprobación de estado para un registro, Route 53 verifica el estado del punto de conexión especificado. Para obtener información sobre cómo Route 53 determina si un punto de conexión tiene un estado correcto, consulte [Cómo determina Amazon Route 53 si la comprobación de estado es correcta](#).

La asociación de una comprobación de estado a un conjunto de registros de recursos solo es útil cuando Route 53 elige entre dos o más registros para responder a una consulta de DNS y desea que Route 53 base la elección parcialmente en el estado de la comprobación de estado. Use las comprobaciones de estado solamente en las siguientes configuraciones:

- Va a comprobar el estado de todos los registros de un grupo de registros que tienen el mismo nombre, tipo y política de enrutamiento (como los registros de conmutación por error o ponderados) y especifica los identificadores de comprobación de estado de todos los registros. Si en la comprobación de estado de un registro se especifica un punto de conexión que no está en buen estado, Route 53 deja de responder a las consultas mediante el valor de dicho registro.
- Seleccione Yes (Sí) en Evaluate Target Health (Evaluar el estado del destino) para un registro de alias o los registros de un grupo de alias de conmutación por error, alias de geolocalización, alias de latencia, alias basado en IP o registro de alias ponderado. Si los registros de alias hacen referencia a registros que no son alias en la misma zona alojada, también debe especificar comprobaciones de estado para estos últimos. Si asocia una comprobación de estado a un registro de alias y también selecciona Yes para Evaluate Target Health, ambos deben evaluarse como verdaderos. Para obtener más información, consulte [¿Qué sucede cuando se asocia una comprobación de estado a un registro de alias?](#).

Si en las comprobaciones de estado se especifica el punto de conexión solo por nombre de dominio, es recomendable crear una comprobación de estado independiente para cada punto de conexión.

Por ejemplo, cree una comprobación de estado para cada servidor HTTP que sirva contenido de `www.ejemplo.com`. Para el valor de Domain name (Nombre de dominio), especifique el nombre de dominio del servidor (por ejemplo, `us-east-2-www.example.com`), no el nombre de los registros (`example.com`).

 Important

En esta configuración, si crea una comprobación de estado cuyo valor de Domain name coincide con el nombre de los registros y luego la asocia con estos, los resultados de la comprobación serán impredecibles.

ID de registro

Escriba un valor que identifique de manera exclusiva este registro en el grupo de registros ponderados.

Valores específicos de registros de alias ponderados

Cuando se crean registros de alias ponderados, hay que especificar los siguientes valores. Para obtener más información, consulte [Elección entre registros de alias y sin alias](#).

Temas

- [Política de direccionamiento](#)
- [Nombre del registro](#)
- [Tipo de registro](#)
- [Valor/ruta de destino del tráfico](#)
- [Peso](#)
- [Health check](#)
- [Evaluate target health](#)
- [ID de registro](#)

Política de direccionamiento

Elija Weighted (Ponderada).

Nombre del registro

Escriba el nombre del dominio o subdominio para el que desea dirigir el tráfico. El valor predeterminado es el nombre de la zona alojada.

Note

Si crea un registro con el mismo nombre que el de la zona alojada, no escriba un valor (por ejemplo, un símbolo @) en el campo Name (Nombre).

Escriba el mismo nombre para todos los registros del grupo de registros ponderados.

Para obtener más información acerca de nombres de registro, consulte [Nombre del registro](#)

Tipo de registro

El tipo de registro de DNS. Para obtener más información, consulte [Tipos de registros de DNS admitidos](#).

Seleccione el valor aplicable en función del AWS recurso al que está enrutando el tráfico:

API regionales personalizadas o API optimizadas para bordes de API Gateway

Selecciona A — IPv4 dirección.

Puntos de conexión de interfaz de Amazon VPC

Seleccione A — IPv4 dirección.

CloudFront distribución

Seleccione A — IPv4 dirección.

Si IPv6 está habilitada para la distribución, cree dos registros, uno con el valor A (IPv4 dirección de tipo) y otro con el valor AAAA (IPv6 dirección).

Servicio de App Runner

Seleccione A — dirección IPv4

Entorno de Elastic Beanstalk con subdominios regionalizados

Seleccione A — IPv4 dirección

Balanceador de carga de ELB

Seleccione una IPv4 dirección O una dirección AAAA IPv6

Bucket de Amazon S3

Seleccione A — dirección IPv4

OpenSearch Servicio

Seleccione una IPv4 dirección o una dirección AAAA IPv6

Otro registro en esta zona alojada

Seleccione el tipo de registro para el que va a crear el alias. Se admiten todos los tipos, excepto NS y SOA.

 Note

Si va a crear un registro de alias con el mismo nombre que la zona alojada (lo que se conoce como ápex de zona), no podrá dirigir el tráfico a un registro en el que el valor de Type (Tipo) sea CNAME. Esto se debe a que el registro de alias debe tener el mismo tipo

que el registro al que está redirigiendo el tráfico y no es posible crear un registro CNAME para el ápex de zona (ni siquiera para un registro de alias).

Seleccione el mismo valor para todos los registros del grupo de registros ponderados.

Valor/ruta de destino del tráfico

El valor que elija de la lista o que escriba en el campo depende del AWS recurso al que dirija el tráfico.

Para obtener información sobre AWS los recursos a los que puede dirigirse, consulte [los valores comunes de los registros de alias a los que se dirige value/route el tráfico](#).

Para obtener más información sobre cómo configurar Route 53 para enrutar el tráfico a AWS recursos específicos, consulte [Enrutar el tráfico de Internet a sus AWS recursos](#).

Peso

Un valor que determina la proporción de consultas de DNS a las que Route 53 responde usando el registro actual. Route 53 calcula la suma de las ponderaciones de los registros que tienen la misma combinación de nombre y tipo de DNS. Luego, Route 53 responde a las consultas en función de la relación entre el peso de un recurso y el total.

No puede crear registros sin ponderación que tengan los mismos valores de Record name (Nombre del registro) y Record type (Tipo de registro) que los registros ponderados.

Escriba un número entero entre 0 y 255. Para deshabilitar el direccionamiento a un recurso, establezca Weight (Ponderación) en 0. Si establece Weight (Ponderación) en 0 para todos los registros del grupo, el tráfico se dirige a todos los recursos con una probabilidad equivalente. De este modo, se asegurará de que no desactivará por error el enrutamiento de un grupo de registros ponderados.

El efecto de establecer Weight (Ponderación) en 0 es diferente cuando se asocian comprobaciones de estado a los registros ponderados. Para obtener más información, consulte [Cómo elige Amazon Route 53 registros cuando está configurado la comprobación de estado](#).

Health check

Si desea que Route 53 verifique el estado de un punto de conexión dado y que solamente responda a las consultas de DNS utilizando este registro cuando el punto de conexión esté en buen estado, seleccione una comprobación de estado.

Route 53 no verifica el estado del punto de conexión especificado en el registro; por ejemplo, el punto de conexión que especifica la dirección IP en el campo Valor. Cuando se selecciona una comprobación de estado para un registro, Route 53 verifica el estado del punto de conexión especificado. Para obtener información sobre cómo Route 53 determina si un punto de conexión tiene un estado correcto, consulte [Cómo determina Amazon Route 53 si la comprobación de estado es correcta](#).

La asociación de una comprobación de estado a un conjunto de registros de recursos solo es útil cuando Route 53 elige entre dos o más registros para responder a una consulta de DNS y desea que Route 53 base la elección parcialmente en el estado de la comprobación de estado. Use las comprobaciones de estado solamente en las siguientes configuraciones:

- Está comprobando el estado de todos los registros de un grupo de registros que tienen el mismo nombre, tipo y política de enrutamiento (como los registros de conmutación por error o ponderados) y especifica la comprobación IDs de estado de todos los registros. Si en la comprobación de estado de un registro se especifica un punto de conexión que no está en buen estado, Route 53 deja de responder a las consultas mediante el valor de dicho registro.
- Seleccione Yes (Sí) en Evaluate Target Health (Evaluar el estado del destino) para un registro de alias o los registros de un grupo de alias de conmutación por error, alias de geolocalización, alias de latencia, alias basado en IP o registro de alias ponderado. Si los registros de alias hacen referencia a registros que no son alias en la misma zona alojada, también debe especificar comprobaciones de estado para estos últimos. Si asocia una comprobación de estado a un registro de alias y también selecciona Yes para Evaluate Target Health, ambos deben evaluarse como verdaderos. Para obtener más información, consulte [¿Qué sucede cuando se asocia una comprobación de estado a un registro de alias?](#).

Si en las comprobaciones de estado se especifica el punto de conexión solo por nombre de dominio, es recomendable crear una comprobación de estado independiente para cada punto de conexión. Por ejemplo, cree una comprobación de estado para cada servidor HTTP que sirva contenido de `www.ejemplo.com`. Para el valor de Domain name (Nombre de dominio), especifique el nombre de dominio del servidor (por ejemplo, `us-east-2-www.example.com`), no el nombre de los registros (`example.com`).

 Important

En esta configuración, si crea una comprobación de estado cuyo valor de Domain name coincide con el nombre de los registros y luego la asocia con estos, los resultados de la comprobación serán impredecibles.

Evaluate target health

Seleccione Sí, si desea que Route 53 determine si debe responder a las consultas de DNS mediante este registro al verificar el estado del recurso especificado mediante Punto de conexión.

Tenga en cuenta lo siguiente:

API Gateway personalizado, regional APIs y optimizado para entornos periféricos APIs

No existen requisitos especiales para establecer Evaluate target health (Evaluar estado del destino) en Yes (Sí) cuando el punto de conexión es una API regional personalizada o una API optimizada para bordes de API Gateway.

CloudFront distribuciones

No puede establecer Evaluar el estado del objetivo en Sí cuando el punto final es una CloudFront distribución.

Entornos de Elastic Beanstalk que tienen subdominios regionalizados

Si especifica un entorno de Elastic Beanstalk en Endpoint y el entorno contiene un balanceador de cargas ELB, ELB direcciona las consultas únicamente a las instancias de Amazon en EC2 buen estado que estén registradas en el balanceador de cargas. (Un entorno contiene automáticamente un balanceador de cargas ELB si incluye más de una EC2 instancia de Amazon). Si estableces Evaluar el estado del objetivo en Sí y ninguna EC2 instancia de Amazon está en buen estado o el propio balanceador de carga está en mal estado, Route 53 redirige las consultas a otros recursos disponibles que estén en buen estado, si los hay.

Si el entorno contiene una sola EC2 instancia de Amazon, no hay requisitos especiales.

Balanceadores de carga de ELB

El comportamiento de la comprobación de estado depende del tipo de balanceador de carga:

- Classic Load Balancers: si especificas un balanceador de carga clásico ELB en Endpoint, ELB dirige las consultas solo a las instancias de EC2 Amazon en buen estado que estén

registradas en el balanceador de cargas. Si establece Evaluate Target Health en Sí y ninguna EC2 instancia está en buen estado o el propio balanceador de carga no está en buen estado, Route 53 redirige las consultas a otros recursos.

- Balanceadores de carga de red y aplicaciones: si especifica un balanceador de carga de red o aplicaciones ELB, y establece Evaluate Target Health (Evaluar estado del destino) en Yes (Sí), Route 53 dirige consultas al balanceador de carga en función del estado de los grupos de destino asociados al balanceador de carga:
 - Para que se considere que un Application Load Balancer o un Network Load Balancer está en buen estado, cada grupo de destinos que contenga destinos debe contener al menos un destino en buen estado. Si cualquier grupo de destinos contiene únicamente destinos en mal estado, se considera que el balanceador de carga está en mal estado y Route 53 envía las consultas a otros recursos.
 - Un grupo de destinos que no tiene destinos registrados se considera que no está en buen estado.

Note

Al crear un balanceador de cargas, se configuran los ajustes para las comprobaciones de estado de ELB; no son comprobaciones de estado de Route 53, pero realizan una función similar. No cree comprobaciones de estado de Route 53 para las EC2 instancias que registre en un balanceador de cargas de ELB.

Buckets de S3

No existen requisitos especiales para establecer Evaluar estado del destino en Sí cuando el punto de conexión es un bucket de S3.

Puntos de enlace de interfaz de Amazon VPC

No existen requisitos especiales para establecer Evaluar estado del destino en Sí cuando el punto de conexión es uno de interfaz de Amazon VPC.

Otros registros de la misma zona alojada

Si el AWS recurso que especifica en Endpoint es un registro o un grupo de registros (por ejemplo, un grupo de registros ponderados) pero no es otro registro de alias, le recomendamos que asocie una comprobación de estado a todos los registros del punto final. Para obtener más información, consulte [¿Qué sucede cuando se omiten las comprobaciones de estado?](#).

ID de registro

Escriba un valor que identifique de manera exclusiva este registro en el grupo de registros ponderados.

Creación de registros mediante la importación de un archivo de zona

Si está migrando desde otro proveedor de servicios DNS, y si su proveedor de servicios DNS actual le permite exportar la configuración DNS actual a un archivo de zona, puede crear rápidamente todos los registros para una zona alojada de Amazon Route 53 importando un archivo de zona.

Note

Un archivo de zona utiliza un formato estándar conocido como BIND para representar registros en un formato de texto. Para obtener más información sobre el formato de un archivo de zona, consulte la página de Wikipedia [Zone file](#). Encontrará más información en [RFC 1034, Domain Names—Concepts and Facilities](#) (sección 3.6.1) y en [RFC 1035, Domain Names—Implementation and Specification](#) (sección 5).

Si desea crear registros importando un archivo de zona, tenga en cuenta lo siguiente:

- El archivo de zona debe estar en formato compatible con RFC.
- El nombre de dominio de los registros del archivo de zona debe coincidir con el nombre de la zona alojada.
- Route 53 es compatible con las palabras clave \$ORIGIN y \$TTL. Si el archivo de zona incluye las palabras clave \$GENERATE o \$INCLUDE, no se podrá realizar la importación y Route 53 devuelve un error.
- Al importar el archivo de zona, Route 53 ignora el registro de SOA del archivo de zona. Route 53 también ignora cualquier registro NS que tenga el mismo nombre que la zona alojada.
- Puede importar un máximo de 1000 registros.
- Si la zona alojada ya contiene registros que aparecen en el archivo de zona, se produce un error en el proceso de importación y no se crean registros.
- En el caso de los registros TXT que contienen caracteres de barra invertida, el proceso de importación del archivo de zona interpreta determinadas secuencias de barras invertidas como caracteres de control. Para incluir caracteres de barra invertida verdaderos en los valores de los registros TXT:

- Utilice barras invertidas dobles (\\) en el archivo de zona para representar verdaderamente una sola barra invertida en el registro TXT final.
- Por ejemplo, si el registro TXT debe contener \\jYTDWqH... (una barra invertida verdadera y j), especifique \\\jYTDWqH... en el archivo de zona.

Esto es especialmente importante para los registros de desafío de ACME y otros registros TXT que contienen verdaderamente caracteres de barra invertida.

- En el caso de los registros TXT largos (como los registros DKIM), el proceso de importación de archivos de zona permite dividir el contenido en varias cadenas. Para crear registros TXT con varias cadenas:
- Utilice líneas distintas en el archivo de zona con el mismo nombre y tipo de registro.

Example

```
example.com. 300 IN TXT "v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC"
example.com. 300 IN TXT
    "7fCC6C13dM9tXuJmUBH7D4Vw8y1ByJ8z9QX2fvLm3pN4sR5tU6vW7xY8zA9bC0dE1f"
example.com. 300 IN TXT
    "G2hI3jK4lM5n06pQ7rS8tU9vW0xY1zA2bC3dE4fG5hI6jK7lM8n09pQ0rS1tU2vW3x"
```

El proceso de importación los combina automáticamente en un único registro TXT con varias cadenas. Cada cadena individual puede contener hasta 65 535 caracteres. No concatene cadenas largas en un solo valor entre comillas.

- Le recomendamos que revise el contenido del archivo de zona para confirmar que los nombres de registro incluyen o excluyen un punto final según corresponda:
- Cuando el nombre de un registro del archivo de zona incluye un punto final (example.com.), la importación lo interpreta como un nombre de dominio completo y crea un registro de Route 53 con ese nombre.
- Si el nombre de un registro del archivo de zona no lleva un punto final (www), el proceso de importación lo concatena con el nombre del dominio del archivo de zona (example.com) y crea un registro de Route 53 con el nombre concatenado (www.example.com).

Si el proceso de exportación no agrega un punto final a los nombres de dominio completos de un registro, el proceso de importación de Route 53 agregará el nombre de dominio al nombre del registro. Por ejemplo, suponga que está importando registros a la zona alojada example.com y el nombre de un registro MX del archivo de zona es mail.example.com,

sin punto final. El proceso de importación de Route 53 crea un registro MX denominado `mail.example.com.example.com`.

 Important

Para los registros CNAME, MX, PTR y SRV, este comportamiento también se aplica al nombre de dominio que se incluye en el valor de RDATA. Por ejemplo, supongamos que tiene un archivo de zona para `example.com`. Si un registro CNAME del archivo de zona (`support`, sin punto final) tiene un valor de RDATA de `www.example.com` (también sin punto final), el proceso de importación crea un registro de Route 53 con el nombre `support.example.com`, que dirige el tráfico a `www.example.com.example.com`. Antes de importar su archivo de zona, revise los valores RDATA y actualícelos si es necesario. En el caso de los registros TXT que contienen barras invertidas, utilice barras invertidas dobles (`\\`) en el archivo de zona para representar realmente barras invertidas.

Route 53 no admite la exportación de registros a un archivo de zona.

 Note

Si crea un registro con el mismo nombre que el de la zona alojada, no escriba un valor (por ejemplo, un símbolo `@`) en el campo Name (Nombre).

Para crear registros mediante la importación de un archivo de zona

1. Obtener un archivo de zona del proveedor de servicios DNS que administra el dominio actualmente. El proceso y la terminología varían de un proveedor de servicios a otro. Consulte la interfaz y la documentación de su proveedor para saber cómo exportar o guardar sus registros en un archivo de zona o un archivo BIND.

Si el proceso no es evidente, solicite al servicio de soporte de su proveedor de DNS actual la información sobre su lista de recursos o su archivo de zona.

2. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
3. En el panel de navegación, elija Zonas alojadas.

4. En la página Zonas alojadas, cree una zona alojada:
 - a. Elija Crear zona alojada.
 - b. Escriba el nombre de su dominio y, opcionalmente, un comentario.
 - c. Elija Create (Crear).
5. Elija Import zone file (Importar archivo de zona).
6. En el panel Import zone file (Importar archivo de zona), pegue el contenido de su archivo de zona en el cuadro de texto Zone file (Archivo de zona).
7. Seleccione Importar.

 Note

En función de la cantidad de registros de su archivo de zona, es posible que tenga que esperar unos minutos hasta que se creen dichos registros.

8. Si utiliza otro servicio DNS para el dominio (algo habitual si registró el dominio con otro registrador), migre el servicio DNS a Route 53. Cuando se haya completado ese paso, el registrador comenzará a identificar Route 53 como su servicio DNS en respuesta a las consultas de DNS para su dominio, y las consultas comenzarán a enviarse a los servidores DNS de Route 53. (En general, pasan uno o dos días hasta que las consultas de DNS comienzan a dirigirse a Route 53, porque los solucionadores de DNS almacenan en su caché la información sobre su servicio DNS anterior todo ese tiempo). Para obtener más información, consulte [Establecer Amazon Route 53 como servicio DNS de un dominio existente](#).

Editar registros

En el siguiente procedimiento se explica cómo editar registros mediante la consola de Amazon Route 53. Para obtener información sobre cómo editar registros mediante la API de Route 53, consulte la referencia [ChangeResourceRecordSets](#) de la API de Amazon Route 53.

 Note

Sus cambios en los registros tardan tiempo en propagarse en los servidores DNS de Route 53. Actualmente, la única forma de comprobar que los cambios se han propagado es mediante la acción de la [GetChange](#) API. Por lo general, los cambios se propagan a todos los servidores de Route 53 en un plazo de 60 segundos.

Edición de registros mediante la consola de Route 53

1. Si no está editando registros de alias, vaya al paso 2.

Si está editando registros de alias que redirigen el tráfico a un ELB Classic Load Balancer, Application Load Balancer o Network Load Balancer, y si creó la zona alojada de Route 53 y el balanceador de carga con cuentas diferentes, lleve a cabo [Obtener el nombre del DNS para un balanceador de carga ELB](#) el procedimiento para obtener el nombre DNS del balanceador de carga.

Si está editando los registros de alias de cualquier otro AWS recurso, vaya al paso 2.

2. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
3. En el panel de navegación, elija Crear zona alojada.
4. En la página Zonas alojadas, elija la fila de la zona alojada que contiene los registros que desea editar.
5. Seleccione la fila del registro que desea editar y, a continuación, ingrese los cambios en el panel Edit record (Editar registro).
6. Ingrese los valores aplicables. Para obtener más información, consulte [Valores que hay que especificar al crear o editar los registros de Amazon Route 53](#).
7. Elija Save changes (Guardar cambios).
8. Si está editando varios registros, repita los pasos 5 a 7.

Eliminar registros

En el siguiente procedimiento, se explica cómo eliminar registros mediante la consola de Route 53. Para obtener información sobre cómo eliminar registros mediante la API de Route 53, consulte la referencia [ChangeResourceRecordSets](#) de la API de Amazon Route 53.

Note

Sus cambios en los registros tardan tiempo en propagarse en los servidores DNS de Route 53. Actualmente, la única forma de comprobar que los cambios se han propagado es mediante la acción de la [GetChange](#) API. Por lo general, los cambios se propagan a todos los servidores de Route 53 en un plazo de 60 segundos.

Para eliminar registros

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En la página Zonas alojadas, elija la fila de la zona alojada que contiene los registros que desea eliminar.
3. En la lista de registros, seleccione el registro que desea eliminar.

Para seleccionar varios registros consecutivos, elija la primera fila, mantenga pulsada la tecla Mayús y elija la última fila. Para seleccionar varios registros no consecutivos, elija la primera fila, mantenga pulsada la tecla Ctrl y elija las demás filas.

No puede eliminar los registros que tengan el valor NS o SOA en Type (Tipo).

4. Elija Eliminar.
5. Elija Delete (Eliminar) para cerrar el cuadro de diálogo.

Descripción de registros

En el siguiente procedimiento se explica cómo enumerar los registros de una zona alojada mediante la consola de Amazon Route 53. Para obtener información sobre cómo enumerar registros mediante la API de Route 53, consulte [ListResourceRecordSets](#) la referencia de la API de Amazon Route 53.

Para enumerar los registros

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Zonas alojadas.
3. En la página Zonas alojadas, elija el nombre de una zona alojada nueva.
4. Para cambiar el modo de búsqueda, seleccione el ícono de engranaje en la esquina superior derecha de la tabla Registros. Elija una de las siguientes opciones:

- Automático

Con este modo, el servicio utiliza un filtro basado en varios registros. Completo para menos de 2000 y rápido para más de 2000 registros.

- Completo

Con este modo, todos los filtros de búsqueda están disponibles, pero es posible que el rendimiento de la búsqueda sea más lento.

- **Rápido**

Con este modo, algunas características avanzadas no están disponibles, pero el rendimiento de la búsqueda será más rápido.

Para visualizar únicamente registros seleccionados, escriba los criterios de búsqueda sobre la lista de registros. En el modo automático, el comportamiento de búsqueda depende de si la zona alojada contiene hasta 2000 registros o más de 2000 registros:

Hasta 2000 registros y modo completo

- Para visualizar los registros que tengan valores específicos, ingrese un valor en la barra de búsqueda y luego pulse Entrar. Por ejemplo, para mostrar los registros que tengan una dirección IP que empiece por 192.0, escriba el valor en el campo Search (Buscar) y pulse Enter (Intro).
- Para visualizar solo los registros que tengan el mismo tipo de registro de DNS, seleccione Record type (Tipo de registro) en la lista desplegable e ingrese el tipo de registro.
- Para visualizar únicamente registros de alias, seleccione Alias (Alias) en la lista desplegable e ingrese **Yes**.
- Para visualizar únicamente registros ponderados, seleccione Routing policy (Política de direccionamiento) en la lista desplegable e ingrese **WEIGHTED**.

Más de 2000 registros y modo rápido

- Puede buscar solo en los nombres de registro, no en los valores de registro. Tampoco puede filtrar en función del tipo de registro o en los registros de alias o ponderados.

Para ello, coloque el cursor en el cuadro de texto Filtro, seleccione Propiedades y, a continuación, Nombre del registro.

- En el caso de los registros que tienen tres etiquetas (tres partes separadas por puntos), al escribir un valor en el campo de búsqueda y pulsar Entrar, la consola de Route 53 realiza automáticamente una búsqueda de comodín en la tercera etiqueta desde la derecha del nombre de registro. Por ejemplo, suponga que la zona alojada example.com contiene 100 registros denominados record1.example.com a record100.example.com. (Record1 es la tercera etiqueta desde la derecha). A continuación se indica lo que sucede cuando se busca en los siguientes valores:

- `record1`: la consola de Route 53 busca `record1*.example.com` (`record1*.example.com`), que devuelve `record1.example.com` (`record1.example.com`), `record10.example.com` (`record10.example.com`) a través de `record19.example.com` (`record19.example.com`) y `record100.example.com` (`record100.example.com`).
- `record1.example.com`: como en el ejemplo anterior, la consola busca `record1*.example.com` (`record1*.example.com`) y devuelve los mismos registros.
- `1 (1)`: la consola busca `1*.example.com` (`1*.example.com`) y no devuelve ningún registro.
- `example` (ejemplo): la consola busca `example*.example.com` (`example*.example.com`) y no devuelve ningún registro.
- `example.com` (`example.com`): en este ejemplo, la consola no realiza una búsqueda de comodín. Devuelve todos los registros de la zona alojada.
- Modo de búsqueda automática: cuando utilice este modo de búsqueda, primero debe proporcionar una propiedad, como el nombre del registro, para poder realizar la búsqueda.

 Note

Si la tercera etiqueta desde la derecha contiene uno o varios guiones (como, por ejemplo `third-label.example.com`) y si busca la parte de la tercera etiqueta justo delante del guion (`third`, en este ejemplo), Route 53 no devolverá ningún registro. En su lugar, incluya el guion (busque `third-`) u omita el carácter que aparece justo delante de este (busque `third`).

- En el caso de los registros que tienen cuatro o más etiquetas, debe especificar el nombre exacto del registro. No se admiten las búsquedas de comodín. Por ejemplo, si la zona alojada incluye un registro llamado `label4.record1.example.com`, puede encontrarlo solo si especifica `label4.record1.example.com` en el campo de búsqueda.

Configuración de la firma de DNSSEC en Amazon Route 53

La firma de extensiones de seguridad del sistema de nombres de dominio (DNSSEC: Domain Name System Security Extensions), permite a los solucionadores de DNS validar que una respuesta DNS proviene de Amazon Route 53 y que no se ha manipulado. Cuando utiliza la firma de DNSSEC, cada respuesta para una zona alojada se firma utilizando criptografía de clave pública. Para obtener información general sobre DNSSEC, consulte la sección DNSSEC de [AWS re:Invent 2021 - Amazon Route 53: A year in review](#).

En este capítulo, explicamos cómo habilitar la firma de DNSSEC para Route 53, cómo trabajar con las claves de firma de claves (KSKs) y cómo solucionar problemas. Puede trabajar con la firma de DNSSEC en la API o mediante programación con ella. Consola de administración de AWS Para obtener más información sobre el uso de la CLI o SDKs el trabajo con Route 53, consulte [Configuración de Amazon Route 53](#).

Antes de habilitar la firma de DNSSEC, tenga en cuenta lo siguiente:

- Para ayudar a evitar una interrupción de la zona y problemas de que el dominio deje de estar disponible, debe abordar y resolver rápidamente los errores de DNSSEC. Le recomendamos encarecidamente que configure una CloudWatch alarma que le avise cada vez que se detecte un `DNSSECKeySigningKeysNeedingAction` error `DNSSECInternalFailure` o error. Para obtener más información, consulte [Supervisión de zonas alojadas mediante Amazon CloudWatch](#).
- En las DNSSEC hay dos tipos de claves: la clave de firma de claves (KSK) y la clave de firma de zonas (ZSK). En la firma de DNSSEC de Route 53, cada KSK se basa en una [clave asimétrica administrada por el cliente](#) en AWS KMS que posea. Usted es responsable de la administración de la KSK, lo que incluye su rotación, en caso de que sea necesario. Route 53 lleva a cabo la administración de ZSK.
- Cuando habilita la firma de DNSSEC para una zona alojada, Route 53 limita el TTL a una semana. Si establece un TTL de más de una semana para los registros de la zona alojada, no aparece ningún error. No obstante, Route 53 impone un TTL de una semana para los registros. Los registros que tienen un TTL de menos de una semana y los registros en otras zonas alojadas que no tienen habilitadas la firma DNSSEC no se ven afectados.
- Cuando utiliza la firma de DNSSEC, no se admiten configuraciones de varios proveedores. Si ha configurado servidores de nombres de etiqueta blanca (también conocidos como servidores de nombres personalizados o de nombres privados), asegúrese de que estos los proporcione un único proveedor de DNS.
- Algunos proveedores de DNS no admiten registros de firmantes de delegación (DS) en su DNS autoritativo. Si su zona principal está alojada en un proveedor de DNS que no admite consultas de DS (no establece un indicador AA en la respuesta a la consulta de DS), cuando habilite DNSSEC en su zona secundaria, esta no se podrá resolver. Asegúrese de que su proveedor de DNS admita los registros de DS.
- Puede ser útil configurar permisos de IAM para permitir que otro usuario, además del propietario de la zona, agregue o elimine registros en la zona. Por ejemplo, un propietario de zona puede agregar una KSK y habilitar la firma y también puede ser responsable de la rotación de claves. No obstante, otra persona podría ser responsable de trabajar con otros registros para la zona alojada.

Para ver una política de IAM de ejemplo, consulte [Permisos de ejemplo para el propietario de un registro de dominio](#).

- Para comprobar si el TLD es compatible con DNSSEC, consulte [Dominios que puede registrar con Amazon Route 53](#).

Temas

- [Activar la firma de DNSSEC y establecer una cadena de confianza](#)
- [Desactivar la firma de DNSSEC](#)
- [Trabajar con claves administradas por el cliente para DNSSEC](#)
- [Trabajar con claves de firma de claves \(\) KSKs](#)
- [Administración de claves KMS y ZSK en Route 53](#)
- [Pruebas de inexistencia de DNSSEC en Route 53](#)
- [Solución de problemas de firma de DNSSEC](#)

Activar la firma de DNSSEC y establecer una cadena de confianza

Los pasos progresivos se aplican al propietario de la zona alojada y al encargado de la zona principal. Puede ser la misma persona, pero si no, el propietario de la zona debe notificar y trabajar con el responsable de la zona principal.

Recomendamos seguir los pasos de este artículo para que su zona se firme e incluya en la cadena de confianza. Los siguientes pasos minimizarán el riesgo de incorporación a DNSSEC.

Note

Asegúrese de leer los requisitos previos antes de comenzar en [Configuración de la firma de DNSSEC en Amazon Route 53](#).

Hay tres pasos que deben realizar para habilitar la firma de DNSSEC, que se describe en las secciones siguientes.

Temas

- [Paso 1: Preparación para activar la firma de DNSSEC](#)
- [Paso 2: Habilitar la firma DNSSEC y crear un KSK](#)

- [Paso 3: Establecer una cadena de confianza](#)

Paso 1: Preparación para activar la firma de DNSSEC

Los pasos de preparación ayudan a minimizar el riesgo de incorporación a DNSSEC mediante la supervisión de la disponibilidad de la zona y la reducción de los tiempos de espera entre activar la firma y la inserción del registro firmante de delegación (DS).

Para prepararse para activar la firma DNSSEC

1. Supervisar la disponibilidad de zonas.

Puede supervisar la zona para comprobar la disponibilidad de sus nombres de dominio. Esto puede ayudarle a solucionar cualquier problema que pueda justificar retroceder un paso atrás después de habilitar la firma DNSSEC. Puede supervisar los nombres de dominio con la mayor parte del tráfico mediante el registro de consultas. Para obtener más información sobre la configuración del registro de consultas, consulte [Monitoreo de Amazon Route 53](#).

La supervisión se puede realizar a través de un script de shell o mediante un servicio de terceros. Sin embargo, no debería ser la única señal para determinar si se requiere una reversión. Es posible que también reciba comentarios de sus clientes debido a que un dominio no está disponible.

2. Reduzca el TTL máximo de la zona.

El TTL máximo de la zona es el registro TTL más largo de la zona. En la siguiente zona de ejemplo, el TTL máximo de la zona es de 1 día (86 400 segundos).

Name	TTL	Clase de registro	Tipo de registro	Registro de datos
ejemplo.com.	900	IN	SOA	ns1.ejemplo.com. hostmaster.ejemplo.com. 200202240 1 10800 15 604800 300

Name	TTL	Clase de registro	Tipo de registro	Registro de datos
ejemplo.com.	900	IN	NS	ns1.ejemplo.com.
route53.ejemplo.com.	86400	IN	TXT	some txt record

La reducción del TTL máximo de la zona ayudará a reducir el tiempo de espera entre activar la firma y la inserción del registro firmante de delegación (DS). Recomendamos reducir el TTL máximo de la zona a 1 hora (3600 segundos). Esto le permite retroceder después de solo una hora si algún solucionador tiene problemas para almacenar en caché los registros firmados.

Reversión: deshacer los cambios TTL.

3. Reduzca el campo mínimo de SOA TTL y de SOA.

El campo mínimo de SOA es el último campo de los datos de registro SOA. En el siguiente registro SOA de ejemplo, el campo mínimo tiene el valor de 5 minutos (300 segundos).

Name	TTL	Clase de registro	Tipo de registro	Registro de datos
ejemplo.com.	900	IN	SOA	ns1.ejemplo.com. hostmaster.ejemplo.com. 200202240 1 10800 15 604800 300

El campo mínimo de SOA TTL y de SOA determina cuánto tiempo los solucionadores recuerdan las respuestas negativas. Después de habilitar la firma, los servidores de nombres de Route 53 empiezan a devolver registros NSEC para obtener respuestas negativas. El NSEC contiene

información que los solucionadores pueden utilizar para sintetizar una respuesta negativa. Si tiene que retroceder porque la información de NSEC provocó que un solucionador asuma una respuesta negativa para un nombre, solo tendrá que esperar el máximo del campo mínimo TTL de SOA y de SOA para que el solucionador filtre las palabras irrelevantes.

Reversión: deshacer los cambios de SOA.

4. Asegúrese de que los cambios mínimos de campo TTL y de SOA sean efectivos.

Úselo [GetChange](#) para asegurarse de que los cambios realizados hasta ahora se hayan propagado a todos los servidores DNS de Route 53.

Paso 2: Habilitar la firma DNSSEC y crear un KSK

Puede habilitar la firma de DNSSEC y crear una clave de firma de claves (KSK) mediante la consola de Route 53 AWS CLI o en ella.

- [CLI](#)
- [Consola](#)

Cuando proporciona o crea una clave de KMS, existen varios requisitos. Para obtener más información, consulte [Trabajar con claves administradas por el cliente para DNSSEC](#).

CLI

Puede utilizar una clave que ya tenga o crear una ejecutando un AWS CLI comando como el siguiente utilizando sus propios valores para `hostedzone_id`, `cmk_arn`, `ksk_name`, y `unique_string` (para que la solicitud sea única):

```
aws --region us-east-1 route53 create-key-signing-key \
  --hosted-zone-id $hostedzone_id \
  --key-management-service-arn $cmk_arn --name $ksk_name \
  --status ACTIVE \
  --caller-reference $unique_string
```

Para obtener más información sobre las claves administradas por el cliente, consulte [Trabajar con claves administradas por el cliente para DNSSEC](#). Véase también [CreateKeySigningKey](#).

Para habilitar la firma de DNSSEC, ejecute un AWS CLI comando como el siguiente, utilizando su propio valor para: `hostedzone_id`

```
aws --region us-east-1 route53 enable-hosted-zone-dnssec \  
--hosted-zone-id $hostedzone_id
```

[Para obtener más información, consulte `enable-hosted-zone-dnssec` y `EnableHostedZone DNSSEC`.](#)

Console

Para habilitar la firma de DNSSEC y crear una KSK

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/route53/>
2. En el panel de navegación, elija Hosted zones (Zonas alojadas) y elija una zona alojada para la que desea habilitar la firma de DNSSEC.
3. En la página DNSSEC, elija Enable DNSSEC signing (Habilitar firma de DNSSEC).

Note

Si la opción de esta sección es Disable DNSSEC signing (Desactivar la firma DNSSEC), ya ha completado el primer paso para activar la firma de DNSSEC. Para terminar, asegúrese de establecer, o de que ya exista, una cadena de confianza para la zona alojada para DNSSEC. Para obtener más información, consulte [Paso 3: Establecer una cadena de confianza](#).

4. En la sección Key-signing key (KSK) creation (Creación de clave de la firma de clave), elija Provide KSK name (Crear nuevo KSK) y en Provide KSK name (Proporcione el nombre de KSK), ingrese un nombre para el KSK que Route 53 creará para usted. Los nombres pueden contener letras, números y guiones bajos (_). Deben ser únicos.
5. En Customer managed CMK (CMK administrada por el cliente), elija la clave administrada por el cliente que debe utilizar Route 53 al crear la KSK por usted. Puede usar una clave administrada por el cliente aplicada a la firma de DNSSEC o crear una nueva clave administrada por el cliente.

Cuando proporciona o crea una clave administrada por el cliente, existen varios requisitos. Para obtener más información, consulte [Trabajar con claves administradas por el cliente para DNSSEC](#).

6. Ingrese el alias de una clave administrada por el cliente existente. Si desea utilizar una nueva clave administrada por el cliente, ingrese un alias para una clave administrada por el cliente y Route 53 creará una para usted.

 Note

Si elige que Route 53 cree una clave administrada por el cliente, tenga en cuenta que se aplican cargos aparte por cada clave administrada por el cliente. Para obtener más información, consulte [Precios de AWS Key Management Service](#).

7. Elija Enable DNSSEC signing (Habilitar firma de DNSSEC).

Después de habilitar la firma de zona, complete los pasos siguientes (si ha utilizado la consola o la CLI):

1. Asegúrese de que la firma de zona sea efectiva.

Si la usó AWS CLI, puede usar el identificador de operación que aparece en el resultado de la `EnableHostedZoneDNSSEC()` llamada para ejecutar [get-change](#) o [GetChange](#) para asegurarse de que todos los servidores DNS de Route 53 firmen las respuestas (status =INSYNC).

2. Espere al menos el TTL máximo de la zona anterior.

Espere a que los solucionadores eliminen todos los registros sin firmar de su caché. Para lograrlo, debe esperar al menos el TTL máximo de la zona anterior. En la zona `example.com` anterior, el tiempo de espera sería de 1 día.

3. Supervisar los informes de problemas de los clientes.

Una vez habilitada la firma de zona, es posible que sus clientes empiecen a ver problemas relacionados con los dispositivos de red y los solucionadores. El período de supervisión recomendado es de 2 semanas.

A continuación, se muestra un ejemplo de cómo podría hacerlo:

- Algunos dispositivos de red pueden limitar el tamaño de la respuesta DNS a menos de 512 bytes, lo que es demasiado pequeño para algunas respuestas firmadas. Estos dispositivos de red deben reconfigurarse para permitir tamaños de respuesta DNS más grandes.

- Algunos dispositivos de red realizan una inspección profunda de las respuestas DNS y eliminan ciertos registros que no entienden, como los utilizados para DNSSEC. Estos dispositivos deben volver a configurarse.
- Los solucionadores de algunos clientes afirman que pueden aceptar una respuesta UDP mayor que la que admite su red. Puede probar la capacidad de red y configurar los solucionadores de forma adecuada. Para obtener más información, consulte [Servidor de prueba de tamaño de respuesta DNS](#).

Reversión: llame a [DisableHostedZoneDNSSEC](#) y, a continuación, revierta los pasos anteriores.

[Paso 1: Preparación para activar la firma de DNSSEC](#)

Paso 3: Establecer una cadena de confianza

Tras habilitar la firma de DNSSEC para una zona alojada en Route 53, establezca una cadena de confianza para esa zona alojada para completar la configuración de firma de DNSSEC. Para ello, cree un registro de Delegation Signer (DS) en la zona alojada principal para su zona alojada utilizando la información que proporciona Route 53. En función de dónde esté registrado su dominio, agregue el registro a la zona alojada principal en Route 53 o en otro registrador de dominios.

Para establecer una cadena de confianza para la firma de DNSSEC

1. Inicie sesión en la consola de Route Consola de administración de AWS 53 y ábrala en. <https://console.aws.amazon.com/route53/>
2. En el panel de navegación, elija Hosted zones (Zonas alojadas) y elija una zona alojada para la que desea establecer la cadena de confianza de DNSSEC. Debe habilitar primero la firma de DNSSEC.
3. En la pestaña DNSSEC signing (Firma de DNSSEC), en DNSSEC signing (Firma de DNSSEC), elija View information to create DS record (Ver información para crear un registro de DS).

Note

Si no ve View information to create DS record (Ver información para crear un registro DS) en esta sección, debe habilitar la firma de DNSSEC antes de establecer la cadena de confianza. Elija Enable DNSSEC signing (Habilitar firma de DNSSEC) y complete los pasos descritos en [Paso 2: Habilitar la firma DNSSEC y crear un KSK](#), y a continuación, vuelva a estos pasos para establecer la cadena de confianza.

4. En Establish a chain of trust (Establecer una cadena de confianza), elija Route 53 registrar (Registrador Route 53) o Another domain registrar (Otro registrador de dominios), en función de dónde esté registrado su dominio.
5. Utilice los valores proporcionados desde el paso 3 para crear un registro DS para la zona alojada principal en Route 53. Si su dominio no está alojado en Route 53, utilice los valores proporcionados para crear un registro DS en el sitio web del registrador de dominios.

Cómo establecer una cadena de confianza para la zona principal:

- Si el dominio se administra a través de Route 53, siga estos pasos:

Asegúrese de configurar el algoritmo de firma (ECDSAP256SHA256 y escriba 13) y el algoritmo de resumen (SHA-256 y tipo 2) correctos.

Si Route 53 es su registrador, haga lo siguiente en la consola de Route 53:

1. Tenga en cuenta los valores Key type (Tipo de clave), Signing algorithm (Algoritmo de firma) y Public key (Clave pública). En el panel de navegación, elija Registered domains.
2. Seleccione un dominio y, a continuación, en la pestaña de claves de DNSSEC, elija Agregar clave.
3. En el cuadro de diálogo Administrar claves de DNSSEC, elija el Tipo de clave y el Algoritmo correctos para el Registrador de Route 53 en los menús desplegables.
4. Copie la Public key (Clave pública) para el registrador de Route 53. En el diálogo Manage DNSSEC keys (Administrar claves de DNSSEC), pegue el valor en el cuadro Public key (Clave pública).
5. Elija Agregar.

Route 53 agregará el registro de DS a la zona principal desde la clave pública. Por ejemplo, si su dominio es `example.com`, el registro de DS se agrega a la zona DNS `.com`.

- Si el dominio se administra en otro registro, siga las instrucciones de la sección Otro registrador de dominio.

Para asegurarse de que los siguientes pasos se realizan sin problemas, introduzca un TTL DS bajo en la zona principal. Recomendamos configurar el TTL DS en 5 minutos (300 segundos) para una recuperación más rápida si necesita retroceder los cambios.

- Cómo establecer una cadena de confianza para la zona secundaria:

Si su zona principal está administrada por otro registro, contacte con el registrador para introducir el registro DS de su zona. Normalmente no podrá ajustar el TTL del registro DS.

- Si su zona principal está alojada en Route 53, póngase en contacto con el propietario de la zona principal para introducir el registro DS de su zona.

Proporcione la `$ds_record_value` al propietario de la zona principal. Puede obtenerlo haciendo clic en Ver información para crear un registro DS en la consola y copiando el campo de registro DS, o llamando a la API [GetDNSSEC](#) y recuperando el valor del campo "DSRecord"

```
aws --region us-east-1 route53 get-dnssec
    --hosted-zone-id $hostedzone_id
```

El propietario de la zona principal puede insertar el registro a través de la consola de Route 53 o la CLI.

- Para insertar el registro DS mediante el uso AWS CLI, el propietario de la zona principal crea y asigna un nombre a un archivo JSON similar al siguiente ejemplo. El propietario de la zona principal podría nombrar al archivo algo así como `inserting_ds.json`.

```
{
  "HostedZoneId": "$parent_zone_id",
  "ChangeBatch": {
    "Comment": "Inserting DS for zone $zone_name",
    "Changes": [
      {
        "Action": "UPSERT",
        "ResourceRecordSet": {
          "Name": "$zone_name",
          "Type": "DS",
          "TTL": 300,
          "ResourceRecords": [
            {
              "Value": "$ds_record_value"
            }
          ]
        }
      }
    ]
  }
}
```

```
}
```

A continuación, ejecute el siguiente comando:

```
aws --region us-east-1 route53 change-resource-record-sets  
    --cli-input-json file://inserting_ds.json
```

- Para insertar el registro DS mediante la consola,

Abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.

En el panel de navegación, elija Hosted zones (Zonas alojadas), el nombre de la zona alojada y luego el botón Create record (Crear registro). Asegúrese de elegir el Enrutamiento sencillo para la Routing policy (Política de enrutamiento).

En el campo Nombre del registro, ingrese el mismo nombre que el `$zone_name`, seleccione DS en el menú desplegable Tipo de registro, ingrese el valor de `$ds_record_value` en el campo Valor y seleccione Crear registros.

Reversión: elimine el DS de la zona principal, espere el TTL DS y, a continuación, revierta los pasos para establecer la confianza. Si la zona principal está alojada en Route 53, el propietario de la zona principal puede cambiar la Action desde UPSERT a DELETE en el archivo JSON y vuelva a ejecutar la CLI de ejemplo anterior.

6. Espere a que las actualizaciones se propaguen, en función del TTL para los registros de dominio.

Si la zona principal está en el servicio DNS de Route 53, el propietario de la zona principal puede confirmar la propagación completa a través de la [GetChangeAPI](#).

De lo contrario, puede sondear periódicamente la zona principal del registro DS y esperar otros 10 minutos después para aumentar la probabilidad de que la inserción del registro DS se propague por completo. Tenga en cuenta que algunos registradores han programado la inserción de DS, por ejemplo, una vez al día.

Cuando introduzca el registro Delegation Signer (DS) en la zona principal, los solucionadores validados que han recogido el DS comenzarán a validar las respuestas de la zona.

Para asegurarse de que los pasos para establecer la confianza se desarrollen sin problemas, complete lo siguiente:

1. Busque el TTL NS máximo.

Hay 2 conjuntos de registros NS asociados a sus zonas:

- El registro NS de la delegación: es el registro NS de su zona mantenida por la zona principal. Puede encontrarlo ejecutando los siguientes comandos Unix (si su zona es ejemplo.com, la zona principal es com):

```
dig -t NS com
```

Elija uno de los registros NS y, a continuación, ejecute lo siguiente:

```
dig @one of the NS records of your parent zone -t NS example.com
```

Por ejemplo:

```
dig @b.gtld-servers.net. -t NS example.com
```

- El registro NS de la zona: es el registro NS de su zona. Puede encontrarlo ejecutando el siguiente comando Unix:

```
dig @one of the NS records of your zone -t NS example.com
```

Por ejemplo:

```
dig @ns-0000.awsdns-00.co.uk. -t NS example.com
```

Tenga en cuenta el TTL máximo para ambas zonas.

2. Espere el TTL NS máximo.

Antes de la inserción de DS, los solucionadores reciben una respuesta firmada, pero no están validando la firma. Cuando se inserta el registro DS, los solucionadores no lo verán hasta que caduque el registro NS de la zona. Cuando los solucionadores recuperen el registro NS, también se devolverá el registro DS.

Si su cliente ejecuta un solucionador en un host con un reloj dessincronizado, asegúrese de que el reloj esté dentro de 1 hora desde la hora correcta.

Tras completar este paso, todos los solucionadores compatibles con DNSSEC validarán su zona.

3. Observe la resolución de nombres.

Debería observar que no hay problemas con los solucionadores que validan su zona. Asegúrese también de tener en cuenta el tiempo necesario para que sus clientes le informen de los problemas.

Recomendamos supervisar hasta 2 semanas.

4. (Opcional) Alargue el DS y el NS. TTLs

Si está satisfecho con la configuración, puede guardar los cambios de TTL y SOA realizados. Tenga en cuenta que Route 53 limita el TTL a 1 semana para las zonas firmadas. Para obtener más información, consulte [Configuración de la firma de DNSSEC en Amazon Route 53](#).

Si puede cambiar el TTL DS, le recomendamos que lo configure en 1 hora.

Desactivar la firma de DNSSEC

Los pasos para desactivar la firma DNSSEC en Route 53 varían en función de la cadena de confianza de la que forma parte la zona alojada.

Por ejemplo, la zona alojada puede tener una zona principal que tenga un registro de Delegation Signer (DS) como parte de una cadena de confianza. Su zona alojada también puede ser una zona principal para zonas secundarias que han habilitado la firma de DNSSEC, que es otra parte de la cadena de confianza. Investigue y determine la cadena de confianza completa para su zona alojada antes de realizar los pasos necesarios para desactivar la firma de DNSSEC.

La cadena de confianza de la zona alojada que habilita la firma de DNSSEC se debe deshacer cuidadosamente a medida que desactiva la firma. Para eliminar la zona alojada de la cadena de confianza, elimine todos los registros de DS que haya en la cadena de confianza que incluye esta zona alojada. Debe hacer lo siguiente, en orden:

1. Elimine todos los registros de DS que esta zona alojada tenga para las zonas secundarias que forman parte de una cadena de confianza.
2. Elimine el registro de DS desde la zona principal. Si tiene una isla de confianza (no hay registros de DS en la zona principal ni registros de DS para zonas secundarias en esta zona), puede omitir este paso.

3. Si no puede eliminar los registros de DS, para eliminar la zona de la cadena de confianza, elimine los registros de NS de la zona principal. Para obtener más información, consulte [Adición o modificación de servidores de nombres y registros de conexión de un dominio](#).

Los siguientes pasos progresivos le permiten supervisar la eficacia de los pasos individuales para evitar problemas de disponibilidad de DNS en su zona.

Para desactivar la firma de DNSSEC

1. Supervisar la disponibilidad de zonas.

Puede supervisar la zona para comprobar la disponibilidad de sus nombres de dominio. Esto puede ayudarle a solucionar cualquier problema que pueda justificar retroceder un paso atrás después de habilitar la firma DNSSEC. Puede supervisar los nombres de dominio con la mayor parte del tráfico mediante el registro de consultas. Para obtener más información sobre la configuración del registro de consultas, consulte [Monitoreo de Amazon Route 53](#).

La supervisión se puede realizar a través de un script de shell o mediante un servicio de pago. Sin embargo, no debería ser la única señal para determinar si se requiere una reversión. Es posible que también reciba comentarios de sus clientes debido a que un dominio no está disponible.

2. Busque el DS TTL actual.

Puede encontrar el TTL DS ejecutando el siguiente comando Unix:

```
dig -t DS example.com example.com
```

3. Busque el TTL NS máximo.

Hay 2 conjuntos de registros NS asociados a sus zonas:

- El registro NS de la delegación: es el registro NS de su zona mantenida por la zona principal. Puede encontrarlo ejecutando los siguientes comandos de Unix:

Busque primero el NS de su zona principal (si su zona es ejemplo.com, la zona principal es com):

```
dig -t NS com
```

Elija uno de los registros NS y, a continuación, ejecute lo siguiente:

```
dig @one of the NS records of your parent zone -t NS example.com
```

Por ejemplo:

```
dig @b.gtld-servers.net. -t NS example.com
```

- El registro NS de la zona: es el registro NS de su zona. Puede encontrarlo ejecutando el siguiente comando Unix:

```
dig @one of the NS records of your zone -t NS example.com
```

Por ejemplo:

```
dig @ns-0000.awsdns-00.co.uk. -t NS example.com
```

Tenga en cuenta el TTL máximo para ambas zonas.

4. Elimine el registro de DS desde la zona principal.

Póngase en contacto con el propietario de la zona principal para eliminar el registro DS.

Reversión: vuelva a insertar el registro de DS, confirme que la inserción de DS es efectiva y espere al TTL NS (no DS) máximo antes de que todos los Resolvers comiencen a validar de nuevo.

5. Confirme que la eliminación del DS es efectiva.

Si la zona principal está en el servicio DNS de Route 53, el propietario de la zona principal puede confirmar la propagación completa a través de la [GetChangeAPI](#).

De lo contrario, puede sondear periódicamente la zona principal del registro DS y esperar otros 10 minutos después para aumentar la probabilidad de que la eliminación del registro DS se propague por completo. Tenga en cuenta que algunos registradores han programado la retirada del DS, por ejemplo, una vez al día.

6. Espere al TTL DS.

Espere a que todos los solucionadores hayan caducado el registro DS de sus cachés.

7. Desactive la firma de DNSSEC y la clave de firma de clave (KSK).

- [CLI](#)
- [Consola](#)

CLI

Llame a [DisableHostedZoneDNSSEC](#) y [DeactivateKeySigningKey](#) APIs

Por ejemplo:

```
aws --region us-east-1 route53 disable-hosted-zone-dnssec \
    --hosted-zone-id $hostedzone_id

aws --region us-east-1 route53 deactivate-key-signing-key \
    --hosted-zone-id $hostedzone_id --name $ksk_name
```

Console

Para desactivar la firma de DNSSEC

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>
2. En el panel de navegación, elija Hosted zones (Zonas alojadas) y elija una zona alojada para la que desea desactivar la firma de DNSSEC.
3. En la página DNSSEC, elija Disable DNSSEC signing (Desactivar firma de DNSSEC).
4. En la página Disable DNSSEC signing (Desactivar firma de DNSSEC), elija una de las siguientes opciones, según el escenario de la zona cuya firma de DNSSEC esté desactivando.
 - Parent zone only (Solo la zona principal) — Esta zona tiene una zona principal con un registro de DS. En este escenario, debe eliminar el registro de DS de la zona principal.
 - Child zones only (Solo las zonas secundarias) — Esta zona tiene un registro de DS para una cadena de confianza con una o más zonas secundarias. En este escenario, debe eliminar los registros de DS de la zona.
 - Parent and child zones (Zonas principales y secundarias) — Esta zona tiene un registro de DS para una cadena de confianza con una o más zonas secundarias y una zona principal con un registro de DS. En este escenario, haga lo siguiente en orden:
 - a. Elimine los registros de DS de la zona.
 - b. Elimine el registro de DS de la zona principal.

Si tiene una isla de confianza, puede omitir este paso.

5. Determine cuál es el TTL para cada registro de DS que elimine en el paso 4. Asegúrese de que el periodo TTL más largo haya caducado.
6. Seleccione la casilla de verificación para confirmar que ha seguido los pasos en orden.
7. Escriba disable (desactivar) en el campo, como se muestra, y elija Disable (Desactivar).

Para desactivar la clave de firma de claves (KSK)

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Hosted zones (Zonas alojadas) y elija una zona alojada para la que desea desactivar la clave de firma de claves (KSK).
3. En la sección Claves de firma de claves (KSKs), elige el KSK que quieres desactivar y, en Acciones, elige Editar KSK, establece el estado del KSK como Inactivo y, a continuación, selecciona Guardar KSK.

[ActivateKeySigningKeyEnableHostedZone APIsReversión](#): llamada y DNSSEC.

Por ejemplo:

```
aws --region us-east-1 route53 activate-key-signing-key \
    --hosted-zone-id $hostedzone_id --name $ksk_name

aws --region us-east-1 route53 enable-hosted-zone-dnssec \
    --hosted-zone-id $hostedzone_id
```

8. Confirme que la desactivación de la firma de zona es efectiva.

Use el identificador de la `EnableHostedZoneDNSSEC()` llamada [GetChange](#) para ejecutar y asegurarse de que todos los servidores DNS de Route 53 hayan dejado de firmar las respuestas (status =). INSYNC

9. Observe la resolución de nombres.

Debe observar que no hay problemas que provoquen que los solucionadores validen su zona. Deje pasar entre 1 y 2 semanas para tener en cuenta el tiempo necesario para que sus clientes le comuniquen los problemas.

10. (Opcional) Limpieza.

Si no va a volver a habilitar la firma, puede limpiar [DeleteKeySigningKey](#) eliminar la clave gestionada KSKs por el cliente correspondiente para ahorrar costes.

Trabajar con claves administradas por el cliente para DNSSEC

Al habilitar la firma de DNSSEC en Amazon Route 53, este servicio crea una clave de firma de claves (KSK) por usted. Para crear una KSK, Route 53 debe usar una clave administrada por el cliente AWS Key Management Service que sea compatible con DNSSEC. En esta sección, se describen los detalles y los requisitos de la clave administrada por el cliente que resultan de utilidad al trabajar con DNSSEC.

Tenga en cuenta lo siguiente cuando trabaje con claves administradas por el cliente para DNSSEC:

- La clave administrada por el cliente que utiliza con la firma de DNSSEC debe estar en la región EE. UU. Este (Norte de Virginia).
- La clave administrada por el cliente debe ser una [clave asimétrica administrada por el cliente](#) con una [especificación de clave ECC_NIST_P256](#). Estas claves administradas por el cliente se utilizan únicamente para firmar y verificar. Para obtener ayuda para crear una clave administrada por el cliente asimétrica, consulte [Creación de claves asimétricas administradas por el cliente en la Guía para](#) desarrolladores. AWS Key Management Service Para obtener ayuda para encontrar la configuración criptográfica de una clave gestionada por el cliente existente, consulte [Visualización de la configuración criptográfica de las claves gestionadas por el cliente](#) en la Guía para desarrolladores. AWS Key Management Service
- Si crea una clave administrada por el cliente para usarla con DNSSEC en Route 53, debe incluir instrucciones de política de claves específicas que otorguen a Route 53 los permisos necesarios. Route 53 debe poder acceder a la clave administrada por el cliente a fin de que pueda crear la KSK automáticamente. Para obtener más información, consulte [Permisos de clave administrados por el cliente de Route 53 necesarios para firmar DNSSEC](#).
- Route 53 puede crear una clave administrada por el cliente AWS KMS para utilizarla con la firma de DNSSEC sin permisos adicionales. AWS KMS No obstante, debe tener permisos específicos

si desea editar la clave después de crearla. Los permisos específicos que debe tener son los siguientes: `kms:UpdateKeyDescription`, `kms:UpdateAlias`, y `kms:PutKeyPolicy`.

- Tenga en cuenta que se aplican cargos aparte por cada clave administrada por el cliente que tenga, independientemente de que usted cree la clave administrada por el cliente o sea Route 53 quien la cree por usted. Para obtener más información, consulte [Precios de AWS Key Management Service](#).

Trabajar con claves de firma de claves (KSKs)

Cuando se habilita la firma de DNSSEC, Route 53 crea una clave de firma de claves (KSK) por usted. Puede tener hasta dos KSKs por zona alojada en Route 53. Después de habilitar la firma de DNSSEC, puede agregar, eliminar o editar su KSKs.

Tenga en cuenta lo siguiente cuando trabaje con su KSKs:

- Antes de poder eliminar una KSK, debe editarla para establecer su estado en Inactive (Inactivo).
- Al habilitar la firma de DNSSEC para una zona alojada, Route 53 limita el TTL a una semana. Si establece un TTL para los registros en la zona alojada en de más de una semana, no aparece ningún error, pero Route 53 aplica un TTL obligatorio de una semana.
- Para ayudar a evitar una interrupción de la zona y problemas de que el dominio deje de estar disponible, debe abordar y resolver rápidamente los errores de DNSSEC. Le recomendamos encarecidamente que configure una CloudWatch alarma que le avise cada vez que se detecte un `DNSSECKeySigningKeysNeedingAction` error `DNSSECInternalFailure` o error. Para obtener más información, consulte [Supervisión de zonas alojadas mediante Amazon CloudWatch](#).
- Las operaciones de KSK descritas en esta sección le permiten rotar las de KSKs su zona. Para obtener más información y un step-by-step ejemplo, consulte Rotación de claves de DNSSEC en la entrada del blog [Configuración de la firma y la validación de DNSSEC con Amazon Route 53](#).

Para trabajar con ella KSKs Consola de administración de AWS, siga las instrucciones de las siguientes secciones.

Agregar una clave de firma de claves (KSK)

Cuando se habilita la firma de DNSSEC, Route 53 crea una clave de firma (KSK) por usted. También puede añadirlos KSKs por separado. Puede tener hasta dos KSKs por zona hospedada en Route 53.

Al crear una KSK, debe proporcionar o solicitar a Route 53 que cree una clave administrada por el cliente para utilizarla con la KSK. Cuando proporciona o crea una clave administrada por el cliente, existen varios requisitos. Para obtener más información, consulte [Trabajar con claves administradas por el cliente para DNSSEC](#).

Siga estos pasos para agregar una KSK en la Consola de administración de AWS.

Para agregar una KSK

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Hosted zones (Zonas alojadas) y elija una zona alojada.
3. En la pestaña de firma de DNSSEC, en Teclas de firma de claves (KSKs), elija Cambiar a la vista avanzada y, a continuación, en Acciones, elija Agregar KSK.
4. En KSK, ingrese un nombre para la KSK que Route 53 creará para usted. Los nombres pueden contener letras, números y guiones bajos (_). Deben ser únicos.
5. Ingrese el alias de una clave administrada por el cliente que se aplique a la firma de DNSSEC o ingrese un alias para la nueva clave administrada por el cliente que Route 53 creará para usted.

 Note

Si elige que Route 53 cree una clave administrada por el cliente, tenga en cuenta que se aplican cargos aparte por cada clave administrada por el cliente. Para obtener más información, consulte [Precios de AWS Key Management Service](#).

6. Elija Create KSK (Crear KSK).

Editar una clave de firma de claves (KSK)

Puede editar el estado de una KSK para establecerlo en Active (Activo) o Inactive (Inactivo). Cuando una KSK está activa, Route 53 usa esa KSK para la firma de DNSSEC. Antes de poder eliminar una KSK, debe editarla para establecer su estado en Inactive (Inactivo).

Siga estos pasos para editar una KSK en la Consola de administración de AWS.

Para editar una KSK

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/route53/>
2. En el panel de navegación, elija Hosted zones (Zonas alojadas) y elija una zona alojada.
3. En la pestaña de firma de DNSSEC, en Teclas de firma de claves (KSKs), elija Cambiar a la vista avanzada y, a continuación, en Acciones, elija Editar KSK.
4. Realice las actualizaciones que desee para la KSK y elija Save (Guardar).

Eliminar una clave de firma de claves (KSK)

Antes de poder eliminar una KSK, debe editarla para establecer su estado en Inactive (Inactivo).

Una de las razones por las que puede eliminar una KSK es como parte de la rotación rutinaria de claves. Rotar claves criptográficas periódicamente es una práctica recomendada. Es posible que su organización tenga una guía estándar sobre la frecuencia con la que debe rotar las claves.

Siga estos pasos para eliminar una KSK en la Consola de administración de AWS.

Para eliminar una KSK

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/route53/>
2. En el panel de navegación, elija Hosted zones (Zonas alojadas) y elija una zona alojada.
3. En la pestaña de firma de DNSSEC, en Teclas de firma de claves (KSKs), elija Cambiar a la vista avanzada y, a continuación, en Acciones, elija Eliminar KSK.
4. Siga las instrucciones para confirmar la eliminación de la KSK.

Administración de claves KMS y ZSK en Route 53

En esta sección se describe la práctica actual que Route 53 utiliza para las zonas habilitadas para la firma de DNSSEC.

Note

Route 53 utiliza la siguiente regla que podría cambiar. Cualquier cambio futuro no reducirá la posición de seguridad de su zona ni de Route 53.

Cómo usa Route 53 lo asociado a tu KSK AWS KMS

En DNSSEC, la KSK se utiliza para generar la firma de registro de recursos (RRSIG) del conjunto de registros de recursos DNSKEY. Todos ACTIVE KSKs se utilizan en la generación RRSIG. Route 53 genera un RRSIG llamando a la Sign AWS KMS API en la clave KMS asociada. Para obtener más información, consulte [Sign](#) (Firmar) en la Guía de la API de AWS KMS. RRSIGsNo se tienen en cuenta para el límite establecido de registros de recursos de la zona.

RRSIG tiene fecha de vencimiento. Para evitar que caduquen, se RRSIGs actualizan periódicamente regenerándolos cada uno a siete días. RRSIGs

También RRSIGs se actualizan cada vez que llamas a cualquiera de las siguientes opciones: APIs

- [ActivateKeySigningKey](#)
- [CreateKeySigningKey](#)
- [DeactivateKeySigningKey](#)
- [DeleteKeySigningKey](#)
- [DisableHostedZoneDNSSEC](#)
- [EnableHostedZoneDNSSEC](#)

Cada vez que Route 53 realiza una actualización, generamos 15 RRSIGs para cubrir los próximos días en caso de que no se pueda acceder a la clave KMS asociada. Para la estimación del costo de la clave KMS, puede basarse en una actualización periódica una vez al día. Es posible que no se pueda acceder a una clave KMS debido a cambios involuntarios en la política de claves de KMS. La clave KMS inaccesible establecerá el estado de la KSK asociada en ACTION_NEEDED. Le recomendamos encarecidamente que supervise esta situación configurando una CloudWatch alarma cada vez que se detecte un DNSSECKeySigningKeysNeedingAction error, ya que al validar las resoluciones, las búsquedas comenzarán a fallar cuando caduque la última RRSIG. Para obtener más información, consulte [Supervisión de zonas alojadas mediante Amazon CloudWatch](#).

Cómo administra Route 53 la ZSK de su zona

Cada nueva zona alojada con firma DNSSEC habilitada tendrá una clave de firma de zona (ZSK) ACTIVE. La ZSK se genera por separado para cada zona alojada y es propiedad de Route 53. El algoritmo clave actual es. ECDSAP256 SHA256

Comenzaremos a realizar una rotación ZSK regular en la zona en un plazo de 7 a 30 días desde el inicio de la firma. En la actualidad, Route 53 utiliza el método de transferencia de claves previa

a la publicación. Para obtener más información, consulte [Pre-Publish Zone Signing Key Rollover](#) (Transferencia de claves de firma de zona previa a la publicación). Este método introducirá otra ZSK en la zona. La rotación se repetirá cada 7 a 30 días.

La Ruta 53 suspenderá la rotación de la ZSK si alguna de las KSK de la zona está en ACTION_NEEDED estado, ya que la Ruta 53 no podrá regenerar los conjuntos de registros de recursos de DNSKEY RRSIGs para tener en cuenta los cambios en la ZSK de la zona. La rotación de ZSK se reanudará automáticamente después de que se haya borrado la condición.

Pruebas de inexistencia de DNSSEC en Route 53

Note

Route 53 utiliza la siguiente regla que podría cambiar. Cualquier cambio futuro no reducirá la posición de seguridad de su zona ni de Route 53.

Hay tres tipos de pruebas de inexistencia en DNSSEC:

- Prueba de la inexistencia de un registro que coincida con el nombre de la consulta.
- Prueba de la inexistencia de un tipo que coincida con el tipo de consulta.
- Prueba de la existencia de un registro comodín utilizado para generar el registro en respuesta.

Route 53 implementa la prueba de inexistencia de un registro que coincide con el nombre de la consulta utilizando el método BL. Para obtener más información, consulte [BL](#). Es un método que produce una representación compacta de la prueba y evita la consulta exhaustiva de nombres de zona.

En los casos en que haya un registro que coincida con el nombre de la consulta pero no con el tipo de consulta (por ejemplo, si se busca web.example). com/AAAA but there is only web.example.com/ Apresente), devolvemos un registro NSEC (siguiente seguro) mínimo que contiene todos los tipos de registros de recursos admitidos.

Cuando Route 53 sintetiza una respuesta de un registro comodín, la respuesta no irá acompañada de un registro seguro siguiente o de un registro NSEC para el comodín. Este registro NSEC se utiliza en algunas implementaciones, normalmente en las que realizan la firma sin conexión, para evitar que las firmas de registros de recursos (RRSIG) de la respuesta se vuelvan a utilizar para falsificar

una respuesta diferente. Route 53 utiliza la firma en línea para los registros que no son de DNSKEY a fin de generar datos RRSIGs específicos para la respuesta que no se pueden reutilizar para una respuesta diferente.

Solución de problemas de firma de DNSSEC

La información de esta sección puede ayudarlo a abordar los problemas relacionados con la firma de DNSSEC, incluida la activación, la inhabilitación y la utilización de las claves de firma de claves (). KSKs

Habilitación de DNSSEC

Asegúrese de leer los requisitos previos en [Configuración de la firma de DNSSEC en Amazon Route 53](#) antes de habilitar la firma de DNSSEC.

Deshabilitación de DNSSEC

Para deshabilitar DNSSEC de manera segura, Route 53 comprobará si la zona de destino está en la cadena de confianza. Comprueba si el elemento principal de la zona de destino tiene algún registro de NS o de DS de la zona de destino. Si la zona de destino no se puede resolver públicamente, por ejemplo, al obtener una respuesta SERVFAIL al consultar NS y DS, Route 53 no puede determinar si es seguro deshabilitar DNSSEC. Puede contactar con su zona principal para solucionar esos problemas y volver a intentar deshabilitar DNSSEC más adelante.

El estado de KSK es Action needed (Acción necesaria)

Una KSK puede cambiar su estado a Acción necesaria (o ACTION_NEEDED en [KeySigningKey](#) estado) cuando el DNSSEC de Route 53 pierde el acceso a uno correspondiente AWS KMS key (debido a un cambio en los permisos o a una eliminación). AWS KMS key

Si el estado de un KSK es Action needed (Acción necesaria), significa que eventualmente provocará una interrupción de la zona para los clientes que utilizan los solucionadores de validación de DNSSEC y debe actuar rápidamente para evitar que una zona de producción no pueda resolverse.

Para corregir el problema, asegúrese de que la clave administrada por el cliente en la que se basa su KSK está habilitada y tiene los permisos correctos. Para obtener más información sobre los permisos necesarios, consulte [Permisos de clave administrados por el cliente de Route 53 necesarios para firmar DNSSEC](#).

Una vez que haya arreglado el KSK, actívalo de nuevo mediante la consola o el AWS CLI, tal y como se describe en. [Paso 2: Habilitar la firma DNSSEC y crear un KSK](#)

Para evitar este problema en el futuro, considere la posibilidad de añadir una Amazon CloudWatch métrica para rastrear el estado de la KSK, tal y como se sugiere en [Configuración de la firma de DNSSEC en Amazon Route 53](#).

El estado de la KSK es Internal failure (Error interno)

Cuando un KSK tiene el estado de fallo interno (o se encuentra INTERNAL_FAILURE en un [KeySigningKey](#) estado), no puede trabajar con ninguna otra entidad del DNSSEC hasta que se resuelva el problema. Debe adoptar medidas antes de poder trabajar con la firma de DNSSEC, incluido el trabajo con esta KSK o con su otra KSK.

Para corregir el problema, vuelva a intentar activar o desactivar la KSK.

[Para corregir el problema al trabajar con el APIs, prueba a habilitar la firma \(EnableHostedZoneDNSSEC\) o inhabilitarla \(DNSSEC\). DisableHostedZone](#)

Es importante que corrija los problemas de tipo Internal failure (Error interno) lo antes posible. No puede realizar ningún otro cambio en la zona alojada hasta que corrija el problema, excepto las operaciones para corregir el Internal failure (Error interno).

Uso de AWS Cloud Map para crear registros y comprobaciones de estado

Si desea dirigir el tráfico de Internet o el tráfico de una Amazon VPC a componentes de aplicaciones o microservicios, puede utilizar AWS Cloud Map para crear registros y, opcionalmente, crear comprobaciones de estado automáticamente. Para obtener más información, consulte la [Guía para desarrolladores de AWS Cloud Map](#).

Restricciones y comportamientos de DNS

La mensajería DNS está sujeta a factores que afectan a cómo crea y utiliza las zonas alojadas y los registros. En esta sección se explican estos factores.

Tamaño de respuesta máximo

Para cumplir con los estándares de DNS, las respuestas enviadas a través de UDP tienen un tamaño máximo de 512 bytes. Las respuestas que superen los 512 bytes se truncan y el servicio de resolución debe volver a emitir la solicitud a través de TCP. Si el solucionador admite EDNS0 (tal y

como se define en [RFC 2671](#)) y anuncia la opción EDNS0 a Amazon Route 53, este servicio permite respuestas de hasta 4096 bytes en UDP, sin truncamiento.

Procesamiento de sección de Authoritative

Para que las consultas se realicen correctamente, Route 53 adjunta registros de servidor de nombres (NS) para la zona alojada correspondiente en la sección de autoridad de la respuesta DNS. En el caso de los nombres que no se encuentran (respuestas NXDOMAIN), Route 53 adjunta el registro del inicio de autoridad (SOA) (tal y como se define en [RFC 1035](#)) para la zona alojada a la sección de autoridad de la respuesta DNS.

Procesamiento de la sección Additional

Route 53 adjunta registros a la sección Additional (Adicional). Si los registros son conocidos y adecuados, el servicio adjunta registros A o AAAA para cualquier objetivo de un registro MX, CNAME, NS o SRV enumerados en la sección de respuesta. Para obtener más información acerca de estos tipos de registros DNS, consulte [Tipos de registros de DNS admitidos](#).

Temas relacionados

Para obtener información acerca de cómo transferir el registro de dominios (no solo el alojamiento de DNS) a Route 53, consulte los temas siguientes:

- [Lista de verificación previa a la transferencia para transferencias de dominios](#): complete esta lista de verificación antes de transferir el registro de dominios para evitar errores de transferencia comunes.
- [Transferencia del registro de un dominio a Amazon Route 53](#): proceso paso a paso para transferir el registro de dominios de otro registrador a Route 53.
- [Transferencia de dominios](#): descripción general de todas las opciones de transferencia de dominios, incluidas las transferencias entre cuentas de AWS.

Uso de flujo de tráfico para dirigir el tráfico DNS

El flujo de tráfico simplifica enormemente el proceso de creación y mantenimiento de registros en configuraciones grandes y complejas.

Administrar registros relacionados en una zona alojada puede resultar difícil en las siguientes circunstancias:

- Tiene muchos recursos que realizan la misma operación, como servidores web que sirven tráfico para el mismo dominio.
- Desea crear un árbol complejo de registros mediante [registros de alias](#) y una combinación de [políticas de direccionamiento de Route 53](#), como latencia, conmutación por error y ponderado.

Ventajas del flujo de tráfico

Para facilitar el seguimiento de los registros y sus relaciones, el flujo de tráfico simplifica la creación de registros DNS con las siguientes características:

Visual editor (Editor visual)

El editor visual de flujo de tráfico le permite crear árboles complejos de registros y ver las relaciones entre los registros. Por ejemplo, puede crear una configuración en la que los registros de alias de latencia hagan referencia a registros ponderados, y los registros ponderados hagan referencia a sus recursos en varias Regiones de AWS. Cada configuración se conoce como una política de tráfico. Puede crear tantas políticas de tráfico como desee sin ningún cargo aplicado.

Control de versiones

Puede crear varias versiones de una política de tráfico para que no tenga que empezar de nuevo cuando la configuración cambie. Las versiones antiguas siguen existiendo hasta que las elimine, hay un límite predeterminado de 1000 versiones por política de tráfico. Opcionalmente, puede dar una descripción a cada versión.

Creación y actualización automática de registros

Una política de tráfico puede representar hasta cientos de registros. El flujo de tráfico le permite crear todos esos registros automáticamente mediante la creación de un registro de política de tráfico. Especifique la zona alojada y el nombre del registro en la raíz del árbol, como example.com o www.example.com y Route 53 crea automáticamente todos los demás registros

del árbol. El registro raíz (el registro de la política de tráfico) aparece en la lista de registros de la zona alojada; el resto de registros están ocultos.

Al crear una nueva versión de una política de tráfico, puede actualizar selectivamente los registros de política de tráfico creados con la versión anterior de política de tráfico. Cuando actualiza un registro de política de tráfico, Route 53 actualiza automáticamente el resto de registros del árbol. También puede revertir rápidamente los cambios actualizando de nuevo un registro de política de tráfico para utilizar una versión anterior de una política de tráfico.

 Note

Puede utilizar el flujo de tráfico para crear registros solo en zonas alojadas públicas.

Política de direccionamiento de geoproximidad

El uso de Flujo de tráfico le permite comprender de forma más intuitiva cómo se enruta el tráfico a cada uno de los puntos de conexión globales mediante el uso del mapa de geoproximidad del editor visual de Flujo de tráfico. Para obtener más información, consulte [Enrutamiento por geoproximidad](#).

Reutilizar para varios registros en diferentes zonas alojadas

Puede utilizar una política de tráfico para crear automáticamente registros en varias zonas alojadas públicas. Por ejemplo, si utiliza los mismos servidores web para varios nombres de dominio, puede usar la misma política de tráfico para crear registros de políticas de tráfico en las zonas alojadas en example.com, example.org y example.net.

Cuando un cliente envía una consulta para el nombre del registro raíz, como example.com o www.example.com, Route 53 responde a la consulta en función de la configuración de la política de tráfico utilizada para crear el registro de política de tráfico correspondiente.

Hay un cargo mensual por cada registro de política de tráfico. Para obtener más información, consulte la sección “Flujo de tráfico” de [Precios de Amazon Route 53](#).

Para minimizar estos cargos, puede crear uno o más registros de alias en una zona alojada que hagan referencia a un registro de política de tráfico en esa zona alojada. Por ejemplo, puede crear un registro de política de tráfico para example.com y, a continuación, crear un registro de alias para www.example.com que haga referencia al registro de política de tráfico.

Crear y administrar políticas de tráfico

Temas

- [Creación de una política de tráfico](#)
- [Valores que especifica cuando crea una política de tráfico](#)
- [Visualización de un mapa que muestra el efecto de la configuración de geoproximidad](#)
- [Creación de versiones adicionales de una política de tráfico](#)
- [Creación de una política de tráfico con un documento JSON](#)
- [Consultar versiones de políticas de tráfico y los registros de políticas asociados](#)
- [Eliminación de versiones de una política de tráfico y políticas de tráfico](#)

Creación de una política de tráfico

Para crear una política de tráfico, siga el procedimiento que se indica a continuación.

Note

Estamos actualizando la consola de Flujo de tráfico para Route 53. Durante el periodo de transición, puede seguir utilizando la consola anterior.

Seleccione la pestaña de la consola que esté utilizando.

- [Nueva consola](#)
- [Consola antigua](#)

New console

Para crear una política de tráfico

1. Diseñe la configuración. Para obtener información acerca de cómo funcionan las configuraciones de enrutamiento DNS complejas, consulte [Configuración de la recuperación ante errores a nivel de DNS](#) [Creación de comprobaciones de estado de Amazon Route 53](#).
2. En función del diseño de la configuración, cree las comprobaciones de estado que desee utilizar para los puntos de enlace.

3. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
4. En el panel de navegación, seleccione Traffic policies.
5. Elija Create traffic policy.
6. Ingrese un nombre y, si lo desea, una descripción. Luego seleccione Siguiente.
7. En el editor, seleccione el tipo de registro de recursos de DNS en el panel Propiedades. Este tipo se asignará a todos los registros de recursos que cree para esta política de tráfico.

Elija Confirmar. Para obtener más información, consulte [Valores que especifica cuando crea una política de tráfico](#).

8. En la página del editor, seleccione Conectar a y luego elija una de las siguientes opciones: Nueva regla de enrutamiento, Nuevo punto de conexión, Regla de enrutamiento existente o Punto de conexión existente. Si seleccionó Nueva regla de enrutamiento, en el panel Propiedades, seleccione la regla de enrutamiento y seleccione Confirmar. A continuación, en el panel Propiedades, introduzca los valores correspondientes. Repita este proceso hasta que la política esté lista. Para obtener más información acerca de los valores de cada tipo de conexión, consulte [Valores que especifica cuando crea una política de tráfico](#).

Puede eliminar reglas, puntos de enlace y ramas de una política de tráfico de las formas siguientes:

- Para eliminar una regla o un punto de conexión, seleccione la regla o el punto de conexión en el editor y, a continuación, seleccione Eliminar en el panel Propiedades.

 Important

Si elimina una regla que tiene reglas secundarias y puntos de enlace, Amazon Route 53 elimina también todos los elementos secundarios.

- Si conecta dos reglas a la misma regla secundaria o punto de conexión y desea eliminar una de las conexiones, coloque el cursor en la conexión que desee eliminar y seleccione Eliminar en el panel Propiedades correspondiente a conexión.
9. Elija Crear política.
 10. En la pestaña Crear registros de políticas, use la nueva política de tráfico para crear uno o más registros de políticas en una zona alojada. Para obtener más información, consulte [Valores que especifica al crear o actualizar un registro de política](#). También puede crear registros de política más adelante, en la misma zona alojada o en otras zonas hospedadas.

Si no desea crear registros de políticas ahora, seleccione Cancelar y la consola mostrará la lista de políticas de tráfico y registros de políticas que ha creado con la AWS cuenta corriente.

11. Si ha especificado valores para los registros de políticas en el paso anterior, elija Crear registros de políticas.

Old console

Para crear una política de tráfico

1. Diseñe la configuración. Para obtener información acerca de cómo funcionan las configuraciones de enrutamiento DNS complejas, consulte [Configuración de la recuperación ante errores a nivel de DNS](#) [Creación de comprobaciones de estado de Amazon Route 53](#).
2. En función del diseño de la configuración, cree las comprobaciones de estado que desee utilizar para los puntos de enlace.
3. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
4. En el panel de navegación, seleccione Traffic policies.
5. Elija Create traffic policy.
6. En la página Name policy, especifique los valores correspondientes. Para obtener más información, consulte [Valores que especifica cuando crea una política de tráfico](#).
7. Elija Siguiente.
8. En la página Create traffic policy (Crear política de tráfico) nombre de la política v1 (v1), especifique los valores aplicables. Para obtener más información, consulte [Valores que especifica cuando crea una política de tráfico](#).

Puede eliminar reglas, puntos de enlace y ramas de una política de tráfico de las formas siguientes:

- Para eliminar una regla o un puntos de conexión, haga clic en la x situada en la esquina superior derecha del cuadro.

 Important

Si elimina una regla que tiene reglas secundarias y puntos de enlace, Amazon Route 53 elimina también todos los elementos secundarios.

- Si conecta dos reglas a la misma regla secundaria o puntos de conexión y desea eliminar una de las conexiones, coloque el cursor en la conexión que desea eliminar y haga clic en la x de esa conexión.

9. Elija Create traffic policy.

10. Opcional: en la pestaña Create policy records with traffic policy (Crear registros de política con política de tráfico), usar la nueva política de tráfico para crear uno o más registros de política en una zona alojada. Para obtener más información, consulte [Valores que especifica al crear o actualizar un registro de política](#). También puede crear registros de política más adelante, en la misma zona alojada o en otras zonas hospedadas.

Si no desea crear registros de políticas ahora, elija Omitir este paso y la consola mostrará la lista de políticas de tráfico y registros de políticas que ha creado con la AWS cuenta corriente.

11. Si ha especificado valores para los registros de política en el paso anterior, elija Create policy record.

Valores que especifica cuando crea una política de tráfico

 Note

Estamos actualizando la consola de Flujo de tráfico para Route 53. Durante el periodo de transición, puede seguir utilizando la consola anterior. La siguiente lista se aplica a ambas consolas, excepto donde se indique lo contrario.

Cuando crea una política de tráfico, especifica los siguientes valores.

-
-
-

-
-
-
-
-

Nombre de la política

Introduzca un nombre que describa la política de tráfico. Este valor aparece en la lista de políticas de tráfico en la consola. No se puede cambiar el nombre de una política de tráfico después de crearla.

Versión

Este valor lo asigna automáticamente Amazon Route 53 al crear una política de tráfico o una nueva versión de una política existente.

Version description

Introduzca una descripción que se aplique a esta versión de la política de tráfico. Este valor aparece en la lista de versiones de políticas de tráfico en la consola.

DNS type

Elija el tipo de DNS que desea que Amazon Route 53 asigne a todos los registros cuando cree un registro de política mediante esta versión de política de tráfico. Para obtener una lista de los tipos admitidos, consulte [Tipos de registros de DNS admitidos](#).

Important

Si va a crear una nueva versión de una política de tráfico existente, puede cambiar el tipo de DNS. Sin embargo, no puede editar un registro de política y elegir una versión de política de tráfico que tenga un tipo de DNS diferente de la versión de política de tráfico que usó para crear el registro de política. Por ejemplo, si ha creado un registro de política mediante una versión de política de tráfico que tiene el tipo de DNS A, no puede editar el registro de política y elegir una versión de política de tráfico que tenga otro valor para tipo de DNS.

Si desea enrutar el tráfico a los siguientes AWS recursos, elija el valor correspondiente:

- CloudFront distribución: elija A: dirección IP en IPv4 formato o AAAA: dirección IP en IPv6 formato.

Note

CloudFront los puntos finales de alias no admiten la evaluación del estado. Sin embargo, puede crear una comprobación de estado para supervisar los puntos CloudFront finales. Para obtener más información, consulte [Creación y actualización de comprobaciones de estado](#).

- Equilibrador de carga de aplicaciones ELB: elija entre A: dirección IP en IPv4 formato o AAAA: dirección IP en formato. IPv6
- Equilibrador de cargas ELB Classic: elija entre A: dirección IP en IPv4 formato o AAAA: dirección IP en formato. IPv6
- Equilibrador de carga de red ELB: elija entre A: dirección IP en IPv4 formato o AAAA: dirección IP en formato. IPv6
- Entorno de Elastic Beanstalk: elija A: dirección IP en formato. IPv4
- Bucket de Amazon S3 configurado como punto de enlace de un sitio web: elija A: dirección IP en IPv4 formato.

Connect to

Elija la regla o puntos de conexión correspondiente en función del diseño de la configuración.

Failover rule

Elija esta opción si desea configurar la conmutación por error activa-pasiva, en la que un recurso asume todo el tráfico cuando está disponible y el otro recurso asume todo el tráfico cuando el primer recurso no está disponible.

Para obtener más información, consulte [Conmutación por error activa-pasiva](#).

Note

La opción Evaluar el estado del destino está marcada de forma predeterminada y evaluará el estado del punto de conexión al que se dirige el tráfico mediante un registro de alias. Si el punto de conexión no recibe tráfico de DNS a través de un registro de alias, desmárquelo y cree una comprobación de estado si desea supervisar el estado del

punto de conexión. Para obtener más información, consulte [Creación y actualización de comprobaciones de estado](#).

Geolocation rule

Elija esta opción si desea que Amazon Route 53 responda a las consultas de DNS en función de la ubicación de los usuarios.

Para obtener más información, consulte [Enrutado de geolocalización](#).

Cuando elija Geolocation rule, elija también el país o el estado en los Estados Unidos del que provengan de las solicitudes.

Note

La opción Evaluar el estado del destino está marcada de forma predeterminada y evaluará el estado del punto de conexión al que se dirige el tráfico mediante un registro de alias. Si el punto de conexión no recibe tráfico de DNS a través de un registro de alias, desmárquelo y cree una comprobación de estado si desea supervisar el estado del punto de conexión. Para obtener más información, consulte [Creación y actualización de comprobaciones de estado](#).

Latency rule

Elija esta opción cuando tenga recursos en varios centros de EC2 datos de Amazon que realicen la misma función y desee que Route 53 responda a las consultas de DNS con los recursos que ofrecen la mejor latencia.

Cuando elija regla de latencia, también escogerá una Región de AWS.

Para obtener más información, consulte [Enrutado basado en latencia](#).

Note

La opción Evaluar el estado del destino está marcada de forma predeterminada y evaluará el estado del punto de conexión al que se dirige el tráfico mediante un registro de alias. Si el punto de conexión no recibe tráfico de DNS a través de un registro de

alias, desmárquelo y cree una comprobación de estado si desea supervisar el estado del punto de conexión. Para obtener más información, consulte [Creación y actualización de comprobaciones de estado](#).

Geoproximity rule

Elija esta opción si desea que Route 53 responda a consultas de DNS en función de la ubicación de los recursos y, de forma opcional, de un sesgo que especifique. El sesgo le permite enviar más tráfico a un recurso o más tráfico desde un recurso.

Cuando elija Geoproximity rule, escriba los siguientes valores:

Ubicación de puntos de conexión

Elija el valor aplicable:

- Personalizado (introduzca las coordenadas): si su punto final no es un AWS recurso, elija Personalizado (introduzca las coordenadas).
- R Región de AWS: si su punto final es un AWS recurso, elija el punto en el Región de AWS que creó el recurso.
- Una zona AWS local: si su punto final es un AWS recurso, elija la zona AWS local en la que creó el recurso.

Si usa Zonas AWS Locales, primero debe habilitarlas. Para obtener más información, consulte la sección [Introducción al uso de zonas locales](#), en la AWS Guía del usuario de zonas locales.

Para conocer las zonas locales disponibles, consulte [Ubicaciones de las zonas locales de AWS](#).

Para obtener más información sobre las diferencias entre las Zonas Locales Regiones de AWS y las Zonas, consulta [Regiones y Zonas](#) en la Guía del EC2 usuario de Amazon.

Important

Una única política de enrutamiento de geoproximidad no puede contener dos o más ubicaciones que estén situadas geográficamente dentro de la misma área metropolitana.

Además, algunas Regiones de AWS Zonas Locales, como EE. UU. Oeste (Oregón) y Portland, EE. UU., están situadas demasiado cerca unas de otras para utilizarlas

dentro de la misma política de enrutamiento de geoproximidad. Si necesita enrutar el tráfico a más de una ubicación dentro de la misma área metropolitana, defina una política de enrutamiento de geoproximidad que dé como resultado una regla de enrutamiento ponderado (WRR) 50/50 para dos puntos de conexión diferentes en el área, lo que distribuye así el tráfico de manera uniforme entre esos puntos de conexión.

Coordinates

Si eligió Custom (enter coordinates) para Endpoint location, escriba la latitud y la longitud de la ubicación del recurso. Tenga en cuenta lo siguiente:

- Latitud representa la ubicación al sur (negativa) o al norte (positiva) del ecuador. Los valores válidos son de -90 grados a 90 grados.
- La longitud representa la ubicación al oeste (negativa) o al este (positiva) del meridiano de Greenwich. Los valores válidos son de -180 grados a 180 grados.
- Puede obtener la latitud y la longitud de algunas aplicaciones de cartografía en línea. Por ejemplo, en Google Maps, la dirección URL de una ubicación específica la latitud y la longitud:

<https://www.google.com/maps/@47.6086111,-122.3409953,20z>

- Puede introducir hasta dos decimales de precisión, por ejemplo, 47.63. Si especifica un valor con mayor precisión, Route 53 trunca el valor a dos lugares después de la decimal. Para latitud y longitud en el ecuador, 0,01 grados corresponde aproximadamente a 0,69 millas.

Sesgo

Para cambiar opcionalmente el tamaño de la región geográfica en la que Route 53 direcciona el tráfico a un recurso, especifique un valor aplicable para Bias (Sesgo):

- Para ampliar el tamaño de la región geográfica en la que Route 53 dirige el tráfico a un recurso, especifique un número entero positivo de 1 a 99 para el sesgo. Route 53 reduce el tamaño de las regiones adyacentes.
- Para contraer el tamaño de la región geográfica en la que Route 53 dirige el tráfico a un recurso, especifique un sesgo negativo de -1 a -99. Route 53 expande el tamaño de las regiones adyacentes.

 Important

El efecto de cambiar el valor de Bias (Sesgo) es relativo, basado en la ubicación de otros recursos, en lugar de absoluto, basado en la distancia. Como resultado, el efecto de un cambio es difícil de predecir. Por ejemplo, en función de dónde estén sus recursos, cambiar el sesgo de 10 a 15 puede suponer la diferencia entre sumar o restar una cantidad de tráfico importante desde el área metropolitana de Nueva York. Le recomendamos que cambie el sesgo en pequeños incrementos y que evalúe los resultados y, a continuación, realice cambios adicionales si procede.

Para obtener más información, consulte [Enrutamiento por geoproximidad](#).

 Note

La opción Evaluar el estado del destino está marcada de forma predeterminada y evaluará el estado del punto de conexión al que se dirige el tráfico mediante un registro de alias. Si el punto de conexión no recibe tráfico de DNS a través de un registro de alias, desmárquelo y cree una comprobación de estado si desea supervisar el estado del punto de conexión. Para obtener más información, consulte [Creación y actualización de comprobaciones de estado](#).

Multivalue answer rule

Elija esta opción si desea que Route 53 responda a las consultas de DNS con hasta ocho respuestas en buen estado seleccionadas al azar de forma aproximada.

Para obtener más información, consulte [Direccionamiento de respuesta con varios valores](#).

 Note

La opción Evaluar el estado del destino está marcada de forma predeterminada y evaluará el estado del punto de conexión al que se dirige el tráfico mediante un registro de alias. Si el punto de conexión no recibe tráfico de DNS a través de un registro de alias, desmárquelo y cree una comprobación de estado si desea supervisar el estado del punto de conexión. Para obtener más información, consulte [Creación y actualización de comprobaciones de estado](#).

Weighted rule

Elija esta opción cuando tenga varios recursos que realicen la misma función (por ejemplo, servidores web que atienden el mismo sitio web) y desee que Route 53 dirija el tráfico a esos recursos en las proporciones que usted especifique (por ejemplo, un tercio a un servidor y dos tercios al otro).

Cuando elija Weighted rule (Regla ponderada), escriba la ponderación que desea aplicar a esta regla.

Para obtener más información, consulte [Direccionamiento ponderado](#).

Note

La opción Evaluar el estado del destino está marcada de forma predeterminada y evaluará el estado del punto de conexión al que se dirige el tráfico mediante un registro de alias. Si el punto de conexión no recibe tráfico de DNS a través de un registro de alias, desmárquelo y cree una comprobación de estado si desea supervisar el estado del punto de conexión. Para obtener más información, consulte [Creación y actualización de comprobaciones de estado](#).

Punto de conexión

Elija esta opción para especificar el recurso, como una CloudFront distribución o un balanceador de cargas ELB, al que desea enrutar las consultas de DNS.

Existing rule

Elija esta opción cuando desee dirigir las consultas DNS a una regla existente en esta política de tráfico. Por ejemplo, puede crear dos o más reglas de geolocalización que dirijan las consultas de diferentes países a la misma regla de conmutación por error. La regla de conmutación por error podría dirigir entonces las consultas a dos balanceadores de carga de ELB.

Esta opción no está disponible si la política de tráfico no incluye ninguna regla.

Existing endpoint

Elija esta opción cuando desee dirigir las consultas DNS a un puntos de conexión existente. Por ejemplo, si tiene dos reglas de conmutación por error, tal vez desee dirigir las consultas DNS para ambas opciones On failover (secundarias) al mismo balanceador de carga de ELB.

Esta opción no está disponible si la política de tráfico no incluye puntos de enlace.

Tipo de valor

Elija la opción aplicable:

CloudFront distribución

Elija esta opción si desea enrutar el tráfico a una CloudFront distribución. La opción solo está disponible si selecciona A: dirección IP en IPv4 formato para el tipo DNS o AAAA: dirección IP en IPv6 formato para el tipo DNS.

Note

CloudFront los puntos finales de alias no admiten la evaluación del estado. Sin embargo, puede crear una comprobación de estado para supervisar los puntos CloudFront finales. Para obtener más información, consulte [Creación y actualización de comprobaciones de estado](#).

Equilibrador de carga de aplicación ELB

Elija esta opción si desea enrutar el tráfico a un balanceador de cargas de aplicaciones ELB. La opción solo está disponible si elige A: dirección IP en IPv4 formato o AAAA: dirección IP en IPv6 formato para el tipo de DNS.

Equilibrador de carga clásico ELB

Elija esta opción si desea enrutar el tráfico a un balanceador de cargas ELB Classic. La opción solo está disponible si selecciona A: dirección IP en IPv4 formato o AAAA: dirección IP en IPv6 formato para el tipo de DNS.

Equilibrador de carga de red ELB

Elija esta opción si desea enrutar el tráfico a un balanceador de cargas de red ELB. La opción solo está disponible si elige A: dirección IP en IPv4 formato o AAAA: dirección IP en IPv6 formato para el tipo de DNS.

Entorno de Elastic Beanstalk

Seleccione esta opción si desea enrutar el tráfico a un entorno de Elastic Beanstalk. La opción solo está disponible si selecciona A: dirección IP en IPv4 formato para el tipo de DNS.

S3 website endpoint

Elija esta opción si desea dirigir el tráfico a un bucket de Amazon S3 configurado como punto de conexión de un sitio web. La opción solo está disponible si selecciona A: dirección IP en IPv4 formato para el tipo de DNS.

Type DNS type value

Elija esta opción si desea que Route 53 responda a las consultas de DNS usando el valor del campo Value (Valor). Por ejemplo, si ha elegido A para el valor de DNS type al crear esta política de tráfico, esta opción de la lista Value type será Type A value. Esto requiere que introduzca una dirección IP en IPv4 formato en el campo Valor. Route 53 responderá a las consultas de DNS que se dirigen a este punto de conexión con la dirección IP del campo Valor.

Valor

Elija o escriba un valor en función de la opción que haya elegido para Value type (Tipo de valor):

CloudFront distribución

Elija una CloudFront distribución de la lista de distribuciones asociadas a la AWS cuenta corriente.

Equilibrador de carga de aplicación ELB

Elija un balanceador de carga de aplicaciones ELB de la lista de balanceadores de carga asociados a la cuenta corriente. AWS

Equilibrador de carga clásico ELB

Elija un balanceador de cargas ELB Classic de la lista de balanceadores de carga asociados a la cuenta corriente. AWS

Equilibrador de carga de red ELB

Elija un balanceador de carga ELB Network de la lista de balanceadores de carga asociados a la cuenta corriente. AWS

Entorno de Elastic Beanstalk

Elija un entorno de Elastic Beanstalk de la lista de entornos asociados con la Cuenta de AWS actual.

S3 website endpoint

Elija un bucket de Amazon S3 de la lista de buckets de Amazon S3 que estén configurados como puntos de enlace de sitios web y que estén asociados a la cuenta corriente AWS .

Important

Cuando cree un registro de política basado en esta política de tráfico, el bucket que elija aquí debe coincidir con el nombre de dominio (como `www.ejemplo.com`) que especifique para [Policy record DNS name](#) en el registro de política. Si Value (Valor) y Policy record DNS name (Nombre DNS de registro de política) no coinciden, Amazon S3 no responderá a las consultas de DNS del nombre del dominio.

Type DNS type value

Introduzca un valor que se corresponda con el valor especificado para DNS type cuando se inició esta política de tráfico. Por ejemplo, si ha elegido MX para DNS type (Tipo de DNS), introduzca dos valores: la prioridad que desea asignar a un servidor de correo electrónico y el nombre de dominio del servidor de correo, como `10 sydney.mail.example.com`.

Para obtener más información acerca de los tipos de DNS admitidos, consulte [Tipos de registros de DNS admitidos](#).

Clave (solo en la consola nueva)

Introduzca un nombre descriptivo para una regla de enrutamiento o un punto de conexión en Clave. Este valor se muestra como el nombre de un nodo en el editor.

Visualización de un mapa que muestra el efecto de la configuración de geoproximidad

Una regla de geoproximidad le permite especificar las ubicaciones de sus recursos, tanto en Regiones de AWS las Zonas Locales como, mediante la latitud y la longitud, en AWS ubicaciones distintas. Cuando crea una regla de geoproximidad, Route 53 enruta el tráfico de Internet al recurso más cercano a los usuarios de forma predeterminada. También puede elegir enrutar más o menos tráfico a un recurso especificando un sesgo que amplía o reduce el área geográfica desde la que se enruta el tráfico a un recurso. Para obtener más información acerca del direccionamiento de geoproximidad, consulte [Enrutamiento por geoproximidad](#).

Note

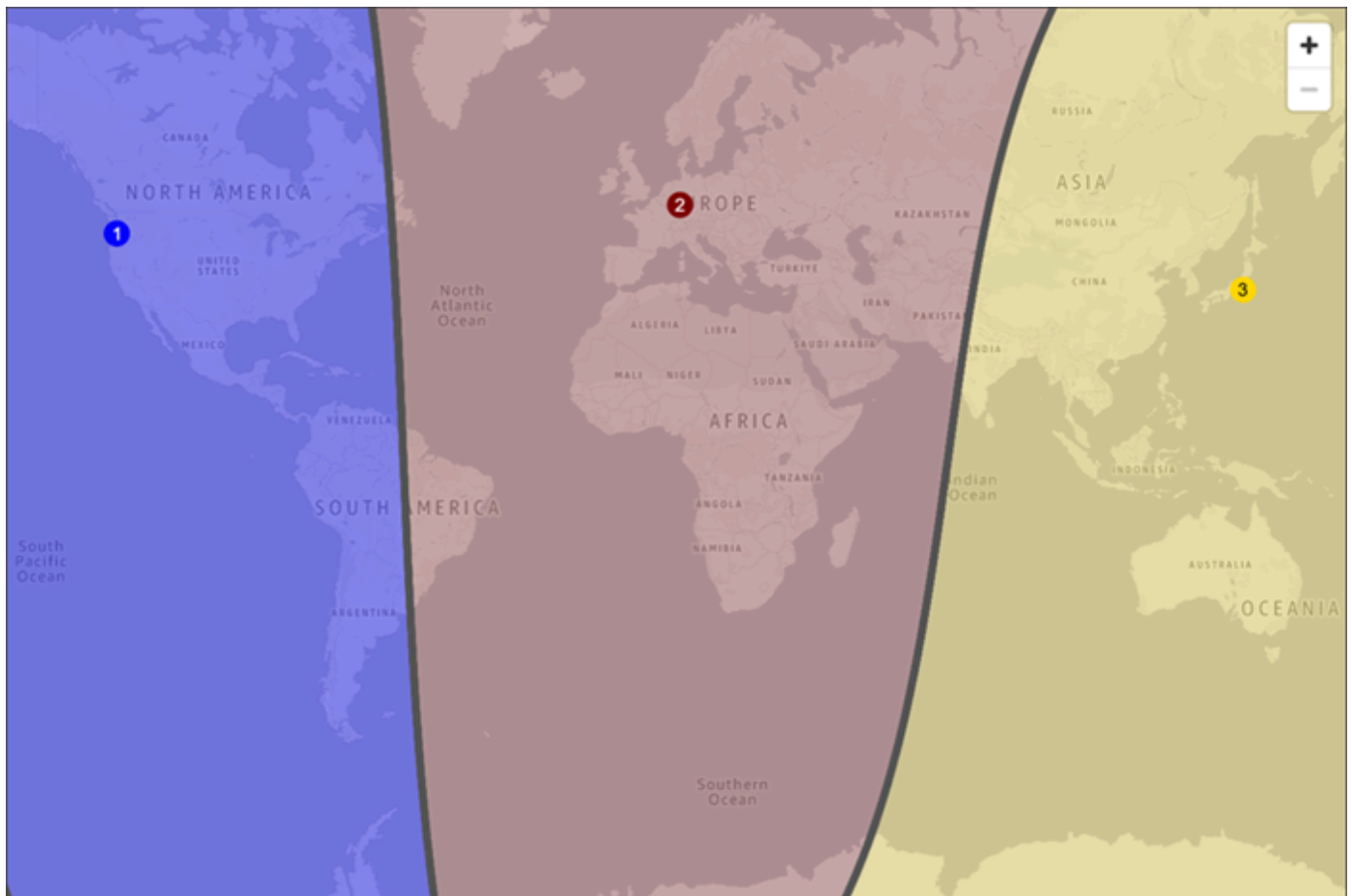
Estamos actualizando la consola de Flujo de tráfico para Route 53. Durante el periodo de transición, puede seguir utilizando la consola anterior.

Seleccione la pestaña de la consola que esté utilizando.

- [Nueva consola](#)
- [Consola antigua](#)

New console

Puede mostrar un mapa que presente el efecto de su configuración de geoproximidad actual. Por ejemplo, si tiene recursos en las regiones Oeste de EE. UU. (Oregón), Europa (Fráncfort) y Asia-Pacífico (Tokio) y si no especifica un sesgo, el mapa tiene el siguiente aspecto.



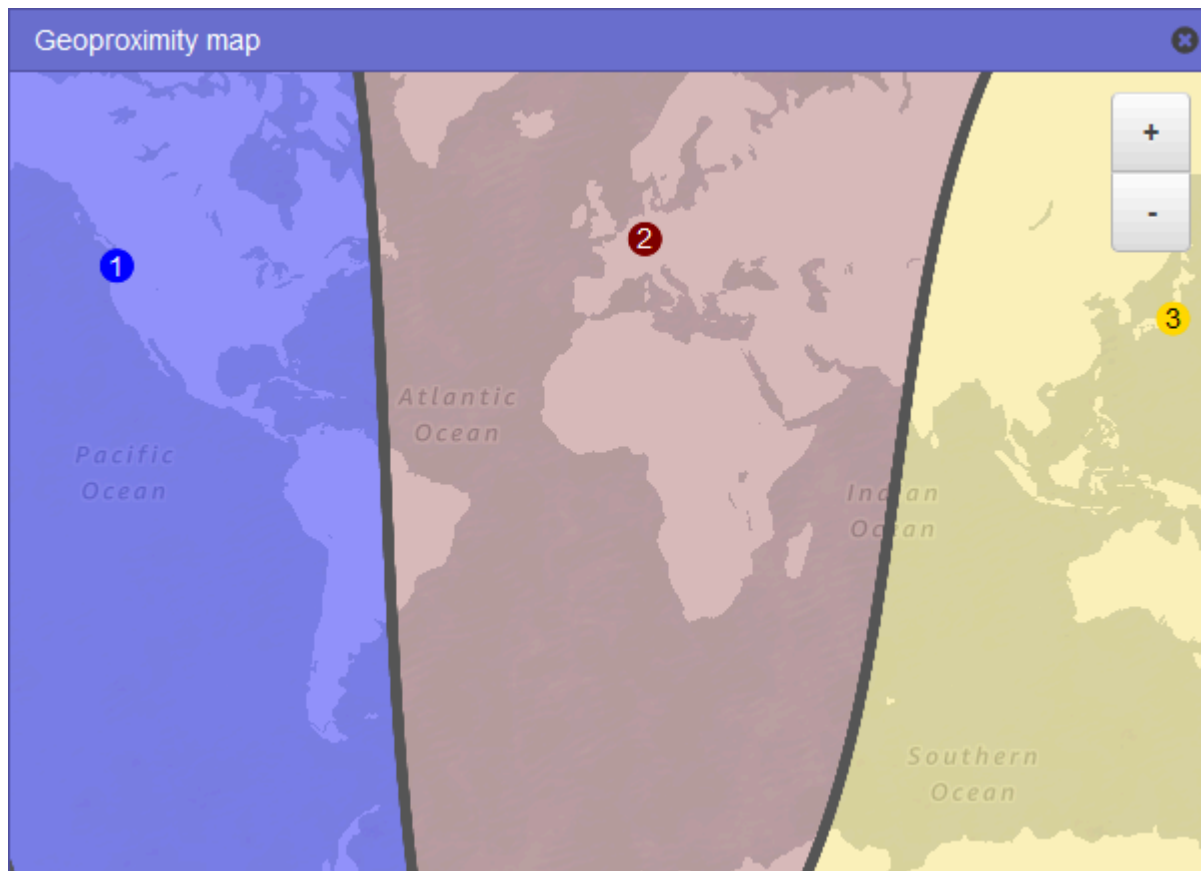
El mapa de una regla de geoproximidad se muestra automáticamente en Propiedades y se actualiza al añadir o eliminar regiones.

Tenga en cuenta lo siguiente:

- El mapa tiene una precisión de un radio de aproximadamente 10 millas (16 kilómetros).
- El mapa se ajusta automáticamente cuando se agregan, editan o eliminan regiones, o cuando se cambia la configuración de sesgo para una región.
- El número de región y el color de cada definición de regla se corresponden con los números y colores del mapa.
- Puede acercar y alejar la imagen para ver más o menos detalles. Utilice los botones + y - del mapa, un panel táctil o la rueda del ratón para cambiar el nivel de zoom. Si no ve la región ni el número de la región, puede ampliar el panel Propiedades, y aparecerán.
- Puede mover el mapa dentro de la ventana para ver áreas específicas. Utilice un panel táctil o haga clic en el mapa y arrástrelo con el ratón. También puede mover el mapa en la ventana del navegador.
- Si tiene varias reglas de geoproximidad en una política, puede ver el mapa solo para una regla a la vez.

Old console

Puede mostrar un mapa que presente el efecto de su configuración de geoproximidad actual. Por ejemplo, si tiene recursos en las regiones Oeste de EE. UU. (Oregón), Europa (Fráncfort) y Asia-Pacífico (Tokio) y si no especifica un sesgo, el mapa tiene el siguiente aspecto.



Para mostrar el mapa para una regla de geoproximidad, seleccione el icono de gráfico situado junto a Mostrar mapa de geoproximidad. (Este icono aparece en la parte superior de la regla). Para ocultar el mapa, vuelva a elegir el icono o la x en la esquina superior derecha del mapa.

Tenga en cuenta lo siguiente:

- El mapa tiene una precisión de un radio de aproximadamente 10 millas (16 kilómetros).
- El mapa se ajusta automáticamente cuando se agregan, editan o eliminan regiones, o cuando se cambia la configuración de sesgo para una región.
- El número de región y el color de cada definición de regla se corresponden con los números y colores del mapa.
- Puede acercar y alejar la imagen para ver más o menos detalles. Utilice los botones + y - del mapa, un panel táctil o la rueda del ratón para cambiar el nivel de zoom.
- Puede mover el mapa dentro de la ventana para ver áreas específicas. Utilice un panel táctil o haga clic en el mapa y arrástrelo con el ratón. También puede mover el mapa en la ventana del navegador.

- Si tiene varias reglas de geoproximidad en una política, puede ver el mapa solo para una regla a la vez.

Creación de versiones adicionales de una política de tráfico

Cuando se edita una política de tráfico, Amazon Route 53 crea automáticamente otra versión de la política de tráfico y conserva las versiones anteriores a menos que decida eliminarlas. La nueva versión tiene el mismo nombre que la política de tráfico que está editando; se diferencia de la versión original por un número de versión que Route 53 incrementa automáticamente. Puede basar la nueva versión de una política de tráfico en cualquier versión existente de una política de tráfico que tenga el mismo nombre.

Route 53 no reutiliza los números de versión para las nuevas versiones de una política de tráfico. Por ejemplo, si crea tres versiones de MyTrafficPolicy, elimina las dos últimas y, a continuación, crea otra, la nueva versión será la versión 4. Al conservar las versiones anteriores, Route 53 garantiza que se pueda restaurar una configuración anterior si una nueva configuración no dirige el tráfico según lo previsto.

Para crear una nueva versión de política de tráfico, siga el procedimiento que se indica a continuación.

Note

Estamos actualizando la consola de Flujo de tráfico para Route 53. Durante el periodo de transición, puede seguir utilizando la consola anterior.

Seleccione la pestaña de la consola que esté utilizando.

- [Nueva consola](#)
- [Consola antigua](#)

New console

Para crear otra versión de una política de tráfico

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.

2. En el panel de navegación, seleccione Traffic policies.
3. Elija el nombre de la política de tráfico de la que desea crear una nueva versión.
4. En la tabla Traffic policy versions situada en la parte superior de la página, seleccione la casilla de verificación de la versión de política de tráfico que desea usar como punto de partida para la nueva versión de política de tráfico.
5. Elija Edit policy as new version.
6. En el cuadro de diálogo Editar política como versión nueva, escriba una descripción de la nueva versión de la política de tráfico. Le recomendamos que especifique una descripción que distinga esta versión de otras versiones de la misma política de tráfico. Cuando se crea un nuevo registro de política, el valor que se especifica aparece en la lista de versiones disponibles para esta política de tráfico.
7. Elija Siguiente.
8. Actualice la configuración según corresponda. Para obtener más información, consulte [Valores que especifica cuando crea una política de tráfico](#).

Puede eliminar reglas, puntos de enlace y ramas de una política de tráfico de las formas siguientes:

- Para eliminar una regla o un punto de conexión, selecciónelo en el editor y, a continuación, seleccione Eliminar en el panel Propiedades.

 Important

Si elimina una regla que tiene reglas secundarias y puntos de enlace, Route 53 elimina también todos los elementos secundarios.

- Si conecta dos reglas a la misma regla secundaria o punto de conexión y desea eliminar una de las conexiones, coloque el cursor en la conexión que desee eliminar y seleccione Eliminar en el panel Propiedades.
9. Cuando termine de realizar cambios, seleccione Save as new version.
 10. Opcional: especifique la configuración para crear uno o varios registros de política en una zona alojada mediante la nueva versión de la política de tráfico. Para obtener más información, consulte [Valores que especifica al crear o actualizar un registro de política](#). También puede crear registros de política más adelante, en la misma zona alojada o en otras zonas hospedadas.

Si no desea crear registros de políticas ahora, seleccione Cancelar y la consola mostrará la lista de políticas de tráfico y registros de políticas que ha creado con la AWS cuenta corriente.

11. Si ha especificado valores para los registros de política en el paso anterior, elija Create policy record.

Old console

Para crear otra versión de una política de tráfico

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, seleccione Traffic policies.
3. Elija el nombre de la política de tráfico de la que desea crear una nueva versión.
4. En la tabla Traffic policy versions situada en la parte superior de la página, seleccione la casilla de verificación de la versión de política de tráfico que desea usar como punto de partida para la nueva versión de política de tráfico.
5. Elija Edit policy as new version.
6. En la página Update description (Actualizar descripción), escriba una descripción para la nueva versión de la política de tráfico. Le recomendamos que especifique una descripción que distinga esta versión de otras versiones de la misma política de tráfico. Cuando se crea un nuevo registro de política, el valor que se especifica aparece en la lista de versiones disponibles para esta política de tráfico.
7. Elija Siguiente.
8. Actualice la configuración según corresponda. Para obtener más información, consulte [Valores que especifica cuando crea una política de tráfico](#).

Puede eliminar reglas, puntos de enlace y ramas de una política de tráfico de las formas siguientes:

- Para eliminar una regla o un puntos de conexión, haga clic en la x situada en la esquina superior derecha del cuadro.

 Important

Si elimina una regla que tiene reglas secundarias y puntos de enlace, Route 53 elimina también todos los elementos secundarios.

- Si conecta dos reglas a la misma regla secundaria o puntos de conexión y desea eliminar una de las conexiones, coloque el cursor en la conexión que desea eliminar y haga clic en la x de esa conexión.

9. Cuando termine de realizar cambios, seleccione Save as new version.
10. Opcional: especifique la configuración para crear uno o varios registros de política en una zona alojada mediante la nueva versión de la política de tráfico. Para obtener más información, consulte [Valores que especifica al crear o actualizar un registro de política](#). También puede crear registros de política más adelante, en la misma zona alojada o en otras zonas hospedadas.

Si no desea crear registros de políticas ahora, elija Omitir este paso y la consola mostrará la lista de políticas de tráfico y registros de políticas que ha creado con la AWS cuenta corriente.

11. Si ha especificado valores para los registros de política en el paso anterior, elija Create policy record.

Creación de una política de tráfico con un documento JSON

Puede crear una nueva política de tráfico o una nueva versión de una política de tráfico existente importando un documento en formato JSON que describa todos los puntos de enlace y reglas que desea incluir en la política de tráfico. Para obtener información sobre el formato del documento JSON y varios ejemplos que puede copiar y revisar, consulte [Formato de documentos de políticas de tráfico](#) en la Referencia de la API de Amazon Route 53.

La forma más sencilla de obtener el documento con formato JSON para una versión de política de tráfico existente es utilizar el `get-traffic-policy` comando de la CLI. AWS Para obtener más información, consulte [get-traffic-policy](#) en la Referencia de comandos de la AWS CLI .

El archivo JSON creado por el comando `get-traffic-policy` incluye barras invertidas (\) como caracteres de escape. Antes de importar el archivo JSON, sustituya todas las barras invertidas por caracteres nulos.

 Note

Estamos actualizando la consola de Flujo de tráfico para Route 53. Durante el periodo de transición, puede seguir utilizando la consola anterior.

Seleccione la pestaña de la consola que esté utilizando.

- [Nueva consola](#)
- [Consola antigua](#)

New console

Para crear una política de tráfico importando un documento JSON

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en.
<https://console.aws.amazon.com/route53/>
2. Para crear una nueva política de tráfico importando un documento JSON, realice los pasos siguientes:
 - a. En el panel de navegación, seleccione Traffic policies.
 - b. Elija Create traffic policy.
 - c. En la página Name policy, especifique los valores correspondientes. Para obtener más información, consulte [Valores que especifica cuando crea una política de tráfico](#).
 - d. Vaya al paso 4.
3. Para crear una nueva versión de una política de tráfico existente importando un documento JSON, realice los pasos siguientes:
 - a. En el panel de navegación, seleccione Traffic policies.
 - b. Elija el nombre de la política de tráfico en la que desea basar la nueva versión.
 - c. En la tabla Traffic policy versions, seleccione la casilla de verificación de la versión en la que desea basar la nueva versión.
 - d. Elija Edit policy as new version.
 - e. En la página Update description (Actualizar descripción), escriba una descripción para la nueva versión.
 - f. Vaya al paso 4.

4. Elija Siguiente.
5. En la página del editor, elija el icono del editor json



situado en la esquina superior derecha del editor.

6. Escriba una nueva política de tráfico, pegue una política de tráfico de ejemplo o pegue una política de tráfico existente.

Para ver ejemplos de políticas, consulte los [ejemplos de políticas de Flujo de tráfico en JSON](#).

7. Elija Actualizar.

Old console

Para crear una política de tráfico importando un documento JSON

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. Para crear una nueva política de tráfico importando un documento JSON, realice los pasos siguientes:
 - a. En el panel de navegación, seleccione Traffic policies.
 - b. Elija Create traffic policy.
 - c. En la página Name policy, especifique los valores correspondientes. Para obtener más información, consulte [Valores que especifica cuando crea una política de tráfico](#).
 - d. Vaya al paso 4.
3. Para crear una nueva versión de una política de tráfico existente importando un documento JSON, realice los pasos siguientes:
 - a. En el panel de navegación, seleccione Traffic policies.
 - b. Elija el nombre de la política de tráfico en la que desea basar la nueva versión.
 - c. En la tabla Traffic policy versions, seleccione la casilla de verificación de la versión en la que desea basar la nueva versión.
 - d. Elija Edit policy as new version.
 - e. En la página Update description (Actualizar descripción), escriba una descripción para la nueva versión.

- f. Vaya al paso 4.
4. Elija Siguiente.
5. Elija Import traffic policy.
6. Escriba una nueva política de tráfico, pegue una política de tráfico de ejemplo o pegue una política de tráfico existente.

Para ver ejemplos de políticas, consulte los [ejemplos de políticas de Flujo de tráfico en JSON](#).

7. Elija Import traffic policy.

Consultar versiones de políticas de tráfico y los registros de políticas asociados

Puede ver todas las versiones que ha creado para una política de tráfico, así como todos los registros de políticas que ha creado mediante cada una de las versiones de la política de tráfico.

Note

Estamos actualizando la consola de Flujo de tráfico para Route 53. Durante el periodo de transición, puede seguir utilizando la consola anterior.

Seleccione la pestaña de la consola que esté utilizando.

- [Nueva consola](#)
- [Consola antigua](#)

New console

Para ver las versiones de una política de tráfico y los registros de política asociados

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, seleccione Traffic policies.
3. Seleccione el nombre vinculado de una política de tráfico.

4. La tabla superior muestra todas las versiones que ha creado de una política de tráfico. La tabla incluye la siguiente información:

Número de versión

El número de cada versión de una política de tráfico que ha creado. Si elige el número de versión, la consola mostrará la configuración de dicha versión.

Number of policy records

El número de registros de política que ha creado mediante esta versión de la política de tráfico.

DNS type

El tipo de DNS especificado al crear la versión de la política de tráfico.

Descripciones de la versión

La descripción especificada al crear la versión de la política de tráfico.

5. La tabla inferior muestra todos los registros de política que ha creado mediante las versiones de políticas de tráfico de la tabla superior. La tabla incluye la siguiente información:

Nombre de DNS

Los nombres DNS a los que ha asociado la política de tráfico.

Status

Entre los valores posibles se incluyen:

Applied

Route 53 ha terminado de crear o actualizar un registro de política y los registros correspondientes.

Creación

Route 53 está creando registros para un nuevo registro de política.

Actualización

Ha actualizado un registro de política y Route 53 está creando un nuevo grupo de registros que sustituirá al grupo existente de registros del nombre DNS especificado.

Eliminación

Route 53 está eliminando un registro de política y los registros asociados.

Con error

Route 53 no pudo crear o actualizar el registro de política ni los registros asociados.

DNS type

El tipo de DNS de todos los registros que Route 53 creó para este registro de política. Cuando edita un registro de política, debe especificar una versión de política de tráfico que tenga el mismo tipo DNS que el tipo DNS del registro de política que está editando.

Versión

Indica la versión de la política de tráfico que se utilizó para crear el registro de política.

TTL (in seconds)

El tiempo, en segundos, en que desea que los solucionadores recursivos de DNS almacenen en caché información sobre este registro. Si especifica un valor más largo (por ejemplo, 172 800 segundos o dos días), pagará menos por el servicio de Route 53 porque los solucionadores recursivos enviarán solicitudes a Route 53 con menos frecuencia. No obstante, la aplicación de los cambios en los registros (por ejemplo, una nueva dirección IP) lleva más tiempo porque los servicios de resolución recursiva usan los valores de su memoria caché durante períodos más largos en lugar de solicitar la información más reciente a Route 53.

Old console

Para ver las versiones de una política de tráfico y los registros de política asociados

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, seleccione Traffic policies.
3. Elija el nombre de una política de tráfico.
4. La tabla superior muestra todas las versiones que ha creado de una política de tráfico. La tabla incluye la siguiente información:

Número de versión

El número de cada versión de una política de tráfico que ha creado. Si elige el número de versión, la consola mostrará la configuración de dicha versión.

Number of policy records

El número de registros de política que ha creado mediante esta versión de la política de tráfico.

DNS type

El tipo de DNS especificado al crear la versión de la política de tráfico.

Version description

La descripción especificada al crear la versión de la política de tráfico.

5. La tabla inferior muestra todos los registros de política que ha creado mediante las versiones de políticas de tráfico de la tabla superior. La tabla incluye la siguiente información:

Policy record DNS name

Los nombres DNS a los que ha asociado la política de tráfico.

Status

Entre los valores posibles se incluyen:

Applied

Route 53 ha terminado de crear o actualizar un registro de política y los registros correspondientes.

Creación

Route 53 está creando registros para un nuevo registro de política.

Actualización

Ha actualizado un registro de política y Route 53 está creando un nuevo grupo de registros que sustituirá al grupo existente de registros del nombre DNS especificado.

Eliminación

Route 53 está eliminando un registro de política y los registros asociados.

Con error

Route 53 no pudo crear o actualizar el registro de política ni los registros asociados.

Version used

Indica la versión de la política de tráfico que se utilizó para crear el registro de política.

DNS type

El tipo de DNS de todos los registros que Route 53 creó para este registro de política. Cuando edita un registro de política, debe especificar una versión de política de tráfico que tenga el mismo tipo DNS que el tipo DNS del registro de política que está editando.

TTL (in seconds)

El tiempo, en segundos, en que desea que los solucionadores recursivos de DNS almacenen en caché información sobre este registro. Si especifica un valor más largo (por ejemplo, 172 800 segundos o dos días), pagará menos por el servicio de Route 53 porque los solucionadores recursivos enviarán solicitudes a Route 53 con menos frecuencia. No obstante, la aplicación de los cambios en los registros (por ejemplo, una nueva dirección IP) lleva más tiempo porque los servicios de resolución recursiva usan los valores de su memoria caché durante períodos más largos en lugar de solicitar la información más reciente a Route 53.

Eliminación de versiones de una política de tráfico y políticas de tráfico

Para eliminar una política de tráfico, debe eliminar todas las versiones (incluida la original) que haya creado para la política de tráfico. Asimismo, para eliminar una versión de una política de tráfico, debe eliminar todos los registros de política que haya creado usando la versión de política de tráfico.

Important

Si elimina registros de política que Amazon Route 53 utiliza para responder a las consultas de DNS, Route 53 dejará de responder a las consultas de los nombres DNS correspondientes. Por ejemplo, si Route 53 utiliza el registro de política de `www.example.com` para responder a las consultas de DNS de `www.example.com` y usted elimina el registro de política, los usuarios no podrán obtener acceso a su sitio web o aplicación web utilizando el nombre de dominio `www.example.com`.

Para eliminar las versiones de una política de tráfico y, opcionalmente, una política de tráfico, realice el siguiente procedimiento:

 Note

Estamos actualizando la consola de Flujo de tráfico para Route 53. Durante el periodo de transición, puede seguir utilizando la consola anterior.

Seleccione la pestaña de la consola que esté utilizando.

- [Nueva consola](#)
- [Consola antigua](#)

New console

Para eliminar las versiones de una políticas de tráfico y una política de tráfico

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, seleccione Traffic policies.
3. Seleccione el nombre vinculado de la política de tráfico cuyas versiones desee eliminar y que, opcionalmente, desee eliminar por completo.
4. Si las versiones de la política de tráfico que desea eliminar en la parte superior de la tabla aparecen en la columna Versión utilizada de la tabla de Registros de políticas, seleccione las casillas de verificación de los registros de políticas correspondientes de la tabla inferior.

Por ejemplo, si desea eliminar la versión 3 de una política de tráfico, pero ha creado uno de los registros de política de la tabla inferior usando la versión 3, seleccione la casilla de verificación de ese registro de política.

5. Seleccione Eliminar registros de políticas y, en el cuadro de diálogo Eliminar registro de políticas, elija Confirmar.
6. Actualice la página hasta que los registros de políticas que ha eliminado ya no aparezcan en la tabla.
7. En la tabla superior, seleccione las casillas de verificación de las versiones de política de tráfico que desea eliminar.

8. Elija Eliminar.
9. Si ha eliminado todas las versiones de la política de tráfico en el paso anterior y desea eliminar también la política de tráfico, actualice la página para que se actualice la pantalla hasta que la tabla esté vacía.
10. En el panel de navegación, seleccione Traffic policies.
11. En la lista de políticas de tráfico, seleccione la casilla de verificación de la política de tráfico que desea eliminar.
12. Elija Delete traffic policy.

Old console

Para eliminar las versiones de una políticas de tráfico y una política de tráfico

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, seleccione Traffic policies.
3. Elija el nombre de la política de tráfico cuyas versiones de política de tráfico desea eliminar y que, opcionalmente, desea eliminar completamente.
4. Si las versiones de la política de tráfico que desea eliminar en la parte superior de la tabla aparecen en la columna Version used de la tabla inferior, seleccione las casillas de verificación de los registros de política correspondientes de la tabla inferior.

Por ejemplo, si desea eliminar la versión 3 de una política de tráfico, pero ha creado uno de los registros de política de la tabla inferior usando la versión 3, seleccione la casilla de verificación de ese registro de política.

5. Elija Delete policy records.
6. Elija el botón de actualización de la tabla inferior para actualizar la pantalla hasta que los registros de política que ha eliminado dejen de aparecer en la tabla.
7. En la tabla superior, seleccione las casillas de verificación de las versiones de política de tráfico que desea eliminar.
8. Elija Delete version.
9. Si ha eliminado todas las versiones de política de tráfico en el paso anterior y desea eliminar también la política de tráfico, elija el botón de actualización de la tabla superior para actualizar la pantalla hasta que la tabla esté vacía.
10. En el panel de navegación, seleccione Traffic policies.

11. En la lista de políticas de tráfico, seleccione la casilla de verificación de la política de tráfico que desea eliminar.
12. Elija Delete traffic policy.

Creación y administración de registros de política

Para enrutar el tráfico de Internet a los recursos que especificó cuando creó una [política de tráfico](#), cree uno o más registros de política. Cada registro de política identifica la zona alojada a la que desea crear el registro de política y el nombre del dominio o subdominio para el que desea enrutar el tráfico. Por ejemplo, si desea enrutar el tráfico para `www.example.com`, especifique el ID de la zona alojada `example.com` y especifique `www.example.com` para Policy record DNS name (Nombre DNS de registro de política).

Si desea utilizar la misma política de tráfico para enrutar el tráfico de varios dominios o subdominios, tiene dos opciones:

- Puede crear un registro de política para cada nombre de dominio o subdominio.
- Puede crear un registro de política y, a continuación, crear registros CNAME o de alias que hagan referencia al registro de política.

Por ejemplo, si desea utilizar la misma política de tráfico para `example.com`, `example.net` y `example.org`, puede hacer cualquiera de las siguientes acciones:

- Cree un registro de política para cada uno.
- Cree un registro de política para uno y, a continuación, cree registros CNAME en las zonas alojadas para los otros dos. En los dos registros CNAME, especifique el nombre del registro para el que creó un registro de política.

Si desea utilizar la misma política de tráfico para un dominio y sus subdominios, como `example.com` y `www.example.com`, puede crear un registro de política para un nombre y, a continuación, crear registros de alias para el resto. Por ejemplo, puede crear un registro de política para `example.com` y, a continuación, crear un registro de alias para `www.example.com` que tenga el registro `example.com` como el destino de alias.

 Note

Hay un cargo mensual por cada registro de política que cree. Si desea utilizar la misma política de tráfico para varios nombres de dominio o subdominio, puede utilizar registros CNAME o de alias para reducir los cargos:

- Si crea un registro de política y uno o más registros CNAME que hagan referencia al registro de política, solo pagará por el registro de política y por las consultas DNS de los registros CNAME.
- Si crea un registro de política y uno o más registros de alias en la misma zona alojada que hacen referencia al registro de política, solo pagará el registro de política y las consultas DNS de los registros de alias.

Temas

- [Creación de registros de política](#)
- [Valores que especifica al crear o actualizar un registro de política](#)
- [Actualización de registros de política](#)
- [Eliminación de registros de política](#)

Creación de registros de política

Para crear un registro de política, siga el procedimiento que se indica a continuación.

 Important

Para cada registro de política que cree, se le cobrará una cuota mensual. Si posteriormente elimina el registro de política, el cargo se prorrateará. Para obtener más información, consulte la sección “Flujo de tráfico” de la página [Precios de Amazon Route 53](#).

 Note

Estamos actualizando la consola de Flujo de tráfico para Route 53. Durante el periodo de transición, puede seguir utilizando la consola anterior.

Seleccione la pestaña de la consola que esté utilizando.

- [Nueva consola](#)
- [Consola antigua](#)

New console

Creación de un registro de política

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, seleccione Policy records.
3. En la página Policy records, elija Create policy records.
4. En la página Create policy records, especifique los valores correspondientes. Para obtener más información, consulte [Valores que especifica al crear o actualizar un registro de política](#).
5. Para añadir registros adicionales a la misma zona alojada, seleccione Añadir registro de políticas.
6. Elija Create policy records.

El estado del registro de política creada puede tardar varios minutos en aparecer como Aplicado.

7. Si desea crear registros de política en otra zona alojada, repita los pasos 3 a 5.

Note

Si el estado del registro de políticas es Fallido, pulse el botón de información situado junto al estado para obtener más información sobre el error. Si necesita más ayuda y desea ponerse en contacto con el servicio de AWS asistencia, consulte [¿Cómo puedo obtener asistencia técnica AWS?](#)

Old console

Creación de un registro de política

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.

2. En el panel de navegación, seleccione Policy records.
3. En la página Policy records, elija Create policy records.
4. En la página Create policy records, especifique los valores correspondientes. Para obtener más información, consulte [Valores que especifica al crear o actualizar un registro de política](#).
5. Elija Create policy records.

El estado del registro de política creada puede tardar varios minutos en aparecer como Aplicado.

6. Si desea crear registros de política en otra zona alojada, repita los pasos 3 a 5.

 Note

Si el estado del registro de políticas es Fallido, pulse el botón de información situado junto al estado para obtener más información sobre el error. Si necesita más ayuda y desea ponerse en contacto con el servicio de AWS asistencia, consulte [¿Cómo puedo obtener asistencia técnica AWS?](#)

Valores que especifica al crear o actualizar un registro de política

 Note

Estamos actualizando la consola de Flujo de tráfico para Route 53. Durante el periodo de transición, puede seguir utilizando la consola anterior. La siguiente lista se aplica a ambas consolas, excepto donde se indique lo contrario.

Cuando crea o actualiza un registro de política, especifica los siguientes valores

- [Traffic policy](#)
- [Version](#)
- [Hosted zone](#)
- [Policy record DNS name](#)
- [TTL](#)

Traffic policy

Elija la política de tráfico cuya configuración desea utilizar para este registro de política.

Versión

Elija la versión de la política de tráfico cuya configuración desea utilizar para este registro de política.

Si va a actualizar un registro de política existente, debe elegir una versión cuyo tipo de DNS coincida con el tipo de DNS actual del registro de política. Por ejemplo, si el tipo de DNS del registro de política es A, debe elegir una versión en la que el tipo de DNS sea A.

Hosted zone

Elija la zona alojada en la que desea crear un registro de política mediante la política de tráfico y la versión especificadas. No se puede cambiar el valor de Hosted zone después de crear un registro de política.

Nombre de DNS (consola nueva), Nombre de DNS del registro de políticas (consola antigua)

Cuando cree un registro de política, ingrese el nombre de dominio o el nombre de subdominio para el que desea que Route 53 responda a las consultas de DNS mediante la configuración de la política de tráfico y la versión especificadas.

Para utilizar la misma configuración para varios nombres de dominio o nombres de subdominio en la zona alojada especificada, elija Agregar registro de políticas (consola nueva) o Agregar otro registro de políticas (consola antigua), e introduzca el nombre de dominio o nombre de subdominio y TTL correspondientes.

No se puede cambiar el valor de Policy record DNS name después de crear un registro de política.

TTL (in seconds)

Escriba el tiempo, en segundos, que desea que los solucionadores recursivos de DNS almacenen en caché información sobre este registro. Si especifica un valor más largo (por ejemplo, 172 800 segundos o dos días), pagará menos por el servicio de Route 53 porque los solucionadores recursivos enviarán solicitudes a Route 53 con menos frecuencia. No obstante, la aplicación de los cambios en los registros (por ejemplo, una nueva dirección IP) lleva más tiempo porque los servicios de resolución recursiva usan los valores de su memoria caché durante períodos más largos en lugar de solicitar la información más reciente a Route 53.

Actualización de registros de política

Para actualizar la configuración de un registro de política, siga el procedimiento que se indica a continuación.

Note

Estamos actualizando la consola de Flujo de tráfico para Route 53. Durante el periodo de transición, puede seguir utilizando la consola anterior.

Seleccione la pestaña de la consola que esté utilizando.

- [Nueva consola](#)
- [Consola antigua](#)

New console

Para actualizar un registro de política

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, seleccione Policy records.
3. En la página Registros de políticas, seleccione la casilla de verificación del registro de políticas que desea actualizar y elija Editar registro de políticas.
4. En la página Edit policy record, especifique los valores correspondientes. Para obtener más información, consulte [Valores que especifica al crear o actualizar un registro de política](#).
5. Elija Edit policy record.

El estado del registro de política creada puede tardar varios minutos en aparecer como Aplicado.

6. Si desea actualizar otro registro de política, repita los pasos 3 a 5.

Note

Si el estado del registro de políticas es Fallido, pulse el botón de información situado junto al estado para obtener más información sobre el error. Si necesita más ayuda y desea

ponerse en contacto con el servicio de AWS asistencia, consulte [¿Cómo puedo obtener asistencia técnica AWS?](#)

Old console

Para actualizar un registro de política

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, seleccione Policy records.
3. En la página Policy records, seleccione la casilla de verificación del registro de política que desea actualizar y elija Edit policy record.
4. En la página Edit policy record, especifique los valores correspondientes. Para obtener más información, consulte [Valores que especifica al crear o actualizar un registro de política](#).
5. Elija Edit policy record.

El estado del registro de política creada puede tardar varios minutos en aparecer como Aplicado.

6. Si desea actualizar otro registro de política, repita los pasos 3 a 5.

Note

Si el estado del registro de políticas es Fallido, pulse el botón de información situado junto al estado para obtener más información sobre el error. Si necesita más ayuda y desea ponerse en contacto con el servicio de AWS asistencia, consulte [¿Cómo puedo obtener asistencia técnica AWS?](#)

Eliminación de registros de política

Para eliminar registros de política, siga el procedimiento que se indica a continuación.

Important

Si elimina registros de política que Amazon Route 53 utiliza para responder a las consultas de DNS, Route 53 dejará de responder a las consultas de los nombres

DNS correspondientes. Por ejemplo, si Route 53 utiliza el registro de política de `www.example.com` para responder a las consultas de DNS de `www.example.com` y usted elimina el registro de política, los usuarios no podrán obtener acceso a su sitio web o aplicación web utilizando el nombre de dominio `www.example.com`.

 Note

Estamos actualizando la consola de Flujo de tráfico para Route 53. Durante el periodo de transición, puede seguir utilizando la consola anterior.

Seleccione la pestaña de la consola que esté utilizando.

- [Nueva consola](#)
- [Consola antigua](#)

New console

Para eliminar un registro de política

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, seleccione Policy records.
3. En la página Registros de políticas, seleccione las casillas de verificación de los registros de políticas que desea eliminar y seleccione Eliminar.
4. En el cuadro de diálogo Eliminar registro de políticas, seleccione Confirmar.

Espere unos minutos y actualice la página para asegurarse de que el registro de la política desaparezca de la lista.

Old console

Para eliminar un registro de política

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.

2. En el panel de navegación, seleccione Policy records.
3. En la página Policy records, seleccione las casillas de verificación de los registros de política que desea eliminar y elija Delete policy record.

Espere unos minutos y actualice la página para asegurarse de que el registro de la política desaparezca de la lista.

¿Qué es el solucionador de VPC Route 53?

El solucionador de VPC de Route 53 responde de forma recursiva a las consultas de DNS de AWS los recursos de registros públicos, los nombres de DNS específicos de Amazon VPC y las zonas alojadas privadas de Amazon Route 53, y está disponible de forma predeterminada en todos. VPCs

Note

Anteriormente, Route 53 VPC Resolver se llamaba Route 53 Resolver, pero se le cambió el nombre cuando se introdujo el Solucionador global de Route 53.

Una Amazon VPC se conecta a un solucionador de VPC en una dirección IP de VPC+2. Esta dirección de VPC+2 se conecta a un solucionador de VPC dentro de una zona de disponibilidad.

Un solucionador de VPC responde automáticamente a las consultas de DNS para:

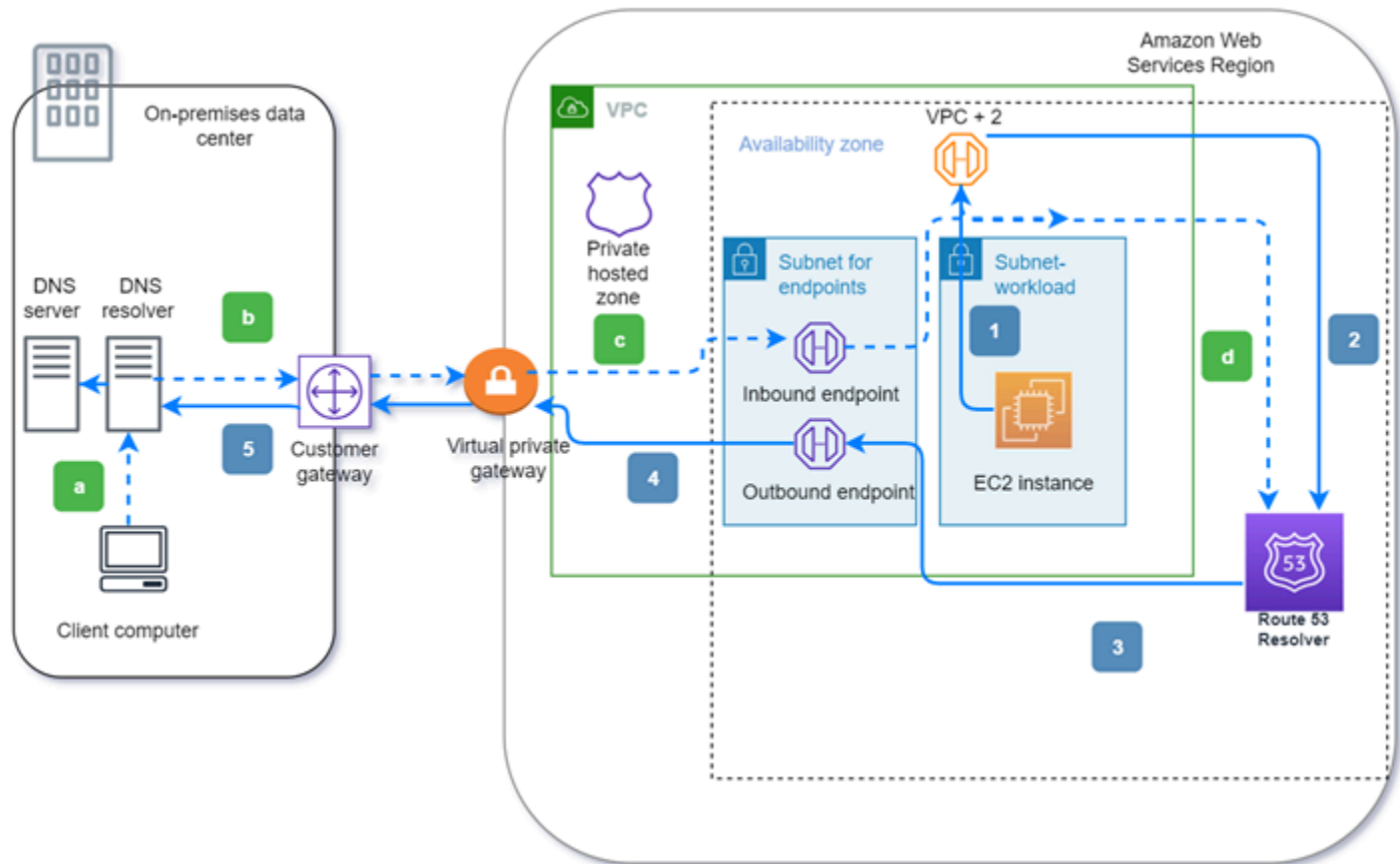
- Nombres de dominio de VPC locales para EC2 instancias (por ejemplo, `ec2-192-0-2-44.compute-1.amazonaws.com`).
- Registros en zonas alojadas privadas (p. ej., `acme.example.com`).
- En el caso de los nombres de dominio público, VPC Resolver realiza búsquedas recursivas en servidores de nombres públicos de Internet.

Si tiene cargas de trabajo que aprovechan tanto VPCs los recursos locales como los locales, también debe resolver los registros DNS alojados en las instalaciones. Del mismo modo, es posible que estos recursos locales necesiten resolver los nombres alojados en ellos. AWS Mediante los puntos finales de Resolver y las reglas de reenvío condicional, puede resolver consultas de DNS entre sus recursos locales y crear una configuración de nube híbrida VPCs a través de VPN o Direct Connect (DX). En concreto:

- Los puntos de conexión de Resolver entrantes permiten realizar consultas de DNS a la VPC desde la red ubicada en las instalaciones u otra VPC.
- Los puntos de conexión de Resolver salientes permiten realizar consultas de DNS desde la VPC a la red ubicada en las instalaciones u otra VPC.

- Las reglas de Resolver permiten crear una regla de reenvío para cada nombre de dominio y especificar el nombre del dominio para el que desea reenviar las consultas de DNS desde la VPC a un solucionador de DNS ubicado en las instalaciones y desde las instalaciones locales a la VPC. Las reglas se aplican directamente a la VPC y se pueden compartir en varias cuentas.

En el siguiente diagrama se muestra la resolución de DNS híbrida con puntos de conexión de Resolver. Tenga en cuenta que el diagrama está simplificado para mostrar solo una zona de disponibilidad.



El siguiente diagrama muestra los siguientes pasos:

Salientes (flechas continuas 1-5):

- Una EC2 instancia de Amazon debe resolver una consulta de DNS al dominio `internal.example.com`. El servidor de DNS con autoridad se encuentra en el centro de datos en las instalaciones. Esta consulta de DNS se envía a la VPC+2 de la VPC que se conecta al VPC Resolver.

2. Se configura una regla de reenvío de VPC Resolver para reenviar consultas a `internal.example.com` en el centro de datos local.
3. La consulta se reenvía a un punto de conexión de salida.
4. El punto final saliente reenvía la consulta al solucionador de DNS local a través de una conexión privada entre y el centro de datos. AWS La conexión puede ser una Direct Connect o ambas AWS Site-to-Site VPN, representada como una puerta de enlace privada virtual.
5. El solucionador de DNS local resuelve la consulta de DNS para `internal.example.com` y devuelve la respuesta a la EC2 instancia de Amazon por la misma ruta, a la inversa.

Entrantes (flechas discontinuas a–d):

- a. Un cliente del centro de datos local debe resolver una consulta de DNS a un AWS recurso del dominio `dev.example.com`. Envía la consulta al solucionador de DNS en las instalaciones.
- b. El solucionador de DNS en las instalaciones tiene una regla de reenvío que dirige las consultas a `dev.example.com` a un punto de conexión de entrada.
- c. La consulta llega al punto final de entrada a través de una conexión privada, por ejemplo AWS Site-to-Site VPN, Direct Connect o representada como una puerta de enlace virtual.
- d. El punto final entrante envía la consulta al Resolver de VPC, y el Resolver de VPC resuelve la consulta de DNS para `dev.example.com` y devuelve la respuesta al cliente por la misma ruta, a la inversa.

Temas

- [Resolución de consultas de DNS entre y tu red VPCs](#)
- [Disponibilidad y escalado del solucionador de VPC Route 53](#)
- [Introducción a Route 53 VPC Resolver](#)
- [Reenviar las consultas de DNS entrantes a tu VPCs](#)
- [Reenvío de consultas de DNS de salida a su red](#)
- [Tutorial sobre las reglas de delegación de Resolver](#)
- [Activar la validación de DNSSEC en Amazon Route 53](#)

Resolución de consultas de DNS entre y tu red VPCs

El solucionador de VPC contiene puntos finales que se configuran para responder a las consultas de DNS desde y hacia el entorno local.

Note

No se admite el reenvío de consultas de DNS privadas a direcciones CIDR + 2 de VPC desde los servidores de DNS de VPC en las instalaciones ni de otro tipo. Esto puede provocar resultados inestables. En su lugar, le recomendamos que utilice un punto de conexión de entrada de Resolver.

También puede integrar la resolución de DNS entre los solucionadores de VPC y los de DNS de la red mediante la configuración de reglas de reenvío. Su red puede incluir cualquier red a la que se pueda acceder desde la VPC, como las siguientes:

- La propia VPC
- Otra VPC interconectada
- Una red local a AWS la que se conecta mediante una VPN o una Direct Connect puerta de enlace de traducción de direcciones de red (NAT)

Antes de empezar a reenviar consultas, debe crear los puntos finales and/or entrantes y salientes de Resolver en la VPC conectada. Estos puntos de conexión proporcionan una ruta para las consultas entrantes o salientes:

Punto final entrante: los solucionadores de DNS de su red pueden reenviar las consultas de DNS al Resolver de VPC de Route 53 a través de este punto final

Hay dos tipos de puntos de enlace de entrada: un punto de enlace de entrada predeterminado que reenvía a las direcciones IP y un punto de enlace de entrada de delegación que delega la autoridad de un subdominio alojado en la zona alojada privada de Route 53 al solucionador de VPC de Route 53. Los puntos de enlace entrantes permiten a los solucionadores de DNS resolver fácilmente los nombres de dominio de AWS recursos, como EC2 instancias o registros, en una zona alojada privada de Route 53. Para obtener más información, consulte [Cómo los solucionadores de DNS de su red reenvían las consultas de DNS a los puntos finales del Resolver](#).

Punto final saliente: VPC Resolver reenvía de forma condicional las consultas a los solucionadores de la red a través de este punto final

Para reenviar las consultas seleccionadas, puede crear reglas de Resolver que especifiquen los nombres de dominio para las consultas de DNS que quiere reenviar (como example.com) y las direcciones IP de los solucionadores de DNS de la red a las que quiere reenviar las consultas. Si una consulta coincide con varias reglas (example.com, acme.example.com), VPC Resolver elige la regla con la coincidencia más específica (acme.example.com) y reenvía la consulta a las direcciones IP que especificó en esa regla. Existen tres tipos de reglas: reenvío, sistema y delegación. Para obtener más información, consulte [Cómo reenvían los puntos de conexión de Resolver las consultas de DNS de su red a su red VPCs](#).

Al igual que Amazon VPC, VPC Resolver es regional. En cada región en la que se VPCs encuentre, puede elegir si desea reenviar las consultas de su red VPCs a su red (consultas salientes), de su red a la suya VPCs (consultas entrantes) o ambas.

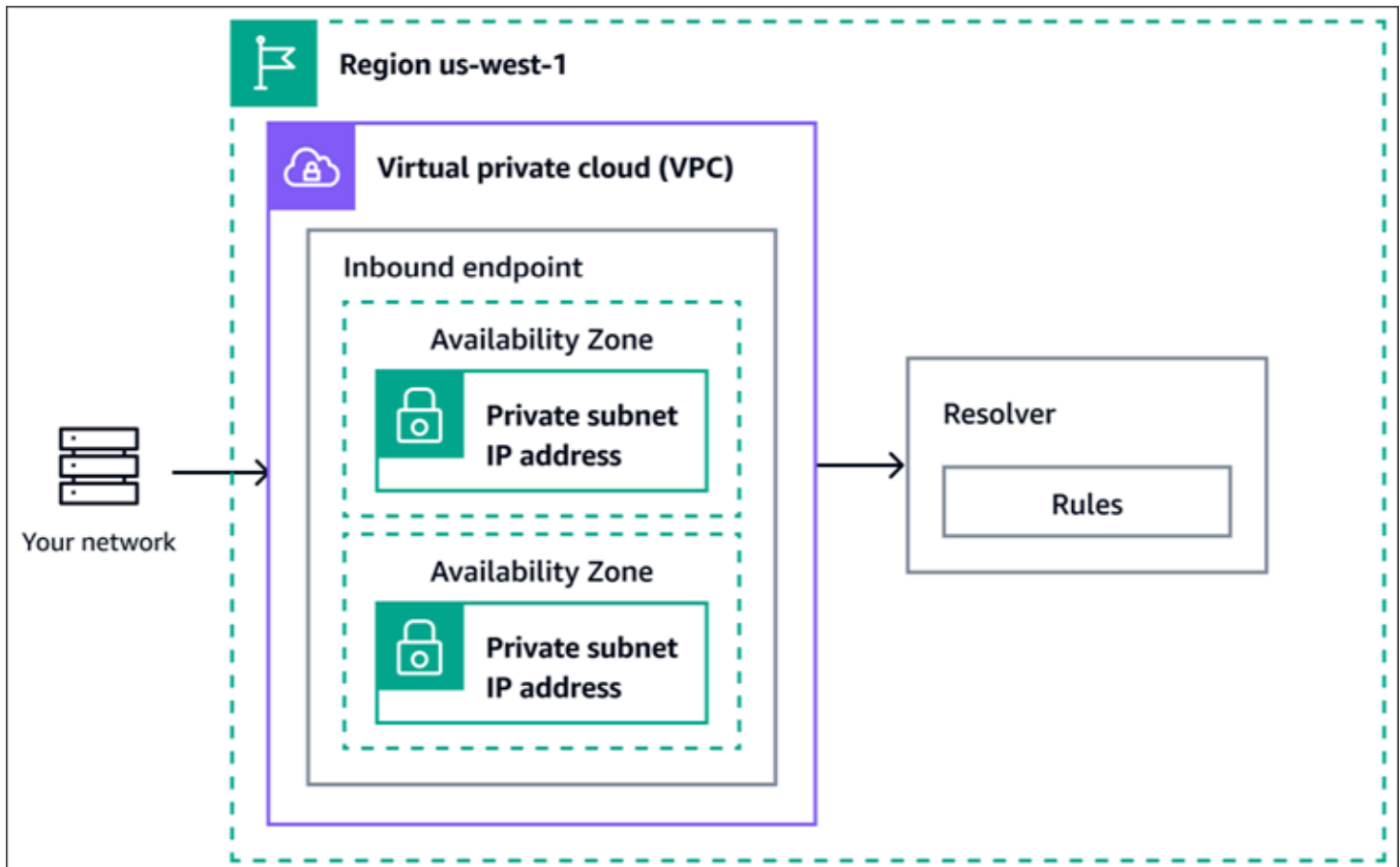
No puede crear puntos de conexión de Resolver en una VPC que no sea de su propiedad. Solo el propietario de la VPC puede crear recursos a nivel de VPC, como puntos de conexión entrantes.

 Note

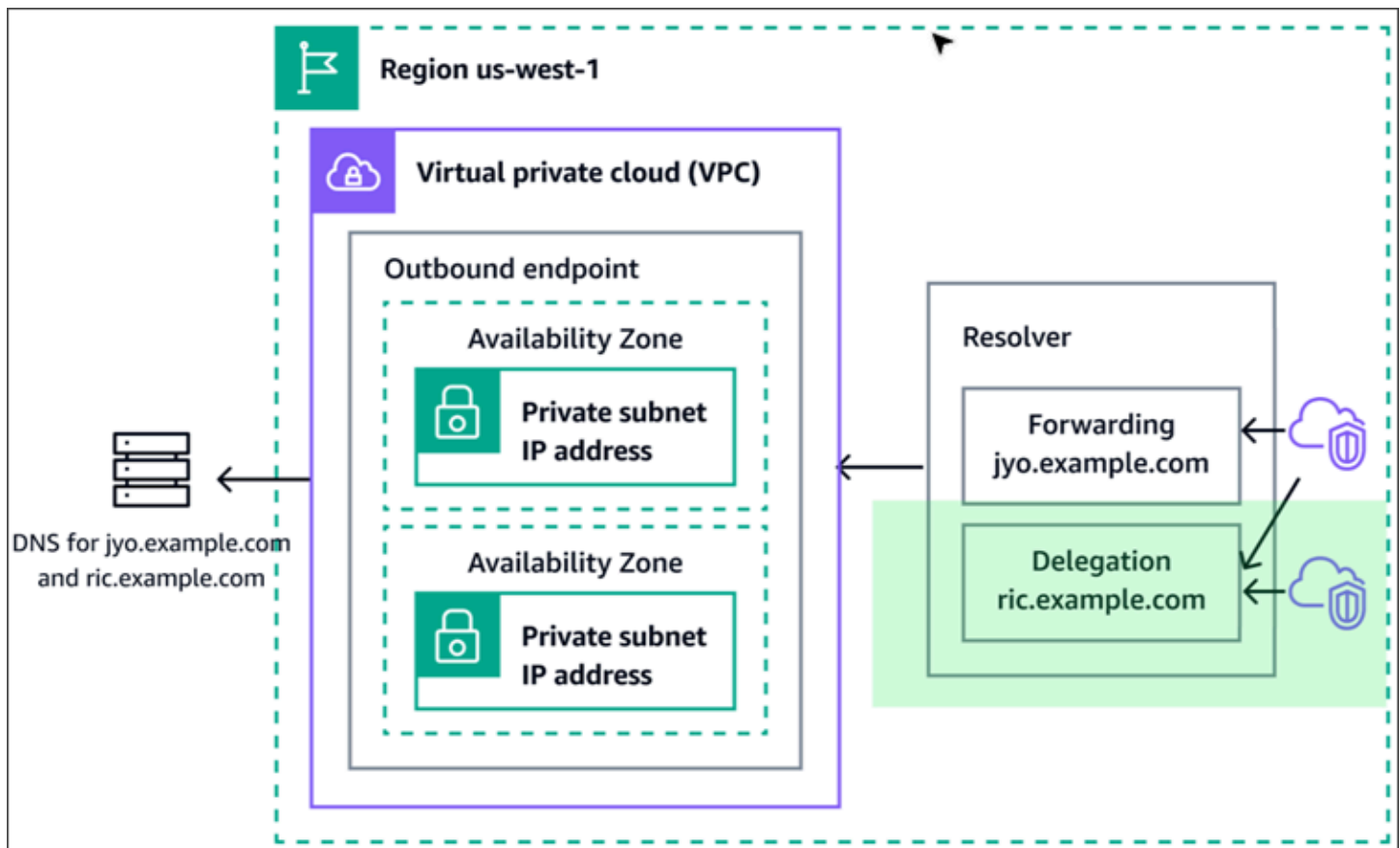
Cuando se crea un punto de conexión de Resolver, no se puede especificar una VPC que tenga el atributo de tenencia de la instancia establecido en dedicated. Para obtener más información, consulte .

Para utilizar el reenvío de entrada o salida, debe crear un punto de conexión de Resolver en la VPC. Como parte de la definición de un punto de conexión, debe especificar las direcciones IP, o delegación de DNS, a las que quiere reenviar las consultas de DNS entrantes o las direcciones IP desde las que quiere que procedan las consultas salientes. Para cada dirección IP y delegación que especifique, VPC Resolver crea automáticamente una interfaz de red elástica de VPC.

El siguiente diagrama muestra la ruta que sigue una consulta de DNS desde un solucionador de DNS de la red hasta los puntos de conexión de Route 53 Resolver.



El siguiente diagrama muestra la ruta de una consulta de DNS desde una EC2 instancia de una de sus instancias VPCs a un solucionador de DNS de su red. El dominio `jyo.example.com` usa una regla de reenvío, mientras que el subdominio `ric.example.com` ha delegado la autoridad de reenvío a VPC Resolver.



Para obtener información general acerca de las interfaces de red de VPC, consulte [Interfaces de red elásticas](#) en la Guía del usuario de Amazon VPC.

Temas

- [Cómo los solucionadores de DNS de su red reenvían las consultas de DNS a los puntos finales del Resolver](#)
- [Cómo reenvían los puntos de conexión de Resolver las consultas de DNS de su red a su red VPCs](#)
- [Consideraciones al crear puntos de conexión de entrada y salida](#)

Cómo los solucionadores de DNS de su red reenvían las consultas de DNS a los puntos finales del Resolver

Para reenviar las consultas de DNS de su red a Route 53 VPC Resolver, debe crear puntos de conexión entrantes en una región. AWS Hay dos categorías de puntos de conexión de entrada: los predeterminados y los de delegación.

Pasos para crear puntos de conexión de entrada predeterminados

1. Debe crear un punto final de entrada de Resolver predeterminado en una VPC y especificar las direcciones IP a las que los resolutores de la red reenvían las consultas de DNS, junto con un grupo de seguridad de VPC que incluye reglas de entrada que permiten el acceso TCP y UDP en el puerto 53. Para obtener instrucciones, consulte [Configuración del enrutamiento entrante](#).

Para cada dirección IP que especifique para el punto de enlace de entrada, el Resolver de VPC crea una interfaz de red elástica de VPC en la VPC en la que creó el punto de enlace de entrada.

2. Configurar los solucionadores de la red para que reenvíen las consultas de DNS de los nombres de dominio aplicables a las direcciones IP que especificó en el punto de conexión de entrada. Para obtener más información, consulte [Consideraciones al crear puntos de conexión de entrada y salida](#).

Así es como VPC Resolver resuelve las consultas de DNS que se originan en la red a través de un punto final de entrada predeterminado:

1. Un navegador web u otra aplicación de la red envía una consulta de DNS para un nombre de dominio que usted reenvía a VPC Resolver.
2. Un solucionador de su red reenvía la consulta a las direcciones IP del punto de conexión de entrada.
3. El punto final entrante reenvía la consulta a VPC Resolver.
4. El solucionador de VPC obtiene el valor aplicable al nombre de dominio en la consulta de DNS, ya sea internamente o mediante una búsqueda recursiva en los servidores de nombres públicos.
5. VPC Resolver devuelve el valor al punto final de entrada.
6. El punto de conexión de entrada devuelve el valor al solucionador de la red.
7. El solucionador de la red devuelve el valor a la aplicación.
8. Con el valor devuelto por VPC Resolver, la aplicación envía una solicitud, por ejemplo, una solicitud de un objeto en un bucket de Amazon S3.

Pasos para crear puntos de conexión de entrada de delegación

1. Se crea un punto final de entrada de Delegation Resolver en una VPC. Para obtener instrucciones, consulte [Configuración del enrutamiento entrante](#).

Para cada dirección IP que especifique para el punto de enlace de entrada, el Resolver de VPC crea una interfaz de red elástica de VPC en la VPC en la que creó el punto de enlace de entrada.

2. Los resolutores de la red se configuran para delegar las consultas de DNS de los nombres de dominio aplicables a VPC Resolver. En el caso de los registros de adherencia, debe introducir las direcciones IP de los puntos de conexión de entrada. Para obtener más información, consulte [Consideraciones al crear puntos de conexión de entrada y salida](#).

Así es como VPC Resolver resuelve las consultas de DNS que se originan en la red a través de un punto final entrante de delegación:

1. Como requisito previo, debe delegar el subdominio que está alojado en la zona alojada privada de la red en las instalaciones. Como delega el subdominio a través del punto de conexión de entrada de delegación, debe utilizar las direcciones IP del punto de conexión de entrada como los registros de adherencia del subdominio que se va a delegar.

 Note

Es posible que también deba incluir los registros de adherencia para asegurarse de que la consulta de DNS se pueda resolver. Si delega un subdominio a servidores de nombres que se encuentran en la misma zona que el dominio principal, necesitará registros de adherencia.

2. Un navegador web u otra aplicación de la red envía una consulta de DNS para un nombre de dominio que usted ha delegado al solucionador de VPC.
3. Un solucionador de su red reenvía la consulta a las direcciones IP del punto de conexión de entrada.
4. El punto final entrante delega la consulta en VPC Resolver.
5. El solucionador de VPC devuelve la dirección del AWS recurso desde la zona alojada privada al punto final de entrada.
6. El punto de conexión de entrada devuelve el valor al solucionador de la red.
7. El solucionador de la red devuelve el valor a la aplicación.
8. Con el valor devuelto por VPC Resolver, la aplicación envía una solicitud, por ejemplo, una solicitud de un objeto en un bucket de Amazon S3.

La creación de un punto final entrante no cambia el comportamiento del VPC Resolver, solo proporciona una ruta desde una ubicación fuera de la red hasta AWS el VPC Resolver.

Cómo reenvían los puntos de conexión de Resolver las consultas de DNS de su red a su red VPCs

Si desea reenviar consultas de DNS desde las EC2 instancias de una o más instancias VPCs de una AWS región a su red, lleve a cabo los siguientes pasos.

1. Se crea un punto final de salida de Resolver en una VPC y se especifican varios valores:
 - La VPC que quiere que atraviesen las consultas de DNS en el recorrido hacia los solucionadores de la red.
 - Un [grupo de seguridad de VPC](#) que incluye reglas de salida que permiten el acceso de TCP y UDP en el puerto 53 (o el puerto que usa para las consultas de DNS en su red).

Para cada dirección IP que especifique para el punto de conexión saliente, VPC Resolver crea una interfaz de red elástica de Amazon VPC en la VPC que especifique. Para obtener más información, consulte [Consideraciones al crear puntos de conexión de entrada y salida](#).

2. Puede crear una o más reglas que especifican los nombres de dominio de las consultas de DNS que desea delegar a VPC Resolver para que las reenvíen o desea que VPC Resolver las reenvíe a los solucionadores de su red. En el caso de las reglas de reenvío, también debe especificar las direcciones IP de los solucionadores. Para obtener más información, consulte [Uso de reglas para controlar qué consultas se reenvían a la red](#).
3. Asocia cada regla a la VPCs que desee reenviar las consultas de DNS a la red.

Uso de reglas para controlar qué consultas se reenvían a la red

Las reglas controlan qué consultas de DNS reenvía el punto final de Resolver a los solucionadores de DNS de la red y qué consultas responde VPC Resolver por sí mismo.

Hay dos formas de categorizar las reglas. Una es según quién crea las reglas:

- Reglas autodefinidas: VPC Resolver crea automáticamente reglas autodefinidas y las asocia a las suyas. VPCs La mayoría de estas reglas se aplican a los nombres de dominio AWS específicos para los que VPC Resolver responde a las consultas. Para obtener más información, consulte [Nombres de dominio para los que VPC Resolver crea reglas de sistema autodefinidas](#).
- Reglas personalizadas: puede crear reglas personalizadas y asociarlas a ellas. VPCs En la actualidad, puede crear dos tipos de reglas personalizadas: las reglas de reenvío condicional, también conocidas como reglas de reenvío, y las reglas de delegación. Las reglas de reenvío

hacen que VPC Resolver reenvíe las consultas de DNS de las VPCs suyas a las direcciones IP de los solucionadores de DNS de la red.

Si creas una regla de reenvío para el mismo dominio que una regla autodefinida, VPC Resolver reenvía las consultas de ese nombre de dominio a los solucionadores de DNS de tu red en función de la configuración de la regla de reenvío.

Las reglas de delegación reenvían las consultas de DNS con los registros de delegación correspondientes a la regla de delegación que coinciden con los registros NS en respuesta a los solucionadores de su red.

Otra forma de categorizar las reglas es según lo que hacen:

- Reglas de reenvío condicional: cree reglas de reenvío condicional (también denominadas reglas de reenvío) cuando quiera reenviar consultas de DNS para nombres de dominio especificados a los solucionadores de DNS de la red.
- Reglas del sistema: las reglas del sistema hacen que VPC Resolver anule selectivamente el comportamiento definido en una regla de reenvío. Al crear una regla del sistema, el solucionador de VPC resuelve las consultas de DNS para subdominios específicos que, de otro modo, resolverían los solucionadores de DNS de la red.

De forma predeterminada, las reglas de reenvío se aplican a un nombre de dominio y todos sus subdominios. Si quiere reenviar las consultas de un dominio a un solucionador de la red, pero no quiere reenviar las consultas a algunos subdominios, debe crear una regla de sistema para los subdominios. Por ejemplo, si crea una regla de reenvío para `example.com` pero no desea reenviar las consultas a `acme.example.com`, debe crear una regla de sistema y especificar `acme.example.com` para el nombre de dominio.

- Regla recursiva: VPC Resolver crea automáticamente una regla recursiva denominada Internet Resolver. Esta regla hace que el Resolver de VPC de Route 53 actúe como un solucionador recursivo para cualquier nombre de dominio para el que no haya creado reglas personalizadas y para los que el Resolver de VPC no haya creado reglas autodefinidas. Para obtener más información acerca de cómo anular este comportamiento, consulte “Reenvío de todas las consultas a su red”, más adelante en este tema.

Puede crear reglas personalizadas que se apliquen a nombres de dominio específicos (el suyo o la mayoría de los nombres de AWS dominio), a los nombres de AWS dominios públicos o a todos los nombres de dominio.

Reenvío a su red de las consultas para nombres de dominio específicos

Para reenviar a su red las consultas de un nombre de dominio específico, como `example.com`, debe crear una regla y especificar ese nombre de dominio. En el caso de las reglas de reenvío, también debe especificar las direcciones IP de los solucionadores de DNS de la red a las que quiere reenviar las consultas. En el caso de las reglas de delegación, debe crear el registro de delegación sobre el que quiere delegar la autoridad a los solucionadores en las instalaciones. A continuación, asocie cada regla a VPCs la que desee reenviar las consultas de DNS a la red. Por ejemplo, puede crear reglas diferentes para los dominios `example.com`, `example.org` y `example.net`. A continuación, puede asociar las reglas a las VPCs de una AWS región en cualquier combinación.

Reenvío a su red de las consultas de `amazonaws.com`

El nombre de dominio `amazonaws.com` es el nombre de dominio público para AWS recursos como EC2 instancias y depósitos de S3. Si quiere reenviar a su red las consultas de `amazonaws.com`, cree una regla, especifique `amazonaws.com` como nombre de dominio y especifique Reenvío o Delegación como tipo de regla, según el método que quiera usar.

Note

VPC Resolver no reenvía automáticamente las consultas de DNS para algunos subdominios de `amazonaws.com`, incluso si se crea una regla de reenvío para `amazonaws.com`. Para obtener más información, consulte [Nombres de dominio para los que VPC Resolver crea reglas de sistema autodefinidas](#). Para obtener más información acerca de cómo anular este comportamiento, consulte “Reenvío de todas las consultas a su red”, a continuación.

Reenvío de todas las consultas a su red

Si quieres reenviar todas las consultas a tu red, debes crear una regla y especificar «.» (punto) para el nombre de dominio y asocie la regla a la VPCs que desee reenviar todas las consultas de DNS a la red. El solucionador de VPC sigue sin reenviar todas las consultas de DNS a la red porque el uso de un solucionador de DNS externo AWS interrumpiría algunas funciones. Por ejemplo, algunos nombres de AWS dominio internos tienen rangos de direcciones IP internos a los que no se puede acceder desde fuera. AWS Para ver una lista de los nombres de dominio para los que las consultas no se reenvían a la red cuando se crea una regla para “.”, consulte [Nombres de dominio para los que VPC Resolver crea reglas de sistema autodefinidas](#).

Sin embargo, las reglas autodefinidas del sistema para el DNS inverso pueden desactivarse, permitiendo que la regla “.” reenvíe todas las consultas de DNS inverso a su red. Para más información acerca de cómo desactivar las reglas autodefinidas, consulte [Reglas de reenvío para consultas de DNS inversas en VPC Resolver](#).

Si desea probar a reenviar a la red las consultas de DNS de todos los nombres de dominio, incluidos los nombres de dominio que quedan excluidos del reenvío de forma predeterminada, puede crear una regla “.” y realizar una de las siguientes operaciones:

- Establecer la marca `enableDnsHostnames` de la VPC en `false`
- Crear reglas para los nombres de dominio que se indican en [Nombres de dominio para los que VPC Resolver crea reglas de sistema autodefinidas](#)

 Important

Si reenvías todos los nombres de dominio a tu red, incluidos los nombres de dominio que VPC Resolver excluye al crear una regla «.» , es posible que algunas funciones dejen de funcionar.

Cómo determina el solucionador de VPC si el nombre de dominio de una consulta coincide con alguna regla

El solucionador de VPC de Route 53 compara el nombre de dominio de la consulta de DNS con el nombre de dominio de las reglas asociadas a la VPC de la que se originó la consulta. VPC Resolver considera que los nombres de dominio coinciden en los siguientes casos:

- Los nombres de dominio coinciden exactamente
- El nombre de dominio en la consulta es un subdominio del nombre de dominio de la regla

Por ejemplo, si el nombre de dominio de la regla es `acme.example.com`, VPC Resolver considera que los siguientes nombres de dominio de una consulta de DNS coinciden:

- `acme.example.com`
- `zenith.acme.example.com`

Los siguientes nombres de dominio no son una coincidencia:

- example.com
- nadir.example.com

Si el nombre de dominio de una consulta coincide con el nombre de dominio de más de una regla (como example.com y www.example.com), VPC Resolver enruta las consultas DNS salientes mediante la regla que contiene el nombre de dominio más específico (www.example.com).

Cómo determina el solucionador de VPC a dónde reenviar las consultas de DNS

Cuando una aplicación que se ejecuta en una EC2 instancia de una VPC envía una consulta de DNS, Route 53 VPC Resolver realiza los siguientes pasos:

1. El solucionador comprueba los nombres de dominio de las reglas.

Si el nombre de dominio de una consulta coincide con el nombre de dominio de una regla de reenvío predeterminada, VPC Resolver reenvía la consulta a la dirección IP que especificó al crear el punto final de salida. A continuación, el punto de conexión de salida reenvía la consulta a las direcciones IP de los solucionadores de la red, que especificó al crear la regla.

Si el registro de delegación en respuesta coincide con la regla de delegación, Resolver delega la autoridad a los solucionadores en las instalaciones a través del punto de conexión de salida asociado a la regla de delegación.

Para obtener más información, consulte [Cómo determina el solucionador de VPC si el nombre de dominio de una consulta coincide con alguna regla](#).

2. El punto de conexión de Resolver reenvía las consultas de DNS en función de la configuración de la regla “.”.

Si el nombre de dominio de una consulta no coincide con el nombre de dominio de ninguna otra regla, VPC Resolver reenvía la consulta en función de la configuración de la opción «» autodefinida. regla (punto). La regla de los puntos se aplica a todos los nombres de dominio, excepto a algunos nombres de dominio AWS internos y nombres de registro en zonas alojadas privadas. Esta regla hace que VPC Resolver reenvíe las consultas de DNS a los servidores de nombres públicos si los nombres de dominio de las consultas no coinciden con ningún nombre de las reglas de reenvío personalizadas. Si desea reenviar todas las consultas a los solucionadores de DNS de su red, puede crear una regla de reenvío personalizada, especificar "." como nombre de dominio, especificar Forwarding (Reenvío) en Type (Tipo) y especificar las direcciones IP de esos solucionadores.

3. VPC Resolver devuelve la respuesta a la aplicación que envió la consulta.

Uso de reglas en varias regiones

El solucionador de VPC de Route 53 es un servicio regional, por lo que los objetos que cree en una AWS región solo están disponibles en esa región. Para utilizar la misma regla en más de una región, debe crear la regla en cada región.

La AWS cuenta que creó una regla puede compartirla con otras AWS cuentas. Para obtener más información, consulte [Compartir las reglas de Resolver con otras AWS cuentas y usar reglas compartidas](#).

Nombres de dominio para los que VPC Resolver crea reglas de sistema autodefinidas

El solucionador crea automáticamente reglas del sistema autodefinidas que definen cómo se resuelven de forma predeterminada las consultas de los dominios seleccionados:

- Para las zonas alojadas privadas y para los nombres EC2 de dominio específicos de Amazon (como `compute.amazonaws.com` y `compute.internal`), las reglas autodefinidas garantizan que tus zonas e EC2 instancias alojadas privadas sigan resolviéndose si creas reglas de reenvío condicional para nombres de dominio menos específicos, como «». (punto) o «com».
- En los nombres de dominio reservados públicamente (como `localhost` y `10.in-addr.arpa`), las prácticas recomendadas de DNS establecen que las consultas se respondan localmente en lugar de reenviarse a servidores de nombres públicos. Véase [RFC 6303, Locally Served DNS Zones](#).

Note

Si crea una regla de reenvío condicional para “.” (punto) o “com”, le recomendamos que también cree una regla del sistema para `amazonaws.com`. (Las reglas del sistema hacen que VPC Resolver resuelva localmente las consultas de DNS para dominios y subdominios específicos). La creación de esta regla del sistema mejora el rendimiento, reduce la cantidad de consultas que se reenvían a la red y reduce los cargos de la resolución de VPC.

Si desea anular una regla autodefinida, puede crear una regla de reenvío condicional para el mismo nombre de dominio.

También existe la posibilidad de desactivar las reglas autodefinidas. Para obtener más información, consulte [Reglas de reenvío para consultas de DNS inversas en VPC Resolver](#).

El solucionador de VPC crea las siguientes reglas autodefinidas.

Reglas para zonas alojadas privadas

Para cada zona alojada privada que asocie a una VPC, el solucionador de VPC crea una regla y la asocia a la VPC. Si asocias la zona alojada privada a varias VPCs, VPC Resolver asocia la regla a la misma. VPCs

La regla tiene el tipo Forward (Reenvío).

Reglas para varios nombres de dominio AWS internos

Todas las reglas para los nombres de dominio internos de esta sección presentan un tipo reenvío. El solucionador de VPC reenvía las consultas DNS de estos nombres de dominio a los servidores de nombres autorizados de la VPC.

Note

El solucionador de VPC crea la mayoría de estas reglas cuando se establece la `enableDnsHostnames` marca de una VPC en: `true`. El Resolver de VPC crea las reglas incluso si no se utilizan puntos finales de Resolver.

El solucionador de VPC crea las siguientes reglas autodefinidas y las asocia a una VPC cuando se establece la marca `enableDnsHostnames` de la VPC en: `true`

- *Region-name*.compute.internal, por ejemplo, eu-west-1.compute.internal. La región us-east-1 no utiliza este nombre de dominio.
- *Region-name*.computar. *amazon-domain-name*, por ejemplo, eu-west-1.compute.amazonaws.com o cn-north-1.compute.amazonaws.com.cn. La región us-east-1 no utiliza este nombre de dominio.
- ec2.internal. Solo la región us-east-1 utiliza este nombre de dominio.
- compute-1.internal. Solo la región us-east-1 utiliza este nombre de dominio.
- compute-1.amazonaws.com. Solo la región us-east-1 utiliza este nombre de dominio.

Las siguientes reglas autodefinidas son para la búsqueda de DNS inversa de las reglas que VPC Resolver crea cuando se establece `enableDnsHostnames` el indicador de la VPC en: `true`

- 10.in-addr.arpa
- 16.172.in-addr.arpa a 31.172.in-addr.arpa
- 168.192.in-addr.arpa
- 254.169.254.169.in-addr.arpa
- Reglas para cada uno de los rangos de CIDR para la VPC. Por ejemplo, si una VPC tiene un rango de CIDR de 10.0.0.0/23, el solucionador de VPC crea las siguientes reglas:
 - 0.0.10.in-addr.arpa
 - 1.0.10.in-addr.arpa

Las siguientes reglas autodefinidas, para los dominios relacionados con localhost, también se crean y asocian a una VPC cuando la marca `enableDnsHostnames` para la VPC se establece en `true`:

- [illegible]

El solucionador de VPC crea las siguientes reglas autodefinidas y las asocia a su VPC cuando conecta la VPC con otra VPC a través de una puerta de enlace de enlace de tránsito o interconexión de VPC, y con la compatibilidad de DNS habilitada:

- La búsqueda de DNS hacia atrás para los rangos de direcciones IP de la VPC del mismo nivel; por ejemplo, 0.192.in-addr.arpa

Si agrega un bloque IPv4 CIDR a una VPC, el solucionador de VPC agrega una regla autodefinida para el nuevo rango de direcciones IP.

- Si la otra VPC se encuentra en otra región, los siguientes nombres de dominio:
 - *Region-name*.compute.internal. La región us-east-1 no utiliza este nombre de dominio.
 - *Region-name*.computar. *amazon-domain-name*. La región us-east-1 no utiliza este nombre de dominio.
 - ec2.internal. Solo la región us-east-1 utiliza este nombre de dominio.
 - compute-1.amazonaws.com. Solo la región us-east-1 utiliza este nombre de dominio.

Una regla para todos los demás dominios

El solucionador de VPC crea un «.» regla (punto) que se aplica a todos los nombres de dominio que no se especificaron anteriormente en este tema. La regla «.» tiene un tipo de recursiva, lo que significa que la regla hace que el Resolver de VPC actúe como un solucionador recursivo.

Consideraciones al crear puntos de conexión de entrada y salida

Antes de crear puntos finales de Resolver entrantes y salientes en una AWS región, tenga en cuenta los siguientes aspectos.

Temas

- [Número de puntos de conexión de entrada y salida en cada región](#)
- [Uso de la misma VPC para los puntos de conexión de entrada y salida](#)
- [Puntos de conexión de entrada y zonas alojadas privadas](#)
- [Emparejamiento de VPC](#)
- [Direcciones IP en subredes compartidas](#)
- [Conexión entre su red y la red en la VPCs que crea los puntos de enlace](#)
- [Al compartir reglas, también comparte los puntos de conexión de salida](#)
- [Elección de protocolos para los puntos de conexión](#)
- [Uso de VPC Resolver si está configurado para la tenencia de instancias dedicadas VPCs](#)

Número de puntos de conexión de entrada y salida en cada región

Si desea integrar el DNS de una AWS región con el VPCs DNS de su red, normalmente necesitará un extremo de entrada de Resolver (para las consultas de DNS que reenvía a su red VPCs) y un punto final de salida (para las consultas que reenvía de su red a su red). VPCs Puede crear varios puntos de conexión de entrada y varios puntos de conexión de salida, pero un punto de conexión es suficiente para gestionar las consultas de DNS para cualquier dirección. Tenga en cuenta lo siguiente:

- Para cada punto de conexión de Resolver, debe especificar dos o más direcciones IP en diferentes zonas de disponibilidad. Cada dirección IP de un punto de conexión puede gestionar un amplio número de consultas de DNS por segundo. (Para obtener información acerca del número máximo actual de consultas por segundo por cada dirección IP de un punto de conexión, consulte [Cuotas](#)

[en el solucionador de VPC Route 53.](#)) Si necesita que VPC Resolver gestione más consultas, puede añadir más direcciones IP a su punto de conexión existente en lugar de añadir otro punto de conexión.

- Los precios de VPC Resolver se basan en la cantidad de direcciones IP de los puntos finales y en la cantidad de consultas de DNS que procesa el punto final. Cada punto de conexión incluye un mínimo de dos direcciones IP. Para obtener más información sobre los precios de VPC Resolver, consulte los precios de [Amazon Route 53](#).
- Cada regla especifica el punto de conexión de salida desde el que se reenvían las consultas de DNS. Si crea varios puntos de conexión de salida en una región de AWS y quiere asociar algunas o todas las reglas de Resolver con cada VPC, tiene que crear varias copias de esas reglas.

Uso de la misma VPC para los puntos de conexión de entrada y salida

Puede crear puntos de enlace entrantes y salientes en la misma VPC o en diferentes VPCs puntos de la misma región.

Para obtener más información, consulte [Prácticas recomendadas de Amazon Route 53](#).

Puntos de conexión de entrada y zonas alojadas privadas

Si desea que VPC Resolver resuelva las consultas de DNS entrantes mediante registros de una zona alojada privada, asocie la zona alojada privada a la VPC en la que creó el punto final de entrada.

Para obtener información sobre cómo asociar zonas alojadas privadas, consulte [VPCs Uso de zonas alojadas privadas](#)

Emparejamiento de VPC

Puede usar cualquier VPC de una AWS región para un punto final entrante o saliente, independientemente de si la VPC que elija está emparejada con otra. VPCs Para obtener más información, consulte [Amazon Virtual Private Cloud \(VPC\)](#).

Direcciones IP en subredes compartidas

Al crear un punto de conexión de entrada o salida, solo puede especificar una dirección IP en una subred compartida si la cuenta actual creó la VPC. Si otra cuenta crea una VPC y comparte una subred en la VPC con su cuenta, no puede especificar una dirección IP en esa subred. Para obtener más información sobre las subredes compartidas, consulte [Trabajar con subredes compartidas VPCs](#) en la Guía del usuario de Amazon VPC.

Conexión entre su red y la red en la VPCs que crea los puntos de enlace

Debe tener una de las siguientes conexiones entre la red y la red en la VPCs que crea los puntos finales:

- Puntos de conexión de entrada: debe configurar una conexión de [Direct Connect](#) o una [conexión de VPN](#) entre su red y cada VPC para la que cree un punto de conexión de entrada o salida.
- Puntos de conexión de salida: debe configurar una conexión de [Direct Connect](#), una [conexión de VPN](#) o una [puerta de enlace de traducción de dirección de red \(NAT\)](#) entre su red y cada VPC para la que cree un punto de conexión de salida.

Al compartir reglas, también comparte los puntos de conexión de salida

Al crear una regla, se especifica el punto de conexión saliente que desea que VPC Resolver utilice para reenviar las consultas de DNS a la red. Si compartes la regla con otra AWS cuenta, también compartes indirectamente el punto final de salida que especificas en la regla. Si ha utilizado más de una AWS cuenta para crear VPCs en una AWS región, puede hacer lo siguiente:

- Cree un punto de conexión de salida en la región.
- Cree reglas con una AWS cuenta.
- Comparte las reglas con todas las AWS cuentas que se hayan creado VPCs en la región.

Esto le permite usar un punto final de salida en una región para reenviar consultas de DNS a su red desde varios puntos de vista, VPCs incluso si VPCs se crearon con AWS cuentas diferentes.

Elección de protocolos para los puntos de conexión

Los protocolos de punto de conexión determinan cómo se transmiten los datos a un punto de conexión de entrada y desde un punto de conexión de salida. No es necesario cifrar las consultas de DNS para el tráfico de VPC porque cada flujo de paquetes de la red se autoriza individualmente según una regla para validar el origen y el destino correctos antes de transmitirlos y entregarlos. Es muy poco probable que la información pase arbitrariamente entre entidades sin la autorización específica tanto de la entidad emisora como de la entidad receptora. Si un paquete se enruta a un destino sin una regla que lo iguale, el paquete se descarta. Para obtener más información, consulte [Características de VPC](#).

Los protocolos disponibles son:

- Do53: DNS a través del puerto 53. Los datos se transmiten mediante el solucionador de VPC sin cifrado adicional. Si bien los datos no pueden ser leídos por terceros, se pueden ver dentro de las AWS redes. Utiliza UDP o TCP para enviar los paquetes. Do53 se utiliza principalmente para el tráfico dentro y entre Amazon VPCs. Actualmente, este es el único protocolo disponible para los puntos de conexión de entrada de delegación.
- DoH: los datos se transmiten a través de una sesión HTTPS cifrada. DoH añade un nivel de seguridad adicional, donde los usuarios no autorizados no pueden descifrar los datos y nadie puede leerlos excepto el destinatario previsto. No está disponible para los puntos de conexión de entrada de delegación.
- Doh-FIPS: los datos se transmiten en una sesión HTTPS cifrada que cumple con el estándar criptográfico FIPS 140-2. Admite solo puntos de conexión de entrada. Para obtener más información, consulte [FIPS PUB 140-2](#). No está disponible para los puntos de conexión de entrada de delegación.

En el caso de un punto de conexión de entrada de reenvío, puede aplicar los protocolos de la siguiente manera:

- Do53 y DoH en combinación.
- Do53 y DOH-FIPS en combinación.
- Do53 solo.
- DoH solo.
- DoH-FIPS solo.
- Ninguno, por lo que se trata como Do53.

Para un punto de conexión de salida, puede aplicar los protocolos de la siguiente manera:

- Do53 y DoH en combinación.
- Do53 solo.
- DoH solo.
- Ninguno, por lo que se trata como Do53.

Consulte también [Valores que se especifican al crear o editar puntos de conexión de entrada](#) y [Valores que se especifican al crear o editar puntos de conexión de salida](#).

Uso de VPC Resolver si está configurado para la tenencia de instancias dedicadas VPCs

Cuando se crea un punto de conexión de Resolver, no se puede especificar una VPC que tenga el [atributo de tenencia de la instancia](#) establecido en `dedicated`. El solucionador de VPC no se ejecuta en hardware de un solo inquilino.

Puede seguir utilizando VPC Resolver para resolver las consultas de DNS que se originan en una VPC. Cree al menos una VPC que tenga el atributo de propiedad de instancia establecido en `default` y especifique esa VPC cuando cree puntos de conexión de entrada y salida.

Al crear una regla de reenvío, puede asociarla con cualquier VPC, independientemente de la configuración del atributo de propiedad de instancia.

Disponibilidad y escalado del solucionador de VPC Route 53

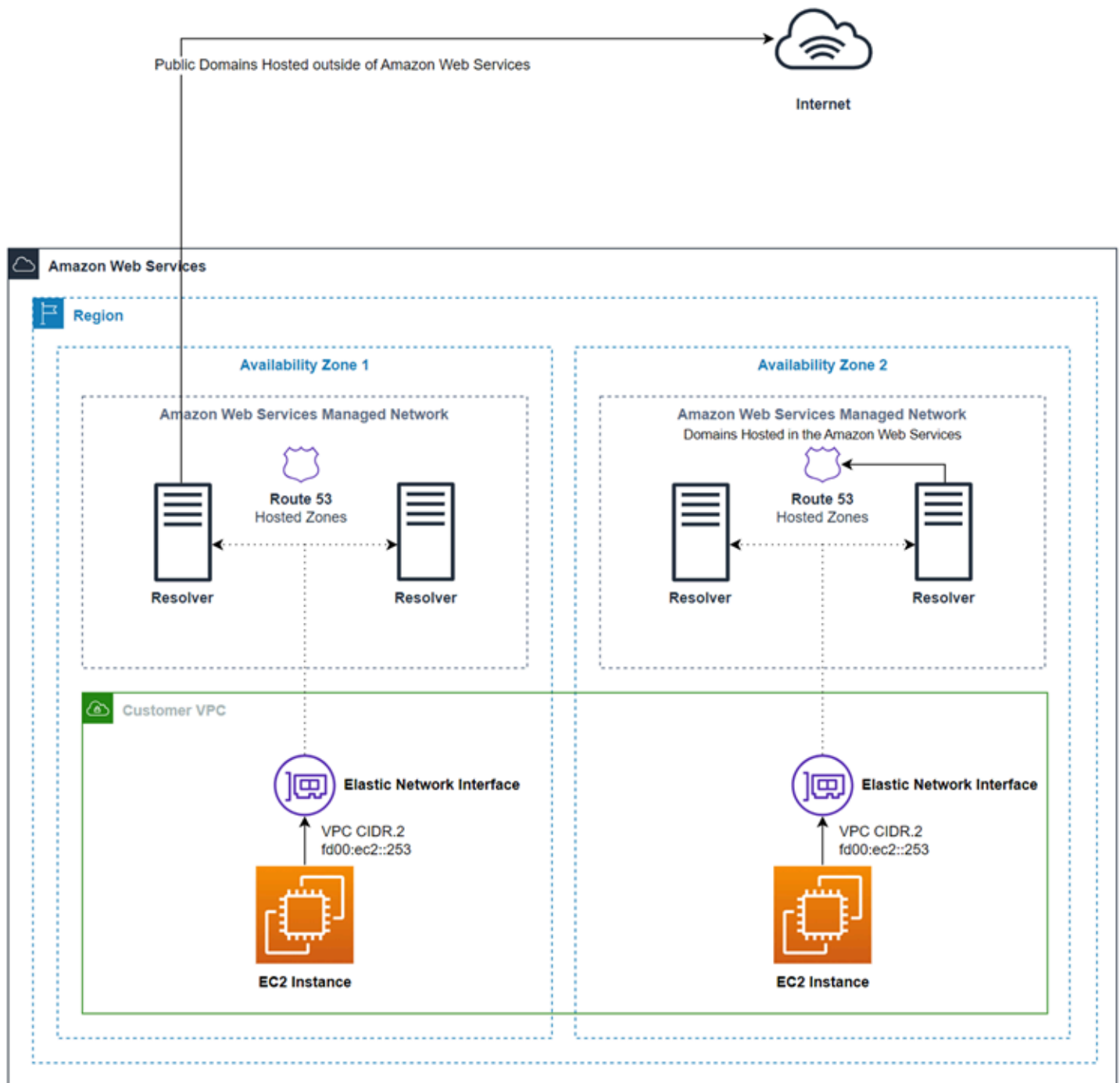
El solucionador de VPC Route 53, que se ejecuta en la dirección CIDR + 2 de Amazon VPC y `fd00:ec2::253`, está disponible de forma predeterminada en todos los servidores y responde de forma recursiva a las consultas de DNS de registros públicos VPCs, nombres de DNS específicos de Amazon VPC y zonas alojadas privadas de Route 53. Hay dos componentes de alta disponibilidad y transparentes para los usuarios que componen el Resolver VPC Route 53: el servicio Nitro Resolver y la flota de Resolver Zonal. El servicio Nitro Resolver es un servicio que se ejecuta en la tarjeta Nitro en las instancias Nitro y en Dom0 en las instancias de generaciones anteriores, y consume los paquetes dirigidos al Resolver de VPC de Route 53 de forma local en el servidor host. Para obtener más información, consulte [El diseño de seguridad del sistema Nitro. AWS](#)

El servicio Nitro Resolver incluye una caché local que puede ayudar a reducir la latencia al responder a las consultas repetidas que una instancia realiza durante un breve período de tiempo. Cuando el servicio Nitro Resolver recibe una consulta para la cual no tiene una respuesta en caché, reenvía la consulta a la flota de Zonal Resolver, una flota de solucionadores de alta disponibilidad que normalmente se encuentran en la misma zona de disponibilidad que la instancia. Cuando se producen errores al momento de administrar las consultas de los servidores de nombres ascendentes u otros componentes de la ruta, el servicio Nitro Resolver suele poder administrar estos errores de forma transparente sin que ello afecte a las cargas de trabajo que se ejecutan en la instancia. Además, si el Resolver detecta que se agota el tiempo de espera en las consultas, se deniegan las conexiones o se produce un error de SERVFAILS en los servidores de nombres del dominio, puede que responda con una respuesta en caché superior al valor Time-To-Live (TTL)

para mejorar la disponibilidad. Las consultas entre el servicio Nitro Resolver y la flota de Zonal Resolver están restringidas a una red estrictamente controlada fuera de la VPC del cliente, a la que los clientes no pueden acceder y están sujetas a rigurosos controles de seguridad. Al administrar las consultas entre el servicio Nitro Resolver y la flota de Zonal Resolver fuera de la VPC, los clientes no pueden interceptar las consultas de DNS dentro de la VPC. Las consultas destinadas a asignar nombres a servidores ajenos a ella AWS atravesarán la red pública de Internet y se originarán en direcciones IP públicas que pertenezcan a la flota de Zonal Resolver. En la actualidad, no admitimos el atributo de subred EDNS0-Client, lo que significa que todas las consultas destinadas a servidores de nombres DNS públicos no incluyen información sobre la dirección IP de origen del cliente.

El servicio Nitro Resolver forma parte de los servicios Link-Local de la instancia. Los servicios de Link-Local incluyen Route 53 VPC Resolver, Amazon Time Service (NTP), Instance Metadata Service (IMDS) y Windows Licensing Service (para instancias de Windows). Estos servicios se escalan con cada interfaz de red elástica que cree en la VPC y cada interfaz de red permite 1024 paquetes por segundo (PPS) destinados a los servicios Link-Local. Se rechazan los paquetes que superen este límite. Puede determinar si ha superado este límite a partir del valor `linklocal_allowance_exceeded` devuelto por `ethtool`. Para obtener más información sobre la `ethtool`, consulta [Supervisa el rendimiento de la red de tu EC2 instancia de Amazon](#) en la Guía del EC2 usuario de Amazon. El CloudWatch agente también puede informar de esta métrica a CloudWatch las métricas. Dado que el solucionador de VPC Route 53 se implementa por interfaz de red, se escala y se vuelve más confiable a medida que se agregan más instancias en más zonas de disponibilidad. No hay un límite agregado por VPC en cuanto al número de consultas, por lo que el Resolver de VPC de Route 53 puede escalar dentro de los límites de una VPC, lo que se basa intrínsecamente en el uso de direcciones de red (NAU). Para obtener más información, consulte [Uso de direcciones de red para la VPC](#) en la Guía del usuario de Amazon Virtual Private Cloud.

En el siguiente diagrama, se muestra una descripción general de cómo el solucionador de VPC de Route 53 resuelve las consultas de DNS en las zonas de disponibilidad.



Introducción a Route 53 VPC Resolver

La consola de VPC Resolver de Route 53 incluye un asistente que le guía por los siguientes pasos para empezar a usar VPC Resolver:

- Crear puntos de conexión: de entrada, de salida o ambos.

- Para los puntos de conexión de salida, cree una o más reglas de reenvío, que especifican los nombres de dominio para los que quiere dirigir las consultas de DNS a la red.
- Si ha creado un punto de conexión de salida, elija la VPC a la que quiere asociar las reglas.

Para configurar el Resolver de VPC de Route 53 mediante el asistente

1. Inicie sesión en la consola de VPC Resolver Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53resolver/>
2. En la página Bienvenido a Route 53 VPC Resolver, elija Configurar puntos finales.
3. En la barra de navegación, elija la región en la que desea crear un punto de conexión del solucionador.
4. En Basic configuration (Configuración básica), elija la dirección en la que desea reenviar las consultas de DNS:
 - Entrantes y salientes: el asistente le guía por los ajustes que le permiten reenviar consultas de DNS de los solucionadores de la red al solucionador de VPC de una VPC y reenviar consultas específicas (como example.com o example.net) desde una VPC a los solucionadores de la red.
 - Solo entrantes: el asistente lo guía a través de la configuración que le permite reenviar las consultas de DNS de los solucionadores de su red al solucionador de VPC en una VPC.
 - Inbound only (Solo salida): el asistente le guía por la configuración que permite reenviar las consultas especificadas de una VPC a los solucionadores de su red.
5. Elija Siguiente.
6. Si eligió Inbound and outbound (Entrada y salida) o Inbound only (Solo entrada), escriba los valores correspondientes para configurar un punto de conexión entrante. A continuación, prosiga con el paso 7. Para obtener más información, consulte [Valores que se especifican al crear o editar puntos de conexión de entrada](#).

Si elige Outbound only (Solo salida), vaya al paso 7.

7. Escriba los valores aplicables para configurar un punto de conexión de salida. Para obtener más información, consulte [Valores que se especifican al crear o editar puntos de conexión de salida](#).
8. Si eligió Inbound and outbound (Entrada y salida) u Outbound only (Solo salida), escriba los valores correspondientes para crear una regla. Para obtener más información, consulte [Valores que se especifican al crear o editar reglas](#).

9. En la página Review and create (Revisar y crear), confirme que la configuración que ha especificado en páginas anteriores sea correcta. Si fuera necesario, elija Edit (Editar) en la sección correspondiente y actualice la configuración. Cuando esté satisfecho con la configuración, haga clic en Submit (Enviar).

 Note

La creación de un punto de conexión de salida tarda uno o dos minutos. No se puede crear otro punto de conexión de salida hasta que no se haya creado el primero.

10. Si desea crear más reglas, consulte [Administración de reglas de reenvío](#).
11. Si creó un punto de conexión de entrada, configure los solucionadores de DNS de la red para que reenvíen las consultas de DNS aplicables a las direcciones IP del punto de conexión de entrada. Para obtener más información, consulte la documentación de su aplicación de DNS.

Reenviar las consultas de DNS entrantes a tu VPCs

Para reenviar las consultas de DNS de su red a VPC Resolver, debe crear un punto final entrante. Un punto de conexión entrante especifica las direcciones IP (del rango de direcciones IP disponibles para la VPC) a las que desea que los solucionadores de DNS de su red reenvíen las consultas de DNS. Esas direcciones IP no son direcciones IP públicas, por lo que, para cada punto final de entrada, debe conectar la VPC a la red mediante Direct Connect una conexión o una conexión VPN.

Al implementar la delegación entrante, delega la autoridad de DNS para un subdominio de su infraestructura de DNS local a VPC Resolver. Para configurar correctamente esta delegación, debe usar las direcciones IP del punto de conexión de entrada como registros de adherencia (registros NS) en el servidor de nombres en las instalaciones para el subdominio que se va a delegar. Por ejemplo, si delega el subdominio «aws.example.com» a VPC Resolver a través de un punto final de delegación entrante con las direcciones IP 10.0.1.100 y 10.0.1.101, debe crear registros NS en su servidor DNS local que apunten a «aws.example.com» a estas direcciones IP. Esto garantiza que las consultas de DNS del subdominio delegado se enruten correctamente al solucionador de VPC a través del punto de enlace de entrada, lo que permite que el solucionador de VPC responda con registros de la zona alojada privada asociada.

Configuración del enrutamiento entrante

Para crear un punto de conexión de entrada, siga el procedimiento que se indica a continuación.

Para crear un punto de conexión de entrada

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/route53/>
2. En el panel de navegación, elija Inbound endpoints (Puntos de conexión de entrada).
3. En la barra de navegación, elija la región en la que desea crear un punto de conexión de entrada.
4. Elija Create inbound endpoint (Crear punto de conexión de entrada).
5. Ingrese los valores aplicables. Para obtener más información, consulte [Valores que se especifican al crear o editar puntos de conexión de entrada](#).
6. Elija Create (Crear).
7. Configure los solucionadores de DNS de la red para que reenvíen las consultas de DNS aplicables a las direcciones IP del punto de conexión de entrada. Para obtener más información, consulte la documentación de su aplicación de DNS.

Valores que se especifican al crear o editar puntos de conexión de entrada

Al crear o editar un punto de conexión de entrada, tiene que especificar los siguientes valores:

ID de Outpost

Si va a crear el punto final para un solucionador de VPC en una AWS Outposts VPC, este es el ID. AWS Outposts

Endpoint name (Nombre del punto de conexión)

Un nombre fácil de recordar que le permite encontrar fácilmente un punto de conexión de entrada en el panel.

Categoría del punto de conexión

Elija Predeterminado o Delegación. Cuando la categoría es Predeterminado, el solucionador de la red reenvía las solicitudes de DNS a la dirección IP del punto de conexión de entrada. Cuando la categoría es Delegación, la autoridad de un dominio se delega en el solucionador de VPC.

VPC in the region-name Region (VPC en la región nombre-región)

Todas las consultas DNS entrantes de la red pasan por esta VPC hasta llegar a VPC Resolver.

Security group for this endpoint (Grupo de seguridad para este punto de conexión)

El ID de uno o varios grupos de seguridad que desea utilizar para controlar el acceso a esta VPC. El grupo de seguridad que especifique debe incluir una o más reglas de entrada. Las reglas de entrada deben permitir el acceso de TCP y UDP en el puerto 53. Si utiliza el protocolo DoH, también tendrá que permitir el puerto 443 en el grupo de seguridad. No puede cambiar este valor después de crear el punto de conexión.

Algunas reglas de grupos de seguridad hacen que se realice un seguimiento de su conexión y, en general, el número máximo de consultas por segundo por dirección IP para un punto de conexión de salida puede ser tan bajo como 1500. Para evitar el seguimiento de la conexión provocado por un grupo de seguridad, consulte [Conexiones sin seguimiento](#).

Note

Para añadir varios grupos de seguridad, utilice el comando `AWS CLI create-resolver-endpoint`. Para obtener más información, consulte [create-resolver-endpoint](#)

Para obtener más información, consulte [Grupos de seguridad de su VPC](#) en la Guía del usuario de Amazon VPC.

Tipo de punto de conexión

El tipo de punto final puede ser una IPv4 dirección IP de pila doble o una dirección IP. IPv6 En el caso de un punto final de doble pila, el punto final tendrá una IPv4 IPv6 dirección a la que el solucionador de DNS de la red pueda reenviar las consultas de DNS.

Note

Por motivos de seguridad, denegamos el acceso directo al IPv6 tráfico de Internet público a todas las IPv6 direcciones IP y de doble pila.

Direcciones IP

Las direcciones IP a las que quiere que los solucionadores de DNS de su red reenvíen las consultas de DNS. Le pedimos que especifique un mínimo de dos direcciones IP para la redundancia. Si ha creado un punto final de entrada de delegación, utilice estas direcciones IP

como registros NS adhesivos para el subdominio para el que quiere delegar la autoridad a VPC Resolver. Tenga en cuenta lo siguiente:

Varias zonas de disponibilidad

Le recomendamos que especifique direcciones IP que se encuentren al menos en dos zonas de disponibilidad. Opcionalmente, puede especificar direcciones IP adicionales en estas u otras zonas de disponibilidad.

Direcciones IP e interfaces de red elásticas de Amazon VPC

Para cada combinación de zona de disponibilidad, subred y dirección IP que especifique, VPC Resolver crea una interfaz de red elástica de Amazon VPC. Para obtener información acerca del número máximo actual de consultas de DNS por segundo por cada dirección IP de un punto de conexión, consulte [Cuotas en el solucionador de VPC Route 53](#). Para obtener información acerca de los precios de cada interfaz de red elástica, consulte “Amazon Route 53” en la [página de precios de Amazon Route 53](#).

Note

El punto de conexión de Resolver tiene una dirección IP privada. Estas direcciones IP no cambiarán a lo largo de la vida de un punto de conexión.

Para cada dirección IP, especifique los siguientes valores. Cada dirección IP debe estar en una zona de disponibilidad de la VPC que especificó en VPC in the region-name Region (VPC en la región nombre-región).

Zona de disponibilidad

La zona de disponibilidad por la que quiere que pasen las consultas de DNS en el recorrido hacia la VPC. La zona de disponibilidad que especifique debe estar configurada con una subred.

Subred

La subred que contiene las direcciones IP que desea asignar a su punto final de Resolver. ENIs Estas son las direcciones a las que enviará las consultas de DNS. La subred debe tener una dirección IP disponible.

La dirección IP de la subred debe coincidir con el Tipo de punto de conexión.

Dirección IP

La dirección IP que quiere asignar a los puntos de conexión de entrada.

Elija si desea que VPC Resolver elija una dirección IP para usted de entre las direcciones IP disponibles en la subred especificada o si desea especificar la dirección IP usted mismo.

Si decide especificar la dirección IP usted mismo, introduzca una IPv6 dirección IPv4 O o ambas.

Protocolos

El protocolo del punto de conexión determina cómo se transmiten los datos al punto de conexión de entrada. Elija uno o varios protocolos en función del nivel de seguridad necesario.

- Do53: (predeterminado) Los datos se retransmiten mediante el solucionador de VPC Route 53 sin cifrado adicional. Si bien los datos no pueden ser leídos por terceros, se pueden ver dentro de las redes. AWS Actualmente, este es el único protocolo disponible para la categoría de puntos de conexión de entrada de Delegación.
- DoH: los datos se transmiten a través de una sesión HTTPS cifrada. El DoH añade un nivel de seguridad adicional, donde los usuarios no autorizados no pueden descifrar los datos y nadie puede leerlos excepto el destinatario previsto.
- Doh-FIPS: los datos se transmiten en una sesión HTTPS cifrada que cumple con el estándar criptográfico FIPS 140-2. Admite solo puntos de conexión de entrada. Para obtener más información, consulte [FIPS PUB 140-2](#).

Note

En el caso de los puntos finales entrantes DOH/DOH-FIPS, existe un problema conocido relacionado con la publicación de una IP de origen incorrecta en el registro de consultas del VPC Resolver.

Para un punto de conexión de entrada, puede aplicar los protocolos de la siguiente manera:

- Do53 y DoH en combinación.
- Do53 y DOH-FIPS en combinación.
- Do53 solo.
- DoH solo.
- DoH-FIPS solo.

- Ninguno, por lo que se trata como Do53.

 Important

No se puede cambiar el protocolo de un punto de conexión de entrada directamente de solo Do53 a solo DoH o DoH-FIPS. Esto es para evitar una interrupción repentina del tráfico entrante que depende de Do53. Para cambiar el protocolo de Do53 a DoH o DoH-FIPS, primero debe habilitar Do53 y DoH o Do53 y DoH-FIPS, para asegurarse de que todo el tráfico entrante se transfiera a través del protocolo DoH o DoH-FIPS y, a continuación, se elimine Do53.

Tags

Especifique una o más claves y los valores correspondientes. Por ejemplo, puede especificar Centro de costos en Key (Clave) y 456 en Value (Valor).

Administración de puntos de conexión de entrada

Para administrar los puntos de conexión de entrada, siga el procedimiento correspondiente.

Temas

- [Visualización y edición de puntos de conexión de entrada](#)
- [Visualización del estado de los puntos de conexión de entrada](#)
- [Eliminación de puntos de conexión de entrada](#)

Visualización y edición de puntos de conexión de entrada

Para ver y editar la configuración de un punto de conexión de entrada, realice el siguiente procedimiento.

Para ver y editar la configuración de un punto de conexión de entrada

1. Inicie sesión en la consola de Route 53 y ábrala en. Consola de administración de AWS <https://console.aws.amazon.com/route53/>
2. En el panel de navegación, elija Inbound endpoints (Puntos de conexión de entrada).
3. En la barra de navegación, elija la región en la que creó el punto de conexión de entrada.

4. Elija la opción correspondiente al punto de entrada cuya configuración desea ver o editar.
5. Elija View details (Ver detalles) o Edit (Editar).

Para obtener información acerca de los valores para los puntos de conexión de entrada, consulte [Valores que se especifican al crear o editar puntos de conexión de entrada](#).

6. Si eligió Edit (Editar), escriba los valores correspondientes y elija Save (Guardar).

Visualización del estado de los puntos de conexión de entrada

Para ver el estado de un punto de conexión de entrada, realice el procedimiento siguiente.

Para ver el estado de un punto de conexión de entrada

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Inbound endpoints (Puntos de conexión de entrada).
3. En la barra de navegación, elija la región en la que creó el punto de conexión de entrada. La columna Status (Estado) contiene uno de los valores siguientes:

Creación

El solucionador de VPC está creando y configurando una o más interfaces de red de Amazon VPC para este punto final.

Operational (En funcionamiento)

Las interfaces de red de Amazon VPC para este punto de conexión están configuradas correctamente y pueden transmitir consultas de DNS entrantes o salientes entre su red y VPC Resolver.

Actualización

El solucionador de VPC está asociando o desasociando una o más interfaces de red con este punto final.

Auto recovering (Recuperación automática)

El solucionador de VPC está intentando recuperar una o más de las interfaces de red asociadas a este punto final. Durante el proceso de recuperación, el punto de conexión opera con una capacidad limitada debido al límite en el número de consultas de DNS por dirección

IP (por interfaz de red). Para ver el límite actual, consulte [Cuotas en el solucionador de VPC Route 53](#).

Action needed (Acción necesaria)

Este punto final está en mal estado y VPC Resolver no puede recuperarlo automáticamente. Para solucionar el problema, le recomendamos que compruebe cada dirección IP que haya asociado al punto de conexión. Para cada dirección IP que no esté disponible, añada otra dirección IP y, a continuación, elimine la dirección IP que no esté disponible. (Un punto de conexión siempre debe incluir al menos dos direcciones IP). Un estado de Action needed (Acción necesaria) puede deberse a varios motivos. Estas son dos causas comunes:

- Se ha eliminado una o más interfaces de red asociadas al punto de conexión mediante Amazon VPC.
- No se pudo crear la interfaz de red por alguna razón ajena al control de VPC Resolver.

Eliminación

El solucionador de VPC está eliminando este punto final y las interfaces de red asociadas.

Eliminación de puntos de conexión de entrada

Para eliminar un punto de conexión de entrada, siga el procedimiento que se indica a continuación.

Important

Si elimina un punto de enlace entrante, las consultas de DNS de su red ya no se reenvían al Resolver de VPC en la VPC que especificó en el punto de enlace.

Para eliminar un punto de conexión de entrada

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/route53/>
2. En el panel de navegación, elija Inbound endpoints (Puntos de conexión de entrada).
3. En la barra de navegación, elija la región en la que creó el punto de conexión de entrada.
4. Elija la opción correspondiente al punto de conexión que desea eliminar.
5. Elija Eliminar.

6. Para confirmar que desea eliminar el punto de conexión, escriba el nombre del punto de conexión y elija Submit (Enviar).

Reenvío de consultas de DNS de salida a su red

Para reenviar a tu red las consultas de DNS que se originan en EC2 instancias de Amazon en una o más VPCs instancias, debes crear un punto de conexión saliente y una o más reglas:

Punto de conexión de salida

Para reenviar las consultas de DNS de su red VPCs a su red, debe crear un punto final saliente. Un punto de conexión saliente especifica las direcciones IP de las que se originan las consultas. Esas direcciones IP, que usted elige entre el rango de direcciones IP disponibles para su VPC, no son direcciones IP públicas. Esto significa que para cada punto de conexión de salida debe conectar la VPC a la red mediante una conexión Direct Connect, una conexión de VPN o una gateway de enlace de traducción de direcciones de red (NAT). Tenga en cuenta que puede usar el mismo punto final de salida para varios VPCs puntos de conexión de la misma región o puede crear varios puntos de enlace salientes. Si desea utilizar su punto de conexión saliente DNS64, puede habilitarlo DNS64 mediante Amazon Virtual Private Cloud. Para obtener más información, consulte [DNS64 y NAT64](#) en la Guía del usuario de Amazon VPC.

El Resolver de VPC elige aleatoriamente la IP de destino de la regla de resolución de VPC y no hay preferencia a la hora de elegir una IP de destino en particular sobre la otra. Si una IP de destino no responde a la solicitud de DNS reenviada, el solucionador de VPC volverá a intentar encontrar una dirección IP aleatoria entre el destino. IPs

Asegúrese de que se pueda acceder a todas las direcciones IP de destino desde los puntos de conexión de Resolver. Si el Resolver de VPC no puede reenviar las consultas de DNS salientes a ninguna de las IP de destino, los tiempos de resolución de DNS pueden prolongarse.

Reglas

Para especificar los nombres de dominio de las consultas que quiere reenviar a los solucionadores de DNS de su red, puede crear una o más reglas. Cada regla de reenvío especifica un nombre de dominio. A continuación, asocie las reglas a VPCs las que desee reenviar las consultas a la red.

Las reglas de delegación saliente siguen principios de delegación específicos que difieren de las reglas de reenvío estándar. Al crear una regla de delegación, el solucionador de VPC evalúa los

registros de delegación de la regla comparándolos con los registros NS de las respuestas de DNS para determinar si se debe realizar la delegación. El solucionador de VPC delegará la autoridad en tus resolutores locales solo cuando haya una coincidencia entre la configuración de la regla de delegación y los registros NS reales devueltos en la respuesta de DNS. A diferencia de las reglas de reenvío que redirigen las consultas en función de la coincidencia de nombres de dominio, las reglas de delegación respetan la cadena de delegación del DNS y solo se activan cuando los servidores de nombres autorizados de la respuesta coinciden con la configuración de delegación.

Para obtener más información, consulte los temas siguientes:

- [Private hosted zones that have overlapping namespaces](#)
- [Private hosted zones and Route 53 VPC Resolver rules](#)

Configuración del enrutamiento saliente

Para configurar el Resolver de VPC para que reenvíe las consultas de DNS que se originan en la VPC a la red, lleve a cabo los siguientes procedimientos.

Important

Tras crear un punto final de salida, debe crear una o varias reglas y asociarlas a una o varias VPCs. Las reglas especifican los nombres de dominio de las consultas de DNS que quiere reenviar a su red.

Para crear un punto de conexión de salida

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Inbound Outbound (Puntos de conexión de salida).
3. En la barra de navegación, elija la región en la que desea crear un punto de conexión de salida.
4. Elija Create outbound endpoint (Crear punto de conexión de salida).
5. Ingrese los valores aplicables. Para obtener más información, consulte [Valores que se especifican al crear o editar puntos de conexión de salida](#).
6. Elija Create (Crear).

 Note

La creación de un punto de conexión de salida tarda uno o dos minutos. No se puede crear otro punto de conexión de salida hasta que no se haya creado el primero.

7. Cree una o más reglas para especificar los nombres de dominio de las consultas de DNS que quiere reenviar a su red. Para obtener más información, consulte el siguiente procedimiento.

Para crear una o varias reglas de reenvío, siga el procedimiento que se indica a continuación.

Para crear reglas de reenvío y asociarlas a una o más VPCs

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, seleccione Reglas.
3. En la barra de navegación, elija la región en la que desee crear la regla.
4. Seleccione Creación de regla.
5. Ingrese los valores aplicables. Para obtener más información, consulte [Valores que se especifican al crear o editar reglas](#).
6. Seleccione Save.
7. Para agregar otra regla, repita los pasos 4 a 6.

Valores que se especifican al crear o editar puntos de conexión de salida

Al crear o editar un punto de conexión de salida, tiene que especificar los siguientes valores:

ID de Outpost

Si va a crear el punto final para un solucionador de VPC en una AWS Outposts VPC, este es el ID. AWS Outposts

Endpoint name (Nombre del punto de conexión)

Un nombre fácil de recordar que le permite encontrar fácilmente un punto de conexión de salida en el panel.

VPC in the region-name Region (VPC en la región nombre-región)

Todas las consultas de DNS salientes atravesarán esta VPC en el recorrido hacia su red.

Security group for this endpoint (Grupo de seguridad para este punto de conexión)

El ID de uno o varios grupos de seguridad que desea utilizar para controlar el acceso a esta VPC. El grupo de seguridad que especifique debe incluir una o más reglas de salida. Las reglas de salida deben permitir el acceso de TCP y UDP en el puerto que utiliza para las consultas de DNS de la red. No puede cambiar este valor después de crear un punto de conexión.

Algunas reglas de los grupos de seguridad harán que se rastree su conexión y podrían afectar al número máximo de consultas por segundo desde el punto de conexión de salida al servidor de nombres de destino. Para evitar el seguimiento de la conexión provocado por un grupo de seguridad, consulte [Conexiones sin seguimiento](#).

Para obtener más información, consulte [Grupos de seguridad de su VPC](#) en la Guía del usuario de Amazon VPC.

Tipo de punto de conexión

El tipo de punto final puede ser una dirección IP de pila doble o una IPv6 dirección IP de doble pila. IPv4 En el caso de un punto final de doble pila, el punto final tendrá una IPv4 IPv6 dirección a la que el solucionador de DNS de la red pueda reenviar las consultas de DNS.

Note

Por motivos de seguridad, denegamos el acceso directo IPv6 del tráfico a la Internet pública a todas las IPv6 direcciones IP y de doble pila.

Direcciones IP

Las direcciones IP de su VPC a las que quiere que VPC Resolver reenvíe las consultas de DNS cuando se dirijan a los resolutores de su red. Estas no son las direcciones IP de los solucionadores de DNS de la red; las direcciones IP de los solucionadores se especifican al crear las reglas que se asocian a uno o más. VPCs Le pedimos que especifique un mínimo de dos direcciones IP para la redundancia.

 Note

El punto de conexión de Resolver tiene una dirección IP privada. Estas direcciones IP no cambiarán a lo largo de la vida de un punto de conexión.

Tenga en cuenta lo siguiente:

Varias zonas de disponibilidad

Le recomendamos que especifique direcciones IP que se encuentren al menos en dos zonas de disponibilidad. Opcionalmente, puede especificar direcciones IP adicionales en estas u otras zonas de disponibilidad.

Direcciones IP e interfaces de red elásticas de Amazon VPC

Para cada combinación de zona de disponibilidad, subred y dirección IP que especifique, VPC Resolver crea una interfaz de red elástica de Amazon VPC. Para obtener información acerca del número máximo actual de consultas de DNS por segundo por cada dirección IP de un punto de conexión, consulte [Cuotas en el solucionador de VPC Route 53](#). Para obtener información acerca de los precios de cada interfaz de red elástica, consulte “Amazon Route 53” en la [página de precios de Amazon Route 53](#).

Orden de direcciones IP

Puede especificar direcciones IP en cualquier orden. Al reenviar consultas de DNS, VPC Resolver no elige las direcciones IP en función del orden en que aparecen las direcciones IP.

Para cada dirección IP, especifique los siguientes valores. Cada dirección IP debe estar en una zona de disponibilidad de la VPC que especificó en VPC in the region-name Region (VPC en la región nombre-región).

Zona de disponibilidad

La zona de disponibilidad por la que quiere que pasen las consultas de DNS en el recorrido hacia su red. La zona de disponibilidad que especifique debe estar configurada con una subred.

Subred

La subred que contiene la dirección IP que quiere que las consultas de DNS se creen en el recorrido hacia su red. La subred debe tener una dirección IP disponible.

La dirección IP de la subred debe coincidir con el Tipo de punto de conexión.

Dirección IP

La dirección IP que quiere que las consultas de DNS se creen en el recorrido hacia su red.

Elija si desea que VPC Resolver elija una dirección IP para usted de entre las direcciones IP disponibles en la subred especificada o si desea especificar la dirección IP usted mismo.

Si decide especificar la dirección IP usted mismo, introduzca una IPv6 dirección IPv4 O o ambas.

Protocolos

El protocolo de punto de conexión determina cómo se transmiten los datos desde el punto de conexión de salida. Elija uno o varios protocolos en función del nivel de seguridad necesario.

- Do53: (predeterminado) Los datos se retransmiten mediante el solucionador de VPC Route 53 sin cifrado adicional. Si bien los datos no pueden ser leídos por terceros, se pueden ver dentro de las redes de AWS .
- DoH: los datos se transmiten a través de una sesión HTTPS cifrada. El DoH añade un nivel de seguridad adicional, donde los usuarios no autorizados no pueden descifrar los datos y nadie puede leerlos excepto el destinatario previsto.

Para un punto de conexión de salida, puede aplicar los protocolos de la siguiente manera:

- Do53 y DoH en combinación.
- Do53 solo.
- DoH solo.
- Ninguno, por lo que se trata como Do53.

Tags

Especifique una o más claves y los valores correspondientes. Por ejemplo, puede especificar Centro de costos en Key (Clave) y 456 en Value (Valor).

Valores que se especifican al crear o editar reglas

Al crear o editar una regla de reenvío, tiene que especificar los siguientes valores:

Nombre de la regla

Un nombre fácil de recordar que permite encontrar fácilmente una regla en el panel.

Tipo de regla

Elija el valor aplicable:

- **Forward (Reenviar):** elija esta opción cuando quiera reenviar consultas de DNS para un nombre de dominio especificado a los solucionadores de la red.
- **Delegar:** elige esta opción si quieres delegar la autoridad de un subdominio, alojado en una zona alojada privada, a tu solucionador local (o a un solucionador de VPC de otra VPC).
- **Sistema:** elija esta opción si desea que VPC Resolver anule selectivamente el comportamiento definido en una regla de reenvío. Al crear una regla del sistema, el solucionador de VPC resuelve las consultas de DNS para subdominios específicos que, de otro modo, resolverían los solucionadores de DNS de la red.

De forma predeterminada, las reglas de reenvío se aplican a un nombre de dominio y todos sus subdominios. Si quiere reenviar las consultas de un dominio a un solucionador de la red, pero no quiere reenviar las consultas a algunos subdominios, debe crear una regla de sistema para los subdominios. Por ejemplo, si crea una regla de reenvío para example.com pero no desea reenviar las consultas a acme.example.com, debe crear una regla de sistema y especificar acme.example.com para el nombre de dominio.

Registro de delegación: solo para reglas de delegación

Las consultas de DNS que coinciden con este dominio se reenvían a los solucionadores de la red.

Note

Como requisito previo para una regla de delegación, debe crear registros NS en la zona alojada privada cuando utilice la delegación de zona alojada privada a punto de conexión de salida. El registro es: NS - servidores de nombres para delegar a través del punto de conexión de salida de Resolver con una regla de delegación. Para obtener más información, consulte [Tipo de registro NS](#).

VPCs que utilizan esta regla

Los VPCs que utilizan esta regla para reenviar consultas de DNS para el nombre o los nombres de dominio especificados. Puede aplicar una regla a tantos VPCs como desee.

Nombre de dominio: solo para las reglas de reenvío

Las consultas de DNS para este nombre de dominio se reenvían a las direcciones IP que especifique en las Target IP addresses (Direcciones IP de destino). Por ejemplo, puede especificar un dominio específico (example.com), un dominio de nivel superior (com) o un punto (.) para reenviar todas las consultas de DNS. Para obtener más información, consulte [Cómo determina el solucionador de VPC si el nombre de dominio de una consulta coincide con alguna regla](#).

Punto de conexión de salida

El solucionador de VPC reenvía las consultas de DNS a través del punto de enlace saliente que especifique aquí a las direcciones IP que especifique en las direcciones IP de destino.

Direcciones IP de destino

Cuando una consulta de DNS coincide con el nombre que especifica en Domain name (Nombre de dominio), el punto de conexión de salida reenvía la consulta a las direcciones IP que especifica aquí. Suelen ser las direcciones IP de los solucionadores de DNS de su red.

Target IP addresses (Direcciones IP de destino) solo está disponible cuando el valor de Rule type (Tipo de regla) es Forward (Reenvío).

Especifique IPv6 las direcciones IPv4 o los protocolos ServerNameIndication que desee utilizar para el punto final. ServerNameIndication solo se aplica cuando el protocolo seleccionado es DoH.

No se admite la resolución de la dirección IP de destino del FQDN de un solucionador DoH que haya en la red a través del punto de conexión de salida. Los puntos de conexión de salida necesitan la dirección IP de destino del solucionador DoH de la red para reenviar las consultas DoH. Si el solucionador DoH de su red necesita el FQDN en el SNI de TLS y en el encabezado del host HTTP, debe proporcionarlo. ServerNameIndication

ServerNameIndication

La indicación del nombre del servidor DoH al que desea reenviar las consultas. Solo se usa si el protocolo es DoH.

Tags

Especifique una o más claves y los valores correspondientes. Por ejemplo, puede especificar Centro de costos en Key (Clave) y 456 en Value (Valor).

Estas son las etiquetas que permiten organizar su Administración de facturación y costos de AWS factura. AWS Para obtener más información sobre el uso de etiquetas para la asignación de costes, consulte [Uso de etiquetas de asignación de costes](#) en la Guía del usuario de AWS Billing .

Administración de puntos de conexión de salida

Para administrar los puntos de conexión de salida, siga el procedimiento correspondiente.

Temas

- [Visualización y edición de puntos de conexión de salida](#)
- [Visualización del estado de los puntos de conexión de salida](#)
- [Eliminación de puntos de conexión de salida](#)

Visualización y edición de puntos de conexión de salida

Para ver y editar la configuración de un punto de conexión de salida, realice el siguiente procedimiento.

Para ver y editar la configuración de un punto de conexión de salida

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Inbound Outbound (Puntos de conexión de salida).
3. En la barra de navegación, elija la región en la que creó el punto de conexión de salida.
4. Elija la opción correspondiente al punto de entrada cuya configuración desea ver o editar.
5. Elija View details (Ver detalles) o Edit (Editar).

Para obtener información acerca de los valores de los puntos de conexión de salida, consulte [Valores que se especifican al crear o editar puntos de conexión de salida](#).

6. Si eligió Edit (Editar), escriba los valores correspondientes y, a continuación, elija Save (Guardar).

Visualización del estado de los puntos de conexión de salida

Para ver el estado de un punto de conexión de salida, realice el procedimiento siguiente.

Para ver el estado de un punto de conexión de salida

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Inbound Outbound (Puntos de conexión de salida).
3. En la barra de navegación, elija la región en la que creó el punto de conexión de salida. La columna Status (Estado) contiene uno de los valores siguientes:

Creación

El solucionador de VPC está creando y configurando una o más interfaces de red de Amazon VPC para este punto final.

Operational (En funcionamiento)

Las interfaces de red de Amazon VPC para este punto de conexión están configuradas correctamente y pueden transmitir consultas de DNS entrantes o salientes entre su red y VPC Resolver.

Actualización

El solucionador de VPC está asociando o desasociando una o más interfaces de red con este punto final.

Auto recovering (Recuperación automática)

El solucionador de VPC está intentando recuperar una o más de las interfaces de red asociadas a este punto final. Durante el proceso de recuperación, el punto de conexión opera con una capacidad limitada debido al límite en el número de consultas de DNS por dirección IP (por interfaz de red). Para ver el límite actual, consulte [Cuotas en el solucionador de VPC Route 53](#).

Action needed (Acción necesaria)

Este punto final está en mal estado y VPC Resolver no puede recuperarlo automáticamente. Para solucionar el problema, le recomendamos que compruebe cada dirección IP que haya asociado al punto de conexión. Para cada dirección IP que no esté disponible, añada otra dirección IP y, a continuación, elimine la dirección IP que no esté disponible. (Un punto de conexión siempre debe incluir al menos dos direcciones IP). Un estado de Action needed (Acción necesaria) puede deberse a varios motivos. Estas son dos causas comunes:

- Se ha eliminado una o más interfaces de red asociadas al punto de conexión mediante Amazon VPC.
- No se pudo crear la interfaz de red por alguna razón ajena al control de VPC Resolver.

Eliminación

El solucionador de VPC está eliminando este punto final y las interfaces de red asociadas.

Eliminación de puntos de conexión de salida

Para poder eliminar un punto de conexión, primero debe eliminar las reglas que estén asociadas a una VPC.

Para eliminar un punto de conexión de salida, siga el procedimiento que se indica a continuación.

Important

Si eliminas un endpoint de salida, VPC Resolver deja de reenviar las consultas de DNS de tu VPC a tu red para las reglas que especifican el endpoint de salida eliminado.

Para eliminar un punto de conexión de salida

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/route53/>
2. En el panel de navegación, elija Inbound Outbound (Puntos de conexión de salida).
3. En la barra de navegación, elija la región en la que creó el punto de conexión de salida.
4. Elija la opción correspondiente al punto de conexión que desea eliminar.
5. Elija Eliminar.
6. Para confirmar que desea eliminar el punto de conexión, escriba el nombre del punto de conexión y, a continuación, elija Submit (Enviar).

Administración de reglas de reenvío

Si desea que VPC Resolver reenvíe las consultas de nombres de dominio específicos a su red, cree una regla de reenvío para cada nombre de dominio y especifique el nombre del dominio para el que desea reenviar las consultas.

Temas

- [Visualización y edición de reglas de reenvío](#)
- [Creación de reglas de reenvío](#)
- [Agregar reglas para búsqueda inversa](#)
- [Asociación de reglas de reenvío a una VPC](#)
- [Anulación de la asociación de reglas de reenvío de una VPC](#)
- [Compartir las reglas de Resolver con otras AWS cuentas y usar reglas compartidas](#)
- [Eliminación de reglas de reenvío](#)
- [Reglas de reenvío para consultas de DNS inversas en VPC Resolver](#)

Visualización y edición de reglas de reenvío

Para ver y editar la configuración de una regla de reenvío, realice el siguiente procedimiento.

Para ver y editar la configuración de una regla de reenvío

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/route53/>
2. En el panel de navegación, seleccione Reglas.
3. En la barra de navegación, elija la región en la que creó la regla.
4. Elija la opción correspondiente a la regla cuya configuración desea ver o editar.
5. Elija View details (Ver detalles) o Edit (Editar).

Para obtener información acerca de los valores para las reglas de reenvío, consulte [Valores que se especifican al crear o editar reglas](#).

6. Si eligió Edit (Editar), escriba los valores correspondientes y, a continuación, elija Save (Guardar).

Creación de reglas de reenvío

Para crear una o varias reglas de reenvío, siga el procedimiento que se indica a continuación.

Para crear reglas de reenvío y asociarlas a una o más VPCs

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, seleccione Reglas.
3. En la barra de navegación, elija la región en la que desee crear la regla.
4. Seleccione Creación de regla.
5. Ingrese los valores aplicables. Para obtener más información, consulte [Valores que se especifican al crear o editar reglas](#).
6. Seleccione Save.
7. Para agregar otra regla, repita los pasos 4 a 6.

Agregar reglas para búsqueda inversa

Si necesita controlar las búsquedas inversas en la VPC, puede agregar reglas al punto de conexión de salida del solucionador.

Para crear la regla de búsqueda inversa

1. Siga los pasos del procedimiento anterior, hasta el paso 5.
2. Cuando especifique la regla, ingrese el campo PTR para la dirección IP o direcciones para las que desea una regla de reenvío de búsqueda inversa.

Por ejemplo, si necesita reenviar búsquedas de direcciones en el rango 10.0.0.0/23, ingrese dos reglas:

- 0.0.10.in-addr.arpa
- 1.0.10.in-addr.arpa

Cualquier dirección IP de esas subredes se referenciará como un subdominio de esos registros PTR; por ejemplo, 10.0.1.161 tendrá una dirección de búsqueda inversa de 161.1.0.10.in-addr.apra, que es un subdominio de 1.0.10.in-addra.apra.

3. Especifique el servidor al que desea reenviar estas búsquedas.
4. Agregue estas reglas al punto de conexión de salida del solucionador.

Tenga en cuenta que al activar `enableDNSTypes` para su VPC, se agregan automáticamente registros PTR. Consulte [¿Qué es el solucionador de VPC Route 53?](#). El procedimiento anterior solo es necesario si desea especificar explícitamente un solucionador para rangos IP determinados; por ejemplo, al reenviar consultas a un servidor de Active Directory.

Asociación de reglas de reenvío a una VPC

Después de crear una regla de reenvío, debe asociarla a una o más VPCs. Las reglas solo funcionarán después de que estén asociadas a una VPC. Al asociar una regla a una VPC, el solucionador de VPC comienza a reenviar las consultas de DNS del nombre de dominio especificado en la regla a los solucionadores de DNS que especificó en la regla. Las consultas atraviesan el punto de conexión de salida que especificó al crear la regla.

Para asociar una regla de reenvío a uno o varios VPCs

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, seleccione Reglas.
3. En la barra de navegación, elija la región en la que creó la regla.
4. Elija el nombre de la regla que desee asociar a una o más VPCs.
5. Elija Asociar VPC.
6. En VPCs la sección Use esta regla, elija la opción a la VPCs que desee asociar la regla.
7. Elija Agregar.

Anulación de la asociación de reglas de reenvío de una VPC

Puede anular la asociación de una regla de reenvío de una VPC en las siguientes circunstancias:

- En el caso de las consultas de DNS que se originan en esta VPC, desea que VPC Resolver deje de reenviar a la red las consultas del nombre de dominio especificado en la regla.
- Quiere eliminar la regla de reenvío. Si una regla está asociada actualmente a una o varias VPCs, debe desasociarla de todas para VPCs poder eliminarla.

Si desea desasociar una regla de reenvío de una o varias VPCs, lleve a cabo el siguiente procedimiento.

Para anular la asociación de una regla de reenvío de una VPC

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/route53/>
2. En el panel de navegación, seleccione Reglas.
3. En la barra de navegación, elija la región en la que creó la regla.
4. Elija el nombre de la regla que desee desasociar de una o más VPCs.
5. Elija la opción de la VPC que desea desasociar de la regla.
6. Elija Desasociar.
7. Escriba disassociate (desasociar) para confirmar.
8. Elija Enviar.

Compartir las reglas de Resolver con otras AWS cuentas y usar reglas compartidas

Puede compartir las reglas de Resolver que creó con una AWS cuenta con otras AWS cuentas. Para compartir reglas, la consola de resolución de VPC de Route 53 se integra con AWS Resource Access Manager. Para obtener más información acerca de Resource Access Manager, consulte la [Guía del usuario de Resource Access Manager](#).

Tenga en cuenta lo siguiente:

Asociar reglas compartidas a VPCs

Si otra AWS cuenta ha compartido una o más reglas con la suya, puede asociar las reglas a la suya VPCs del mismo modo que asoció las reglas que creó con la suya VPCs. Para obtener más información, consulte [Asociación de reglas de reenvío a una VPC](#).

Eliminación o dejar de compartir una regla

Si comparte una regla con otras cuentas y, a continuación, la elimina o deja de compartirla, y si la regla estaba asociada a una o más cuentas VPCs, Route 53 VPC Resolver comienza a procesar las consultas de DNS para esas cuentas en VPCs función de las reglas restantes. El comportamiento es el mismo que si anula la asociación de la regla con la VPC.

Si se comparte una regla en una unidad organizativa (OU) y una cuenta de la OU se mueve a otra unidad organizativa, se eliminarán todas las asociaciones de la regla compartida con cualquier VPC de la cuenta. Sin embargo, si la regla de resolución de VPC ya estaba compartida con la OU de destino, la asociación de VPC permanecerá intacta y no se disociará.

Número máximo de reglas y asociaciones

Cuando una cuenta crea una regla y la comparte con una o más cuentas, se aplica el número máximo de reglas por AWS región a la cuenta que creó la regla.

Cuando una cuenta con la que se comparte una regla asocia la regla a una o más VPCs, el número máximo de asociaciones entre reglas y VPCs por región se aplica a la cuenta con la que se comparte la regla.

Para conocer las cuotas actuales de VPC Resolver, consulte [Cuotas en el solucionador de VPC Route 53](#)

Permisos

Para compartir una regla con otra AWS cuenta, debe tener permiso para usar la [PutResolverRulePolicy](#) acción.

Restricciones en la AWS cuenta con la que se comparte una regla

La cuenta con la que se comparte una regla no puede cambiar o eliminar la regla.

Etiquetado

Solo la cuenta que creó una regla puede añadir, eliminar o consultar etiquetas de la regla.

Para ver el estado actual de uso compartido de una regla (incluida la cuenta que compartió la regla o la cuenta con la que se comparte una regla) y para compartir reglas con otra cuenta, siga el procedimiento que se indica a continuación.

Para ver el estado de uso compartido y las reglas de uso compartido con otra AWS cuenta

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, seleccione Reglas.
3. En la barra de navegación, elija la región en la que creó la regla.

La columna Sharing status (Estado de uso compartido) muestra el estado actual de uso compartido de las reglas creadas por la cuenta actual o que se comparten con la cuenta actual:

- No compartida: la AWS cuenta actual creó la regla y la regla no se comparte con ninguna otra cuenta.

- Shared by me (Compartido por mí): la cuenta actual creó la regla y la compartió con una o varias cuentas.
 - Shared with me (Compartido conmigo): otra cuenta creó la regla y la compartió con la cuenta actual.
4. Elija el nombre de la regla cuya información de uso compartido desea mostrar o que desea compartir con otra cuenta.

En la *rule name* página Regla:, el valor de Propietario muestra el ID de la cuenta que creó la regla. Es la cuenta actual a menos que el valor de Sharing status (Estado de uso compartido) sea Shared with me (Compartido conmigo). En ese caso, Owner (Propietario) es la cuenta que creó la regla y la compartió con la cuenta actual.

5. Elija Share (Compartir)para ver información adicional o para compartir la regla con otra cuenta. Aparecerá una página en la consola de Resource Access Manager, en función del valor de Sharing status (Estado de uso compartido):
 - Not shared (No compartido): aparece la página Create resource share (Crear recurso compartido de recursos). Para obtener más información acerca de cómo compartir la regla con otra cuenta, unidad organizativa u organización, vaya al paso 6.
 - Shared by me (Compartido por mí): la página Shared resources (Recursos compartidos) muestra las reglas y otros recursos que son propiedad de la cuenta actual y que están compartidos con otras cuentas.
 - Shared with me (Compartido conmigo): la página Shared resources (Recursos compartidos) muestra las reglas y otros recursos que son propiedad de otras cuentas y que están compartidos con la cuenta actual.
6. Para compartir una regla con otra AWS cuenta, unidad organizativa u organización, especifique los siguientes valores.

 Note

No se puede actualizar la configuración de uso compartido. Si desea cambiar cualquiera de los siguientes valores, debe volver a compartir una regla con la nueva configuración y, a continuación, quitar la configuración de uso compartido anterior.

Description (Descripción)

Escriba una breve descripción que le ayude a recordar por qué compartió la regla.

Recursos

Seleccione la casilla de verificación correspondiente a la regla que desea compartir.

Entidades principales

Introduzca el número de AWS cuenta, el nombre de la OU o el nombre de la organización.

Tags

Especifique una o más claves y los valores correspondientes. Por ejemplo, puede especificar Centro de costos en Key (Clave) y 456 en Value (Valor).

Estas son las etiquetas Administración de facturación y costos de AWS que permiten organizar su AWS factura; también puede utilizarlas para otros fines. Para obtener más información sobre el uso de etiquetas para la asignación de costes, consulte [Uso de etiquetas de asignación de costes](#) en la Guía del usuario de AWS Billing .

Eliminación de reglas de reenvío

Para eliminar una regla de reenvío, realice el procedimiento siguiente.

Tenga en cuenta lo siguiente:

- Si la regla de reenvío está asociada a alguna VPCs, debe desasociarla de la regla VPCs antes de poder eliminarla. Para obtener más información, consulte [Anulación de la asociación de reglas de reenvío de una VPC](#).
- No puede eliminar la regla Internet Resolver (Solucionador de Internet) predeterminada, que tiene un valor Recursive (Recursivo) para Type (Tipo). Esta regla hace que el Resolver de VPC de Route 53 actúe como un solucionador recursivo para cualquier nombre de dominio para el que no haya creado reglas personalizadas y para los que el Resolver de VPC no haya creado reglas autodefinidas. Para obtener más información acerca de cómo se clasifican las reglas, consulte [Uso de reglas para controlar qué consultas se reenvían a la red](#).

Para eliminar una regla de reenvío

1. Inicie sesión en la consola de Route Consola de administración de AWS 53 y ábrala en. <https://console.aws.amazon.com/route53/>
2. En el panel de navegación, seleccione Reglas.
3. En la barra de navegación, elija la región en la que creó la regla.
4. Elija la opción correspondiente a la regla que desea eliminar.
5. Elija Eliminar.
6. Para confirmar que desea eliminar la regla, escriba el nombre de la regla y elija Submit (Enviar).

Reglas de reenvío para consultas de DNS inversas en VPC Resolver

Cuando `enableDnsHostnames` y `enableDnsSupport` se configuran `true` para una nube privada virtual (VPC) desde Amazon VPC, VPC Resolver crea automáticamente reglas de sistema definidas automáticamente para las consultas de DNS inversas. Para obtener más información sobre esta configuración, consulte [Atributos DNS en su VPC](#) en la Guía para desarrolladores de Amazon VPC.

Las reglas de reenvío para consultas de DNS inversas son especialmente útiles para servicios como SSH o Active Directory, que tienen la opción de autenticar a los usuarios realizando una búsqueda DNS inversa de la dirección IP desde la que un cliente está intentando conectarse a un recurso. Para obtener más información acerca de reglas del sistema autodefinidas, consulte [Nombres de dominio para los que VPC Resolver crea reglas de sistema autodefinidas](#).

Puede desactivar estas reglas y modificar todas las consultas de DNS inversas para que, por ejemplo, se reenvíen a los servidores de nombres locales para su resolución.

Después de desactivar las reglas automáticas, cree reglas para reenviar las consultas a sus recursos locales en función de sus necesidades. Para obtener más información sobre cómo administrar reglas de reenvío, consulte [Administración de reglas de reenvío](#).

Para desactivar reglas autodefinidas

1. Inicie sesión en la consola de Route Consola de administración de AWS 53 y ábrala en. <https://console.aws.amazon.com/route53/>
2. En el panel de navegación, en VPC Resolver, elija y VPCs, a continuación, elija un ID de VPC.

3. En Autodefined rules for reverse DNS resolution (Reglas autodefinidas para la resolución DNS inversa), desmarque la casilla de verificación. Si la casilla de verificación ya está desactivada, puede seleccionarla para activar la resolución DNS inversa autodefinida.

Para obtener información relacionada APIs, consulte Configuración de [VPC Resolver](#). APIs

Tutorial sobre las reglas de delegación de Resolver

La regla de delegación permite al solucionador de VPC llegar a los servidores de nombres que alojan la zona delegada a través del punto final de salida especificado. Mientras que la regla de reenvío informa al solucionador de VPC que reenvíe las consultas de DNS a los servidores de nombres que coincidan con el dominio especificado a través del punto final de salida, la regla de delegación informa al solucionador de VPC que debe llegar a los servidores de nombres delegados a través del punto final de salida especificado cuando se devuelven los registros NS delegados. El solucionador de VPC envía una consulta a los servidores de nombres delegados cuando los registros NS de la respuesta de DNS coinciden con el nombre de dominio especificado en el registro de delegación.

Pasos para utilizar la delegación saliente a través del punto de conexión de Resolver

1. Cree un punto final de salida de Resolver en la VPC desde el que desee que se originen las consultas de DNS a los resolutores de la red.

Puede utilizar la siguiente API o el comando de CLI:

- [API de CreateResolverEndpoint](#)
- [CLI de create-resolver-endpoint](#)

2. Cree una o más reglas de delegación que especifiquen los nombres de dominio para los que se deben delegar las consultas a la red a través del punto de conexión de salida especificado.

Ejemplo de creación de reglas de delegación con CLI:

```
aws route53resolver create-resolver-rule \  
--region REGION \  
--creator-request-id delegateruletest \  
--delegation-record example.com \  
--name delegateruletest \  
--rule-type DELEGATE \  

```

```
--resolver-endpoint-id outbound endpoint ID
```

3. Asocie la regla de delegación a VPCs la que desee delegar las consultas.

Puede utilizar la siguiente API o el comando de CLI:

- [AssociateResolverRule](#)API.
- [associate-resolver-rules](#)Comando CLI.

Tipos de delegación admitidos por el punto de conexión de salida de Resolver

El solucionador de VPC admite dos tipos de delegación saliente:

- Delegación saliente de la zona alojada privada de Route 53 a VPC Resolver:

Delega un subdominio de una zona alojada privada a un servidor DNS en las instalaciones o a una zona alojada pública de Internet mediante la delegación saliente. Esta delegación saliente le permite dividir la administración de sus registros de DNS entre la zona alojada privada y la zona delegada. La delegación se puede hacer con o sin un registro de adherencia en una zona alojada privada en función de la configuración de DNS. Para obtener más información, consulte [De una zona alojada privada a un punto de conexión de salida](#).

- Delegación saliente a saliente de VPC Resolver:

Delega un subdominio de su servidor DNS en las instalaciones a otro servidor en las instalaciones en una ubicación igual o diferente mediante la delegación entre puntos de conexión de salida. Esto es similar a la delegación de una zona alojada privada a un punto de conexión de salida, donde puede delegar a una zona alojada en su servidor de nombres en las instalaciones. Para obtener más información, consulte [Entre puntos de salida](#).

Ejemplo de configuración de delegación saliente de una zona alojada privada de Route 53 a VPC Resolver

Supongamos que se tiene una configuración de DNS en la que la zona alojada principal está alojada en una zona alojada privada de Route 53 en una Amazon VPC y los subdominios se delegan a servidores de nombres alojados en Europa, Asia y América del Norte. Todas las consultas de DNS se pasan a través del solucionador de VPC.

Siga los pasos de ejemplo para configurar la zona alojada privada y el solucionador de VPC.

Configuración de una zona alojada privada para la delegación saliente

1. Para la configuración de la zona alojada privada:

Zona alojada principal: `hr.example.com`

```
$TTL      86400 ; 24 hours
$ORIGIN hr.example.com
@ 1D IN     SOA @      root (20200322001 3H 15 1w 3h)
@ 1D IN     NS @
eu.hr.example.com IN NS ns1.eu.hr.example.com.
apac.hr.example.com IN NS ns2.apac.hr.example.com.
na.hr.example.com IN NS ns3.na.hr.example.net. # Out of Zone Delegation

ns1.eu.hr.example.com IN A 10.0.0.30 # Glue Record
ns2.apac.hr.example.com IN A 10.0.0.40 # Glue Record
```

2. Para el servidor de nombres en las instalaciones en la región de Europa:

- Zona alojada: `eu.hr.example.com`, IP del NS: `10.0.0.30`

```
$TTL      86400 ; 24 hours
$ORIGIN eu.hr.example.com
@ 1D IN     SOA @      root (20200322001 3H 15 1w 3h)
@ 1D IN     NS @

test.eu.hr.example.com IN A 1.2.3.4
```

3. Para el servidor de nombres en las instalaciones en la región de Asia:

Zona alojada: `apac.hr.example.com`, `10.0.0.40`

El servidor de nombres de APAC puede delegar el subdominio a otros servidores de nombres.

```
$TTL      86400 ; 24 hours
$ORIGIN apac.hr.example.com
@ 1D IN     SOA @      root (20200322001 3H 15 1w 3h)
@ 1D IN     NS @

test.apac.hr.example.com IN A 5.6.7.8
```

```
engineering.apac.hr.example.com IN NS ns1.engineering.apac.hr.example.com
sales.apac.hr.example.com IN NS ns2.sales.apac.hr.example.com
ns1.engineering.apac.hr.example.com IN A 10.0.0.80
ns2.sales.apac.hr.example.com IN A 10.0.0.90
```

Zona alojada: `engineering.apac.hr.example.com`, `10.0.0.80`

```
$TTL 86400 ; 24 hours
$ORIGIN engineering.apac.hr.example.com
@ 1D IN SOA @ root (20200322001 3H 15 1w 3h)
@ 1D IN NS @
test.engineering.apac.hr.example.com IN A 1.1.1.1
```

4. Para el servidor de nombres en las instalaciones en la región de América del Norte:

Zona alojada: `na.hr.example.net`, IP del NS: `10.0.0.50`

```
$TTL 86400 ; 24 hours
$ORIGIN na.hr.example.net
@ 1D IN SOA @ root (20200322001 3H 15 1w 3h)
@ 1D IN NS @
ns3.na.hr.example.net. IN A 10.0.0.50
test.na.hr.example.com IN A 9.10.11.12
```

Configuración de VPC Resolver

- Para el solucionador de VPC, debe configurar una regla de reenvío y dos reglas de delegación:

Regla de reenvío

1. Para reenviar el registro de out-of-zone delegación, de modo que el solucionador de VPC de Route 53 conozca la IP del NS delegado para reenviar la solicitud inicial.

`domain-name: hr.example.net target-ips: 10.0.0.50`

Reglas de delegación

1. Regla de delegación para la delegación en la zona:

`delegation-record: hr.example.com`

2. Regla de delegación para la delegación fuera de la zona:

delegation-record: hr.example.net

Ejemplo de configuración de delegación entre puntos de salida

En lugar de tener la zona alojada principal en una Amazon VPC, supongamos que se tiene una configuración de DNS en la que la zona alojada principal se encuentra en la ubicación central en las instalaciones y los subdominios se delegan a servidores de nombres alojados en Europa, Asia y América del Norte. Todas las consultas de DNS se pasan a través del solucionador de VPC.

Siga los pasos de ejemplo para configurar el DNS local y el solucionador de VPC.

Configuración de DNS en las instalaciones

1. Para el servidor de nombres en las instalaciones en la región central:

- Zona alojada principal: hr.example.com

Zona alojada hr.example.com, IP del NS: 10.0.0.20

```
$TTL      86400 ; 24 hours
$ORIGIN hr.example.com
@ 1D IN     SOA @      root (20200322001 3H 15 1w 3h)
@ 1D IN     NS @
eu.hr.example.com IN NS ns1.eu.hr.example.com.
apac.hr.example.com IN NS ns2.apac.hr.example.com.
na.hr.example.com IN NS ns3.na.hr.example.net. # Out of zone delegation

ns1.eu.hr.example.com IN A 10.0.0.30 # Glue record
ns2.apac.hr.example.com IN A 10.0.0.40 # Glue record
```

2. Para el servidor de nombres en las instalaciones en la región de Europa (la configuración de los servidores de nombres de Europa, Asia y América del Norte es la misma que la de la delegación de una zona alojada privada a un punto de conexión de salida):

- Zona alojada: eu.hr.example.com, IP del NS: 10.0.0.30

```
$TTL      86400 ; 24 hours
```

```
$ORIGIN eu.hr.example.com
@ 1D IN SOA @ root (20200322001 3H 15 1w 3h)
@ 1D IN NS @

test.eu.hr.example.com IN A 1.2.3.4
```

3. Para el servidor de nombres en las instalaciones en la región de Asia:

Zona alojada: apac.hr.example.com, 10.0.0.40

El servidor de nombres de APAC puede delegar el subdominio a otros servidores de nombres.

```
$TTL 86400 ; 24 hours
$ORIGIN apac.hr.example.com
@ 1D IN SOA @ root (20200322001 3H 15 1w 3h)
@ 1D IN NS @

test.apac.hr.example.com IN A 5.6.7.8
engineering.apac.hr.example.com IN NS ns1.engineering.apac.hr.example.com
sales.apac.hr.example.com IN NS ns2.sales.apac.hr.example.com
ns1.engineering.apac.hr.example.com IN A 10.0.0.80
ns2.sales.apac.hr.example.com IN A 10.0.0.90
```

Zona alojada: engineering.apac.hr.example.com, 10.0.0.80

```
$TTL 86400 ; 24 hours
$ORIGIN engineering.apac.hr.example.com
@ 1D IN SOA @ root (20200322001 3H 15 1w 3h)
@ 1D IN NS @
test.engineering.apac.hr.example.com IN A 1.1.1.1
```

4. Para el servidor de nombres en las instalaciones en la región de América del Norte:

Zona alojada: na.hr.example.net, IP del NS: 10.0.0.50

```
$TTL 86400 ; 24 hours
$ORIGIN na.hr.example.net
@ 1D IN SOA @ root (20200322001 3H 15 1w 3h)
@ 1D IN NS @
ns3.na.hr.example.net. IN A 10.0.0.50
test.na.hr.example.com IN A 9.10.11.12
```

Configuración de VPC Resolver

- Para el VPC Resolver, debe configurar reglas de reenvío y reglas de delegación:

Reglas de reenvío

1. Para reenviar la solicitud inicial de modo que las consultas se reenvíen a la zona alojada principal `hr.example.com` en la ubicación central:

`domain-name: hr.example.com target-ips: 10.0.0.20`

2. Para reenviar el registro de out-of-zone delegación, de modo que el solucionador de VPC conozca la dirección IP del servidor de nombres delegado para reenviar la solicitud inicial:

`domain-name: hr.example.net target-ips: 10.0.0.50`

Reglas de delegación

1. Regla de delegación para la delegación en la zona:

`registro de delegación: hr.example.com`

2. Regla de delegación para la delegación fuera de la zona:

`delegation-record: hr.example.net`

Activar la validación de DNSSEC en Amazon Route 53

Al habilitar la validación de DNSSEC para una virtual private cloud (VPC) en Amazon Route 53, las firmas DNSSEC se verifican criptográficamente para garantizar que la respuesta no se ha manipulado. Habilite la validación DNSSEC en la página de detalles de la VPC.

El solucionador de VPC aplica la validación de DNSSEC a los nombres públicos firmados cuando realiza una resolución de DNS recursiva.

Sin embargo, si la resolución de VPC reenvía a otra resolución de DNS, esa resolución está realizando una resolución de DNS recursiva y, por lo tanto, también debe aplicar la validación de DNSSEC.

 Important

Activar la validación DNSSEC puede afectar la resolución de DNS para los registros DNS públicos de recursos de AWS en una VPC, lo que podría provocar una interrupción. Tenga en cuenta que activar o desactivar la validación de DNSSEC puede tardar varios minutos.

 Note

En este momento, el solucionador de VPC Route 53 de su VPC (también conocido como AmazonProvided DNS) ignora el bit del encabezado EDNS DO (DNSSEC OK) y el bit CD (Checking Disabled) de la consulta de DNS. Si ha configurado DNSSEC, esto significa que, si bien el solucionador de VPC realiza la validación de DNSSEC, no devuelve los registros de DNSSEC ni establece el bit AD en la respuesta. Por lo tanto, el solucionador de VPC no admite actualmente la realización de su propia validación de DNSSEC. Si necesita hacer esto, tendrá que realizar su propia resolución de DNS recursiva.

Para habilitar la validación DNSSEC para una VPC

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/route53/>
2. En el panel de navegación, en VPC Resolver, elija. VPCs
3. En Validación de DNSSEC, seleccione la casilla de verificación. Si la casilla de verificación ya está seleccionada, puede desactivarla para eliminar la validación de DNSSEC.

Tenga en cuenta que activar o desactivar la validación de DNSSEC puede tardar varios minutos.

Enrutar el tráfico de Internet a sus AWS recursos

Puede usar Amazon Route 53 para dirigir el tráfico a una variedad de AWS recursos.

- [Enrutamiento del tráfico a una API de Amazon API Gateway mediante su nombre de dominio](#)
- [Enrutar el tráfico a una CloudFront distribución de Amazon mediante tu nombre de dominio](#)
- [Enrutamiento del tráfico a una EC2 instancia de Amazon](#)
- [Enrutar el tráfico a un AWS App Runner servicio](#)
- [Enrutar el tráfico a una AWS Global Accelerator](#)
- [Enrutar el tráfico a un AWS Elastic Beanstalk entorno](#)
- [Direccionamiento del tráfico a un balanceador de carga ELB](#)
- [Enrutamiento del tráfico a un sitio web alojado en un bucket de Amazon S3](#)
- [Enrutamiento del tráfico a un punto de conexión de interfaz de Amazon Virtual Private Cloud mediante el nombre de dominio](#)
- [Enrutamiento del tráfico a Amazon WorkMail](#)
- [Enrutamiento del tráfico al punto final OpenSearch del dominio de Amazon Service](#)
- [Enrutamiento del tráfico al punto de conexión del dominio del servicio de Amazon VPC Lattice](#)
- [Enrutar el tráfico a otros recursos AWS](#)
- [Creación de recursos de resolución de VPC de Amazon Route 53 y Route 53 con AWS CloudFormation](#)

Enrutamiento del tráfico a una API de Amazon API Gateway mediante su nombre de dominio

Puede utilizar Amazon API Gateway para crear, publicar, mantener, supervisar y proteger APIs. Puede crear APIs esos AWS servicios de acceso u otros servicios web además de los datos almacenados en la AWS nube.

El método que utilice para dirigir tráfico de dominio a una API de API Gateway es el mismo, independientemente de si ha creado un punto de conexión de API Gateway regional o un punto de conexión de API Gateway optimizada para bordes. Si crea un punto de conexión de API Gateway privado, el proceso es algo diferente.

- Punto de conexión de la API regional: se crea un registro de alias de Route 53 que dirige el tráfico al punto de conexión de la API regional.
- Punto de conexión de la API optimizada para bordes: crea un registro de alias de Route 53 que dirige el tráfico a la API optimizada para bordes. Esto hace que el tráfico se dirija a la CloudFront distribución asociada a la API optimizada para entornos periféricos.
- Punto de conexión de API privada: se crea un registro de alias de Route 53 que dirige el tráfico a su punto de conexión de API privada mediante un punto de conexión de VPC de interfaz para API Gateway en una zona alojada privada.

Un registro de alias es una extensión de Route 53 a DNS similar a un registro CNAME. Para obtener una comparación de los registros de alias y CNAME, consulte [Elección entre registros de alias y sin alias](#).

 Note

Route 53 no cobra por las consultas de alias a API Gateway APIs u otros AWS recursos.

Temas

- [Requisitos previos](#)
- [Configuración de Route 53 para dirigir el tráfico a un punto de conexión de interfaz de API Gateway](#)

Requisitos previos

Para comenzar, necesita lo siguiente:

- Una API de API Gateway que tiene un nombre de dominio personalizado, como `api.example.com`, que coincide con el nombre del registro de Route 53 que quiere crear.

Para obtener más información, consulte los temas siguientes:

- [Configuración de nombres de dominio personalizados para HTTP APIs](#) en la Guía para desarrolladores de Amazon API Gateway.
- [Configuración de nombres de dominio personalizados para REST APIs](#) en la Guía para desarrolladores de Amazon API Gateway.

- [Configuración de nombres de dominio personalizados WebSocket APIs en la Guía para desarrolladores de Amazon API Gateway](#).
- [Nombres de dominio personalizados para uso privado APIs en API Gateway](#) en la Guía para desarrolladores de Amazon API Gateway.
- Un nombre de dominio registrado. Puede utilizar Amazon Route 53 como su registrador de dominio o puede usar otro registrador.
- Route 53 como el servicio DNS del dominio. Si registra el nombre de dominio a través de Route 53, configuraremos automáticamente Route 53 como servicio DNS del dominio.

Para obtener información completa sobre el uso de Route 53 como proveedor de servicios DNS para su dominio, consulte [Establecer Amazon Route 53 como servicio DNS de un dominio existente](#).

Configuración de Route 53 para dirigir el tráfico a un punto de conexión de interfaz de API Gateway

Para configurar Route 53 a fin de dirigir el tráfico a un punto de conexión de interfaz de API Gateway, siga este procedimiento.

Custom domain names for public APIs

El siguiente procedimiento describe cómo enrutar el tráfico a un punto final de API Gateway para obtener un nombre de dominio personalizado para el público APIs.

Enrutamiento del tráfico a un punto de conexión de API Gateway

1. Si ha creado la zona alojada de Route 53 y el punto de conexión con la misma cuenta, vaya al paso 2.

Si ha creado la zona alojada y el punto de conexión utilizando cuentas diferentes, obtenga el nombre de dominio de destino correspondiente al nombre de dominio personalizado que desea utilizar:

- a. Inicie sesión en la consola de API Gateway Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/apigateway/>.
- b. En el panel de navegación, elija Custom Domain Names (Nombres de dominio personalizados).

- c. Seleccione el nombre de dominio personalizado que desea utilizar, obtenga el valor de API Gateway domain name (Nombre de dominio de API Gateway).
2. Abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
3. En el panel de navegación, elija Zonas alojadas.
4. Elija el nombre de la zona alojada que tiene el nombre de dominio que desea utilizar para direccionar el tráfico a su API.
5. Elija Crear registro.
6. Especifique los siguientes valores:

 Important

Le recomendamos que active Alias. En el caso de los nombres de dominio que no utilizan un registro de alias de Route 53, es posible que surjan problemas si utiliza una VPC con DNS privado habilitado para invocar una API privada. El DNS privado anula el comportamiento de resolución de DNS predeterminado en la VPC, lo que puede provocar conflictos con los registros DNS externos.

Política de direccionamiento

Elija la política de direccionamiento aplicable. Para obtener más información, consulte [Elección de una política de enrutado](#).

Nombre del registro

Escriba el nombre de dominio que desea utilizar para direccionar el tráfico a su API.

La API a la que quiere dirigir el tráfico debe incluir un nombre de dominio personalizado, como api.example.com, que coincida con el nombre del registro de Route 53.

Alias

Si utiliza el método de creación de registros Quick create (Creación rápida), active Alias (Alias).

Valor/ruta de destino del tráfico

Elija Alias to API Gateway API (Alias para la API de API Gateway) y, a continuación, elija la región de la que proviene el punto de conexión.

La forma de especificar el valor de Endpoint depende de si creó la zona alojada y la API con la misma AWS cuenta o con cuentas diferentes:

- La misma cuenta: la lista de nombres de dominio de destino incluye solo los APIs que tienen un nombre de dominio personalizado que coincide con el valor que especificó para el nombre de registro. Elija el valor aplicable.
- Diferentes cuentas: ingrese el valor que obtuvo en el paso 1 de este procedimiento.

Tipo de registro

Elija A — IPv4 dirección.

Evaluate target health

Para controlar la conmutación por error de DNS, configure las comprobaciones de estado personalizadas. Para ver un ejemplo, consulte [Configurar comprobaciones de estado personalizadas para la conmutación por error de DNS](#) en la guía del usuario de API Gateway.

7. Elija Crear registros.

Por lo general, los cambios se propagan a todos los servidores de Route 53 en un plazo de 60 segundos. Cuando finalice la propagación, podrá direccionar el tráfico a su API mediante el nombre del registro de alias que ha creado en este procedimiento.

Custom domain names for private APIs

El siguiente procedimiento describe cómo enrutar el tráfico a un punto final de API Gateway para obtener un nombre de dominio personalizado de forma privada APIs.

Enrutamiento del tráfico a un punto de conexión de API Gateway

1. Abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Zonas alojadas.
3. Elija el nombre de la zona alojada privada que tiene el nombre de dominio que desea utilizar para direccionar el tráfico a su API.
4. Elija Crear registro.
5. Especifique los siguientes valores:

Política de direccionamiento

Elija la política de direccionamiento aplicable. Para obtener más información, consulte [Elección de una política de enrutado](#).

Nombre del registro

Escriba el nombre de dominio que desea utilizar para direccionar el tráfico a su API.

La API a la que quiere dirigir el tráfico debe incluir un nombre de dominio personalizado, como `api.example.com`, que coincida con el nombre del registro de Route 53.

Alias

Active Alias.

Valor/ruta de destino del tráfico

Elija Alias para el punto de conexión de VPC. Elija la región de la que proviene el punto de conexión y luego seleccione el punto de conexión de VPC.

Tipo de registro

Si lo utiliza IPv6 para su punto final de VPC, cree un tipo de registro AAAA. Si utiliza la pila doble para el punto de conexión de VPC, cree un tipo de registro AAAA y un tipo de registro A.

Evaluate target health

Para controlar la conmutación por error de DNS, configure las comprobaciones de estado personalizadas. Para ver un ejemplo, consulte [Configurar comprobaciones de estado personalizadas para la conmutación por error de DNS](#) en la guía del usuario de API Gateway.

6. Elija Crear registros.

Por lo general, los cambios se propagan a todos los servidores de Route 53 en un plazo de 60 segundos. Cuando finalice la propagación, podrá direccionar el tráfico a su API mediante el nombre del registro de alias que ha creado en este procedimiento.

Enrutar el tráfico a una CloudFront distribución de Amazon mediante tu nombre de dominio

En este tema se proporcionan procedimientos exhaustivos para enrutar el tráfico de DNS a cualquier CloudFront distribución de Amazon. Si estás configurando un sitio web estático con Amazon CloudFront y Amazon Simple Storage Service, consulta [Usa una CloudFront distribución de Amazon para ofrecer un sitio web estático](#) el tutorial completo.

Puedes usar Amazon CloudFront, la red de entrega de AWS contenido (CDN), como una forma de acelerar la entrega de tu contenido web. CloudFront puede ofrecer todo su sitio web (incluido contenido dinámico, estático, de streaming e interactivo) mediante una red global de ubicaciones periféricas. Los usuarios que solicitan su contenido se enrutan automáticamente a la ubicación periférica que les ofrece la latencia más baja.

Note

Puede dirigir el tráfico a una CloudFront distribución solo para las zonas alojadas públicamente.

Para utilizarla CloudFront para distribuir el contenido de su sitio web, cree una distribución y especifique su configuración. Por ejemplo, especifique el bucket de Amazon S3 o el servidor HTTP del que CloudFront desea obtener su contenido, si desea que solo los usuarios seleccionados tengan acceso a su contenido y si desea que los usuarios usen HTTPS.

Cuando cree una distribución, CloudFront asigne un nombre de dominio a la distribución, por ejemplo. `d111111abcdef8.cloudfront.net` Puedes usar este nombre de dominio URLs para tu contenido, por ejemplo:

```
http://d111111abcdef8.cloudfront.net/logo.jpg
```

Como alternativa, puedes usar tu propio nombre de dominio en URLs, por ejemplo:

```
http://example.com/logo.jpg
```

Sigue los pasos de la Guía para CloudFront desarrolladores de Amazon para usar tu propio nombre de dominio en los archivos de una CloudFront distribución, URLs en lugar del nombre de dominio que se CloudFront asigna a tu distribución. Para obtener más información sobre cómo usar tu propio

nombre de dominio con una CloudFront distribución, consulta [Cómo usar nombres de dominio personalizados URLs añadiendo nombres de dominio alternativos \(\) CNAMEs](#).

Cuando utilice un nombre de dominio de Route 53 con una CloudFront distribución, utilice Amazon Route 53 para crear un [registro de alias](#) que apunte a su CloudFront distribución. Un registro de alias es una extensión de Route 53 para DNS. Es similar a un registro CNAME, pero puede crear un registro de alias tanto para el dominio raíz, por ejemplo, example.com, como para los subdominios, por ejemplo, www.example.com. (Puede crear registros CNAME solo para subdominios). Cuando Route 53 recibe una consulta de DNS que coincide con el nombre y el tipo de un registro de alias, este responde con el nombre de dominio que esté asociado con su distribución.

Note

Route 53 no cobra por las consultas de alias a CloudFront distribuciones u otros AWS recursos.

Requisitos previos

Para comenzar, necesita lo siguiente:

1. Un nombre de dominio registrado. Puede utilizar Amazon Route 53 como su registrador de dominio o puede usar otro registrador.
2. Route 53 como el servicio DNS del dominio. Si registra el nombre de dominio a través de Route 53, configuraremos automáticamente Route 53 como servicio DNS del dominio.

Para obtener información completa sobre el uso de Route 53 como proveedor de servicios DNS para su dominio, consulte [Establecer Amazon Route 53 como servicio DNS de un dominio existente](#).

3. Una CloudFront distribución o un inquilino CloudFront de distribución. La distribución debe incluir un nombre de dominio alternativo que coincida con el nombre de dominio que desea utilizar para su distribución URLs en lugar del nombre de dominio CloudFront asignado a su distribución. En el caso CloudFront de un arrendatario de distribución, debe contener el nombre de dominio que desee utilizar para su URLs.

Por ejemplo, si quieres que tu contenido contenga el URLs nombre de dominio example.com, el campo Nombre de dominio alternativo de la distribución debe incluir example.com.

Para obtener más información, consulta la siguiente documentación en la Guía para CloudFront desarrolladores de Amazon:

- [Lista de tareas para la creación de una distribución](#)
- [Cómo crear o actualizar una distribución mediante la consola de CloudFront](#)

 Note

Si vas a crear un sitio web estático, consulta Cómo [empezar con un sitio web estático seguro](#) en la Guía para CloudFront desarrolladores de Amazon para obtener instrucciones de configuración completas.

4. (Opcional) Solicita un certificado público para que CloudFront las distribuciones de Amazon requieran HTTPS. Para obtener más información, consulte [DNS validation AWS Certificate Manager\(Validación de DNS\)](#) en la Guía del usuario de AWS Certificate Manager .

Configuración de Amazon Route 53 para enrutar el tráfico a una CloudFront distribución

Para configurar Amazon Route 53 para que dirija el tráfico a una CloudFront distribución, sigue estos pasos. Para obtener más información sobre cómo usar tu propio nombre de dominio con una CloudFront distribución, consulta Cómo [usar nombres de dominio personalizados URLs añadiendo nombres de dominio alternativos \(CNAMEs\)](#) en la Guía para CloudFront desarrolladores de Amazon.

 Note

Por lo general, los cambios se propagan a todos los servidores de Route 53 en un plazo de 60 segundos. Cuando los cambios se propaguen, podrá dirigir el tráfico a su CloudFront distribución utilizando el nombre del registro de alias que cree en este procedimiento.

Para dirigir el tráfico a una distribución de CloudFront

1. Obtenga el nombre de dominio CloudFront asignado a su distribución y determine si IPv6 está activado:
 - a. Inicie sesión en Consola de administración de AWS y abra la CloudFront consola en <https://console.aws.amazon.com/cloudfront/v4/home>.

- b. En la columna ID (ID), seleccione el nombre vinculado de la distribución a la que desea dirigir el tráfico (no la casilla de verificación).
- c. En la pestaña General, obtenga el valor del campo Distribution domain name (Nombre del dominio de distribución).
- d. En la pestaña General, en la sección Configuración, selecciona editar y desplázate para comprobar si el IPv6 campo IPv6 está habilitado para la distribución. Si IPv6 está activado, tendrá que crear dos registros de alias para la distribución, uno para enrutar el IPv4 tráfico a la distribución y otro para enrutar el IPv6 tráfico. Elija Cancelar.

Para obtener más información, consulte [Habilitar IPv6](#) en el tema [Valores que especifique al crear o actualizar una distribución](#) en la Guía para CloudFront desarrolladores de Amazon.

2. En el caso de un arrendatario de CloudFront distribución,
 - a. Seleccione SaaS en el menú de navegación de la izquierda, luego Inquilinos de distribución y elija el inquilino de distribución con el nombre de dominio al que desee enrutar el tráfico.
 - b. En la sección Detalles generales, copie el valor de Punto de conexión.
3. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
4. En el panel de navegación, elija Zonas alojadas.
5. Elija el nombre vinculado de la zona alojada para el dominio que quiere usar para enrutar el tráfico a su CloudFront distribución.
6. Elija Crear registro.
7. Especifique los siguientes valores:

Nombre del registro

Introduzca el nombre de dominio que desee utilizar para dirigir el tráfico a su CloudFront distribución. El valor predeterminado es el nombre de la zona alojada.

Por ejemplo, si el nombre de la zona alojada es example.com y desea utilizar acme.example.com para dirigir el tráfico a su distribución, escriba acme.

Tipo de registro

Elija A — IPv4 dirección.

Si IPv6 está habilitada para la distribución y va a crear un segundo registro, elija AAAA: IPv6 dirección.

Alias

Active Alias.



Important

Debe crear un registro de alias para que la CloudFront distribución funcione.

Dirigir tráfico a

Elija Alias para la CloudFront distribución. Elija el nombre de dominio que CloudFront se asignó a la distribución cuando la creó. Este es el valor que ha obtenido en el paso 1.

Para un arrendatario de CloudFront distribución, elija el punto final en el paso 2.

Evaluate target health

Acepte el valor predeterminado de No.

Política de direccionamiento

Elija la política de direccionamiento aplicable. Para obtener más información, consulte [Elección de una política de enrutado](#).

8. Elija Crear registros.
9. Si IPv6 está habilitado para la distribución, repita los pasos 5 a 7. Especifique la misma configuración excepto para el campo Tipo de registro, tal como se explica en el paso 6.

Enrutamiento del tráfico a una EC2 instancia de Amazon

Amazon EC2 proporciona capacidad informática escalable en la AWS nube. Puede lanzar un entorno informático EC2 virtual (una instancia) mediante una plantilla preconfigurada (una Amazon Machine Image o AMI). Al lanzar una EC2 instancia, instala EC2 automáticamente el sistema operativo (Linux o Microsoft Windows) y el software adicional incluido en la AMI, como el software de servidor web o de base de datos.

Si aloja un sitio web o ejecuta una aplicación web en una EC2 instancia, puede dirigir el tráfico de su dominio, como example.com, a su servidor mediante Amazon Route 53.

Requisitos previos

Para comenzar, necesita lo siguiente:

- Una EC2 instancia de Amazon. Para obtener información sobre el lanzamiento de una EC2 instancia, consulta la siguiente documentación:
 - Linux: consulte [Introducción a las instancias de Amazon EC2 Linux](#) en la Guía del EC2 usuario de Amazon
 - Microsoft Windows: consulte [Introducción a las instancias de Amazon EC2 Windows](#) en la Guía del EC2 usuario de Amazon

Important

Te recomendamos que también crees una [dirección IP elástica](#) y la asocies a tu EC2 instancia. Una dirección IP elástica garantiza que la dirección IP de su EC2 instancia de Amazon nunca cambiará. Para obtener información relacionada con los precios, consulte [Precios para direcciones IP elásticas](#).

- Un nombre de dominio registrado. Puede utilizar Amazon Route 53 como su registrador de dominio o puede usar otro registrador.
- Route 53 como el servicio DNS del dominio. Si registra el nombre de dominio a través de Route 53, configuraremos automáticamente Route 53 como servicio DNS del dominio.

Para obtener información completa sobre el uso de Route 53 como proveedor de servicios DNS para su dominio, consulte [Establecer Amazon Route 53 como servicio DNS de un dominio existente](#).

Configuración de Amazon Route 53 para enrutar el tráfico a una EC2 instancia de Amazon

Para configurar Amazon Route 53 para que enrute el tráfico a una EC2 instancia, lleve a cabo el siguiente procedimiento.

Para enrutar el tráfico a una EC2 instancia de Amazon

1. Obtenga la dirección IP de la EC2 instancia de Amazon:

- a. Inicia sesión en la EC2 consola de Amazon Consola de administración de AWS y ábrela en <https://console.aws.amazon.com/ec2/>.
- b. En la lista de regiones de la esquina superior derecha de la consola, elija la región en la que haya lanzado la instancia.
- c. En el panel de navegación, seleccione Instances (Instancias).
- d. En la tabla, elija la instancia a la que desea dirigir el tráfico.
- e. En el panel inferior, en la pestaña Descripción, obtén el valor de Elastic IPs.

Si no ha asociado una dirección IP elástica a la instancia, obtenga el valor de IPv4 Public IP.

2. Abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
3. En el panel de navegación, elija Zonas alojadas.
4. Elija el nombre de la zona alojada que coincida con el nombre del dominio que desee utilizar para dirigir el tráfico.
5. Elija Crear registro.
6. Especifique los siguientes valores:

Política de direccionamiento

Elija la política de direccionamiento aplicable. Para obtener más información, consulte [Elección de una política de enrutado](#).

Nombre del registro

Ingresa el nombre de dominio que desees usar para enrutar el tráfico a tu EC2 instancia. El valor predeterminado es el nombre de la zona alojada.

Por ejemplo, si el nombre de la zona alojada es example.com y quieres usar acme.example.com para enrutar el tráfico a tu EC2 instancia, ingresa acme.

Valor/ruta de destino del tráfico

Elija IP address or another value depending on the record type (Dirección IP u otro valor en función del tipo de registro). Escriba la dirección IP que obtuvo en el paso 1.

Tipo de registro

Elija A — IPv4 dirección.

TTL (segundos)

Acepte el valor predeterminado de 300.

7. Elija Crear registros.

Por lo general, los cambios se propagan a todos los servidores de Route 53 en un plazo de 60 segundos. Cuando finalice la propagación, podrá enrutar el tráfico a su EC2 instancia utilizando el nombre del registro que creó en este procedimiento.

Important

Si libera la IP elástica, asegúrese también de eliminar el registro DNS que apunta a ella. Si no lo hace, tendrá un registro DNS colgante del que podrá apoderarse un usuario no autorizado.

Enrutar el tráfico a un AWS App Runner servicio

AWS App Runner es un servicio totalmente gestionado que facilita a los desarrolladores la implementación de aplicaciones web en contenedores a gran APIs escala y sin necesidad de experiencia previa en infraestructura. Comience con el código fuente o la imagen de un contenedor. App Runner crea e implementa la aplicación web automáticamente, equilibra la carga del tráfico con el cifrado, se escala para satisfacer sus necesidades de tráfico y facilita la comunicación de sus servicios con otros AWS servicios y aplicaciones que se ejecutan en una Amazon VPC privada. Con App Runner, en lugar de pensar en servidores o en escalar, tiene más tiempo para concentrarse en las aplicaciones. Para obtener más información, consulte [¿Qué es AWS App Runner?](#) en la Guía para desarrolladores de AWS App Runner .

Important

Amazon Route 53 actualmente admite registros de alias para AWS App Runner los servicios que se creen después del 1 de agosto de 2022.

Para dirigir el tráfico a un servicio de App Runner, utilice Amazon Route 53 a fin de crear un [registro de alias](#) que apunte al servicio. Un registro de alias es una extensión de Route 53 para DNS. Es similar a un registro CNAME, salvo que puede crear un registro de alias tanto para el dominio raíz,

por ejemplo, `example.com`, como para los subdominios, por ejemplo, `www.example.com` (`http://www.example.com/`). Solo puede crear registros CNAME para subdominios.

 Note

Route 53 no aplica cargos por consultas de alias al servicio de App Runner u otros recursos de AWS .

Requisitos previos

Para comenzar, necesita lo siguiente:

- Un servicio de App Runner. Para obtener más información sobre la creación de un servicio de App Runner, consulte [Getting started with App Runner](#) (Introducción a App Runner).
- Un nombre de dominio registrado. Puede utilizar Amazon Route 53 como su registrador de dominio o puede usar otro registrador.
- Route 53 como el servicio DNS del dominio. Si registra el nombre de dominio a través de Route 53, configuraremos automáticamente Route 53 como servicio DNS del dominio.

Para obtener información completa sobre el uso de Route 53 como proveedor de servicios DNS para su dominio, consulte [Establecer Amazon Route 53 como servicio DNS de un dominio existente](#).

- Se asoció el dominio personalizado a su servicio de App Runner. Para obtener más información, consulte [Managing custom domain names for App Runner](#) (Administración de nombres de dominio personalizados para App Runner).
- Configure el registro de validación de certificados devuelto por App Runner a la zona alojada en Route 53 para iniciar el proceso de validación del dominio. Para obtener más información, consulte [DNS validation AWS Certificate Manager\(Validación de DNS\)](#) en la Guía del usuario de AWS Certificate Manager .

Configuración de Amazon Route 53 para dirigir el tráfico a un servicio de App Runner

Para configurar Amazon Route 53 a fin de dirigir el tráfico a un servicio de App Runner, siga este procedimiento.

Para dirigir el tráfico a un servicio de App Runner

1. Abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Zonas alojadas.
3. Elija el nombre de la zona alojada que coincida con el nombre del dominio que desee utilizar para dirigir el tráfico.
4. Elija Crear registro.
5. Especifique los siguientes valores:

Política de direccionamiento

Elija la política de direccionamiento aplicable. Para obtener más información, consulte [Elección de una política de enrutado](#).

Nombre del registro

Ingrese el nombre de dominio que quiere utilizar para dirigir el tráfico al servicio de App Runner. El valor predeterminado es el nombre de la zona alojada.

Por ejemplo, si el nombre de la zona alojada es example.com y quiere utilizar acme.example.com para dirigir el tráfico al servicio de App Runner, ingrese acme.

Valor/ruta de destino del tráfico

Elija Alias to App Runner Service (Alias del servicio de App Runner) y, a continuación, seleccione la Región de AWS. Elija el nombre de dominio del entorno en el que desea enrutar el tráfico.

Tipo de registro

Acepte el valor predeterminado, A — IPv4 dirección.

Evaluate target health

Seleccione No. Para obtener información sobre cómo evaluar el estado del destino, consulte [Evaluate target health](#).

6. Elija Crear registros.

Por lo general, los cambios se propagan a todos los servidores de Route 53 en un plazo de 60 segundos. Cuando finalice la propagación, podrá dirigir el tráfico a su servicio de App Runner mediante el nombre del registro de alias que ha creado en este procedimiento.

Enrutar el tráfico a una AWS Global Accelerator

AWS Global Accelerator es un servicio en el que se crean aceleradores para mejorar el rendimiento de las aplicaciones para los usuarios locales y globales. El servicio reacciona al instante ante los cambios en el estado o la configuración para garantizar que el tráfico de Internet de los clientes se dirija siempre a puntos de conexión en buen estado. Global Accelerator incluye una arquitectura tolerante a fallos e incorpora AWS Shield Standard sistemas automatizados de mitigación en línea de DDoS de los ataques tipo S. Para obtener más información, consulte [Qué es Global Accelerator](#) en la AWS Global Accelerator guía para desarrolladores.

De forma predeterminada, Global Accelerator le proporciona direcciones IP estáticas que puede asociar a su acelerador. Las direcciones IP estáticas se transmiten de forma aleatoria desde la red AWS perimetral. Los aceleradores incluyen un nombre de DNS predeterminado, pero, en la mayoría de las situaciones, puede configurar el DNS para que use su nombre de dominio personalizado (como `www.example.com`) con el acelerador, en lugar de usar las direcciones IP estáticas asignadas o el nombre de DNS predeterminado.

Note

Route 53 no aplica cargos por consultas de alias a Global Accelerator u otros recursos de AWS.

Requisitos previos

Para comenzar, necesita lo siguiente:

- Un acelerador. Puede crear un acelerador estándar o un acelerador de enrutamiento personalizado. Para obtener más información, consulte [Crear un acelerador estándar](#) y [Crear un acelerador de enrutamiento personalizado](#).
- Un nombre de dominio registrado. Puede utilizar Amazon Route 53 como su registrador de dominio o puede usar otro registrador.
- Route 53 como el servicio DNS del dominio. Si registra el nombre de dominio a través de Route 53, configuraremos automáticamente Route 53 como servicio DNS del dominio.

Para obtener información completa sobre el uso de Route 53 como proveedor de servicios DNS para su dominio, consulte [Establecer Amazon Route 53 como servicio DNS de un dominio existente](#).

Configuración de Amazon Route 53 para enrutar el tráfico a un acelerador

Para configurar Amazon Route 53 a fin de enrutar el tráfico a un acelerador, siga este procedimiento.

Cómo enrutar el tráfico a un acelerador

1. Abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Zonas alojadas.
3. Elija el nombre de la zona alojada que coincida con el nombre del dominio que desee utilizar para dirigir el tráfico.
4. Elija Crear registro.
5. Especifique los siguientes valores:

Política de direccionamiento

Elija la política de direccionamiento aplicable. Para obtener más información, consulte [Elección de una política de enrutado](#).

Nombre del registro

Introduzca el nombre de dominio que quiera utilizar para enrutar el tráfico a su acelerador. El valor predeterminado es el nombre de la zona alojada.

Por ejemplo, si el nombre de la zona alojada es example.com y desea utilizar acme.example.com para enrutar el tráfico a su Global Accelerator, escriba acme.

Valor/ruta de destino del tráfico

Seleccione Alias a Global Accelerator y, a continuación, seleccione Región de AWS. Seleccione el nombre de DNS del acelerador.

Puede ingresar el nombre de DNS de un acelerador que creó con la Cuenta de AWS actual o con una Cuenta de AWS distinta.

Tipo de registro

Acepte el valor predeterminado, A — IPv4 dirección.

Evalue target health

Acepte el valor predeterminado de Yes (Sí).

6. Elija Crear registros.

Por lo general, los cambios se propagan a todos los servidores de Route 53 en un plazo de 60 segundos. Cuando finalice la propagación, podrá enrutar el tráfico a su acelerador mediante el uso del nombre del registro de alias que ha creado en este procedimiento.

Enrutar el tráfico a un AWS Elastic Beanstalk entorno

Si lo utiliza AWS Elastic Beanstalk para implementar y administrar aplicaciones en la AWS nube, puede usar Amazon Route 53 para enrutar el tráfico de DNS de su dominio, como example.com, a un entorno de Elastic Beanstalk nuevo o existente.

Para dirigir el tráfico de DNS en un entorno de Elastic Beanstalk, consulte los procedimientos en los siguientes temas.

Note

En estos procedimientos se supone que ya está utilizando Route 53 como el servicio DNS de su dominio. Si utiliza otro servicio DNS, consulte [Establecer Amazon Route 53 como servicio DNS de un dominio existente](#) a fin de obtener información acerca del uso de Route 53 como proveedor de servicios DNS para su dominio.

Temas

- [Implementación de una aplicación en un entorno de Elastic Beanstalk](#)
- [Obtención del nombre de dominio del entorno de Elastic Beanstalk](#)
- [Creación de un registro de Amazon Route 53 que dirija el tráfico al entorno de Elastic Beanstalk](#)

Implementación de una aplicación en un entorno de Elastic Beanstalk

Si ya tiene un entorno de Elastic Beanstalk al que desea dirigir el tráfico, vaya a [Obtención del nombre de dominio del entorno de Elastic Beanstalk](#).

Creación de una aplicación e implementación en un entorno de Elastic Beanstalk

- Para obtener más información acerca de la creación de una aplicación y su implementación en un entorno de Elastic Beanstalk, consulte [Introducción a Elastic Beanstalk](#) en la AWS Elastic Beanstalk Guía para desarrolladores.

Obtención del nombre de dominio del entorno de Elastic Beanstalk

Si ya conoce el nombre de dominio de su entorno de Elastic Beanstalk, vaya a [Creación de un registro de Amazon Route 53 que dirija el tráfico al entorno de Elastic Beanstalk](#).

Obtención del nombre de dominio del entorno de Elastic Beanstalk

1. Inicie sesión en la consola de Elastic Beanstalk Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/elasticbeanstalk/>
2. En la lista de aplicaciones, busque la aplicación a la que desea direccionar el tráfico y obtenga el valor de URL. En el panel de navegación, elija Applications (Aplicaciones), y, a continuación, seleccione la aplicación en la lista.

Para obtener más información acerca de la URL, consulte [Nombre de dominio de su entorno de Elastic Beanstalk](#) en la Guía para desarrolladores de Elastic Beanstalk.

Creación de un registro de Amazon Route 53 que dirija el tráfico al entorno de Elastic Beanstalk

Un registro de Amazon Route 53 contiene la configuración que controla cómo se dirige el tráfico a su entorno de Elastic Beanstalk. Cree un registro CNAME o un registro de alias, en función de si el nombre de dominio del entorno incluye la región, como us-east-2, en la que ha implementado el entorno. Los nuevos entornos incluyen la región en el nombre de dominio, pero no así los entornos que se han creado antes de principios de 2016. Para ver una comparación de registros CNAME y de alias, consulte [Elección entre registros de alias y sin alias](#).

Si el nombre de dominio no incluye la región

Debe crear un registro CNAME. Sin embargo, debido a las limitaciones que impone DNS, puede crear registros CNAME solo para subdominios, no para el nombre de dominio raíz. Por ejemplo, si su nombre de dominio es example.com, puede crear un registro que dirija el tráfico de acme.example.com a su entorno de Elastic Beanstalk, pero no puede crear un registro que dirija el tráfico de example.com a su entorno de Elastic Beanstalk.

Lea el procedimiento [Creación de un registro CNAME para dirigir el tráfico a un entorno de Elastic Beanstalk](#).

Si el nombre de dominio incluye la región

Puede crear un registro de alias. Un registro de alias es específico de Route 53 y tiene dos ventajas significativas sobre los registros CNAME:

- Puede crear registros de alias para el nombre de dominio raíz o para subdominios. Por ejemplo, si su nombre de dominio es example.com, puede crear un registro que dirija las solicitudes de example.com o acme.example.com a su entorno de Elastic Beanstalk.
- Route 53 no aplica cargos por las solicitudes que utilizan un registro de alias para dirigir el tráfico.

Lea el procedimiento [Creación de un registro de alias de Amazon Route 53 para dirigir el tráfico a un entorno de Elastic Beanstalk](#).

Creación de un registro CNAME para dirigir el tráfico a un entorno de Elastic Beanstalk

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/route53/>
2. En el panel de navegación, elija Zonas alojadas.
3. Elija el nombre de la zona alojada que desea utilizar para dirigir el tráfico a su entorno de Elastic Beanstalk.
4. Elija Crear registro.
5. Elija Cambiar para crear rápidamente
6. Especifique los siguientes valores:

Política de direccionamiento

Elija la política de direccionamiento aplicable. Para obtener más información, consulte [Elección de una política de enrutado](#).

Nombre del registro

Escriba el nombre de dominio que desea utilizar para dirigir el tráfico a su entorno de Elastic Beanstalk. El valor predeterminado es el nombre de la zona alojada.

Por ejemplo, si el nombre de la zona alojada es example.com y desea utilizar acme.example.com para dirigir el tráfico a su entorno, escriba acme.

 Important

No se puede crear un registro CNAME que tenga el mismo nombre que la zona alojada.

Alias

Si utiliza el método de creación de registros Quick create (Creación rápida), active Alias (Alias).

Valor/ruta de destino del tráfico

Elija IP address or another value depending on the record type (Dirección IP u otro valor en función del tipo de registro) y especifique el valor que obtiene al realizar el procedimiento en el tema [Obtención del nombre de dominio del entorno de Elastic Beanstalk](#). Si ha usado cuentas diferentes para crear la zona alojada de Route 53 y el entorno de Elastic Beanstalk, ingrese los atributos CNAME del entorno de Elastic Beanstalk.

Tipo de registro

Elija CNAME.

TTL (segundos)

Acepte el valor predeterminado de 300.

7. Elija Crear registros.

Por lo general, los cambios se propagan a todos los servidores de Route 53 en un plazo de 60 segundos.

Creación de un registro de alias de Amazon Route 53 para dirigir el tráfico a un entorno de Elastic Beanstalk

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Zonas alojadas.
3. Elija el nombre de la zona alojada que desea utilizar para dirigir el tráfico a su entorno de Elastic Beanstalk.

4. Elija Crear registro.
5. Especifique los siguientes valores:

Política de direccionamiento

Elija la política de direccionamiento aplicable. Para obtener más información, consulte [Elección de una política de enrutado](#).

Nombre del registro

Escriba el nombre de dominio que desea utilizar para dirigir el tráfico a su entorno de Elastic Beanstalk. El valor predeterminado es el nombre de la zona alojada.

Por ejemplo, si el nombre de la zona alojada es example.com y desea utilizar acme.example.com para dirigir el tráfico a su entorno, escriba acme.

Valor/ruta de destino del tráfico

Elija Alias to Elastic Beanstalk environment (Entorno de Alias a Elastic Beanstalk) y, a continuación, elija la región de la que proviene el punto de conexión. Elija el nombre de dominio del entorno en el que desea enrutar el tráfico. Es el valor que obtiene al realizar el procedimiento del tema [Obtención del nombre de dominio del entorno de Elastic Beanstalk](#).

Si ha usado cuentas diferentes para crear la zona alojada de Route 53 y el entorno de Elastic Beanstalk, ingrese el atributo CNAME del entorno de Elastic Beanstalk.

Tipo de registro

Acepte la IPv4 dirección A — por defecto.

Evaluate target health

Acepte el valor predeterminado de Yes (Sí).

6. Elija Crear registros.

Por lo general, los cambios se propagan a todos los servidores de Route 53 en un plazo de 60 segundos. Cuando finalice la propagación, podrá dirigir el tráfico a su entorno de Elastic Beanstalk mediante el nombre del registro de alias que ha creado en este procedimiento.

Direccionamiento del tráfico a un balanceador de carga ELB

Si alojas un sitio web en varias EC2 instancias de Amazon, puedes distribuir el tráfico a tu sitio web entre las instancias mediante un balanceador de cargas ELB (ELB). El servicio ELB escala automáticamente el balanceador de carga a medida que cambia el tráfico a su sitio web a lo largo del tiempo. Asimismo, el balanceador de carga puede monitorizar el estado de las instancias registradas y dirige el tráfico de dominio solo a las instancias con estado correcto.

Para dirigir el tráfico de dominio a un balanceador de carga de ELB, utilice Amazon Route 53 a fin de crear un [registro de alias](#) que apunte a su balanceador de carga. Un registro de alias es una extensión de Route 53 para DNS. Es similar a un registro CNAME, pero puede crear un registro de alias tanto para el dominio raíz, por ejemplo, example.com, como para los subdominios, por ejemplo, www.example.com. (Puede crear registros CNAME solo para subdominios).

Note

Route 53 no aplica cargos por consultas de alias a los balanceadores de carga de ELB u otros recursos de AWS .

Requisitos previos

Para comenzar, necesita lo siguiente:

- Un balanceador de carga de ELB. Puede usar ELB Classic, Application Load Balancer o Network Load Balancer. Para obtener información sobre la creación de un balanceador de carga, consulta [Cómo empezar con ELB en la Guía del usuario de Elastic Load Balancing](#).

Asigne un nombre al balanceador de carga que le ayude a recordar su finalidad más tarde. El nombre que especifique al crear un balanceador de carga es el que elegirá al crear un registro de alias en la consola de Route 53.

- Un nombre de dominio registrado. Puede utilizar Route 53 como su registrador de dominio o puede usar otro registrador.
- Route 53 como el servicio DNS del dominio. Si registra el nombre de dominio a través de Route 53, configuraremos automáticamente Route 53 como servicio DNS del dominio.

Para obtener información completa sobre el uso de Route 53 como proveedor de servicios DNS para su dominio, consulte [Establecer Amazon Route 53 como servicio DNS de un dominio existente](#).

Configuración de Amazon Route 53 para dirigir el tráfico a un balanceador de carga de ELB

Para configurar Amazon Route 53 a fin de dirigir el tráfico a un balanceador de carga de ELB, siga este procedimiento.

Para dirigir el tráfico a balanceador de carga de ELB

1. Si ha creado la zona alojada de Route 53 y el balanceador de carga de ELB utilizando la misma cuenta, vaya al paso 2.

Si ha creado la zona alojada y el balanceador de carga de ELB usando cuentas diferentes, siga el procedimiento de [Obtener el nombre del DNS para un balanceador de carga ELB](#) para obtener el nombre de DNS del balanceador de carga.

2. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/route53/>
3. En el panel de navegación, elija Zonas alojadas.
4. Elija el nombre de la zona alojada que tenga el nombre de dominio que desea utilizar para dirigir el tráfico al balanceador de carga.
5. Elija Crear registro.
6. Especifique los siguientes valores:

Política de direccionamiento

Elija la política de direccionamiento aplicable. Para obtener más información, consulte [Elección de una política de enrutado](#).

Nombre del registro

Escriba el nombre de dominio o subdominio que desea utilizar para dirigir el tráfico a su balanceador de carga de ELB. El valor predeterminado es el nombre de la zona alojada.

Por ejemplo, si el nombre de la zona alojada es `example.com` y desea utilizar `acme.example.com` para dirigir el tráfico a su balanceador de carga, escriba `acme`.

Alias

Si utiliza el método de creación de registros `Quick create` (Creación rápida), active `Alias` (Alias).

Valor/ruta de destino del tráfico

Elija `Alias to Application and Classic Load Balancer` (Alias para aplicación y balanceador de carga clásico) o `Alias to Network Load Balancer` (Alias para balanceador de carga de red) y, a continuación, elija la región de la que proviene el punto de conexión.

Si creaste la zona alojada y el balanceador de cargas ELB con la misma AWS cuenta, elige el nombre DNS que asignaste al balanceador de cargas cuando lo creaste.

Si ha creado la zona alojada y el equilibrador de carga de ELB mediante cuentas diferentes, escriba el valor que obtuvo en el paso 1 de este procedimiento.

Note

La consola antepone `dualstack.` al nombre DNS de la aplicación y de `Classic Load Balancer` únicamente desde la misma AWS cuenta. Cuando un cliente, como un navegador web, solicita la dirección IP para su nombre de dominio (`example.com`) o nombre de subdominio (`www.example.com`), el cliente puede solicitar una IPv4 dirección (un registro `A`), una IPv6 dirección (un registro `AAAA`) o ambas IPv4 y IPv6 direcciones (en solicitudes independientes con el primero). IPv4 La designación `dualstack.` permite a Route 53 responder con la dirección IP adecuada del balanceador de carga en función del formato de dirección IP que ha solicitado el cliente. Tendrá que anteponer `dualstack.` para la aplicación y el `Classic Load Balancer` desde la otra cuenta.

Tipo de registro

Elija `A` — IPv4 dirección.

Evaluate target health

Si desea que Route 53 dirija el tráfico en función del estado de los recursos, elija Yes (Sí). Para obtener más información sobre la comprobación del estado de los recursos, consulte [Creación de comprobaciones de estado de Amazon Route 53](#).

7. Elija Crear registros.

Por lo general, los cambios se propagan a todos los servidores de Route 53 en un plazo de 60 segundos. Cuando finalice la propagación, podrá dirigir el tráfico a su balanceador de carga mediante el nombre del registro de alias que ha creado en este procedimiento.

Enrutamiento del tráfico a un sitio web alojado en un bucket de Amazon S3

En este tema se explican procedimientos exhaustivos para enrutar el tráfico de DNS a cualquier bucket de Amazon Simple Storage Service configurado para el alojamiento de sitios web estáticos. Si planea configurar un sitio web estático con Amazon Simple Storage Service, consulte [Uso de su dominio para un sitio web estático en un bucket de Amazon S3](#) para ver el tutorial completo.

Amazon Simple Storage Service (Amazon S3) proporciona un [almacenamiento en la nube](#) seguro, duradero y con un alto grado de escalabilidad. Puede configurar un bucket de S3 para alojar un sitio web estático que puede incluir páginas web y archivos de comandos de cliente. (S3 no es compatible con el scripting en el lado del servidor).

Para dirigir el tráfico de dominio a un bucket de S3, utilice Amazon Route 53 a fin de crear un [registro de alias](#) que apunte a su bucket. Un registro de alias es una extensión de Route 53 para DNS. Es similar a un registro CNAME, salvo que puede crear un registro de alias tanto para el dominio raíz, por ejemplo, example.com, como para los subdominios, por ejemplo, www.example.com. Puede crear registros CNAME solo para subdominios.

Note

Route 53 no aplica cargos por consultas de alias a los buckets de S3 u otros recursos de AWS.

Requisitos previos

Para comenzar, necesita lo siguiente:

- Un bucket de S3 configurado para alojar un sitio web estático.

Para obtener más información, consulte [Tutorial: Configuración de un sitio web estático mediante un dominio personalizado registrado con Route 53](#) en la Guía del usuario de Amazon Simple Storage Service.

Important

El bucket debe tener el mismo nombre que el dominio o subdominio. Por ejemplo, si desea usar el subdominio `acme.example.com`, el nombre del bucket debe ser `acme.example.com`.

Puede dirigir el tráfico para un dominio y sus subdominios, como `example.com` y `www.example.com`, a un solo bucket. Cree un bucket para el dominio y cada subdominio, y configúrelos todos menos uno para redirigir el tráfico al bucket restante.

Note

Un bucket de S3 que esté configurado como punto final de un sitio web no admite SSL/TLS, por lo que es necesario enrutar el tráfico a la CloudFront distribución y utilizar el bucket de S3 como origen de la distribución.

Para obtener instrucciones sobre cómo crear una CloudFront distribución, consulte.

[Enrutar el tráfico a una CloudFront distribución de Amazon mediante tu nombre de dominio](#)

- Un nombre de dominio registrado. Puede utilizar Route 53 como su registrador de dominio o puede usar otro registrador.
- Route 53 como el servicio DNS del dominio. Si registra el nombre de dominio a través de Route 53, configuraremos automáticamente Route 53 como servicio DNS del dominio.

Para obtener información completa sobre el uso de Route 53 como proveedor de servicios DNS para su dominio, consulte [Establecer Amazon Route 53 como servicio DNS de un dominio existente](#).

Configuración de Amazon Route 53 para dirigir el tráfico a un bucket de S3

Para configurar Amazon Route 53 a fin de que dirija el tráfico a un bucket de S3 configurado para alojar un sitio web estático, siga este procedimiento.

Para dirigir el tráfico a un bucket de S3

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Zonas alojadas.
3. Elija el nombre de la zona alojada que tiene el nombre de dominio que desea utilizar para dirigir el tráfico a su bucket de S3.
4. Elija Crear registro.
5. Especifique los siguientes valores:

Nombre del registro

Escriba el nombre de dominio que desea utilizar para dirigir el tráfico a su bucket de S3. El valor predeterminado es el nombre de la zona alojada.

Por ejemplo, si el nombre de la zona alojada es example.com y desea utilizar acme.example.com para dirigir el tráfico a su bucket, escriba acme.

Tipo de registro

Elija A — IPv4 dirección.

Alias

Active Alias.

Dirigir tráfico a

Elija Alias to S3 website endpoint (Alias para el punto de conexión del sitio web de S3) y, a continuación, elija la región de la que proviene el punto de conexión.

Elija el bucket que tiene el mismo nombre que ha especificado para Record name (Nombre del registro).

La lista incluye un bucket solo si el bucket cumple los siguientes requisitos:

- El nombre del bucket es el mismo que el del registro que está creando.

- El bucket está configurado como punto de conexión de sitio web.
- El bucket lo creó la cuenta de AWS actual.

Si creó el bucket con otra cuenta de AWS , ingrese el nombre de la región en la que creó el bucket de S3. Para ver el formato correcto del nombre de la región, consulte la columna Punto de conexión de sitio web de la tabla [Puntos de conexión de sitio web de Amazon S3](#) en la Referencia general de Amazon Web Services.

Evaluate target health

Seleccione No. Para obtener información sobre cómo evaluar el estado del destino, consulte [Evaluate target health](#).

Política de direccionamiento

Elija la política de direccionamiento aplicable. Para obtener más información, consulte [Elección de una política de enrutado](#).

6. Elija Crear registros.

Por lo general, los cambios se propagan a todos los servidores de Route 53 en un plazo de 60 segundos. Cuando finalice la propagación, podrá dirigir el tráfico a su bucket de S3 mediante el nombre del registro de alias que ha creado en este procedimiento.

Enrutamiento del tráfico a un punto de conexión de interfaz de Amazon Virtual Private Cloud mediante el nombre de dominio

Puede utilizarlo AWS PrivateLink para acceder a servicios seleccionados con un punto final de interfaz Amazon Virtual Private Cloud (Amazon VPC). Estos servicios incluyen algunos AWS servicios, los servicios que alojan otros AWS clientes y socios por su cuenta VPCs y los servicios de AWS Marketplace socios compatibles.

Para dirigir el tráfico de dominio a un punto de conexión de interfaz, use Amazon Route 53 a fin de crear un registro de alias. Un registro de alias es una extensión de Route 53 para DNS. Es similar a un registro CNAME, pero puede crear un registro de alias tanto para el dominio raíz, por ejemplo, example.com, como para los subdominios, por ejemplo, www.example.com. Puede crear registros CNAME solo para subdominios.

 Note

Route 53 no cobra por las consultas de alias a los puntos finales de la interfaz u otros AWS recursos.

Temas

- [Requisitos previos](#)
- [Configuración de Amazon Route 53 para dirigir el tráfico a un punto de conexión de interfaz de Amazon VPC](#)

Requisitos previos

Para comenzar, necesita lo siguiente:

- Un punto de conexión de interfaz de Amazon VPC. Para obtener más información, consulte [Puntos de conexión de VPC de interfaz \(AWS PrivateLink\)](#) en la Guía del usuario de Amazon VPC.
- Un nombre de dominio registrado. Puede utilizar Amazon Route 53 como su registrador de dominio o puede usar otro registrador.
- Route 53 como el servicio DNS del dominio. Si registra el nombre de dominio a través de Route 53, configuraremos automáticamente Route 53 como servicio DNS del dominio.

Para obtener información completa sobre el uso de Route 53 como proveedor de servicios DNS para su dominio, consulte [Establecer Amazon Route 53 como servicio DNS de un dominio existente](#).

Configuración de Amazon Route 53 para dirigir el tráfico a un punto de conexión de interfaz de Amazon VPC

Para configurar Amazon Route 53 a fin de dirigir el tráfico a un punto de conexión de interfaz de Amazon VPC, siga este procedimiento.

Para direccionar el tráfico a un punto de conexión de interfaz de Amazon VPC

1. Si ha creado la zona alojada de Route 53 y el punto de conexión de interfaz de Amazon VPC utilizando la misma cuenta, vaya al paso 2.

Si ha creado la zona alojada y el punto de conexión de interfaz utilizando cuentas diferentes, obtenga el nombre de servicio correspondiente al punto de conexión de interfaz:

- a. Inicie sesión en la consola de Amazon VPC Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/vpc/>
 - b. En el panel de navegación, elija Puntos de conexión.
 - c. En el panel derecho, elija el punto de conexión al que desea direccionar el tráfico de Internet.
 - d. En el panel inferior, obtenga el valor del nombre de DNS, por ejemplo, `vpce-0fd00dd593example-dexample.cloudtrail.us-west-2.vpce.amazonaws.com`.
2. Abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
 3. En el panel de navegación, elija Zonas alojadas.
 4. Elija el nombre de la zona alojada que tiene el nombre de dominio que desea utilizar para dirigir el tráfico a su punto de conexión de interfaz.
 5. Elija Crear registro.
 6. Especifique los siguientes valores:

Política de direccionamiento

Elija la política de direccionamiento aplicable. Para obtener más información, consulte [Elección de una política de enrutado](#).

Nombre del registro

Ingrese el nombre de dominio que desea utilizar para dirigir el tráfico a su punto de conexión de interfaz de Amazon VPC.

Alias

Si utiliza el método de creación de registros Quick create (Creación rápida), active Alias (Alias).

Valor/ruta de destino del tráfico

Elija Alias to VPC endpoint (Alias para el punto de conexión de la VPC) y, a continuación, elija la región de la que proviene el punto de conexión.

La forma de especificar el valor de los puntos de enlace depende de si ha creado la zona alojada y el punto final de la interfaz con la misma AWS cuenta o con cuentas diferentes:

- La misma cuenta: elija la lista y busque la categoría Amazon VPC endpoints (Puntos de enlace de Amazon VPC). A continuación, elija el nombre de DNS del punto de conexión de interfaz al que desea direccionar el tráfico de Internet.
- Diferentes cuentas: ingrese el valor que obtuvo en el paso 1 de este procedimiento.

Tipo de registro

Elija A — IPv4 dirección.

Evaluate target health

Seleccione No. Para obtener información sobre cómo evaluar el estado del destino, consulte [Evaluate target health](#).

7. Elija Crear registros.

Por lo general, los cambios se propagan a todos los servidores de Route 53 en un plazo de 60 segundos. Cuando finalice la propagación, podrá direccionar el tráfico a su punto de conexión de interfaz mediante el nombre del registro de alias que ha creado en este procedimiento.

Enrutamiento del tráfico a Amazon WorkMail

Puedes usar Route 53 para dirigir el tráfico a tu dominio de WorkMail correo electrónico de Amazon. El nombre de la zona alojada de Route 53 (como example.com) debe coincidir con el nombre de un WorkMail dominio de Amazon.

Note

Puedes enrutar el tráfico a un WorkMail dominio de Amazon solo para las zonas alojadas públicas.

Para enrutar el tráfico a Amazon WorkMail, lleve a cabo los cuatro procedimientos siguientes.

Para configurar Amazon Route 53 como su servicio DNS y añadir una WorkMail organización de Amazon y un dominio de correo electrónico

1. Si no ha registrado el nombre de dominio que desea utilizar en sus direcciones de email (como juan@example.com), registre el dominio ahora para saber que el dominio está disponible. Para obtener más información, consulte [Registrar un nuevo dominio](#).

Si Amazon Route 53 no es el servicio DNS del dominio de correo electrónico que has añadido a Amazon WorkMail, migra el servicio DNS del dominio a Route 53. Para obtener más información, consulte [Establecer Amazon Route 53 como servicio DNS de un dominio existente](#).

2. Añade una WorkMail organización de Amazon y un dominio de correo electrónico. Para obtener más información, consulta [Cómo empezar para nuevos usuarios](#) en la Guía del WorkMail administrador de Amazon.

Para crear un registro TXT de Route 53 para Amazon WorkMail

1. En el panel de navegación de la WorkMail consola de Amazon, selecciona Dominios.
2. Elige el nombre del dominio de correo electrónico, como example.com, que quieres usar para enrutar el tráfico a Amazon WorkMail.
3. Abra otra pestaña del navegador y abra la [consola de Route 53](#).
4. En la consola de Route 53, haga lo siguiente:
 - a. En el panel de navegación, elija Zonas alojadas.
 - b. Elige el nombre de la zona alojada que quieres usar para tu dominio de WorkMail correo electrónico de Amazon.
5. En la WorkMail consola de Amazon, en la sección Paso 1: Verificar la propiedad del dominio, ve a la columna Hostname y copia la parte del valor que precede al nombre de tu dominio de correo electrónico.

Por ejemplo, si tu dominio de WorkMail correo electrónico de Amazon es example.com y el valor de Hostname es _amazonses.example.com, copia _amazonses.

6. En la consola de Route 53, haga lo siguiente:
 - a. Elija Create record (Crear registro) y elija Simple routing (Direccionamiento sencillo).
 - b. En Record name (Nombre del registro), pegue el valor que ha copiado en el paso 5.
 - c. En Record type (Tipo de registro), elija TXT – Text (TXT: texto).
7. En la WorkMail consola de Amazon, para el registro TXT, copia el valor de la columna Value, incluidas las comillas.
8. En la consola de Route 53, haga lo siguiente:

- a. Para Value/Route traffic to (Valor/ruta de destino del tráfico), elija IP address or another value depending on the record type (Dirección IP u otro valor en función del tipo de registro) y pegue el valor que ha copiado en el paso 7.

No cambie otras opciones de configuración.

- b. Seleccione Crear.

Para crear un registro MX de Route 53 para Amazon WorkMail

1. En la WorkMail consola de Amazon, en la sección Paso 2: Finalizar la configuración del dominio, ve a la fila que tiene el tipo de registro MX y copia el valor de la columna Valor.
2. En la consola de Route 53, haga lo siguiente:

- a. Elija Crear registro.
- b. Para Value/Route traffic to (Valor/ruta de destino del tráfico), elija IP address or another value depending on the record type (Dirección IP u otro valor en función del tipo de registro) y pegue el valor que ha copiado en el paso 1.
- c. Para Record type (Tipo de registro), elija MX – Mail Exchange (MX: intercambio de correo).

No cambie otras opciones de configuración.

- d. Elija Crear registros.

Para crear cuatro registros CNAME de Route 53 para Amazon WorkMail

1. En la WorkMail consola de Amazon, en la sección Paso 2: Finalizar la configuración del dominio, ve a la primera fila que tenga el tipo de registro CNAME. En la columna Hostname, copie la parte del valor que precede al nombre de su dominio de email.

Por ejemplo, si tu dominio de WorkMail correo electrónico de Amazon es example.com y el valor de Hostname es autodiscover.example.com, copia autodiscover.

2. En la consola de Route 53, haga lo siguiente:
 - a. Elija Crear registro.
 - b. En Record name (Nombre del registro), pegue el valor que ha copiado en el paso 1.
 - c. En Record type (Tipo de registro), elija CNAME – Canonical Name (CNAME: nombre canónico).

3. En la WorkMail consola de Amazon, en la primera fila que tenga el tipo de registro CNAME, copia el valor de la columna Value.
4. En la consola de Route 53, haga lo siguiente:
 - a. Para Value/Route traffic to (Valor/ruta de destino del tráfico), elija IP address or another value depending on the record type (Dirección IP u otro valor en función del tipo de registro) y pegue el valor que ha copiado en el paso 3.

No cambie otras opciones de configuración.
 - b. Elija Crear registros.
5. Repita los pasos 1 a 4 para el resto de los registros CNAME que aparecen en la WorkMail consola de Amazon.

Enrutamiento del tráfico al punto final OpenSearch del dominio de Amazon Service

Amazon OpenSearch Service es un servicio gestionado que facilita la implementación, el funcionamiento y el escalado de OpenSearch clústeres en Nube de AWS. Un dominio de OpenSearch Service es sinónimo de un clúster OpenSearch de servicios. Los dominios son clústeres con la configuración, los tipos de instancia, los recuentos de instancias y los recursos de almacenamiento que especifique. Para obtener más información, consulta [Qué es Amazon OpenSearch Service](#) en la Guía para desarrolladores OpenSearch de Amazon Service.

Requisitos previos

Para comenzar, necesita lo siguiente:

Un dominio de OpenSearch servicio que tenga un nombre de dominio personalizado, como example.com, que coincida con el nombre del registro de Route 53 que desea crear.

Para obtener más información, consulte los temas siguientes:

- [Cómo empezar](#) en la Guía para desarrolladores OpenSearch de Amazon Service.
- [Cómo crear un punto de conexión personalizado](#) en la Guía para desarrolladores de Amazon OpenSearch Service.

Configuración de Amazon Route 53 para enrutar el tráfico a un punto final OpenSearch de dominio de Amazon Service

Para usar Route 53 para enrutar el tráfico al OpenSearch Servicio, primero debe utilizar el punto de enlace del dominio proporcionado por el OpenSearch Servicio. Este punto final de doble pila se proporciona solo si el punto final personalizado está habilitado en un dominio de OpenSearch servicio con modo de red de doble pila. Para obtener más información, consulta Cómo [crear un punto de conexión personalizado](#) en la Guía para desarrolladores de Amazon OpenSearch Service.

Para enrutar el tráfico a un punto final OpenSearch del servicio

1. Ve a Iniciar sesión en la consola <https://aws.amazon.com> y selecciona Iniciar sesión en ella.
2. En Analytics, selecciona Amazon OpenSearch Service.
3. En Clústeres administrados, seleccione Dominios.
4. En la página Dominios, seleccione el nombre del dominio al que desea enrutar el tráfico.
5. En la página de detalles del dominio, copie el valor de Punto de conexión del dominio v2 (pila doble).
6. Abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
7. En el panel de navegación, elija Zonas alojadas.
8. Elija el nombre vinculado de la zona alojada para el dominio que quiere usar para enrutar el tráfico al punto final del OpenSearch servicio. El nombre de dominio debe coincidir con el punto final personalizado definido en el OpenSearch servicio.
9. Elija Crear registro.

Puede usar el asistente para crear los registros o bien elegir Switch to quick create (Cambiar a creación rápida).

10. Especifique los siguientes valores:

Política de direccionamiento

Elija la política de direccionamiento aplicable. Para obtener más información, consulte [Elección de una política de enrutado](#).

Nombre del registro

Introduzca el nombre de dominio que desee utilizar para enrutar el tráfico al punto final del dominio de OpenSearch servicio. El valor predeterminado es el nombre de la zona alojada.

Por ejemplo, si el nombre de la zona alojada es example.com y desea utilizar acme.example.com para dirigir el tráfico a su distribución, escriba acme.

Alias

Si utiliza el método de creación de registros Quick create (Creación rápida), active Alias (Alias).

Valor/ruta de destino del tráfico

Elige Alias to OpenSearch Service Domain Endpoint. Elija la región en la que se creó el dominio de OpenSearch servicio y elija el valor que obtuvo en el paso 5.

Tipo de registro

Elija la IPv4 dirección A, la IPv6 dirección AAAA o ambas para la pila doble.

Evaluate target health

Seleccione No. Para obtener información sobre cómo evaluar el estado del destino, consulte [Evaluate target health](#).

11. Elija Crear registros.

Enrutamiento del tráfico al punto de conexión del dominio del servicio de Amazon VPC Lattice

Amazon VPC Lattice es un servicio de redes de aplicaciones totalmente administrado que puede utilizar para conectar, proteger y supervisar los servicios de su aplicación. Puede usar VPC Lattice con una única nube privada virtual (VPC) o en varias VPCs de una o más cuentas. Para obtener más información, consulte [What is Amazon VPC Lattice](#) en la Guía del usuario de Amazon VPC Lattice.

Requisitos previos

Para comenzar, necesita lo siguiente:

Un dominio del servicio de VPC Lattice que tenga un nombre de dominio personalizado, como example.com, que coincida con el nombre del registro de Route 53 que desee crear.

Para obtener más información, consulte [Associate a custom domain name with your service](#) en la Guía del usuario de Amazon VPC Lattice.

Configuración de Amazon Route 53 para enrutar el tráfico a un punto de conexión del dominio del servicio de VPC Lattice

Para usar Route 53 para enrutar el tráfico al dominio del servicio de Amazon VPC Lattice, primero debe obtener el punto de conexión de servicio del dominio que proporciona VPC Lattice. Para obtener más información, consulte [Associate a custom domain name with your service](#) en la Guía del usuario de Amazon VPC Lattice.

Cómo enrutar el tráfico al punto de conexión del dominio del servicio de VPC Lattice.

1. Ve a Iniciar sesión en la consola <https://aws.amazon.com> y selecciona Iniciar sesión en la consola.
2. En Redes y entrega de contenido, seleccione VPC.
3. En Lattice PrivateLink y Lattice, elija Lattice Services.
4. Cree un servicio de VPC Lattice o seleccione un servicio de VPC Lattice existente.

Note

Al crear un servicio de VPC Lattice, debe especificar una configuración de dominio personalizada y proporcionar un nombre de dominio personalizado. Si elige un servicio existente, también debe tener un dominio personalizado.

5. En Configuración del dominio, copie el valor del nombre de dominio personalizado.
6. Abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>
7. En el panel de navegación, elija Zonas alojadas.
8. Elija el nombre vinculado de la zona alojada correspondiente al dominio que desee utilizar para enrutar el tráfico al punto de conexión de dominio del servicio de VPC Lattice. El nombre de dominio debe coincidir con el punto de conexión del dominio personalizado definido en VPC Lattice.
9. Elija Crear registro.

Puede usar el asistente para crear los registros o bien elegir Switch to quick create (Cambiar a creación rápida).

10. Especifique los siguientes valores:

Política de direccionamiento

Elija la política de direccionamiento aplicable. Para obtener más información, consulte [Elección de una política de enrutado](#).

Nombre del registro

Ingresa el nombre de dominio que quiera utilizar para enrutar el tráfico al punto de conexión del dominio del servicio de VPC Lattice. El valor predeterminado es el nombre de la zona alojada.

Por ejemplo, si el nombre de la zona alojada es example.com y desea utilizar acme.example.com para dirigir el tráfico a su distribución, escriba acme.

Alias

Si utiliza el método de creación de registros Quick create (Creación rápida), active Alias (Alias).

Valor/ruta de destino del tráfico

Seleccione Alias al servicio de VPC Lattice. Seleccione la región en la que se creó el dominio del servicio de VPC Lattice y luego el valor que obtuvo en el paso 5.

Tipo de registro

Elija la IPv4 dirección A, la IPv6 dirección AAAA o ambas para la pila doble.

Evaluate target health

Seleccione No. Para obtener información sobre cómo evaluar el estado del destino, consulte [Evaluate target health](#).

11. Elija Crear registros.

Enrutar el tráfico a otros recursos AWS

La lista siguiente incluye una lista de temas de otras guías sobre cómo utilizar Route 53 para dirigir el tráfico a esos servicios.

- [Uso de AWS Cloud Map](#) en la Guía del usuario de AWS Cloud Map .
- [Administre dominios personalizados](#) en la Guía para AWS App Runner desarrolladores.

- [Using Route 53 as a DNS provider](#) (Uso de Route 53 como proveedor de DNS) en la Guía del usuario de AWS Transfer Family .
- [Uso de Route 53 para apuntar un dominio a una instancia de Amazon Lightsail](#).

Creación de comprobaciones de estado de Amazon Route 53

Las comprobaciones de estado de Amazon Route 53 monitorean el estado y el rendimiento de sus aplicaciones web, servidores web y otros recursos. Cada comprobación de estado que cree puede monitorizar uno de los siguientes elementos:

- El estado de un recurso especificado, como un servidor web.
- El estado de otras comprobaciones de estado.
- El estado de la alarma de Amazon CloudWatch.
- Además, con el Controlador de recuperación de aplicaciones de Amazon (ARC), puede configurar comprobaciones de estado del control de enrutamiento con registros de conmutación por error de DNS para administrar la conmutación por error del tráfico de la aplicación. Para obtener más información, consulte la [Guía para desarrolladores del Controlador de recuperación de aplicaciones de Amazon \(ARC\)](#).

Para obtener Información general de los tipos de comprobaciones de estado, consulte [Tipos de comprobaciones de estado de Amazon Route 53](#). Para obtener información sobre la creación de comprobaciones de estado, consulte [Creación y actualización de comprobaciones de estado](#).

Después de crear una comprobación de estado, puede obtener el estado de la comprobación de estado, recibir notificaciones cuando cambie el estado y configurar la recuperación ante errores a nivel de DNS:

Obtención del estado y las notificaciones de la comprobación de estado

Puede ver el estado actual y reciente de las comprobaciones de estado en la consola de Route 53. También puede trabajar con las comprobaciones de estado mediante programación, a través de uno de los AWS SDK, la AWS Command Line Interface, AWS Tools for Windows PowerShell o la API de Route 53.

Si desea recibir una notificación cuando cambie el estado de una comprobación de estado, puede configurar una alarma de Amazon CloudWatch para cada comprobación de estado.

Para obtener información sobre la visualización del estado de la comprobación de estado y recibir notificaciones, consulte [Monitorizar el estado de la comprobación de estado y recibir notificaciones](#).

Configuración de la recuperación ante errores a nivel de DNS

Si tiene varios recursos que realizan la misma función, puede configurar la conmutación por error a nivel de DNS para que Route 53 dirija el tráfico de un recurso con estado incorrecto a otro con estado correcto. Por ejemplo, si tiene dos servidores web y el estado de un servidor web deja de ser correcto, Route 53 puede dirigir el tráfico al otro. Para obtener más información, consulte [Configuración de la recuperación ante errores a nivel de DNS](#).

Temas

- [Tipos de comprobaciones de estado de Amazon Route 53](#)
- [Cómo determina Amazon Route 53 si la comprobación de estado es correcta](#)
- [Creación, actualización y eliminación de comprobaciones de estado](#)
- [Configuración de la recuperación ante errores a nivel de DNS](#)
- [Denominar y etiquetar comprobaciones de estado](#)
- [Usar comprobaciones de estado con versiones de la API de Amazon Route 53 que sean anteriores al 2012-12-12](#)

Tipos de comprobaciones de estado de Amazon Route 53

Puede crear los tipos de comprobaciones de estado de Amazon Route 53 siguientes:

Comprobaciones de estado que monitorizan un punto de conexión

Puede configurar una comprobación de estado que monitorice un punto de conexión que especifique por dirección IP o por nombre de dominio. En los intervalos regulares que especifique, Route 53 envía solicitudes automatizadas a través de Internet a su aplicación, servidor u otro recurso para comprobar que está accesible, disponible y funcional. También puede configurar la comprobación de estado para que realice solicitudes similares a los que hacen los usuarios, como solicitar una página web de una URL específica.

Comprobaciones de estado que monitorean otras comprobaciones de estado (comprobaciones de estado calculadas)

Puede crear una comprobación de estado que monitoree si Route 53 considera otras comprobaciones de estado correctas o incorrectas. Una situación en la que podría ser útil se da cuando tiene varios recursos que realizan la misma función, como varios servidores web, y

su preocupación principal es saber si un número mínimo de recursos tienen un estado correcto. Puede crear una comprobación de estado para cada recurso sin configurar la notificación para dichas comprobaciones de estado. A continuación, puede crear una comprobación de estado que monitoree el estado de las demás comprobaciones de estado y que le notifique solo cuando el número de recursos web disponibles esté por debajo de un umbral especificado.

Comprobaciones de estado que monitorean las alarmas de CloudWatch

Puede crear alarmas de CloudWatch que monitoreen el estado de las métricas de CloudWatch, como el número de eventos de lectura limitados de una base de datos de Amazon DynamoDB o el número de hosts Elastic Load Balancing que se considera que tienen un estado correcto. Después de crear una alarma, puede crear una comprobación de estado que monitoree el mismo flujo de datos que monitoree CloudWatch para la alarma.

Para mejorar la resistencia y la disponibilidad, Route 53 no espera a que la alarma de CloudWatch cambie al estado ALARM. El estado de una comprobación de estado cambia de correcto a incorrecto según el flujo de datos y los criterios de la alarma de CloudWatch.

Route 53 es compatible con las alarmas de CloudWatch que tienen las siguientes características:

- Métricas de resolución estándar. Las métricas de alta resolución no se admiten. Para obtener más información, consulte [Métricas de alta resolución](#) en la Guía del usuario de Amazon CloudWatch.
- Estadísticas: Average, Minimum, Maximum, Sum y SampleCount. Las estadísticas extendidas no se admiten.
- Route 53 no admite alarmas “M de N”. Para obtener más información, consulte [Evaluación de una alarma](#) en la Guía del usuario de Amazon CloudWatch.
- Una comprobación de estado solo puede supervisar una alarma de CloudWatch que exista en la misma cuenta de AWS que la comprobación de estado.
- Route 53 no admite alarmas que usan [cálculos de métricas](#) para consultar varias métricas de CloudWatch.

Controlador de enrutamiento del controlador de recuperación de aplicaciones de Amazon (ARC)

Las comprobaciones de estado de ARC están asociadas a controles de enrutamiento, que son simples conmutadores de encendido/apagado. Configure cada comprobación de estado del control de enrutamiento con un registro DNS de conmutación por error. A continuación, simplemente puede actualizar los controles de enrutamiento en ARC para redirigir el tráfico y conmutar por error sus aplicaciones; por ejemplo, entre zonas de disponibilidad o regiones

de AWS. Para obtener más información, consulte [Routing control in ARC](#) en la Guía para desarrolladores de ARC.

Cómo determina Amazon Route 53 si la comprobación de estado es correcta

El método que utiliza Amazon Route 53 para determinar si una comprobación de estado es correcta depende del tipo de comprobación de estado.

Cómo determina Route 53 el estado de las comprobaciones de estado que monitorean un punto de conexión

Route 53 dispone de comprobadores de estado en ubicaciones situadas por todo el mundo. Cuando se crea una comprobación de estado que monitoriza un punto de conexión, los comprobadores de estado comienzan a enviar solicitudes al punto de conexión especificado para determinar si está en buen estado. Es posible elegir las ubicaciones que quiere que utilice Route 53 y especificar el intervalo entre comprobaciones: cada 10 segundos o cada 30 segundos. Tenga en cuenta que los comprobadores de estado de Route 53 en distintos centros de datos no se coordinan entre sí, por lo que a veces aparecerán varias solicitudes por segundo independientemente del intervalo elegido, seguidas de unos segundos sin comprobaciones de estado.

Cada comprobador de estado evalúa el estado del punto de conexión en función de dos valores:

- Tiempo de respuesta. Un recurso puede ser responder con lentitud o no responder a una solicitud de comprobación de estado por diversas razones. Por ejemplo, el recurso está desactivado para realizar tareas de mantenimiento, está sufriendo un ataque de denegación de servicio distribuido (DDoS) o la red se encuentra fuera de servicio.
- Si el punto de conexión responde o no a una serie de comprobaciones de estado consecutivas especificadas (el umbral de error)

Route 53 agrega los datos de los comprobadores de estado y determina si el punto de conexión está en buen estado:

- Si más del 18 % de los comprobadores de estado comunican que el estado de un punto de conexión es correcto, Route 53 considera que está en buen estado.

- Si el 18 % o menos de los comprobadores de estado comunican que el estado de un punto de conexión es correcto, Route 53 considera que está en mal estado.

El valor del 18% se ha elegido para garantizar que los comprobadores de estado de varias regiones consideren que el punto de conexión está en buen estado. Esto evita que un punto de conexión se considere que está en mal estado solo porque las condiciones de la red le han aislado de algunas ubicaciones de comprobación de estado. Este valor podría cambiar en una versión futura.

El tiempo de respuesta que un comprobador de estado concreto emplea para determinar si un punto de conexión está en buen estado depende del tipo de comprobación de estado:

- Comprobaciones de estado de HTTP y HTTPS Route 53 debe poder establecer una conexión TCP con el punto de conexión en cuatro segundos. Además, el punto de conexión debe responder con un código de estado HTTP de 2xx o 3xx en un plazo de dos segundos después de la conexión.

 Note

Las comprobaciones de mantenimiento HTTPS no validan los certificados SSL/TLS, por lo que las comprobaciones no fallan si un certificado no es válido o ha caducado.

- Comprobaciones de estado de TCP: Route 53 debe poder establecer una conexión TCP con el punto de conexión en diez segundos.
- Comprobaciones de estado de HTTP y HTTPS con coincidencia de cadenas: al igual que sucede con las comprobaciones de estado de HTTP y HTTPS, Route 53 debe poder establecer una conexión TCP con el punto de conexión en cuatro segundos y el punto de conexión debe responder con un código de estado HTTP de 2xx o 3xx en dos segundos después de la conexión.

Después de que un comprobador de estado de Route 53 reciba el código de estado HTTP, debe recibir el cuerpo de la respuesta desde el punto de conexión en los próximos dos segundos. Route 53 busca en el cuerpo de la respuesta una cadena que especifique. La cadena debe aparecer en su totalidad en los primeros 5120 bytes del cuerpo de la respuesta o el punto de conexión no superará la comprobación de estado. Si usa la consola de Route 53, especifique la cadena en el campo Search String (Buscar cadena). Si utiliza la API de Route 53, especifique la cadena en el elemento `SearchString` al crear la comprobación de estado.

Para las comprobaciones de estado que monitoreen un punto de conexión (excepto las comprobaciones de estado de TCP), si la respuesta del punto de conexión incluye encabezados,

los encabezados deben estar en el formato que se define en RFC7230, Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing, [sección 3.2, "Header Fields"](#).

Route 53 considera que una nueva comprobación de estado es correcta hasta que haya suficientes datos para determinar el estado real, correcto o no. Si ha elegido la opción de invertir el estado de comprobación de estado, Route 53 considera que una nueva comprobación de estado no es correcta hasta que haya suficientes datos.

Cómo determina Route 53 el estado de las comprobaciones de estado que monitorean otras comprobaciones de estado

Una comprobación de estado puede monitorear el estado de otras comprobaciones de estado; este tipo se conoce como una comprobación de estado calculada. La comprobación de estado que realiza el monitoreo es la comprobación de estado principal y las que se monitorean son las comprobaciones de estado secundarias. Una comprobación de estado principal puede monitorear el estado de hasta 255 comprobaciones de estado secundarias. A continuación, se explica cómo funciona el monitoreo:

- Route 53 agrega hasta el número de comprobaciones de estado secundarias que se consideran correctas.
- Route 53 compara ese número con el número de comprobaciones de estado secundarias que deben ser correctas para que el estado de una comprobación de estado principal se considere correcto.

Para obtener más información, consulte [Monitorizar otras comprobaciones de estado \(comprobaciones de estado calculadas\)](#) en [Valores que especifica al crear o actualizar comprobaciones de estado](#).

Route 53 considera que una nueva comprobación de estado es correcta hasta que haya suficientes datos para determinar el estado real, correcto o no. Si ha elegido la opción de invertir el estado de comprobación de estado, Route 53 considera que una nueva comprobación de estado no es correcta hasta que haya suficientes datos.

Cómo determina Route 53 el estado de las comprobaciones de estado que monitorean las alarmas de CloudWatch

Cuando se crea una comprobación de estado basada en una alarma de CloudWatch, Route 53 monitorea el flujo de datos de la alarma correspondiente en lugar de monitorear el estado de la

alarma. Si el flujo de datos indica que el estado de la alarma es OK (Correcto), se considera que la comprobación de estado es correcta. Si la transmisión de datos indica que el estado es Alarm, se considera que la comprobación de estado es incorrecta. Si la transmisión de datos no proporciona información suficiente para determinar el estado de la alarma, el estado de la comprobación de estado depende de la configuración de Health check status (Estado de la comprobación de estado): correcto, incorrecto o último estado desconocido. (En la API de Route 53, esta configuración es `InsufficientDataHealthStatus`.)

Route 53 no admite alarmas de CloudWatch entre cuentas.

 Note

Dado que las comprobaciones de estado de Route 53 monitorean los flujos de datos de CloudWatch en lugar del estado de las alarmas de CloudWatch, no puede forzar el cambio del estado de una comprobación de estado mediante la operación [SetAlarmState](#) de la API CloudWatch.

Route 53 considera que una nueva comprobación de estado es correcta hasta que haya suficientes datos para determinar el estado real, correcto o no. Si ha elegido la opción de invertir el estado de comprobación de estado, Route 53 considera que una nueva comprobación de estado no es correcta hasta que haya suficientes datos.

Creación, actualización y eliminación de comprobaciones de estado

 Important

Si desea actualizar o eliminar las comprobaciones de estado que están asociadas con registros, consulte las tareas de [Actualizar o eliminar comprobaciones de estado cuando está configurada la recuperación ante errores a nivel de DNS](#) antes de continuar.

En esta sección se tratan los siguientes temas relacionados con la administración de las comprobaciones de estado de Route 53:

1. Creación y actualización de las comprobaciones de estado:

- Aprenda a crear y actualizar comprobaciones de estado con la consola de Route 53.
 - Comprenda los valores que debe especificar al crear o actualizar las comprobaciones de estado, como la supervisión de los puntos de conexión, el protocolo, la dirección IP, el nombre de dominio y las opciones de configuración avanzadas.
2. Valores que se muestran al crear una comprobación de estado:
 - Descubra los valores que muestra la consola de Route 53 en función de los datos introducidos al crear una comprobación de estado, como la URL completa o la dirección IP y el puerto.
 3. Actualización de las comprobaciones de estado para los cambios de alarma de CloudWatch:
 - Descubra cómo actualizar una comprobación de estado al cambiar la configuración de la alarma de CloudWatch asociada.
 4. Eliminación de comprobaciones de estado:
 - Siga estos pasos para eliminar comprobaciones de estado con la consola de Route 53.
 5. Actualización o eliminación de comprobaciones de estado cuando está configurada la conmutación por error de DNS:
 - Conozca las tareas recomendadas que se deben realizar al actualizar o eliminar las comprobaciones de estado asociadas a los registros de DNS para garantizar una configuración adecuada del enrutamiento y de la conmutación por error.
 6. Configuración de las reglas de enrutador y de firewall:
 - Comprenda cómo configurar las reglas del enrutador y del firewall para permitir el tráfico de entrada desde los comprobadores de estado de Route 53, lo que garantiza que las comprobaciones de estado se realicen de forma correcta.

Si sigue la información que se proporciona en esta sección, puede crear, actualizar y eliminar de forma eficaz las comprobaciones de estado de Route 53, administrar su configuración y garantizar una integración adecuada con las políticas de enrutamiento y conmutación por error de DNS.

Temas

- [Creación y actualización de comprobaciones de estado](#)
- [Valores que especifica al crear o actualizar comprobaciones de estado](#)
- [Valores que muestra Amazon Route 53 al crear una comprobación de estado](#)
- [Actualizar comprobaciones de estado al cambiar la configuración de la alarma de CloudWatch \(comprobaciones de estado que monitorean solo una alarma de CloudWatch\)](#)
- [Desactivación o activación de las comprobaciones de estado](#)

- [Inversión de una comprobación de estado](#)
- [Eliminar comprobaciones de estado](#)
- [Actualizar o eliminar comprobaciones de estado cuando está configurada la recuperación ante errores a nivel de DNS](#)
- [Configuración de las reglas de enrutador y de firewall para las comprobaciones de estado de Amazon Route 53](#)

Creación y actualización de comprobaciones de estado

En el siguiente procedimiento se describe cómo crear y actualizar comprobaciones de estado con la consola de Route 53.

Note

Estamos en proceso de actualización de la consola de comprobaciones de estado para Route 53. Durante el periodo de transición, puede seguir utilizando la consola anterior.

Seleccione la pestaña de la consola que esté utilizando.

- [New console](#)
- [Consola antigua](#)

New console

Cómo crear o actualizar una comprobación de estado

1. Si desea actualizar las comprobaciones de estado que ya están asociadas con registros, realice las tareas recomendadas de [Actualizar o eliminar comprobaciones de estado cuando está configurada la recuperación ante errores a nivel de DNS](#).
2. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
3. En el panel de navegación, elija Health Checks.
4. Si desea actualizar una comprobación de estado existente, seleccione el ID vinculado de la comprobación de estados y, a continuación, elija Editar.

Si desea crear una comprobación de estado, elija Crear comprobación de estado.

5. Ingrese los valores aplicables. Tenga en cuenta que algunos valores no se pueden cambiar después de crear una comprobación de estado. Para obtener más información, consulte [Valores que especifica al crear o actualizar comprobaciones de estado](#).
6. Elija Crear comprobación de estado.

 Note

Route 53 considera que una nueva comprobación de estado es correcta hasta que haya suficientes datos para determinar el estado real, correcto o no.

7. Asocie la comprobación de estado con uno o varios registros de Route 53. Para obtener información sobre cómo crear y actualizar registros, consulte [Uso de registros](#).

Old console

Cómo crear o actualizar una comprobación de estado

1. Si desea actualizar las comprobaciones de estado que ya están asociadas con registros, realice las tareas recomendadas de [Actualizar o eliminar comprobaciones de estado cuando está configurada la recuperación ante errores a nivel de DNS](#).
2. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
3. En el panel de navegación, elija Health Checks.
4. Si desea actualizar una comprobación de estado existente, selecciónela y, a continuación, elija Edit Health Check.

Si desea crear una comprobación de estado, elija Create Health Check. Si necesita más información sobre cada opción de configuración, mueva el puntero del ratón sobre una etiqueta para que aparezca la información sobre herramientas.

5. Ingrese los valores aplicables. Tenga en cuenta que algunos valores no se pueden cambiar después de crear una comprobación de estado. Para obtener más información, consulte [Valores que especifica al crear o actualizar comprobaciones de estado](#).
6. Elija Create Health Check.

 Note

Route 53 considera que una nueva comprobación de estado es correcta hasta que haya suficientes datos para determinar el estado real, correcto o no. Si ha elegido la opción de invertir el estado de comprobación de estado, Route 53 considera que una nueva comprobación de estado no es correcta hasta que haya suficientes datos.

7. Asocie la comprobación de estado con uno o varios registros de Route 53. Para obtener información sobre cómo crear y actualizar registros, consulte [Uso de registros](#).

Valores que especifica al crear o actualizar comprobaciones de estado

Al crear o actualizar comprobaciones de estado, especifica los valores aplicables. Tenga en cuenta que no puede cambiar algunos valores después de crear una comprobación de estado.

Temas

- [Monitorización de un punto de conexión](#)
- [Monitorizar otras comprobaciones de estado \(comprobaciones de estado calculadas\)](#)
- [Monitoreo de una alarma CloudWatch](#)
- [Configuración avanzada \(solo "Monitor an endpoint" \(Monitorización de un punto de conexión\)\)](#)
- [Recibir notificaciones cuando se produzca un error en una comprobación de estado](#)

Nombre

Opcional, pero recomendado: el nombre que desea asignar a la comprobación de estado.

Si especifica un valor en el campo Name (Nombre), Route 53 agrega una etiqueta a la comprobación de estado, asigna el valor Name (Nombre) a la clave de etiqueta y el valor que especifique al valor de etiqueta. El valor de la etiqueta Name (Nombre) aparece en la lista de comprobaciones de estado en la consola de Route 53, lo que le permite distinguir fácilmente las comprobaciones de estado entre ellas.

Para obtener más información sobre el etiquetado y las comprobaciones de estado, consulte [Denominar y etiquetar comprobaciones de estado](#).

Qué se debe monitorizar

Si desea que esta comprobación de estado monitorice un punto de conexión o el estado de otras comprobaciones de estado:

- Punto de conexión: Route 53 monitorea el estado de un punto de conexión que se especifique. Puede especificar el punto de conexión proporcionando un nombre de dominio o una dirección IP y un puerto.

Note

Si especifica un punto de conexión que no es de AWS, se aplica un cargo adicional. Para obtener más información, como una definición de los puntos de enlace de AWS, consulte “Comprobaciones de estado” en la página de [Precios de Route 53](#).

- Status of other health checks (calculated health check) (Estado de las demás comprobaciones de estado (comprobación de estado calculada)): Route 53 determina si esta comprobación de estado es correcta basándose en el estado de otras comprobaciones de estado que especifique. También puede especificar cuántas comprobaciones de estado necesitan ser correctas para que esta comprobación de estado se considere correcta.
- State of CloudWatch alarm data stream (Flujo de datos del estado de la alarma de CloudWatch): Route 53 determina si esta comprobación de estado es correcta al monitorear el flujo de datos de una alarma de CloudWatch.

Monitorización de un punto de conexión

Note

Estamos en proceso de actualización de la consola de comprobaciones de estado para Route 53. Durante el periodo de transición, puede seguir utilizando la consola anterior.

Seleccione la pestaña de la consola que esté utilizando.

- [New console](#)
- [Consola antigua](#)

New console

Si desea que esta comprobación de estado monitorice un punto de conexión, especifique los siguientes valores:

- Especificación de los puntos de conexión
- Dirección IP
- Nombre del dominio

Specify endpoint by

Si desea especificar el punto de conexión mediante una dirección IP o un nombre de dominio.

Después de crear una comprobación de estado, no puede cambiar el valor de Specify endpoint by.

IP address (solo "Specify endpoint by IP address")

Elija el protocolo en el menú desplegable e introduzca la dirección IP, el puerto y la ruta en el cuadro de texto.

- El protocolo puede ser uno de los siguientes:

HTTP: Route 53 intenta establecer una conexión TCP. Si se realiza correctamente, Route 53 envía una solicitud HTTP y espera el código de estado HTTP de 2xx o 3xx.

- HTTPS: Route 53 intenta establecer una conexión TCP. Si se realiza correctamente, Route 53 envía una solicitud HTTP y espera el código de estado HTTP de 2xx o 3xx.

Important

Si elige HTTPS, el punto de conexión debe admitir TLS v1.0, v1.1 o v1.2.

Si elige HTTPS para el valor de Protocol, se aplica un cargo adicional. Para obtener más información, consulte [Precios de Route 53](#).

- TCP: Route 53 intenta establecer una conexión TCP.

Para obtener más información, consulte [Cómo determina Amazon Route 53 si la comprobación de estado es correcta](#).

Después de crear una comprobación de estado, no puede cambiar el valor de Protocol.

Para la Dirección IP, puede ingresar una dirección IPv4 o IPv6 del punto de conexión en el que desea que Route 53 realice comprobaciones de estado si elige Especificar punto de conexión por dirección IP.

Route 53 no puede comprobar el estado de los puntos de enlace en los que la dirección IP está en rangos locales, privados, no direccionables o de multidifusión. Para obtener más información sobre las direcciones IP para las que no puede crear comprobaciones de estado, consulte los siguientes documentos:

- [RFC 5735, Special Use IPv4 Addresses \(RFC 5735, direcciones IPv4 de uso especial\)](#)
- [RFC 6598, IANA-Reserved IPv4 Prefix for Shared Address Space \(RFC 6598, prefijo IPv4 reservado por IANA para el espacio de direcciones compartidas\)](#).
- [RFC 5156, Special-Use IPv6 Addresses \(RFC 5156, direcciones IPv6 de uso especial\)](#)

Si el punto de conexión es una instancia de Amazon EC2, le recomendamos que cree una dirección IP elástica, la asocie a la instancia de EC2 y especifique la dirección IP elástica. De este modo se garantiza que nunca cambiará la dirección IP de la instancia. Para obtener más información, consulte [Dirección IP elástica \(EIP\)](#) en la Guía del usuario de Amazon EC2.

Si elimina la instancia de Amazon EC2, asegúrese de eliminar también la comprobación de estado asociada a la EIP. Para obtener más información, consulte [Prácticas recomendadas de las comprobaciones de estado de Amazon Route 53](#).

 Note

Si especifica un punto de conexión que no es de AWS, se aplica un cargo adicional. Para obtener más información, como una definición de los puntos de enlace de AWS, consulte “Comprobaciones de estado” en la página de [Precios de Route 53](#).

Para el puerto, ingrese el puerto en el punto de conexión en el que desea que Route 53 realice comprobaciones de estado.

Para la ruta (solo para los protocolos HTTP y HTTPS), introduzca la ruta que desea que Route 53 solicite cuando realiza comprobaciones de estado. La ruta puede ser cualquier valor para el que el punto de conexión devuelva un código de estado de HTTP de 2xx o 3xx cuando el punto de conexión se encuentre en buen estado, como el archivo /docs/route53-

health-check.html. También puede incluir parámetros de cadena de consulta, por ejemplo, /welcome.html?language=jp&login=y. Si no incluye una barra inclinada inicial (/), Route 53 agrega una en forma automática.

Domain name (solo "Specify endpoint by domain name", todos los protocolos)

El nombre de dominio (example.com) o de subdominio (backend.example.com) del punto de conexión en el que desea que Route 53 realice comprobaciones de estado, si elige Especificar punto de conexión por nombre de dominio.

Si decide especificar el punto de conexión por nombre de dominio, Route 53 envía una consulta de DNS para resolver el nombre de dominio que especifique en Nombre de dominio al intervalo que especifique en Intervalo de solicitud. Mediante una dirección IP que devuelve DNS, Route 53 comprueba el estado del punto de conexión.

 Note

Si especifica el punto de conexión por nombre de dominio, Route 53 solo utiliza IPv4 para enviar las comprobaciones de estado al punto de conexión. Si no hay ningún registro con un tipo A para el nombre que especifique en Domain name, en la comprobación de estado se produce el error de que no se ha podido realizar la resolución de DNS.

Si desea comprobar el estado de los registros de conmutación por error, geolocalización, geoproximidad, latencia, multivalor o ponderados y decide especificar el punto de conexión por nombre de dominio, le recomendamos que cree una comprobación de estado para cada punto de conexión. Por ejemplo, cree una comprobación de estado para cada servidor HTTP que sirva contenido de www.ejemplo.com. Para el valor de Domain name (Nombre de dominio), especifique el nombre de dominio del servidor (por ejemplo, us-east-2-www.example.com), no el nombre de los registros (www.example.com).

 Important

En esta configuración, si crea una comprobación de estado cuyo valor de Domain name coincide con el nombre de los registros y luego la asocia con estos, los resultados de la comprobación serán impredecibles.

Además, si el valor del Protocolo es HTTP o HTTPS, Route 53 pasa el valor de Nombre de dominio en el encabezado Host, tal como se describe en Nombre de host, anteriormente en esta lista. Si el valor de Protocolo (Protocolo) es TCP, Route 53 no pasa un encabezado Host.

 Note

Si especifica un punto de conexión que no es de AWS, se aplica un cargo adicional. Para obtener más información, como una definición de los puntos de enlace de AWS, consulte “Comprobaciones de estado” en la página de [Precios de Route 53](#).

Old console

Si desea que esta comprobación de estado monitorice un punto de conexión, especifique los siguientes valores:

- Specify endpoint by
- Protocolo
- Dirección IP
- Nombre de host
- Puerto
- Nombre del dominio
- Ruta

Specify endpoint by

Si desea especificar el punto de conexión mediante una dirección IP o un nombre de dominio.

Después de crear una comprobación de estado, no puede cambiar el valor de Specify endpoint by.

Protocolo

El método que desea que Route 53 use para comprobar el estado de su punto de conexión:

- HTTP: Route 53 intenta establecer una conexión TCP. Si se realiza correctamente, Route 53 envía una solicitud HTTP y espera el código de estado HTTP de 2xx o 3xx.
- HTTPS: Route 53 intenta establecer una conexión TCP. Si se realiza correctamente, Route 53 envía una solicitud HTTP y espera el código de estado HTTP de 2xx o 3xx.

 Important

Si elige HTTPS, el punto de conexión debe admitir TLS v1.0, v1.1 o v1.2.

Si elige HTTPS para el valor de Protocol, se aplica un cargo adicional. Para obtener más información, consulte [Precios de Route 53](#).

- TCP: Route 53 intenta establecer una conexión TCP.

Para obtener más información, consulte [Cómo determina Amazon Route 53 si la comprobación de estado es correcta](#).

Después de crear una comprobación de estado, no puede cambiar el valor de Protocol.

IP address (solo "Specify endpoint by IP address")

La dirección IPv4 o IPv6 del punto de conexión en el que desea que Route 53 realice comprobaciones de estado si elige Especificar punto de conexión por dirección IP.

Route 53 no puede comprobar el estado de los puntos de enlace en los que la dirección IP está en rangos locales, privados, no direccionables o de multidifusión. Para obtener más información sobre las direcciones IP para las que no puede crear comprobaciones de estado, consulte los siguientes documentos:

- [RFC 5735, Special Use IPv4 Addresses \(RFC 5735, direcciones IPv4 de uso especial\)](#)
- [RFC 6598, IANA-Reserved IPv4 Prefix for Shared Address Space \(RFC 6598, prefijo IPv4 reservado por IANA para el espacio de direcciones compartidas\)](#).
- [RFC 5156, Special-Use IPv6 Addresses \(RFC 5156, direcciones IPv6 de uso especial\)](#)

Si el punto de conexión es una instancia de Amazon EC2, le recomendamos que cree una dirección IP elástica, la asocie a la instancia de EC2 y especifique la dirección IP elástica. De este modo se garantiza que nunca cambiará la dirección IP de la instancia. Para obtener más información, consulte [Dirección IP elástica \(EIP\)](#) en la Guía del usuario de Amazon EC2.

Si elimina la instancia de Amazon EC2, asegúrese de eliminar también la comprobación de estado asociada a la EIP. Para obtener más información, consulte [Prácticas recomendadas de las comprobaciones de estado de Amazon Route 53](#).

 Note

Si especifica un punto de conexión que no es de AWS, se aplica un cargo adicional. Para obtener más información, como una definición de los puntos de enlace de AWS, consulte “Comprobaciones de estado” en la página de [Precios de Route 53](#).

Host name (solo "Specify endpoint by IP address", protocolos HTTP y HTTPS únicamente)

El valor que desea que Route 53 pase en el encabezado de Host en las comprobaciones de estado HTTP y HTTPS. Normalmente es el nombre de DNS completo del sitio web en el que desea que Route 53 realice las comprobaciones de estado. A continuación indicamos cómo se crea el encabezado Host cuando Route 53 comprueba el estado de un punto de conexión:

- Si especifica un valor de **80** para Port (Puerto) y HTTP para Protocol (Protocolo), Route 53 pasa al punto de enlace un encabezado Host que contiene el valor de Host name (Nombre de host).
- Si especifica un valor de **443** para Port (Puerto) y HTTPS para Protocol (Protocolo), Route 53 pasa al punto de enlace un encabezado Host que contiene el valor de Host name (Nombre de host).
- Si especifica otro valor para Port y HTTP o HTTPS para Protocol (Protocolo), Route 53; pasa al punto de enlace un encabezado Host que contiene el valor *Host name:Port* (Nombre de host: Puerto).

Si decide especificar el punto de conexión por dirección IP y no especifica un valor en el campo Host name (Nombre de host), Route 53 sustituye el valor de IP address (Dirección IP) en el encabezado Host en todos los casos anteriores.

Puerto

El puerto en el punto de conexión en el que desea que Route 53 realice comprobaciones de estado.

Domain name (solo "Specify endpoint by domain name", todos los protocolos)

El nombre de dominio (example.com) o de subdominio (backend.example.com) del punto de conexión en el que desea que Route 53 realice comprobaciones de estado, si elige Especificar punto de conexión por nombre de dominio.

Si decide especificar el punto de conexión por nombre de dominio, Route 53 envía una consulta de DNS para resolver el nombre de dominio que especifique en Nombre de dominio

al intervalo que especifique en Intervalo de solicitud. Mediante una dirección IP que devuelve DNS, Route 53 comprueba el estado del punto de conexión.

 Note

Si especifica el punto de conexión por nombre de dominio, Route 53 solo utiliza IPv4 para enviar las comprobaciones de estado al punto de conexión. Si no hay ningún registro con un tipo A para el nombre que especifique en Domain name, en la comprobación de estado se produce el error de que no se ha podido realizar la resolución de DNS.

Si desea comprobar el estado de los registros de conmutación por error, geolocalización, geoproximidad, latencia, multivalor o ponderados y decide especificar el punto de conexión por nombre de dominio, le recomendamos que cree una comprobación de estado para cada punto de conexión. Por ejemplo, cree una comprobación de estado para cada servidor HTTP que sirva contenido de `www.ejemplo.com`. Para el valor de Domain name (Nombre de dominio), especifique el nombre de dominio del servidor (por ejemplo, `us-east-2-www.example.com`), no el nombre de los registros (`www.example.com`).

 Important

En esta configuración, si crea una comprobación de estado cuyo valor de Domain name coincide con el nombre de los registros y luego la asocia con estos, los resultados de la comprobación serán impredecibles.

Además, si el valor del Protocolo es HTTP o HTTPS, Route 53 pasa el valor de Nombre de dominio en el encabezado Host, tal como se describe en Nombre de host, anteriormente en esta lista. Si el valor de Protocol (Protocolo) es TCP, Route 53 no pasa un encabezado Host.

 Note

Si especifica un punto de conexión que no es de AWS, se aplica un cargo adicional. Para obtener más información, como una definición de los puntos de enlace de AWS, consulte “Comprobaciones de estado” en la página de [Precios de Route 53](#).

Path (protocolos HTTP y HTTPS únicamente)

La ruta que desea que Route 53 solicite cuando realiza comprobaciones de estado. La ruta puede ser cualquier valor para el que su punto de conexión devolverá un código de estado de HTTP de 2xx o 3xx cuando el estado del punto de conexión sea correcto, como el archivo `/docs/route53-health-check.html`. También puede incluir parámetros de cadena de consulta, como `./welcome.html?language=jp&login=y`. Si no incluye una barra inclinada inicial (/), Route 53 agrega una automáticamente.

Monitorizar otras comprobaciones de estado (comprobaciones de estado calculadas)

Note

Estamos en proceso de actualización de la consola de comprobaciones de estado para Route 53. Durante el periodo de transición, puede seguir utilizando la consola anterior.

Seleccione la pestaña de la consola que esté utilizando.

- [New console](#)
- [Consola antigua](#)

New console

Si desea que esta comprobación de estado monitorice el estado de otras comprobaciones de estado, especifique los siguientes valores:

- Health checks to monitor
- Report healthy when

Health checks to monitor

Las comprobaciones de estado que desea que Route 53 monitoree para determinar el estado de esta comprobación de estado.

Puede añadir hasta 256 comprobaciones de estado a Health checks to monitor. Para eliminar una comprobación de estado de la lista, elija la x a la derecha del resalte de la comprobación de estado.

 Note

No puede configurar una comprobación de estado calculada para monitorizar el estado de otras comprobaciones de estado.

Si desactiva una comprobación de estado que está monitoreando una comprobación de estado calculada, Route 53 considera que la comprobación de estado desactivada es correcta ya que calcula si dicha comprobación calculada es correcta. Si desea que la comprobación de estado desactivada no se considere correcta, marque la casilla *Invert health check status* (Invertir estado de la comprobación de estado).

Report healthy when

El cálculo que desea que lleve a cabo Route 53 para determinar si esta comprobación de estado es correcta:

- Report healthy when at least x of y selected health checks are healthy (Notificar como correcto cuando como mínimo x de las y comprobaciones de estado seleccionadas sean correctas): Route 53 considera que esta comprobación de estado es correcta cuando el número especificado de comprobaciones de estado que ha agregado a Health checks to monitor (Comprobaciones de estado que deben monitorearse) es correcto. Tenga en cuenta lo siguiente:
 - Si especifica un número superior al número de comprobaciones de estado en Health checks to monitor (Comprobaciones de estado que deben monitorearse), Route 53 siempre considera que esta comprobación de estado es incorrecta.
 - Si especifica 0, Route 53 siempre considerará que esta comprobación de estado es correcta.
- Report healthy when all health checks are healthy (AND) (Notificar estado correcto cuando el estado de todas las comprobaciones de estado sea correcto (Y)): Route 53 considera que esta comprobación de estado es correcta solo cuando todas las comprobaciones de estado que ha agregado a Health checks to monitor (Comprobaciones de estado que deben monitorearse) son correctas.
- Report healthy when one or more health checks are healthy (OR) (Notificar estado correcto cuando el estado de una o varias comprobaciones de estado sea correcto (O)): Route 53 considera que esta comprobación de estado es correcta cuando al menos una de las comprobaciones de estado que ha agregado a Health checks to monitor (Comprobaciones de estado que deben monitorearse) es correcta.

Old console

Si desea que esta comprobación de estado monitorice el estado de otras comprobaciones de estado, especifique los siguientes valores:

- Health checks to monitor
- Report healthy when
- Invert health check status
- Deshabilitado

Health checks to monitor

Las comprobaciones de estado que desea que Route 53 monitoree para determinar el estado de esta comprobación de estado.

Puede añadir hasta 256 comprobaciones de estado a Health checks to monitor. Para eliminar una comprobación de estado de la lista, elija la x a la derecha del resalte de la comprobación de estado.

Note

No puede configurar una comprobación de estado calculada para monitorizar el estado de otras comprobaciones de estado.

Si desactiva una comprobación de estado que está monitoreando una comprobación de estado calculada, Route 53 considera que la comprobación de estado desactivada es correcta ya que calcula si dicha comprobación calculada es correcta. Si desea que la comprobación de estado desactivada no se considere correcta, marque la casilla Invert health check status (Invertir estado de la comprobación de estado).

Report healthy when

El cálculo que desea que lleve a cabo Route 53 para determinar si esta comprobación de estado es correcta:

- Report healthy when at least x of y selected health checks are healthy (Notificar como correcto cuando como mínimo x de las y comprobaciones de estado seleccionadas sean correctas): Route 53 considera que esta comprobación de estado es correcta cuando el número especificado de comprobaciones de estado que ha agregado a Health checks to

monitor (Comprobaciones de estado que deben monitorearse) es correcto. Tenga en cuenta lo siguiente:

- Si especifica un número superior al número de comprobaciones de estado en Health checks to monitor (Comprobaciones de estado que deben monitorearse), Route 53 siempre considera que esta comprobación de estado es incorrecta.
- Si especifica 0, Route 53 siempre considerará que esta comprobación de estado es correcta.
- Report healthy when all health checks are healthy (AND) (Notificar estado correcto cuando el estado de todas las comprobaciones de estado sea correcto (Y)): Route 53 considera que esta comprobación de estado es correcta solo cuando todas las comprobaciones de estado que ha agregado a Health checks to monitor (Comprobaciones de estado que deben monitorearse) son correctas.
- Report healthy when one or more health checks are healthy (OR) (Notificar estado correcto cuando el estado de una o varias comprobaciones de estado sea correcto (O)): Route 53 considera que esta comprobación de estado es correcta cuando al menos una de las comprobaciones de estado que ha agregado a Health checks to monitor (Comprobaciones de estado que deben monitorearse) es correcta.

Cómo invertir el estado de la comprobación de estado (solo en la consola antigua)

Para invertir una comprobación de estado en la nueva consola, consulte [Inversión de una comprobación de estado](#).

Elija si desea que Route 53 invierta el estado de una comprobación de estado. Si elige esta opción, Route 53 considera que las comprobaciones de estado son incorrectas cuando el estado es correcto y viceversa.

Desactivado (solo en la consola antigua)

Para deshabilitar una comprobación de estado en la nueva consola, consulte [Desactivación o activación de las comprobaciones de estado](#).

Impide que Route 53 realice comprobaciones de estado. Cuando se desactiva una comprobación de estado, Route 53 deja de agregar el estado de las comprobaciones de estado de referencia.

Después de desactivar una comprobación de estado, Route 53 considera que el estado de la comprobación siempre es correcto. Si ha configurado la conmutación por error a nivel de DNS, Route 53 continúa direccionando el tráfico a los recursos correspondientes. Si desea detener el enrutamiento de tráfico a un recurso, invierta la comprobación de estado.

 Note

Los cargos por una comprobación de estado se aplican cuando la comprobación está deshabilitada.

Monitoreo de una alarma CloudWatch

 Note

Estamos en proceso de actualización de la consola de comprobaciones de estado para Route 53. Durante el periodo de transición, puede seguir utilizando la consola anterior.

Seleccione la pestaña de la consola que esté utilizando.

- [New console](#)
- [Consola antigua](#)

New console

Si desea que esta comprobación de estado monitoree el estado de una alarma de CloudWatch, especifique los siguientes valores:

- CloudWatch alarm (Alarma de CloudWatch)
- Health check status (Estado de la comprobación de estado)

CloudWatch alarm (Alarma de CloudWatch)

Elija la alarma de CloudWatch que quiere que Route 53 utilice para determinar si esta comprobación de estado es correcta. La alarma de CloudWatch debe estar en la misma Cuenta de AWS que la comprobación de estado.

 Note

Route 53 es compatible con las alarmas de CloudWatch que tienen las siguientes características:

- Métricas de resolución estándar. Las métricas de alta resolución no se admiten. Para obtener más información, consulte [Métricas de alta resolución](#) en la Guía del usuario de Amazon CloudWatch.
 - Estadísticas: Average, Minimum, Maximum, Sum y SampleCount. Las estadísticas extendidas no se admiten.
 - Route 53 no admite alarmas “M de N”. Para obtener más información, consulte [Evaluación de una alarma](#) en la Guía del usuario de Amazon CloudWatch.
- Route 53 no admite alarmas que usan [cálculos de métricas](#) para consultar varias métricas de CloudWatch.

Si desea crear una alarma, siga estos pasos:

1. Seleccione Create (Crear). La consola de CloudWatch aparece en una nueva pestaña del navegador.
2. Ingrese los valores aplicables. Para obtener más información, consulte [Creación o edición de una alarma de CloudWatch](#) en la Guía del usuario de Amazon CloudWatch.
3. Regrese a la pestaña del navegador en la que aparece la consola de Route 53.
4. Elija el botón de actualización situado junto a la lista CloudWatch alarm.
5. Elija la nueva alarma en la lista.

 Important

Si cambia la configuración de la alarma de CloudWatch después de crear una comprobación de estado, debe actualizar la comprobación de estado. Para obtener más información, consulte [Actualizar comprobaciones de estado al cambiar la configuración de la alarma de CloudWatch \(comprobaciones de estado que monitorean solo una alarma de CloudWatch\)](#).

Health check status (Estado de la comprobación de estado)

Elija el estado de la comprobación de estado (correcto, incorrecto o último estado conocido) cuando CloudWatch no tenga suficientes datos para determinar el estado de la alarma que eligió para CloudWatch alarm (Alarma de CloudWatch). Si decide utilizar el último

estado conocido, Route 53 usa el estado de la comprobación de estado de la última vez que CloudWatch tuvo datos suficientes para determinar el estado de la alarma. En el caso de las nuevas comprobaciones de estado que no tienen un último estado conocido, el estado predeterminado para la comprobación de estado es correcto.

El valor de Health check status (Estado de la comprobación de estado) proporciona un estado temporal cuando el flujo de datos de una métrica de CloudWatch no está disponible brevemente. (Route 53 monitorea los flujos de datos para las métricas de CloudWatch, no el estado de la alarma correspondiente). Si la métrica no va a estar disponible con frecuencia o durante largos períodos de tiempo (más de unas cuantas horas), le recomendamos que no utilice el último estado conocido.

Old console

Si desea que esta comprobación de estado monitoree el estado de una alarma de CloudWatch, especifique los siguientes valores:

- CloudWatch alarm (Alarma de CloudWatch)
- Health check status (Estado de la comprobación de estado)
- Invert health check status
- Deshabilitado

CloudWatch alarm (Alarma de CloudWatch)

Elija la alarma de CloudWatch que quiere que Route 53 utilice para determinar si esta comprobación de estado es correcta. La alarma de CloudWatch debe estar en la misma Cuenta de AWS que la comprobación de estado.

Note

Route 53 es compatible con las alarmas de CloudWatch que tienen las siguientes características:

- Métricas de resolución estándar. Las métricas de alta resolución no se admiten. Para obtener más información, consulte [Métricas de alta resolución](#) en la Guía del usuario de Amazon CloudWatch.
- Estadísticas: Average, Minimum, Maximum, Sum y SampleCount. Las estadísticas extendidas no se admiten.

- Route 53 no admite alarmas “M de N”. Para obtener más información, consulte [Evaluación de una alarma](#) en la Guía del usuario de Amazon CloudWatch. Route 53 no admite alarmas que usan [cálculos de métricas](#) para consultar varias métricas de CloudWatch.

Si desea crear una alarma, siga estos pasos:

1. Seleccione Create (Crear). La consola de CloudWatch aparece en una nueva pestaña del navegador.
2. Ingrese los valores aplicables. Para obtener más información, consulte [Creación o edición de una alarma de CloudWatch](#) en la Guía del usuario de Amazon CloudWatch.
3. Regrese a la pestaña del navegador en la que aparece la consola de Route 53.
4. Elija el botón de actualización situado junto a la lista CloudWatch alarm.
5. Elija la nueva alarma en la lista.

 Important

Si cambia la configuración de la alarma de CloudWatch después de crear una comprobación de estado, debe actualizar la comprobación de estado. Para obtener más información, consulte [Actualizar comprobaciones de estado al cambiar la configuración de la alarma de CloudWatch \(comprobaciones de estado que monitorean solo una alarma de CloudWatch\)](#).

Health check status (Estado de la comprobación de estado)

Elija el estado de la comprobación de estado (correcto, incorrecto o último estado conocido) cuando CloudWatch no tenga suficientes datos para determinar el estado de la alarma que eligió para CloudWatch alarm (Alarma de CloudWatch). Si decide utilizar el último estado conocido, Route 53 usa el estado de la comprobación de estado de la última vez que CloudWatch tuvo datos suficientes para determinar el estado de la alarma. En el caso de las nuevas comprobaciones de estado que no tienen un último estado conocido, el estado predeterminado para la comprobación de estado es correcto.

El valor de Health check status (Estado de la comprobación de estado) proporciona un estado temporal cuando el flujo de datos de una métrica de CloudWatch no está disponible

brevemente. (Route 53 monitorea los flujos de datos para las métricas de CloudWatch, no el estado de la alarma correspondiente). Si la métrica no va a estar disponible con frecuencia o durante largos períodos de tiempo (más de unas cuantas horas), le recomendamos que no utilice el último estado conocido.

Cómo invertir el estado de la comprobación de estado (solo en la consola antigua)

Para invertir una comprobación de estado en la nueva consola, consulte [Inversión de una comprobación de estado](#).

Elija si desea que Route 53 invierta el estado de una comprobación de estado. Si elige esta opción, Route 53 considera que las comprobaciones de estado son incorrectas cuando el estado es correcto y viceversa.

Desactivado (solo en la consola antigua)

Para deshabilitar una comprobación de estado en la nueva consola, consulte [Desactivación o activación de las comprobaciones de estado](#).

Impide que Route 53 realice comprobaciones de estado. Cuando se desactiva una comprobación de estado, Route 53 detiene el monitoreo de las métricas de CloudWatch correspondientes.

Después de desactivar una comprobación de estado, Route 53 considera que el estado de la comprobación siempre es correcto. Si ha configurado la conmutación por error a nivel de DNS, Route 53 continúa direccionando el tráfico a los recursos correspondientes. Si quiere detener el enrutamiento de tráfico a un recurso, invierta la comprobación de estado.

 Note

Los cargos por una comprobación de estado se aplican cuando la comprobación está deshabilitada.

Configuración avanzada (solo "Monitor an endpoint" (Monitorización de un punto de conexión))

Note

Estamos en proceso de actualización de la consola de comprobaciones de estado para Route 53. Durante el periodo de transición, puede seguir utilizando la consola anterior.

- [New console](#)
- [Consola antigua](#)

New console

- Intervalo de solicitud
- Failure threshold
- Coincidencia de cadenas
- Búsqueda de cadenas
- Latency graphs
- Habilitación de SNI
- Nombre de host

Intervalo de solicitud

El número de segundos entre el momento en que cada comprobador de estado de Route 53 obtiene una respuesta de su punto de conexión y el momento en que se envía la siguiente solicitud de comprobación de estado. Si elige un intervalo de 30 segundos, cada uno de los comprobadores de estado de Route 53 de los centros de datos de todo el mundo enviará a su punto de conexión una solicitud de comprobación de estado cada 30 segundos. De media, su punto de conexión recibirá una solicitud de comprobación de estado sobre cada dos segundos. Si elige un intervalo de 10 segundos, el punto de conexión recibirá más de una solicitud por segundo.

Tenga en cuenta que los comprobadores de estado de Route 53 en distintos centros de datos no se coordinan entre sí, por lo que a veces aparecerán varias solicitudes por segundo

independientemente del intervalo elegido, seguidas de unos segundos sin comprobaciones de estado.

Después de crear una comprobación de estado, no puede cambiar el valor de Request interval.

 Note

Si elige Fast (10 seconds) para el valor de Request interval, se aplica un cargo adicional. Para obtener más información, consulte [Precios de Route 53](#).

Failure threshold

El número de comprobaciones de estado consecutivas que un punto de conexión debe superar o fallar para que Route 53 cambie el estado actual del punto de conexión de incorrecto a correcto y viceversa. Para obtener más información, consulte [Cómo determina Amazon Route 53 si la comprobación de estado es correcta](#).

String matching (solo HTTP y HTTPS)

Si desea que Route 53 determine el estado de un punto de conexión mediante el envío de una solicitud HTTP o HTTPS al punto de conexión y la búsqueda de una cadena especificada en el cuerpo de la respuesta. Si el cuerpo de la respuesta contiene el valor que ha especificado en Search string (Cadena de búsqueda), Route 53 considera que el estado del punto de conexión es correcto. En caso contrario, o si el punto de conexión no responde, Route 53 considera el estado del punto de conexión es incorrecto. La cadena de búsqueda debe aparecer en su totalidad en los primeros 5 120 bytes del cuerpo de la respuesta.

Después de crear una comprobación de estado, no puede cambiar el valor de String matching.

 Note

Si elige Yes para el valor de String matching, se aplica un cargo adicional. Para obtener más información, consulte [Precios de Route 53](#).

Cómo manejan los comprobadores de estado una respuesta comprimida

Si el punto de conexión es un servidor web que devuelve una respuesta comprimida, el comprobador de estado de Route 53 descomprimirá la respuesta antes de comprobar la

cadena de búsqueda especificada solo si el servidor web comprimió la respuesta utilizando un algoritmo de compresión compatible con los comprobadores de estado. Los comprobadores de estado admiten los siguientes algoritmos de compresión:

- Gzip
- Deflate

Si la respuesta se comprime utilizando otro algoritmo, el comprobador de estado no puede descomprimir la respuesta antes de buscar la cadena. En este caso, la búsqueda casi siempre fallará y Route 53 considerará que el punto de conexión no es correcto.

Search string (solo cuando se ha habilitado "String matching")

La cadena que desea que busque Route 53 en el cuerpo de la respuesta de su punto de conexión. La longitud máxima es de 255 caracteres.

Route 53 tiene en cuenta las mayúsculas y minúsculas cuando busca Search string (Cadena de búsqueda) en el cuerpo de la respuesta.

Latency graphs

Elija si desea que Route 53 mida la latencia entre comprobadores de estado en múltiples regiones de AWS y su punto de conexión. Si elige esta opción, aparecen gráficos de latencia de CloudWatch en la pestaña Latency (Latencia) de la página Health checks (Comprobaciones de estado) de la consola de Route 53. Si los comprobadores de estado de Route 53 no pueden conectarse al punto de conexión, Route 53 no puede mostrar gráficos de latencia para dicho punto de conexión.

Después de crear una comprobación de estado, no puede cambiar el valor de Latency measurements.

 Note

Si configura Route 53 para medir la latencia entre los comprobadores de estado y el punto de conexión, se aplica un cargo adicional. Para obtener más información, consulte [Precios de Route 53](#).

Enable SNI (solo HTTPS)

Especifique si quiere que Route 53 envíe el nombre de host al punto de conexión en el mensaje `client_hello` durante la negociación de TLS. Esto permite que el punto de conexión responda a la solicitud HTTPS con el certificado de SSL/TLS aplicable.

Algunos puntos de conexión requieren que las solicitudes de HTTPS incluyan el nombre de host en el mensaje `client_hello`. Si no habilita la SNI, es posible que el estado de la comprobación de estado muestre un error. El mensaje de error dependerá de cómo esté configurado el servidor para responder a la solicitud que no contiene información sobre la SNI. Una comprobación de estado también puede registrar un estado por otras razones. Si SNI está habilitado y siendo recibido el error, consulte la configuración de SSL/TLS en su punto de conexión y confirme que el certificado es válido.

Tenga en cuenta los siguientes requisitos:

- El punto de conexión debe admitir SNI.
- El certificado de SSL/TLS en el punto de conexión incluye un nombre de dominio en el campo `Common Name` y posiblemente varios más en el campo `Subject Alternative Names`. Uno de los nombres de dominio del certificado debe coincidir con el valor que especifique en `Host name`.

Health checker regions

Elija si desea que Route 53 compruebe el estado del punto de conexión mediante comprobadores de estado en las regiones recomendadas o mediante comprobadores de estado en las regiones que especifique.

Si actualiza una comprobación de estado para eliminar una región que ha estado realizando comprobaciones de estado, Route 53 sigue llevando a cabo las comprobaciones desde dicha región durante un máximo de una hora. De este modo, se garantiza que algunos comprobadores de estado comprueben siempre el punto de conexión (por ejemplo, si reemplaza tres regiones por otras cuatro distintas).

Si elige `Customize (Personalizar)`, elija la `x` de una región para eliminarla. Haga clic en el espacio de la parte inferior de la lista para devolver una región a la lista. Debe especificar al menos tres regiones.

Host name (solo "Specify endpoint by IP address", protocolos HTTP y HTTPS únicamente)

El valor que desea que Route 53 pase en el encabezado de `Host` en las comprobaciones de estado HTTP y HTTPS. Normalmente es el nombre de DNS completo del sitio web en el que

desea que Route 53 realice las comprobaciones de estado. A continuación indicamos cómo se crea el encabezado Host cuando Route 53 comprueba el estado de un punto de conexión:

- Si especifica un valor de **80** para Port (Puerto) y HTTP para Protocol (Protocolo), Route 53 pasa al punto de conexión un encabezado Host que contiene el valor de Host name (Nombre de host).
- Si especifica un valor de **443** para Puerto y HTdTPS para Protocolo, Route 53 pasa al punto de conexión un encabezado Host que contiene el valor de Nombre de host.
- Si especifica otro valor para Port y HTTP o HTTPS para Protocol (Protocolo), Route 53; pasa al punto de conexión un encabezado Host que contiene el valor *Host name:Port* (Nombre de host: Puerto).

Si decide especificar el punto de conexión por dirección IP y no especifica un valor en el campo Host name (Nombre de host), Route 53 sustituye el valor de IP address (Dirección IP) en el encabezado Host en todos los casos anteriores.

Old console

Si elige la opción para monitorizar un punto de conexión, también puede especificar las siguientes opciones:

- Intervalo de solicitud
- Failure threshold
- Coincidencia de cadenas
- Búsqueda de cadena
- Gráfica de latencia
- Habilitación de SNI
- Regiones de comprobadores de estado
- Invert health check status
- Deshabilitado

Intervalo de solicitud

El número de segundos entre el momento en que cada comprobador de estado de Route 53 obtiene una respuesta de su punto de conexión y el momento en que se envía la siguiente

solicitud de comprobación de estado. Si elige un intervalo de 30 segundos, cada uno de los comprobadores de estado de Route 53 de los centros de datos de todo el mundo enviará a su punto de conexión una solicitud de comprobación de estado cada 30 segundos. De media, su punto de conexión recibirá una solicitud de comprobación de estado sobre cada dos segundos. Si elige un intervalo de 10 segundos, el punto de conexión recibirá más de una solicitud por segundo.

Tenga en cuenta que los comprobadores de estado de Route 53 en distintos centros de datos no se coordinan entre sí, por lo que a veces aparecerán varias solicitudes por segundo independientemente del intervalo elegido, seguidas de unos segundos sin comprobaciones de estado.

Después de crear una comprobación de estado, no puede cambiar el valor de Request interval.

 Note

Si elige Fast (10 seconds) para el valor de Request interval, se aplica un cargo adicional. Para obtener más información, consulte [Precios de Route 53](#).

Failure threshold

El número de comprobaciones de estado consecutivas que un punto de conexión debe superar o fallar para que Route 53 cambie el estado actual del punto de conexión de incorrecto a correcto y viceversa. Para obtener más información, consulte [Cómo determina Amazon Route 53 si la comprobación de estado es correcta](#).

String matching (solo HTTP y HTTPS)

Si desea que Route 53 determine el estado de un punto de conexión mediante el envío de una solicitud HTTP o HTTPS al punto de conexión y la búsqueda de una cadena especificada en el cuerpo de la respuesta. Si el cuerpo de la respuesta contiene el valor que ha especificado en Search string (Cadena de búsqueda), Route 53 considera que el estado del punto de conexión es correcto. En caso contrario, o si el punto de conexión no responde, Route 53 considera el estado del punto de conexión es incorrecto. La cadena de búsqueda debe aparecer en su totalidad en los primeros 5 120 bytes del cuerpo de la respuesta.

Después de crear una comprobación de estado, no puede cambiar el valor de String matching.

 Note

Si elige Yes para el valor de String matching, se aplica un cargo adicional. Para obtener más información, consulte [Precios de Route 53](#).

Cómo manejan los comprobadores de estado una respuesta comprimida

Si el punto de conexión es un servidor web que devuelve una respuesta comprimida, el comprobador de estado de Route 53 descomprimirá la respuesta antes de comprobar la cadena de búsqueda especificada solo si el servidor web comprimió la respuesta utilizando un algoritmo de compresión compatible con los comprobadores de estado. Los comprobadores de estado admiten los siguientes algoritmos de compresión:

- Gzip
- Deflate

Si la respuesta se comprime utilizando otro algoritmo, el comprobador de estado no puede descomprimir la respuesta antes de buscar la cadena. En este caso, la búsqueda casi siempre fallará y Route 53 considerará que el punto de conexión no es correcto.

Search string (solo cuando se ha habilitado "String matching")

La cadena que desea que busque Route 53 en el cuerpo de la respuesta de su punto de conexión. La longitud máxima es de 255 caracteres.

Route 53 tiene en cuenta las mayúsculas y minúsculas cuando busca Search string (Cadena de búsqueda) en el cuerpo de la respuesta.

Latency graphs

Elija si desea que Route 53 mida la latencia entre comprobadores de estado en múltiples regiones de AWS y su punto de conexión. Si elige esta opción, aparecen gráficos de latencia de CloudWatch en la pestaña Latency (Latencia) de la página Health checks (Comprobaciones de estado) de la consola de Route 53. Si los comprobadores de estado de Route 53 no pueden conectarse al punto de conexión, Route 53 no puede mostrar gráficos de latencia para dicho punto de conexión.

Después de crear una comprobación de estado, no puede cambiar el valor de Latency measurements.

 Note

Si configura Route 53 para medir la latencia entre los comprobadores de estado y el punto de conexión, se aplica un cargo adicional. Para obtener más información, consulte [Precios de Route 53](#).

Enable SNI (solo HTTPS)

Especifique si quiere que Route 53 envíe el nombre de host al punto de conexión en el mensaje `client_hello` durante la negociación de TLS. Esto permite que el punto de conexión responda a la solicitud HTTPS con el certificado de SSL/TLS aplicable.

Algunos puntos de conexión requieren que las solicitudes de HTTPS incluyan el nombre de host en el mensaje `client_hello`. Si no habilita la SNI, es posible que el estado de la comprobación de estado muestre un error. El mensaje de error depende de cómo esté configurado el servidor para responder a la solicitud que no contiene información sobre la SNI. Una comprobación de estado también puede registrar un estado por otras razones. Si SNI está habilitado y siendo recibido el error, consulte la configuración de SSL/TLS en su punto de conexión y confirme que el certificado es válido.

Tenga en cuenta los siguientes requisitos:

- El punto de conexión debe admitir SNI.
- El certificado de SSL/TLS en el punto de conexión incluye un nombre de dominio en el campo `Common Name` y posiblemente varios más en el campo `Subject Alternative Names`. Uno de los nombres de dominio del certificado debe coincidir con el valor que especifique en `Host name`.

Health checker regions

Elija si desea que Route 53 compruebe el estado del punto de conexión mediante comprobadores de estado en las regiones recomendadas o mediante comprobadores de estado en las regiones que especifique.

Si actualiza una comprobación de estado para eliminar una región que ha estado realizando comprobaciones de estado, Route 53 sigue llevando a cabo las comprobaciones desde dicha región durante un máximo de una hora. De este modo, se garantiza que algunos comprobadores de estado comprueben siempre el punto de conexión (por ejemplo, si reemplaza tres regiones por otras cuatro distintas).

Si elige Customize (Personalizar), elija la x de una región para eliminarla. Haga clic en el espacio de la parte inferior de la lista para devolver una región a la lista. Debe especificar al menos tres regiones.

Cómo invertir el estado de la comprobación de estado (solo en la consola antigua)

Para invertir una comprobación de estado en la nueva consola, consulte [Inversión de una comprobación de estado](#).

Elija si desea que Route 53 invierta el estado de una comprobación de estado. Si elige esta opción, Route 53 considera que una comprobación de estado es incorrecta cuando el estado es correcto y viceversa. Por ejemplo, es posible que desee que Route 53 considere que el estado de una comprobación de estado es incorrecto si configura una coincidencia de cadenas y el punto de conexión devuelve un valor especificado.

Desactivado (solo en la consola antigua)

Para deshabilitar una comprobación de estado en la nueva consola, consulte [Desactivación o activación de las comprobaciones de estado](#).

Impide que Route 53 realice comprobaciones de estado. Cuando se desactiva una comprobación de estado, Route 53 deja de intentar establecer una conexión TCP con el punto de conexión.

Después de desactivar una comprobación de estado, Route 53 considera que el estado de la comprobación siempre es correcto. Si ha configurado la conmutación por error a nivel de DNS, Route 53 continúa direccionando el tráfico a los recursos correspondientes. Si desea detener el enrutamiento de tráfico a un recurso, invierta la comprobación de estado.

 Note

Los cargos por una comprobación de estado se aplican cuando la comprobación está deshabilitada.

Recibir notificaciones cuando se produzca un error en una comprobación de estado

Utilice las siguientes opciones para configurar la notificación por correo electrónico cuando se produzca un error en una comprobación de estado:

- [Create alarm](#)

- [Send notification to](#)
- [Topic name](#)
- [Recipient email addresses](#)

Create alarm (solo al crear comprobaciones de estado)

Especifique si desea crear una alarma de CloudWatch predeterminada. Si elige Sí, CloudWatch le envía una notificación de Amazon SNS cuando el estado de este punto de conexión cambia a incorrecto y Route 53 considera que el estado del punto de conexión es incorrecto durante un minuto.

 Note

Si quiere que CloudWatch le envíe otra notificación de Amazon SNS cuando el estado recupere un estado correcto, puede crear otra alarma después de crear la comprobación de estado. Para obtener más información, consulte [Creación de las alarmas de Amazon CloudWatch](#) en la Guía del usuario de Amazon CloudWatch.

Si desea crear una alarma para una comprobación de estado ya existente o desea recibir notificaciones cuando Route 53 considere que el estado del punto de conexión es incorrecto durante más o menos de un minuto (el valor predeterminado), seleccione No y agregue una alarma después de crear la comprobación de estado. Para obtener más información, consulte [Monitorear comprobaciones de estado mediante CloudWatch](#).

Send notification to (solo al crear una alarma)

Especifique si desea que CloudWatch envíe notificaciones a un tema de Amazon SNS ya existente o a otro nuevo:

- Existing SNS topic (Tema de SNS ya existente): seleccione el nombre del tema en la lista. El tema debe estar en la región EE. UU. Este (Norte de Virginia).
- New SNS topic (Tema de SNS nuevo): ingrese un nombre para el tema en Topic name (Nombre del tema) e ingrese las direcciones de correo electrónico a las que desee enviar notificaciones en Recipients (Destinatarios). Separe las direcciones con comas (,), punto y coma (;) o espacios.

Route 53 creará el tema en la región EE. UU. Este (Norte de Virginia).

Topic name (solo al crear un tema SNS)

Si ha especificado New SNS Topic, escriba el nombre del nuevo tema.

Recipient email addresses (solo al crear un tema SNS)

Si ha especificado New SNS topic, escriba las direcciones de email a las que desea enviar notificaciones. Separe los nombres con comas (,), punto y coma (;) o espacios.

Valores que muestra Amazon Route 53 al crear una comprobación de estado

La página Create Health Check (Crear comprobación de estado) muestra los siguientes valores en función de los valores que haya escrito:

URL

La URL completa (para las comprobaciones de estado de HTTP o HTTPS) o la dirección IP y el puerto (para comprobaciones de estado de TCP) a la que enviará Route 53 las solicitudes al realizar las comprobaciones de estado.

Tipo de comprobación de estado

Puede ser Basic o Basic + additional options según la configuración que haya especificado para esta comprobación de estado. Para obtener información sobre los precios de las opciones adicionales, consulte [Precios de Route 53](#).

Actualizar comprobaciones de estado al cambiar la configuración de la alarma de CloudWatch (comprobaciones de estado que monitorean solo una alarma de CloudWatch)

Si crea una comprobación de estado de Route 53 que monitorea el flujo de datos de una alarma de CloudWatch y después actualiza la configuración en la alarma de CloudWatch, Route 53 no actualiza automáticamente la configuración de la alarma en la comprobación de estado. Si desea que la comprobación de estado comience a usar la nueva configuración de alarma, debe actualizar la comprobación de estado.

 Note

Para actualizar una comprobación de estado mediante programación, puede utilizar la API `UpdateHealthCheck`. Solo tiene que especificar los valores actuales de `AlarmIdentifier` y `Region`, y Route 53 obtendrá la última configuración de CloudWatch. Para obtener más información, consulte [UpdateHealthCheck](#) en la Referencia de la API de Amazon Route 53.

 Note

Estamos en proceso de actualización de la consola de comprobaciones de estado para Route 53. Durante el periodo de transición, puede seguir utilizando la consola anterior.

Seleccione la pestaña de la consola que esté utilizando.

- [New console](#)
- [Consola antigua](#)

New console

Cómo actualizar una comprobación de estado con la nueva configuración de la alarma de CloudWatch

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Comprobaciones de estado.
3. Seleccione el ID vinculado de la comprobación de estado que desea actualizar.
4. Seleccione Editar.

En una nota se explica que ha cambiado la alarma de CloudWatch correspondiente a la comprobación de estado. El campo Details muestra la nueva configuración de la alarma.

5. Seleccione Save.

Old console

Para actualizar una comprobación de estado con la nueva configuración de la alarma de CloudWatch (consola)

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Health Checks.
3. Seleccione la casilla de la comprobación de estado que desea actualizar.
4. Elija Edit health check.

En una nota se explica que ha cambiado la alarma de CloudWatch correspondiente a la comprobación de estado. El campo Details muestra la nueva configuración de la alarma.

5. Seleccione Save.

Desactivación o activación de las comprobaciones de estado

La desactivación de una comprobación de estado impide que Route 53 realice comprobaciones de estado. Cuando se desactiva una comprobación de estado, Route 53 deja de agregar el estado de las comprobaciones de estado de referencia. Después de desactivar una comprobación de estado, Route 53 considera que el estado de la comprobación siempre es correcto. Si ha configurado la conmutación por error a nivel de DNS, Route 53 continúa direccionando el tráfico a los recursos correspondientes. Si desea detener el enrutamiento del tráfico a un recurso, cambie el valor de Invertido.

Note

Estamos en proceso de actualización de la consola de comprobaciones de estado para Route 53. Durante el periodo de transición, puede seguir utilizando la consola anterior.

Puede activar o desactivar una comprobación de estado en la consola antigua al crear o editar la comprobación de estado. Para obtener más información, consulte [Valores que especifica al crear o actualizar comprobaciones de estado](#).

Para desactivar las comprobaciones de estado en la nueva consola, realice el siguiente procedimiento.

Cómo activar o desactivar una comprobación de estado (solo en la nueva consola)

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Comprobaciones de estado.
3. En la columna Acciones, seleccione los tres puntos y, a continuación, Desactivar o Activar.

O bien, seleccione el ID vinculado de la comprobación de estado que desee activar o desactivar.

4. En la tabla Configuración, el campo Estado especifica si la comprobación de estado está activada o desactivada.
5. Para activar o desactivar la comprobación de estado, elija Desactivar o Activar.

Inversión de una comprobación de estado

Si invierte una comprobación de estado, Route 53 considera que la comprobación de estado es incorrecta cuando el estado es correcto y viceversa.

Note

Estamos en proceso de actualización de la consola de comprobaciones de estado para Route 53. Durante el periodo de transición, puede seguir utilizando la consola anterior.

Puede invertir una comprobación de estado de la consola antigua si crea o edita la comprobación de estado. Para obtener más información, consulte [Valores que especifica al crear o actualizar comprobaciones de estado](#).

Para invertir las comprobaciones de estado en la nueva consola, realice el siguiente procedimiento.

Cómo invertir una comprobación de estado (solo en la consola nueva)

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Comprobaciones de estado.
3. En la columna Acciones, seleccione los tres puntos y, a continuación, Invertir.

O bien, seleccione el ID vinculado de la comprobación de estado que desea invertir.

4. En la tabla Configuración, el campo Invertido especifica si la comprobación de estado está invertida (Sí) o no (No).
5. Seleccione Invertir para invertir la comprobación de estado.

Si desea deshacer el estado invertido y el campo Invertido es Sí, vuelva a seleccionar Invertir.

Eliminar comprobaciones de estado

Para desactivar las comprobaciones de estado, realice el siguiente procedimiento.

Note

Si utiliza AWS Cloud Map y ha configurado AWS Cloud Map para crear una comprobación de estado de Route 53 al registrar una instancia, no puede utilizar la consola de Route 53 para eliminar la comprobación de estado. La comprobación de estado se elimina automáticamente al anular el registro de la instancia. Pueden transcurrir varias horas hasta que la comprobación de estado deje de aparecer en la consola de Route 53.

Note

Estamos en proceso de actualización de la consola de comprobaciones de estado para Route 53. Durante el periodo de transición, puede seguir utilizando la consola anterior.

Seleccione la pestaña de la consola que esté utilizando.

- [New console](#)
- [Consola antigua](#)

New console

Cómo eliminar una comprobación de estado

1. Si desea eliminar las comprobaciones de estado que están asociadas con registros, realice las tareas recomendadas de [Actualizar o eliminar comprobaciones de estado cuando está configurada la recuperación ante errores a nivel de DNS](#).

2. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
3. En el panel de navegación, elija Comprobaciones de estado.
4. Seleccione el ID vinculado de la comprobación de estado que quiere eliminar.
5. Elija Eliminar.
6. Escriba **confirm** en el cuadro de texto y, a continuación, elija Eliminar.

Old console

Para eliminar una comprobación de estado (consola)

1. Si desea eliminar las comprobaciones de estado que están asociadas con registros, realice las tareas recomendadas de [Actualizar o eliminar comprobaciones de estado cuando está configurada la recuperación ante errores a nivel de DNS](#).
2. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
3. En el panel de navegación, elija Health Checks.
4. En el panel de la derecha, seleccione la comprobación de estado que desea eliminar.
5. Elija Delete Health Check.
6. Elija Yes, Delete para confirmar.

Actualizar o eliminar comprobaciones de estado cuando está configurada la recuperación ante errores a nivel de DNS

Cuando desee actualizar o eliminar las comprobaciones de estado que están asociadas con registros o desee cambiar registros que tienen comprobaciones de estado asociadas, debe considerar cómo los cambios afectan al direccionamiento de las consultas de DNS y la configuración de recuperación ante errores a nivel de DNS.

Important

Route 53 no le impide eliminar una comprobación de estado aunque esté asociada con uno o varios registros. Si elimina una comprobación de estado sin actualizar los registros asociados, el estado futuro de la comprobación de estado no puede predecirse y podría

cambiar. Esto afectará al direccionamiento de las consultas de DNS para la configuración de recuperación ante errores a nivel de DNS.

Para actualizar o eliminar las comprobaciones de estado que ya están asociadas con registros, le recomendamos que realice las tareas siguientes:

1. Identificar los registros que están asociados con las comprobaciones de estado. Para identificar los registros que están asociados con una comprobación de estado, debe realizar una de estas acciones:
 - Revisar los registros de cada zona alojada utilizando la consola de Route 53. Para obtener más información, consulte [Descripción de registros](#).
 - Ejecutar la acción de la API `ListResourceRecordSets` en cada zona alojada y revisar la respuesta. Para obtener más información, consulte [ListResourceRecordSets](#) en la Referencia de la API de Amazon Route 53.
2. Evaluar el cambio de comportamiento que se derivará de la actualización o la eliminación de las comprobaciones de estado, o de la actualización de registros. En función de dicha evaluación, determinar qué cambios se deben realizar.

Para obtener más información, consulte . [¿Qué sucede cuando se omiten las comprobaciones de estado?](#)

3. Cambiar las comprobaciones de estado y los registros según corresponda. Para obtener más información, consulte los temas siguientes:
 - [Creación y actualización de comprobaciones de estado](#)
 - [Editar registros](#)
4. Eliminar las comprobaciones de estado que ya no utilice, si hubiera alguna. Para obtener más información, consulte [Eliminar comprobaciones de estado](#).

Configuración de las reglas de enrutador y de firewall para las comprobaciones de estado de Amazon Route 53

Cuando Route 53 comprueba el estado de un punto de conexión, envía una solicitud HTTP, HTTPS o TCP a la dirección IP y el puerto especificados al crear la comprobación de estado. Para una comprobación de estado se realice correctamente, las reglas del enrutador y del firewall deben

permitir el tráfico entrante desde las direcciones IP que usan los comprobadores de estado de Route 53.

Para ver la lista actual de direcciones IP de los comprobadores de estado de Route 53 para los servidores de nombres de Route 53 y para otros servicios de AWS, consulte [Rangos de direcciones IP de servidores de Amazon Route 53](#).

En Amazon EC2, los grupos de seguridad actúan de firewalls. Para obtener más información, consulte [Grupos de seguridad de Amazon EC2](#) en la Guía del usuario de Amazon EC2. Para configurar los grupos de seguridad y permitir las comprobaciones de estado de Route 53, puede permitir el tráfico de entrada desde cada rango de dirección IP o puede usar una lista de prefijos administrada por AWS.

Para usar la lista de prefijos administrada por AWS, modifique el grupo de seguridad para permitir el tráfico entrante desde `com.amazonaws.<region>.route53-healthchecks`, donde `<region>` es la Región de AWS de su instancia o recurso de Amazon EC2. Si utiliza las comprobaciones de estado de Route 53 para comprobar los puntos de conexión de IPv6, también debe permitir el tráfico entrante de `com.amazonaws.<region>.ipv6.route53-healthchecks` desde allí.

Para obtener más información sobre las listas de prefijos administradas por AWS, consulte [Trabajar con listas de prefijos administradas por AWS](#) en la Guía del usuario de Amazon VPC.

Important

Cuando agregue direcciones IP a una lista de direcciones IP permitidas, agregue todas las del intervalo CIDR de cada una de las regiones de AWS que especificó cuando creó las comprobaciones de estado, así como el intervalo CIDR global. Es posible que las solicitudes de comprobación de estado procedan de una única dirección IP en una región. Sin embargo, esta dirección IP puede cambiar en cualquier momento a otra de las direcciones IP de dicha región.

Si desea asegurarse de incluir las direcciones IP actuales y anteriores del comprobador de estado, agregue los rangos de direcciones IP ALL /26 y /18 a la lista de permitidos. Para obtener más información, consulte [Rangos de direcciones IP de AWS](#) en la Referencia general de AWS.

Cuando agrega la lista de prefijos administradas por AWS a su grupo de seguridad entrante, agregará automáticamente todos los rangos necesarios.

Configuración de la recuperación ante errores a nivel de DNS

Si tiene varios recursos que realizan la misma función, como, por ejemplo, más de un servidor HTTP o servidor de correo, puede configurar Amazon Route 53 para que compruebe el estado de los recursos y responda a las consultas de DNS solo mediante los recursos con un estado correcto. Por ejemplo, suponga que su sitio web `example.com`, se hospeda en seis servidores, dos en cada uno de los tres centros de datos de todo el mundo. Puede configurar Route 53 para comprobar el estado de los servidores y responder a las consultas de DNS de `example.com` empleando solo los servidores cuyo estado es correcto.

Route 53 puede comprobar el estado de los recursos en configuraciones simples y complejas:

- En configuraciones simples, cree un grupo de registros con el mismo nombre y tipo, por ejemplo, un grupo de registros ponderados con un tipo A para `example.com`. A continuación, configure Route 53 para comprobar el estado de los recursos correspondientes. Route 53 responde a las consultas de DNS en función del estado de los recursos. Para obtener más información, consulte [Cómo funcionan las comprobaciones de estado en configuraciones simples de Amazon Route 53](#).
- En configuraciones más complejas, cree un árbol de registros que dirija el tráfico en función de varios criterios. Por ejemplo, si la latencia para los usuarios es el criterio más importante, podría usar los registros de alias de latencia para dirigir el tráfico a la región que proporciona la mejor latencia. Los registros de alias de latencia podrían tener registros ponderados en cada región como el alias de destino. Los registros ponderados podrían dirigir el tráfico a instancias EC2 en función del tipo de instancia. Al igual que en una configuración simple, puede configurar Route 53 para dirigir el tráfico según el estado de los recursos. Para obtener más información, consulte [Cómo funcionan las comprobaciones de estado en configuraciones complejas de Amazon Route 53](#).

Temas

- [Lista de tareas para configurar la recuperación ante errores a nivel de DNS](#)
- [Cómo funcionan las comprobaciones de estado en configuraciones simples de Amazon Route 53](#)
- [Cómo funcionan las comprobaciones de estado en configuraciones complejas de Amazon Route 53](#)
- [Cómo elige Amazon Route 53 registros cuando está configurado la comprobación de estado](#)
- [Conmutación por error activa-activa y activa-pasiva](#)
- [Configuración de la conmutación por error en una zona alojada privada](#)

- [Cómo Amazon Route 53 evita los problemas de conmutación por error](#)

Lista de tareas para configurar la recuperación ante errores a nivel de DNS

Para utilizar Route 53 para configurar la conmutación por error a nivel de DNS, realice las siguientes tareas:

1. Dibuje un diagrama de árbol completo de la configuración e indique qué tipo de registro va a crear (alias ponderado, conmutación por error, latencia, etc.) para cada nodo. Al principio del árbol coloque los registros del nombre de dominio, como example.com, que los usuarios utilizarán para obtener acceso a su sitio o aplicación web.

Los tipos de registros que aparecen en el diagrama de árbol dependen de la complejidad de la configuración:

- En una configuración simple, el diagrama no incluirá ningún registro de alias o los registros de alias dirigirán el tráfico directamente a un recurso, como un balanceador de carga de ELB, en lugar de hacerlo a otro registro de Route 53. Para obtener más información, consulte [Cómo funcionan las comprobaciones de estado en configuraciones simples de Amazon Route 53](#).
- En una configuración compleja, el diagrama incluirá una combinación de registros de alias (tales como alias ponderado y alias de conmutación por error) y registros sin alias en un árbol de varios niveles, como los ejemplos del tema [Cómo funcionan las comprobaciones de estado en configuraciones complejas de Amazon Route 53](#).

Note

Para crear de forma rápida y sencilla los registros para las configuraciones de direccionamiento complejas y asociar los registros con las comprobaciones de estado, puede utilizar el editor visual de flujo de tráfico y guardar la configuración como una política de tráfico. A continuación, puede asociar la política de tráfico con uno o varios nombres de dominio (como example.com) o nombres de subdominio (como www.example.com) en la misma zona alojada o en varias zonas hospedadas. Además, puede revertir las actualizaciones si la nueva configuración no tiene el desempeño previsto. Para obtener más información, consulte [Uso de flujo de tráfico para dirigir el tráfico DNS](#).

Para obtener más información, consulte la documentación siguiente:

- [Elección de una política de enrutado](#)
- [Elección entre registros de alias y sin alias](#)

2. Cree las comprobaciones de estado de los recursos para los que no puede crear registros de alias; por ejemplo, servidores de Amazon EC2 y servidores de email que se ejecutan en su centro de datos. Asociará estas comprobaciones de estado con los registros sin alias.

Para obtener más información, consulte [Creación, actualización y eliminación de comprobaciones de estado](#).

3. Si es necesario, configure las reglas del enrutador y del firewall para que Route 53 pueda enviar solicitudes periódicas a los puntos de enlace que ha especificado en las comprobaciones de estado. Para obtener más información, consulte [Configuración de las reglas de enrutador y de firewall para las comprobaciones de estado de Amazon Route 53](#).
4. Cree todos los registros sin alias en el diagrama y asocie las comprobaciones de estado que ha creado en el paso 2 con los registros aplicables.

Si está configurando la recuperación ante errores a nivel de DNS en una configuración que no incluye registros de alias, omita las restantes tareas.

5. Cree los registros de alias que dirijan el tráfico a los recursos de AWS; por ejemplo, balanceadores de carga de ELB y distribuciones de CloudFront. Si desea que Route 53 pruebe otra rama del árbol cuando el estado de un recurso no sea correcto, configure el valor de Evaluate Target Health (Evaluar estado del destino) en Yes (Sí) para cada uno de sus registros de alias. (Evaluate Target Health (Evaluar estado del destino) no se admite en algunos recursos de AWS).
6. Comenzando en la parte inferior del diagrama de árbol que creó en el paso 1, cree los registros de alias que direccionan el tráfico a los registros que creó en los pasos 4 y 5. Si desea que Route 53 pruebe otra rama del árbol cuando el estado de todos los registros sin alias no sea correcto en una rama del árbol, configure el valor de Evaluate Target Health (Evalúe estado del destino) en Yes (Sí) para cada uno de sus registros con alias.

Recuerde que no puede crear un registro de alias que direcciona el tráfico a otro registro hasta que haya creado el otro registro.

Cómo funcionan las comprobaciones de estado en configuraciones simples de Amazon Route 53

Cuando tenga dos o más recursos que realizan la misma función, como, por ejemplo, dos o más servidores web para example.com, puede utilizar las siguientes características de comprobación de estado para dirigir el tráfico únicamente a los recursos en buen estado:

Comprobar el estado de las instancias EC2 y otros recursos (registros sin alias)

Si dirige el tráfico a los recursos para los que no puede crear registros de alias, como las instancias EC2, debe crear un registro y una comprobación de estado para cada recurso. A continuación, asocie cada comprobación de estado con el registro aplicable. Las comprobaciones de estado verifican periódicamente el estado de los recursos correspondientes y Route 53 dirige el tráfico solo a los recursos cuyo estado indican como correcto las comprobaciones de estado.

Evaluar el estado de un recurso de AWS (registros de alias)

Si utiliza [registros de alias](#) para dirigir el tráfico a determinados recursos de AWS, como los balanceadores de carga de ELB, puede configurar Route 53 para evaluar el estado del recurso y para dirigir el tráfico solo a los recursos cuyo estado sea correcto. Al configurar un registro de alias para evaluar el estado de un recurso, no necesita crear una comprobación de estado para él.

A continuación se ofrece información general de cómo configurar Route 53 para que compruebe el estado de los recursos en configuraciones simples:

1. Identifique los recursos que desea que monitoree Route 53. Por ejemplo, puede monitorizar todos los servidores HTTP que responden a las solicitudes de example.com.
2. Cree las comprobaciones de estado de los recursos para los que no puede crear registros de alias, por ejemplo, instancias y servidores de EC2 que se ejecutan en su centro de datos. Especifique cómo enviar las solicitudes de comprobación de estado al recurso: qué protocolo desea utilizar (HTTP, HTTPS o TCP), qué dirección IP y puerto se debe usar y, en el caso de las comprobaciones de estado HTTP/HTTPS, un nombre de dominio y una ruta.

 Note

Si utiliza recursos para los que puede crear registros de alias, por ejemplo, equilibradores de carga de ELB, no cree comprobaciones de estado para dichos recursos.

Una configuración común consiste en crear una comprobación de estado para cada recurso y usar la misma dirección IP para el punto de conexión de comprobación de y el recurso. La comprobación de estado envía solicitudes a la dirección IP especificada.

 Note

Route 53 no puede comprobar el estado de los recursos que tienen una dirección IP en rangos locales, privados, no direccionables o de multidifusión. Para obtener más información sobre las direcciones IP para las que no puede crear comprobaciones de estado, consulte [RFC 5735, direcciones IPv4 de uso especial](#) y [RFC 6598, prefijo IPv4 reservado por IANA para el espacio de direcciones compartidas](#).

Para obtener más información sobre la creación de comprobaciones de estado, consulte [Creación, actualización y eliminación de comprobaciones de estado](#).

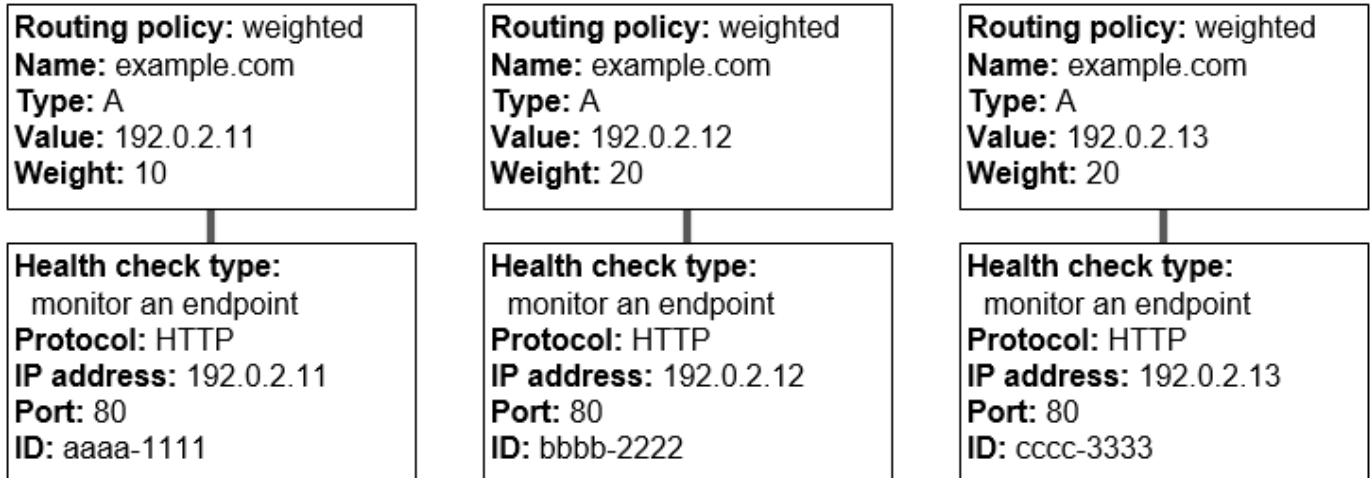
3. Tal vez deba configurar las reglas del enrutador y del firewall para que Route 53 pueda enviar solicitudes periódicas a los puntos de enlace que ha especificado en las comprobaciones de estado. Para obtener más información, consulte [Configuración de las reglas de enrutador y de firewall para las comprobaciones de estado de Amazon Route 53](#).
4. Cree un grupo de registros para sus recursos, por ejemplo, un grupo de registros ponderados. Puede combinar registros de alias y sin alias, pero todos deben tener el mismo valor en Name (Nombre), Type (Tipo) y Routing Policy (Política de direccionamiento).

La forma de configurar Route 53 para que compruebe el estado de los recursos depende de si está creando registros de alias o registros sin alias:

- Registros de alias: especifique Yes (Sí) para Evaluate Target Health (Evaluar estado del destino).

- Registros sin alias: asocie las comprobaciones de estado que creó en el paso 2 con los registros correspondientes.

Cuando finalice, la configuración se parecerá al diagrama siguiente, que incluye solo registros sin alias.



Para obtener información adicional sobre cómo crear registros mediante la consola de Route 53, consulte [Creación de registros con la consola de Amazon Route 53](#).

5. Si creó comprobaciones de estado, Route 53 envía periódicamente solicitudes al punto de conexión de cada comprobación de estado; no realiza la comprobación de estado cuando recibe una consulta de DNS. En función de las respuestas, Route 53 decide si los puntos de enlace tienen un estado correcto y usa esa información para determinar cómo responden a las consultas. Para obtener más información, consulte [Cómo determina Amazon Route 53 si la comprobación de estado es correcta](#).

Route 53 no comprueba el estado del recurso especificado en el registro, como la dirección IP que se especifica en un registro A para example.com. Cuando asocia una comprobación de estado a un registro, Route 53 comienza a comprobar el estado del punto de conexión especificado en la comprobación de estado. También puede configurar Route 53 para monitorear el estado de otras comprobaciones de estado o los flujos de datos de alarmas de CloudWatch. Para obtener más información, consulte [Tipos de comprobaciones de estado de Amazon Route 53](#).

Sucede lo siguiente cuando Route 53 recibe una consulta de example.com:

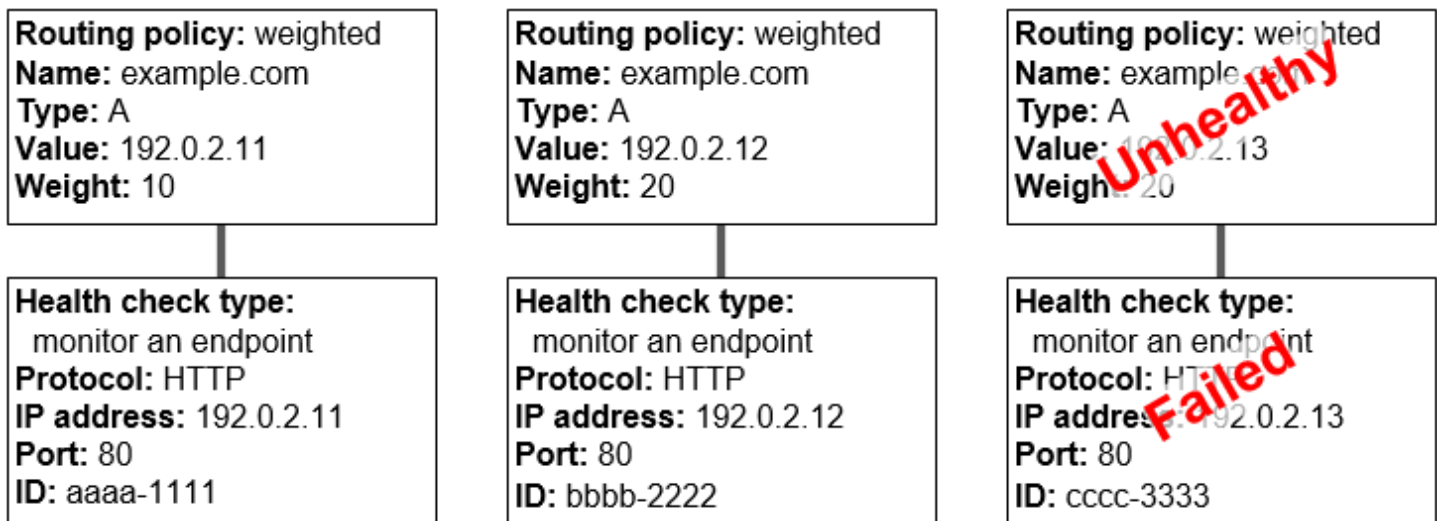
1. Route 53 elige un registro en función de la política de direccionamiento. En este caso, elige un registro según su ponderación.
2. Determina el estado del actual registro seleccionado consultando el estado de la comprobación de estado para dicho registro.
3. Si el registro seleccionado no tiene un estado correcto, Route 53 elige otro registro. Esta vez, no se tiene en cuenta el registro con estado incorrecto.

Para obtener más información, consulte [Cómo elige Amazon Route 53 registros cuando está configurado la comprobación de estado](#).

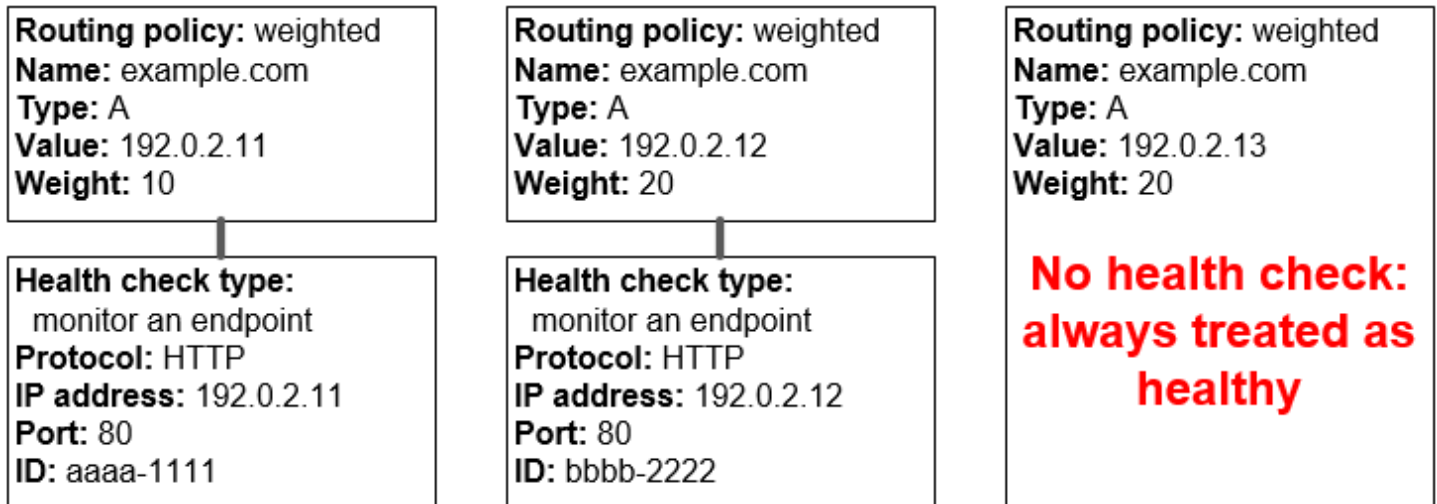
4. Cuando Route 53 encuentra un registro con estado correcto, responde a la consulta con el valor aplicable, como la dirección IP en un registro A.

En el siguiente ejemplo se muestra un grupo de registros ponderados en el que el tercer registro tiene un estado incorrecto. Inicialmente, Route 53 selecciona un registro en función de la ponderación de los tres registros. Si Route 53 selecciona por primera vez el registro con estado incorrecto, selecciona otro registro, pero esta vez omite la ponderación del tercer registro del cálculo:

- Cuando Route 53 selecciona inicialmente entre los tres registros, responde a las solicitudes utilizando el primer registro el 20 % del tiempo: $10/(10+20+20)$.
- Cuando Route 53 determina que el tercer registro tiene un estado incorrecto, responde a las solicitudes con el primer registro aproximadamente el 33 % del tiempo: $10/(10+20)$.



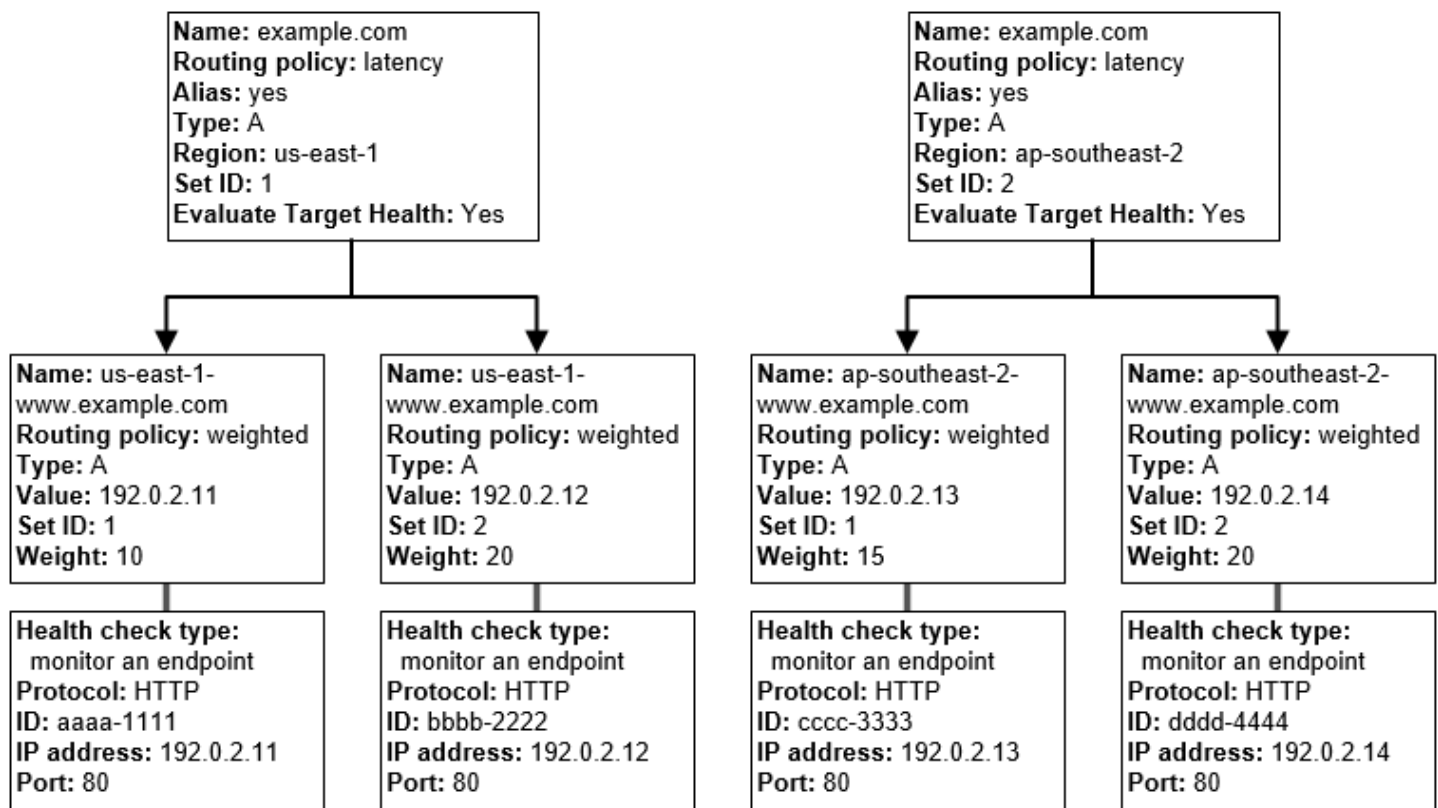
Si omite una comprobación de estado de uno o varios registros de un grupo de registros, Route 53 no tiene forma de determinar el estado del recurso correspondiente. Route 53 trata estos registros como si tuvieran un estado correcto.



Cómo funcionan las comprobaciones de estado en configuraciones complejas de Amazon Route 53

La comprobación del estado de los recursos en las configuraciones complejas funciona de la misma forma que en las configuraciones simples. No obstante, en las configuraciones complejas se utiliza una combinación de registros de alias (como alias ponderados y alias de conmutación por error) y registros sin alias para crear un árbol de decisiones que ofrece mayor control sobre cómo responde Route 53 a las solicitudes.

Por ejemplo, puede usar los registros de alias de latencia para seleccionar una región próxima a un usuario y utilizar registros ponderados para dos o más recursos en cada registro con el fin de protegerse frente al error de un solo punto de conexión o una zona de disponibilidad. En el siguiente diagrama se muestra esta configuración.



A continuación se explica cómo se configuran Amazon EC2 y Route 53. Comencemos en la parte inferior del árbol, ya que es el orden en que creará los registros:

- Tiene dos instancias EC2 en cada una de las dos regiones, us-east-1 y ap-southeast-2. Desea que Route 53 dirija el tráfico a las instancias EC2 en función de si su estado es correcto, por lo que crea una comprobación de estado para cada instancia. Puede configurar cada comprobación de estado para que envíe solicitudes de comprobación a la instancia correspondiente en la dirección IP elástica de la instancia.

Route 53 es un servicio global, por lo que no especifica la región en la que desea crear las comprobaciones de estado.

- Desea dirigir el tráfico a las dos instancias en cada región en función del tipo de instancia, por lo que crea un registro ponderado para cada instancia y asigna una ponderación a cada registro. (Puede cambiar la ponderación más adelante para dirigir más o menos el tráfico a una instancia). También puede asociar la comprobación de estado aplicable a cada instancia.

Al crear los registros, utilice nombres como us-east-1-www.example.com. y ap-southeast-2-www.example.com. Espere hasta llegar al principio del árbol para asignar a los registros los

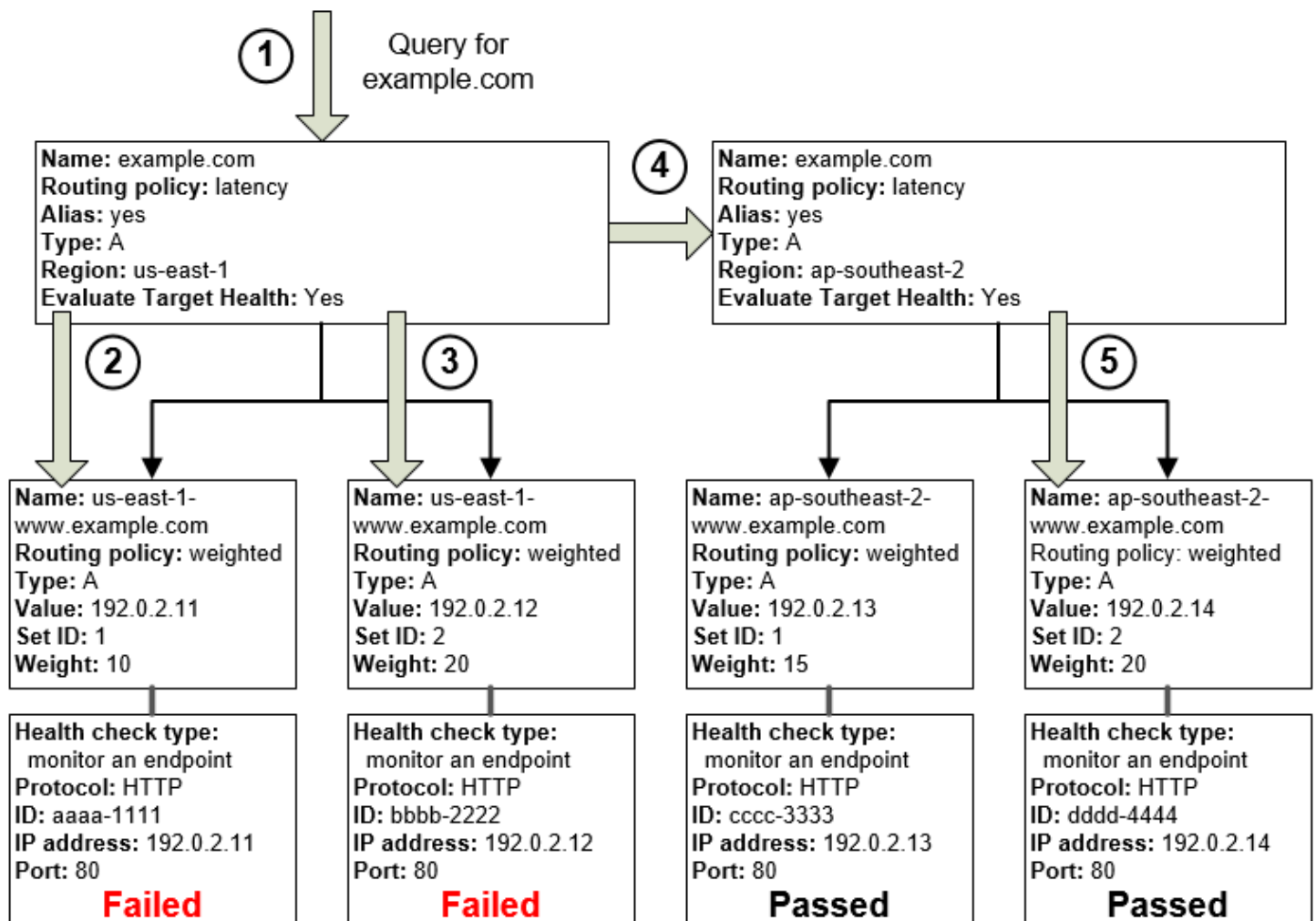
nombres que los usuarios utilizarán para obtener acceso a su sitio o aplicación web, por ejemplo, example.com.

- Desea dirigir el tráfico a la región que proporciona la latencia más baja para los usuarios, por lo que elige la [política de direccionamiento](#) de latencia para los registros en la parte superior del árbol.

Desea dirigir el tráfico a los registros de cada región, no directamente a los recursos de cada región (los registros ponderados ya se encargan de hacerlo). Como resultado, crea [registros de alias](#) de latencia.

Al crear los registros de alias, les asigna el nombre que desea que los usuarios utilicen para obtener acceso a su sitio o aplicación web, por ejemplo, example.com. Los registros de alias dirigen el tráfico de example.com a los registros de us-east-1-www.example.com y ap-southeast-2-www.example.com.

Para ambos registros de alias de latencia, configure el valor de Evaluate Target Health en Yes. Esto hace que Route 53 determine si hay los recursos con estado incorrecto en una región antes de intentar dirigir el tráfico a ella. En caso contrario, Route 53 elige un recurso con estado correcto en la otra región.



El diagrama anterior ilustra la siguiente secuencia de eventos:

1. Route 53 recibe una consulta de `example.com`. En función de la latencia del usuario que realiza la solicitud, Route 53 selecciona el registro de alias de latencia de la región `us-east-1`.
2. Route 53 selecciona un registro ponderado basándose en la ponderación. Evaluate Target Health (Evaluar estado del destino) es `Yes` (Sí) para el registro de alias de latencia, por lo que Route 53 comprueba el estado del registro ponderado seleccionado.
3. Se ha producido un error en la comprobación de estado, por lo que Route 53 elige otro registro ponderado basándose en la ponderación y comprueba su estado. Este registro también tiene un estado incorrecto.
4. Route 53 vuelve a esa rama del árbol, busca el registro de alias de latencia con la siguiente mejor latencia y elige el registro para `ap-southeast-2`.

5. Route 53 selecciona de nuevo un registro basándose en la ponderación y, a continuación, comprueba el estado del recurso seleccionado. El estado del recurso es correcto, por lo que Route 53 devuelve el valor aplicable en la respuesta a la consulta.

Temas

- [¿Qué sucede cuando se asocia una comprobación de estado a un registro de alias?](#)
- [¿Qué sucede cuando se omiten las comprobaciones de estado?](#)
- [¿Qué sucede cuando se desactiva la evaluación del estado del destino?](#)

¿Qué sucede cuando se asocia una comprobación de estado a un registro de alias?

Puede asociar una comprobación de estado a un registro de alias en su lugar o además de configurar el valor de Evaluate Target Health en Yes. No obstante, por lo general, resulta más útil que Route 53 responda a las consultas basándose en el estado de los recursos subyacentes: los servidores HTTP, los servidores de base de datos y otros recursos a los que hagan referencia los registros. Por ejemplo, suponga la siguiente configuración:

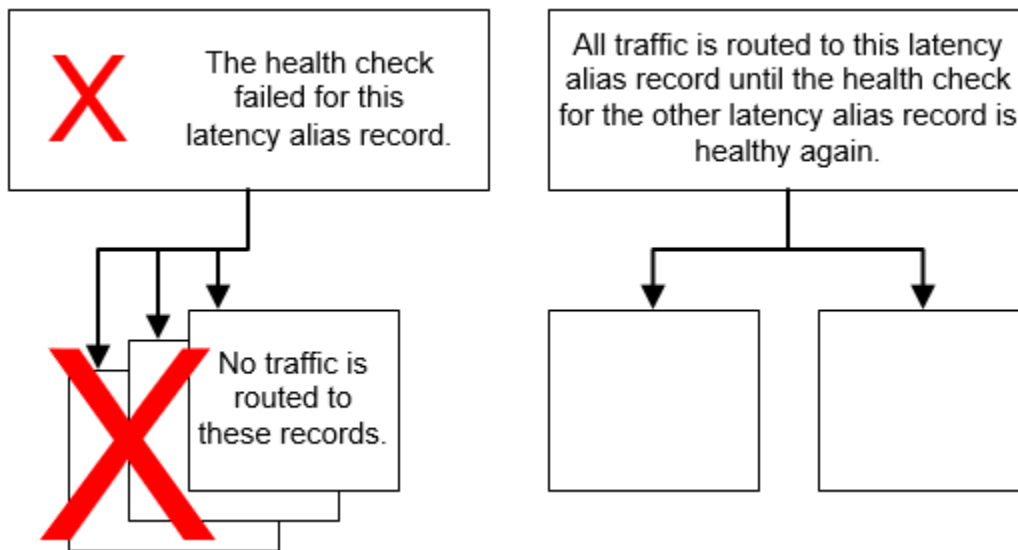
- Asigna una comprobación de estado a un registro de alias de latencia cuyo destino de alias es un grupo de registros ponderados.
- Configure el valor de Evaluate Target Health en Yes para el registro de alias de latencia.

En esta configuración, se deben cumplir las dos condiciones siguientes para que Route 53 devuelva el valor aplicable para un registro ponderado:

- Se debe superar la comprobación de estado asociada al registro de alias de latencia.
- Se debe considerar que el estado de al menos un registro ponderado es correcto, ya sea porque está asociado con una comprobación de estado superada o porque no está asociado a una comprobación de estado. En este último caso, Route 53 siempre considera que el registro ponderado tiene un estado correcto.

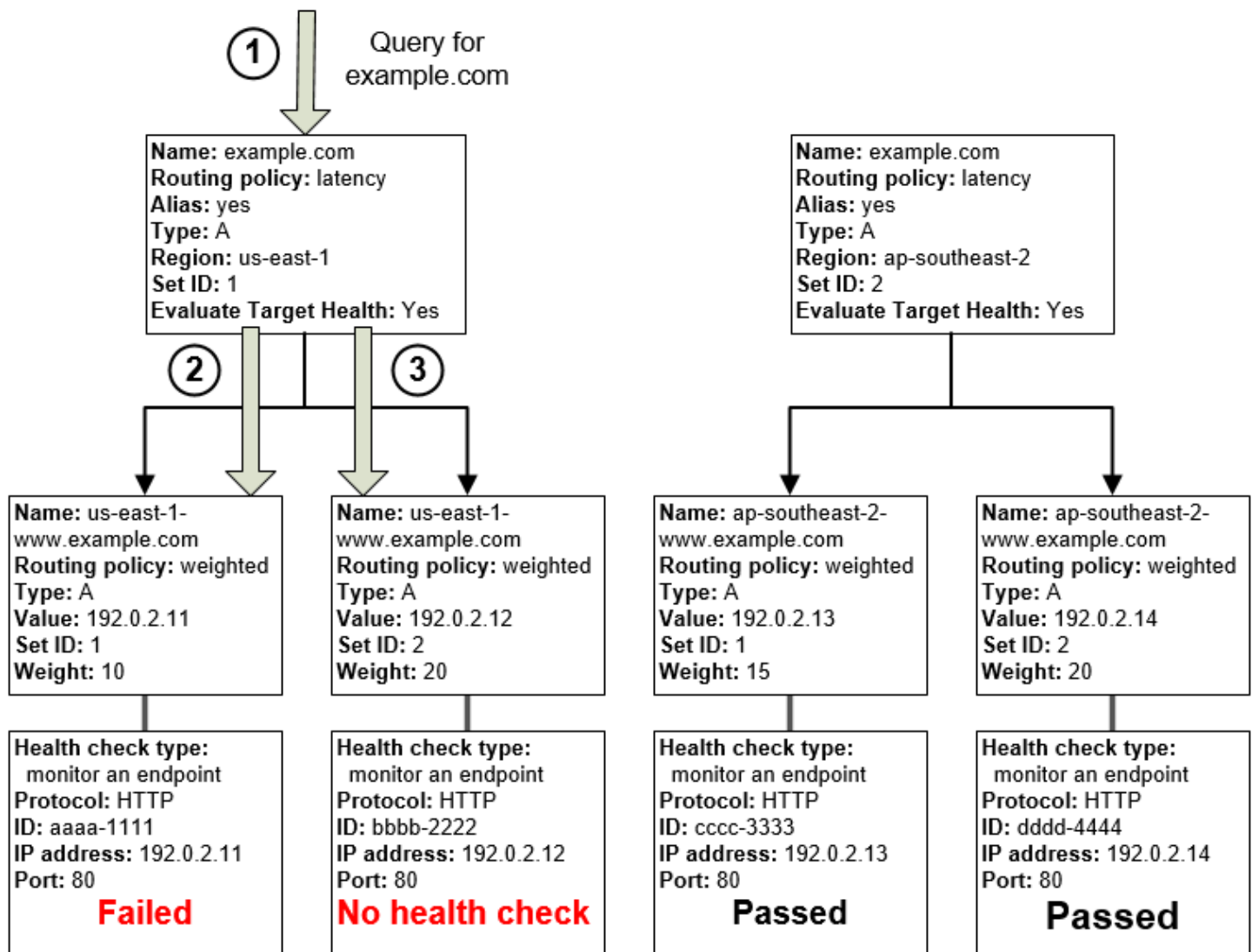
En la siguiente ilustración, no se pudo realizar la comprobación de estado del registro de alias de latencia en la parte superior izquierda. Por consiguiente, Route 53 deja de responder a las consultas mediante cualquiera de los registros ponderados a los que hace referencia el registro de alias de latencia, aunque todos tengan un estado correcto. Route 53 comienza a considerar estos registros ponderados de nuevo solo cuando la comprobación de estado del registro de alias de latencia

vuelve a ser correcta. (Puede consultar las excepciones en). [Cómo elige Amazon Route 53 registros cuando está configurado la comprobación de estado.](#))



¿Qué sucede cuando se omiten las comprobaciones de estado?

En una configuración compleja, es importante asociar las comprobaciones de estado a todos los registros sin alias. En el ejemplo siguiente falta una comprobación de estado en uno de los registros ponderados de la región us-east-1.



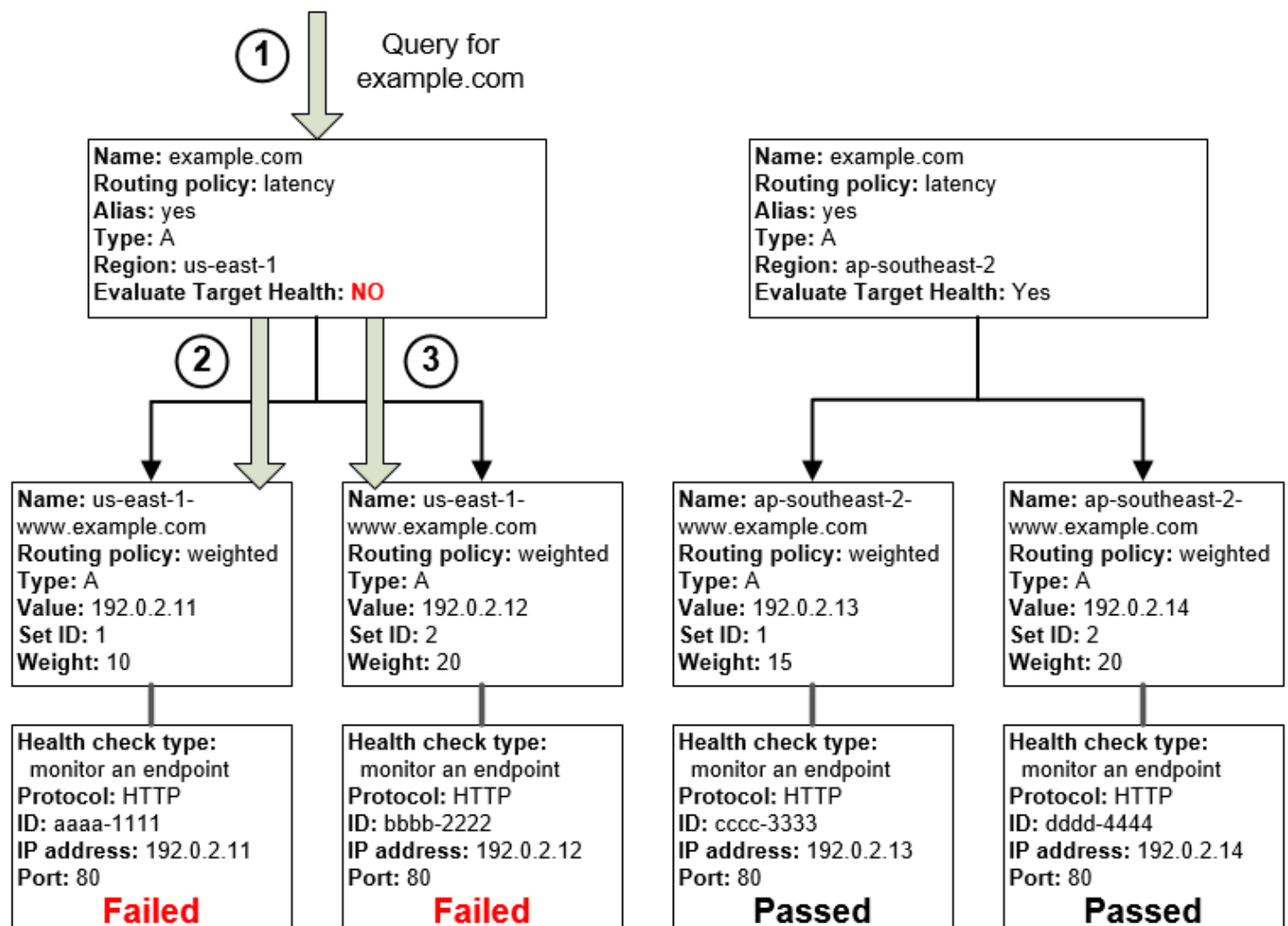
A continuación se indica lo que sucede cuando se omite una comprobación de estado en un registro sin alias en esta configuración:

1. Route 53 recibe una consulta de `example.com`. En función de la latencia del usuario que realiza la solicitud, Route 53 selecciona el registro de alias de latencia de la región `us-east-1`.
2. Route 53 busca en el destino de alias el registro de alias de latencia y comprueba el estado de las comprobaciones de estado correspondientes. Se ha producido un error en la comprobación de estado de un registro ponderado, por lo que ese registro no se tiene en cuenta.
3. El otro registro ponderado del destino de alias para la región `us-east-1` no tiene comprobación de estado. El estado del recurso correspondiente puede ser correcto o no serlo pero, sin una comprobación de estado, Route 53 no tiene forma de saberlo. Route 53 supone que el estado del recurso es correcto y devuelve el valor aplicable en la respuesta a la consulta.

¿Qué sucede cuando se desactiva la evaluación del estado del destino?

Por lo general, debe configurar Evaluate Target Health (Evaluar estado del destino) en Yes (Sí) para todos los registros de alias de un árbol. Si establece Evaluate Target Health (Evaluar estado del destino) en No, Route 53 sigue dirigiendo el tráfico a los registros a los que hace referencia un registro de alias, aunque las comprobaciones de estado de dichos registros den error.

En el siguiente ejemplo, todos los registros ponderados tienen comprobaciones de estado asociadas, pero Evaluate Target Health (Evaluar estado del destino) se ha configurado en No para el registro de alias de latencia de la región us-east-1:



A continuación se indica lo que sucede cuando se configura Evaluate Target Health en No para un registro de alias en esta configuración:

1. Route 53 recibe una consulta de example.com. En función de la latencia del usuario que realiza la solicitud, Route 53 selecciona el registro de alias de latencia de la región us-east-1.

2. Route 53 determina cuál es el destino de alias para el registro de alias de latencia y realiza las comprobaciones de estado correspondientes. En ambas el estado es incorrecto.
3. Como el valor de Evaluate Target Health (Evaluar estado del destino) es No para el registro de alias de latencia para la región us-east-1, Route 53 debe elegir un registro de esta rama en vez de volver a la rama y buscar un registro con estado correcto en la región ap-southeast-2.

Cómo elige Amazon Route 53 registros cuando está configurado la comprobación de estado

Si configura la comprobación de todos los registros de un grupo de registros que tienen el mismo nombre, el mismo tipo (por ejemplo, A o AAAA) y la misma política de direccionamiento (por ejemplo, ponderada o conmutación por error), Route 53 responde a las consultas de DNS eligiendo un registro con estado correcto y devolviendo el valor aplicable de ese registro.

Por ejemplo, suponga que crea tres registros A ponderados y asigna comprobaciones de estado a los tres. Si la comprobación de estado de uno de los registros no es correcta, Route 53 responde a las consultas de DNS con las direcciones IP en uno de los otros dos registros.

A continuación se muestra cómo elige Route 53 un registro con estado correcto:

1. Route 53 elige inicialmente un registro en función de la política de direccionamiento y de los valores que especifique para cada registro. Por ejemplo, en el caso de los registros ponderados, Route 53 elige un registro en función de la ponderación que se especifique para cada registro.
2. Route 53 determina si el estado del registro es correcto:
 - Registro sin alias con una comprobación de estado asociada: si ha asociado una comprobación de estado a un registro sin alias, Route 53 comprueba el estado actual de la comprobación de estado.

Route 53 comprueba periódicamente el estado del punto de conexión que se especifica en una comprobación de estado; no realiza la comprobación de estado cuando llega la consulta de DNS.

Puede asociar comprobaciones de estado con registros de alias, pero le recomendamos que asocie las comprobaciones de estado solo con registros sin alias. Para obtener más información, consulte [¿Qué sucede cuando se asocia una comprobación de estado a un registro de alias?](#).

- Registro de alias con la evaluación de estado del destino configurada en Yes (Sí): Route 53 comprueba el estado del recurso al que hace referencia el registro de alias; por ejemplo, un balanceador de carga de ELB u otro registro en la misma zona alojada.
3. Si el estado del registro es correcto, Route 53 responde a la consulta con el valor aplicable, como una dirección IP.

Si el estado del registro no es correcto, Route 53 elige otro registro utilizando los mismos criterios y repite el proceso hasta que encuentra un registro con estado correcto.

Route 53 utiliza los siguientes criterios al elegir un registro:

Los registros sin una comprobación de estado siempre se encuentran en estado correcto

Si un registro de un grupo de registros que tienen el mismo nombre y tipo no tiene una comprobación de estado asociada, Route 53 siempre considera que tiene un estado correcto y siempre lo incluye entre las posibles respuestas a una consulta.

Si ningún registro tiene estado correcto, el estado de todos los registros es correcto

Si ninguno de los registros de un grupo de registros tiene un estado correcto, Route 53 debe devolver algo en respuesta a las consultas de DNS, pero no tiene base para elegir un registro u otro. En este caso, Route 53 considera que todos los registros del grupo tienen un estado correcto y selecciona uno en función de la política de direccionamiento y los valores que especifique para cada registro.

Registros ponderados que tienen una ponderación de 0

Si agrega comprobaciones de estado a todos los registros de un grupo de registros ponderados, pero asigna ponderaciones distintas de cero a algunos registros y ponderaciones cero a otros, las comprobaciones de estado funcionan igual que si todos los registros tuvieran ponderaciones distintas de cero con las excepciones siguientes:

- Route 53 tiene en cuenta inicialmente solo los registros con ponderación distinta de cero, si los hubiera.
- Si todos los registros con una ponderación mayor que 0 tienen un estado incorrecto, Route 53 tiene en cuenta los registros con ponderación cero.

Dado que Route 53 considerará los registros con ponderación cero en algunas circunstancias, es importante asegurarse de que el destino con ponderación cero también tenga una respuesta viable a una consulta de DNS.

Para obtener más información acerca de los registros ponderados, consulte [Comprobaciones de estado y enrutamiento ponderado](#).

Registros de alias

También puede configurar la comprobación de estado de los registros de alias si establece Evaluate Target Health (Evaluar estado del destino) en Yes (Sí) para cada registro de alias. Esto hace que Route 53 evalúe el estado del recurso al que el registro redirige el tráfico; por ejemplo, un balanceador de carga de ELB u otro registro en la misma zona alojada.

Por ejemplo, suponga que el destino de alias de un registro de alias es un grupo de registros ponderados que tienen ponderaciones distintas de cero:

- Siempre que al menos uno de los registros ponderados tenga un estado correcto, Route 53 considera que el estado del registro de alias es correcto.
- Si ninguno de los registros ponderados tiene un estado correcto, Route 53 considera que el estado del registro de alias no es correcto.
- Route 53 deja de tener en cuenta los registros de dicha rama del árbol hasta que al menos un registro ponderado vuelve a tener un estado correcto.

Para obtener más información, consulte [Cómo funcionan las comprobaciones de estado en configuraciones complejas de Amazon Route 53](#).

Registros de conmutación por error

Por lo general, los registros de conmutación por error funcionan igual que otros tipos de direccionamiento. Cree comprobaciones de estado y asócielas con registros sin alias, y establezca Evaluate Target Health (Evaluar estado del destino) en Yes (Sí) para los registros de alias. Tenga en cuenta lo siguiente:

- Los registros principales y secundarios puede ser registros sin alias o registros de alias.
- Si asocia las comprobaciones de estado con los registros de conmutación por error principal y secundario, Route 53 responde a las solicitudes del siguiente modo:
 - Si Route 53 considera que el registro principal tiene un estado correcto (si el estado del punto de conexión de la comprobación de estado es correcto), Route 53 solo devuelve el registro principal en respuesta a una consulta de DNS.
 - Si Route 53 considera que el estado del registro principal es incorrecto y el del secundario es correcto, Route 53 devuelve el registro secundario.
 - Si Route 53 considera que el estado de los registros principal y secundario es incorrecto, Route 53 devuelve el registro principal.

- Al configurar el registro secundario, la adición de una comprobación de estado es opcional. Si omite la comprobación de estado para el registro secundario y si el estado del punto de conexión de comprobación de estado del registro principal es incorrecto, Route 53 siempre responde a las consultas de DNS con el registro secundario. Esto se aplica aunque el estado del registro secundario sea incorrecto.

Para obtener más información, consulte los temas siguientes:

- [Configuración de la conmutación por error activa-pasiva con un recurso principal y otro secundario](#)
- [Configuración de la conmutación por error activa-pasiva con varios recursos principales y secundarios](#)

Conmutación por error activa-activa y activa-pasiva

Puede usar la comprobación de estado de Route 53 para establecer las configuraciones de conmutación por error activa-activa y activa-pasiva. Configure la conmutación por error activa-activa con una [política de direccionamiento](#) (o una combinación de políticas de direccionamiento) distinta de conmutación por error y la conmutación por error activa-pasiva con la política de direccionamiento de conmutación por error.

Temas

- [Conmutación por error activa-activa](#)
- [Conmutación por error activa-pasiva](#)

Conmutación por error activa-activa

Utilice esta configuración de conmutación por error cuando desee que todos los recursos estén disponibles la mayor parte del tiempo. Cuando un recurso deje de estar disponible, Route 53 puede detectar que su estado es incorrecto y dejar de incluirlo al responder a las consultas.

En la conmutación por error activa-activa, todos los registros que tienen el mismo nombre, el mismo tipo (por ejemplo, A o AAAA) y la misma política de direccionamiento (por ejemplo, ponderada o de latencia) están activos a menos que Route 53 considere que su estado no es correcto. Route 53 puede responder a una consulta de DNS utilizando cualquier registro con estado correcto.

Conmutación por error activa-pasiva

Utilice una configuración de conmutación por error activa-pasiva cuando desee que un recurso o un grupo de recursos principal esté disponible la mayor parte del tiempo y desee que un recurso o un grupo de recursos secundario esté en espera en el caso de que los recursos principales dejen de estar disponibles. Al responder a las consultas, Route 53 solo incluye los recursos principales correctos. Si todos los recursos principales tienen un estado incorrecto, Route 53 comienza a incluir únicamente los recursos secundarios correctos en la respuesta a las consultas de DNS.

Temas

- [Configuración de la conmutación por error activa-pasiva con un recurso principal y otro secundario](#)
- [Configuración de la conmutación por error activa-pasiva con varios recursos principales y secundarios](#)
- [Configuración de la conmutación por error activa-pasiva con registros ponderados](#)

Configuración de la conmutación por error activa-pasiva con un recurso principal y otro secundario

Para crear una configuración de conmutación por error activa-pasiva con un registro principal y otro secundario, cree los registros y especifique para Failover (Conmutación por error) para la política de direccionamiento. Cuando el estado del recurso principal es correcto, Route 53 responde a las consultas de DNS utilizando el registro principal. Cuando el estado del recurso principal no es correcto, Route 53 responde a las consultas de DNS utilizando el registro secundario.

Configuración de la conmutación por error activa-pasiva con varios recursos principales y secundarios

También puede asociar varios recursos con el registro principal, el registro secundario o ambos. En esta configuración, Route 53 considera que el estado del registro de conmutación por error principal es correcto siempre que al menos uno de los recursos asociados tenga un estado correcto. Para obtener más información, consulte [Cómo elige Amazon Route 53 registros cuando está configurado la comprobación de estado](#).

Para configurar la conmutación por error activa-pasiva con varios recursos para el registro principal o secundario, realice las siguientes tareas.

1. Cree una comprobación de estado para cada recurso al que desee dirigir el tráfico, por ejemplo, una instancia EC2 o un servidor web de su centro de datos.

 Note

Si va a dirigir el tráfico a recursos de AWS para los que puede crear [registros de alias](#), no cree comprobaciones de estado para dichos recursos. Al crear los registros de alias, establezca Evaluate Target Health (Evaluar estado del destino) en Yes (Sí).

Para obtener más información, consulte [Creación y actualización de comprobaciones de estado](#).

2. Cree registros para sus recursos principales y especifique los siguientes valores:

- Asigne a cada registro el mismo nombre, tipo y política de direccionamiento. Por ejemplo, podría crear tres registros A ponderados que se denominen failover-primary.example.com.
- Si va a usar recursos de AWS para los que puede crear registros de alias, especifique Yes (Sí) para Evaluate Target Health (Evaluar estado del destino).

Si va a utilizar recursos para los que no puede crear registros de alias, asocie la comprobación de estado aplicable del paso 1 a cada registro.

Para obtener más información, consulte [Creación de registros con la consola de Amazon Route 53](#).

3. Cree registros para sus recursos secundarios, si corresponde, y especifique los siguientes valores:

- Asigne a cada registro el mismo nombre, tipo y política de direccionamiento. Por ejemplo, podría crear tres registros A ponderados que se denominen failover-secondary.example.com.
- Si va a usar recursos de AWS para los que puede crear registros de alias, especifique Yes (Sí) para Evaluate Target Health (Evaluar estado del destino).

Si va a utilizar recursos para los que no puede crear registros de alias, asocie la comprobación de estado aplicable del paso 1 a cada registro.

 Note

Algunos clientes usan un servidor web como su recurso principal y un bucket de Amazon S3 configurado como un punto de conexión de sitio web como su recurso secundario. El bucket de S3 contiene un mensaje "no disponible temporalmente" simple. Si utiliza dicha configuración, puede omitir este paso y crear un registro de alias de conmutación por error para el recurso secundario en el paso 4.

4. Cree dos registros de alias de conmutación por error, uno principal y otro secundario, y especifique los siguientes valores:

Registro principal

- Name (Nombre): especifique el nombre del dominio (example.com) o el nombre del subdominio (www.example.com) para el que desea que Route 53 dirija el tráfico.
- Alias: especifique Yes (Sí).
- Alias Target (Destino de alias): especifique el nombre de los registros que creó en el paso 2.
- Routing Policy (Política de direccionamiento): especifique Failover (Conmutación por error).
- Failover Record Type (Tipo de registro de conmutación por error): especifique Primary (Principal).
- Evaluate Target Health (Evaluar estado del destino): especifique Yes (Sí).
- Associate with Health Check (Asociar con comprobación de estado): especifique No.

Registro secundario

- Name (Nombre): especifique el mismo nombre que indicó para el registro principal.
- Alias: especifique Yes (Sí).
- Alias Target (Destino de alias): si ha creado registros para su recurso secundario en el paso 3, especifique el nombre de los registros. Si utiliza un bucket de Amazon S3 para el recurso secundario, especifique el nombre de DNS del punto de conexión de sitio web.
- Routing Policy (Política de direccionamiento): especifique Failover (Conmutación por error).
- Failover Record Type (Tipo de registro de conmutación por error): especifique Secondary (Secundario).
- Evaluate Target Health (Evaluar estado del destino): especifique Yes (Sí).
- Associate with Health Check (Asociar con comprobación de estado): especifique No.

Configuración de la conmutación por error activa-pasiva con registros ponderados

También puede utilizar registros ponderados para la conmutación por error activa-pasiva, con salvedades. Si especifica ponderaciones distintas de cero para algunos registros y ponderaciones cero para otros, Route 53 responde a las consultas de DNS utilizando solo registros con estado correcto que tengan ponderaciones distintas de cero. Si todos los registros con una ponderación mayor que 0 tienen un estado incorrecto, Route 53 responde a las consultas utilizando los registros con ponderación cero.

 Note

Todos los registros con ponderaciones distintas de cero deben tener un estado incorrecto antes de que Route 53 comience a responder a las consultas de DNS con registros que tengan ponderaciones de cero. Esto puede provocar que aplicación o sitio web no sea fiable si el último recurso correcto, por ejemplo, un servidor web, no puede controlar todo el tráfico cuando otros recursos no están disponibles.

Configuración de la conmutación por error en una zona alojada privada

Si va a crear registros de conmutación por error en una zona alojada privada, tenga en cuenta lo siguiente:

- Los comprobadores de estado de Route 53 están fuera de la VPC. Para comprobar el estado de un punto de conexión en una VPC por dirección IP, debe asignar una dirección IP pública a la instancia en la VPC.
- Puede crear una métrica de CloudWatch, asociar una alarma a la métrica y, a continuación, crear una comprobación de estado que se base en el flujo de datos de la alarma. Por ejemplo, puede crear una métrica de CloudWatch que compruebe el estado de la métrica `StatusCheckFailed` de EC2, agregar una alarma a la métrica y, a continuación, crear una comprobación de estado que se base en el flujo de datos de la alarma para verificar las instancias dentro de una Virtual Private Cloud (VPC) que solo tienen direcciones IP privadas. Para obtener más información acerca de cómo crear las métricas y las alarmas de CloudWatch mediante la consola de CloudWatch, consulte la [Guía del usuario de Amazon CloudWatch](#).

Para obtener más información, consulte [Uso de zonas alojadas privadas](#) y [Monitorear comprobaciones de estado mediante CloudWatch](#).

Cómo Amazon Route 53 evita los problemas de conmutación por error

Los algoritmos de conmutación por error implementados por Route 53 se han diseñado no solo para dirigir el tráfico a puntos de enlace con estado correcto, sino también para mitigar los desastres provocados por comprobaciones de estado y aplicaciones configuradas incorrectamente, sobrecargas de los puntos de enlace y errores de partición.

Temas

- [Cómo Amazon Route 53 evita errores en cascada](#)
- [Cómo controla Amazon Route 53 las particiones de Internet](#)

Cómo Amazon Route 53 evita errores en cascada

Como primera defensa frente a los errores en cascada, cada algoritmo de direccionamiento de solicitud (tales como ponderados y conmutación por error) tiene un modo de último recurso. En este modo especial, cuando se considera que el estado de todos los registros es incorrecto, el algoritmo de Route 53 cambia a considerar que el estado de todos los registros es correcto.

Por ejemplo, si todas las instancias de una aplicación, en varios hosts, rechazan las solicitudes de comprobación de estado, los servidores DNS de Route 53 elegirán una respuesta y la devolverán en vez de no devolver ninguna respuesta de DNS o de devolver una respuesta NXDOMAIN (dominio no existente). Una aplicación puede responder a los usuarios y no superar las comprobaciones de estado, por lo que esto proporciona algún tipo de protección frente a la configuración errónea.

Del mismo modo, si una aplicación está sobrecargada y uno de tres puntos de enlace no supera sus comprobaciones de estado, por lo que se excluye de las respuestas de DNS de Route 53, Route 53 distribuye las respuestas entre los dos puntos de enlace restantes. Si los puntos de enlace restantes no pueden controlar la carga adicional y producen un error, Route 53 vuelve a la distribución de las solicitudes en los tres puntos de enlace.

Cómo controla Amazon Route 53 las particiones de Internet

Aunque poco frecuentes, en ocasiones hay particiones de Internet importantes, lo que significa que grandes regiones geográficas no pueden comunicarse entre sí a través de Internet. Durante estas particiones, las ubicaciones de Route 53 pueden llegar a conclusiones distintas sobre el estado de un punto de conexión que pueden ser diferentes del estado comunicado a CloudWatch. Los comprobadores de estado de Route 53 de cada región de AWS están enviando constantemente estados de comprobación de estado a todas las ubicaciones de Route 53. Durante las particiones de Internet, cada ubicación de Route 53 podría tener acceso únicamente a un conjunto parcial de estos estados, normalmente de las regiones más próximas.

Por ejemplo, durante una partición de Internet que afecta a la conectividad a América del Sur y desde esa región, los servidores DNS de Route 53 en la ubicación América del Sur (São Paulo) de Route 53 podrían tener un acceso adecuado a los puntos de enlace de comprobación de estado en la región de AWS América del Sur (São Paulo), pero un acceso deficiente a otros puntos de enlace. Al mismo tiempo, Route 53 en EE. UU. Este (Ohio) podría tener un acceso deficiente a los puntos de

enlace de comprobación de estado de la región América del Sur (São Paulo) y llegar a la conclusión de que el estado de los registros es incorrecto.

Particiones como estas pueden dar lugar a situaciones en las que las ubicaciones de Route 53 llegan a conclusiones distintas sobre el estado de los puntos de enlace, basándose en su visibilidad local de estos puntos de enlace. Por este motivo, cada ubicación de Route 53 considera que el estado de un punto de conexión es correcto cuando solo una parte de los comprobadores de estado accesible considera que lo es.

Denominar y etiquetar comprobaciones de estado

Puede agregar etiquetas a las comprobaciones de estado de Amazon Route 53, lo que le permite asignar un nombre a cada comprobación de estado que sea más comprensible que el ID de comprobación de estado. Son las mismas etiquetas que proporciona Administración de facturación y costos de AWS para organizar la factura de AWS. Para obtener más información sobre el uso de etiquetas para la asignación de costes, consulte [Uso de etiquetas de asignación de costes para informes de facturación personalizados](#) en la Guía del usuario de AWS Billing.

Cada etiqueta consta de una clave (el nombre de la etiqueta) y un valor de etiqueta, ambos definidos por el usuario. Al agregar etiquetas a una comprobación de estado, le recomendamos que agregue una etiqueta que tenga los siguientes valores para la clave y el valor:

- key (clave) – Name (Nombre)
- value (valor): nombre que quiere dar a la comprobación de estado.

El valor de la etiqueta Name (Nombre) aparece en la lista de comprobaciones de estado en la consola de Route 53, lo que le permite distinguir inmediatamente una comprobación de otra. Para ver otras etiquetas de una comprobación de estado, puede seleccionarla y, a continuación, elegir la pestaña Tags (Etiquetas).

Para obtener más información acerca de las etiquetas, consulte los siguientes temas:

- Para agregar, editar o eliminar la etiqueta Name (Nombre) al agregar o editar comprobaciones de estado en la consola de Route 53 consulte [Creación y actualización de comprobaciones de estado](#).
- Para obtener información general sobre el etiquetado de recursos de Route 53 consulte [Etiquetado de recursos de Amazon Route 53](#).

Restricciones de las etiquetas

Se aplican las siguientes restricciones básicas a las etiquetas:

- Número máximo de etiquetas por recurso: 50 en la consola nueva y 10 en la antigua.
- Longitud máxima de Key (Clave): 128 caracteres Unicode
- Longitud máxima de Value (Valor): 256 caracteres Unicode
- Valores válidos para Key (Clave) y Value (Valor): letras mayúsculas y minúsculas del conjunto de caracteres UTF-8, números, espacios y los siguientes caracteres: `_ . : / = + - y @`.
- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas
- No utilice el prefijo `aws :` para claves o valores; su uso está reservado para AWS.

Añadir, editar y eliminar etiquetas para comprobaciones de estado

En los siguientes procedimientos se muestra cómo utilizar las etiquetas para las comprobaciones de estado en la consola de Route 53.

Note

Estamos en proceso de actualización de la consola de comprobaciones de estado para Route 53. Durante el periodo de transición, puede seguir utilizando la consola anterior.

Seleccione la pestaña de la consola que esté utilizando.

- [New console](#)
- [Consola antigua](#)

New console

Para añadir etiquetas a las comprobaciones de estado

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Comprobaciones de estado.
3. Seleccione el ID vinculado de la comprobación de estado para la que desea añadir etiquetas.

4. En la página inferior, seleccione la pestaña Etiquetas, luego, seleccione Administrar y, a continuación, Agregar nuevas etiquetas.
5. Introduzca un nombre para la etiqueta en el campo Clave e ingrese un valor en el campo Valor.
6. Seleccione Save.

Para editar etiquetas de comprobaciones de estado

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Comprobaciones de estado.
3. Seleccione el ID vinculado de una comprobación de estado.
4. En el panel inferior, elija la pestaña Etiquetas y, a continuación, elija Administrar.
5. Ahora, puede editar y agregar más etiquetas.
6. Seleccione Save.

Para eliminar etiquetas de comprobaciones de estado

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Comprobaciones de estado.
3. Seleccione el ID vinculado de una comprobación de estado.
4. En el panel inferior, elija la pestaña Etiquetas y, a continuación, elija Administrar.
5. Junto a la etiqueta que desea eliminar, seleccione Eliminar.
6. Seleccione Save.

Old console

Para añadir etiquetas a las comprobaciones de estado

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Health Checks.

3. Seleccione una comprobación de estado, o seleccione varias si desea añadir la misma etiqueta a más de una comprobación de estado.
4. En el panel inferior, elija la pestaña Tags y, a continuación, elija Add/Edit Tags.
5. En el cuadro de diálogo Add/Edit Tags, escriba el nombre de la etiqueta en el campo Key y escriba un valor en el campo Value.
6. Elija Apply changes.

Para editar etiquetas de comprobaciones de estado

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Health Checks.
3. Seleccione una comprobación de estado.

Si selecciona varias comprobaciones de estado que compartan la misma etiqueta, no podrá editar el valor para todas ellas de forma simultánea. Sin embargo, tenga en cuenta que puede editar el valor de una etiqueta que aparece en varias comprobaciones de estado si selecciona las que tengan la etiqueta y al menos una que no.

Por ejemplo suponga que selecciona varias comprobaciones de estado que tienen una etiqueta Cost Center (Centro de costos) y otra que no. Elige la opción para añadir una etiqueta y especifica Cost Center (Centro de costos) para la clave y 777 para el valor. En el caso de las comprobaciones de estado que ya tengan una etiqueta Cost Center (Centro de costes), Route 53 cambia el valor a 777. Para la otra comprobación de estado que no tiene la etiqueta Cost Center, Route 53 agrega una y establece el valor en 777.

4. En el panel inferior, elija la pestaña Tags y, a continuación, elija Add/Edit Tags.
5. En el cuadro de diálogo Add/Edit Tags, edite el valor.
6. Seleccione Save.

Para eliminar etiquetas de comprobaciones de estado

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Health Checks.

3. Seleccione una comprobación de estado, o seleccione varias si desea eliminar la misma etiqueta de más de una comprobación de estado.
4. En el panel inferior, elija la pestaña Tags y, a continuación, elija Add/Edit Tags.
5. En el cuadro de diálogo Add/Edit Tags, elija la **X** junto a la etiqueta que desee eliminar.
6. Seleccione Save.

Usar comprobaciones de estado con versiones de la API de Amazon Route 53 que sean anteriores al 2012-12-12

Las comprobaciones de estado se admiten a partir de la versión 2012-12-12 de la API de Amazon Route 53. Si una zona alojada contiene registros para los que se han configurado comprobaciones de estado, le recomendamos que use solo la API de 2012-12-12 o posterior. Tenga en cuenta las siguientes restricciones sobre el uso de las comprobaciones de estado con versiones anteriores de la API.

- La acción `ChangeResourceRecordSets` no puede crear ni eliminar registros que incluyan los elementos `EvaluateTargetHealth`, `Failover` o `HealthCheckId`.
- La acción `ListResourceRecordSets` puede enumerar los registros que incluyen estos elementos, pero los elementos no se incluyen en la salida. En su lugar, el elemento `Value` de la respuesta contiene un mensaje que indica que el registro incluye un atributo incompatible.

Monitorizar el estado de la comprobación de estado y recibir notificaciones

El estado de las comprobaciones de estado se monitorea en la consola de Amazon Route 53. También puede configurar alarmas de CloudWatch y recibir notificaciones automáticas cuando cambie el estado de la comprobación de estado.

Temas

- [Ver el estado de la verificación de salud y el motivo de los fallos de la verificación de salud](#)
- [Monitorización de la latencia entre los comprobadores de estado y el punto de conexión](#)
- [Monitorear comprobaciones de estado mediante CloudWatch](#)

Ver el estado de la verificación de salud y el motivo de los fallos de la verificación de salud

En la consola de Route 53 puede ver el estado (correcto o incorrecto) de las comprobaciones de estado tal como lo comunican los comprobadores de estado de Route 53. Para todas las comprobaciones de estado excepto las calculadas, también puede ver el motivo del último error de comprobación de estado, por ejemplo, los comprobadores de estado no han podido establecer una conexión con el punto de conexión.

Note

Estamos en proceso de actualización de la consola de comprobaciones de estado para Route 53. Durante el periodo de transición, puede seguir utilizando la consola anterior.

Seleccione la pestaña de la consola que esté utilizando.

- [New console](#)
- [Consola antigua](#)

New console

Cómo ver el estado y el último motivo de error de una comprobación de estado

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Comprobaciones de estado.
3. Para obtener información general de todas las comprobaciones de estado (correctas o incorrectas), consulte la columna Status (Estado). Para obtener más información, consulte [Cómo determina Amazon Route 53 si la comprobación de estado es correcta](#).
4. Para todas las comprobaciones de estado excepto las calculadas, puede ver el estado de los comprobadores de estado de Route 53 que están comprobando el estado de un punto de conexión especificado.
5. Elija el ID vinculado a la comprobación de estado de la que desea ver los detalles.
6. En el panel inferior, elija la pestaña Comprobadores de estado.

Note

Las nuevas comprobaciones de estado se deben propagar a los comprobadores de estado de Route 53 antes de que el estado de la comprobación de estado y el último motivo de error aparezcan en la columna Status (Estado). Hasta que finalice la propagación, en el mensaje de la columna se explica que el estado no está disponible.

7. La tabla incluye los siguientes valores:

Health checker IP

La dirección IP del comprobador de estado de Route 53 que ha realizado la comprobación de estado.

Last checked

Fecha y hora de la comprobación de estado o fecha y hora del último error.

Estado

El estado actual de la comprobación de estado o el motivo del último error en la comprobación de estado.

Old console

Cómo ver el estado y el último motivo de error de una comprobación de estado

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Health Checks.
3. Para obtener información general de todas las comprobaciones de estado (correctas o incorrectas), consulte la columna Status (Estado). Para obtener más información, consulte [Cómo determina Amazon Route 53 si la comprobación de estado es correcta](#).
4. Para todas las comprobaciones de estado excepto las calculadas, puede ver el estado de los comprobadores de estado de Route 53 que están comprobando el estado de un punto de conexión especificado. Seleccione la comprobación de estado.
5. En el panel inferior, elija la pestaña Health Checkers.

Note

Las nuevas comprobaciones de estado se deben propagar a los comprobadores de estado de Route 53 antes de que el estado de la comprobación de estado y el último motivo de error aparezcan en la columna Status (Estado). Hasta que finalice la propagación, en el mensaje de la columna se explica que el estado no está disponible.

6. Elija si desea consultar el estado actual de la comprobación de estado o la fecha y hora del último error, así como el motivo. En la tabla de la pestaña Status se incluyen los siguientes valores:

Health checker IP

La dirección IP del comprobador de estado de Route 53 que ha realizado la comprobación de estado.

Last checked

La fecha y la hora de la comprobación de estado o la fecha y la hora del último error, según la opción que seleccione en la parte superior de la pestaña Status.

Estado

El estado actual de la comprobación de estado o el motivo del último error de la comprobación de estado, según la opción que seleccione en la parte superior de la pestaña Status.

Monitorización de la latencia entre los comprobadores de estado y el punto de conexión

Al crear una comprobación de estado, si decide monitorear el estado de un punto de conexión (no el estado de otras comprobaciones de estado) y elige la opción Gráficos de latencia) puede ver los siguientes valores en los gráficos de CloudWatch en la consola de Route 53:

- El tiempo medio, en milisegundos, que tardan los comprobadores de estado de Route 53 en establecer una conexión TCP con el punto de conexión
- El tiempo medio, en milisegundos, que tardan los comprobadores de estado de Route 53 en recibir el primer byte de la respuesta a una solicitud HTTP o HTTPS
- El tiempo medio, en milisegundos, que tardan los comprobadores de estado de Route 53 en completar el protocolo SSL/TLS

Note

No puede habilitar la monitorización de latencia de las comprobaciones de estado existentes.

Important

Los comprobadores de estado se ejecutan en 16 zonas de disponibilidad redundantes. Ocasionalmente, una zona de disponibilidad puede no estar disponible debido a implementaciones, actualizaciones, mantenimiento, etc. El sistema de comprobación de estado está diseñado para tener en cuenta esto sin ningún impacto en el cliente.

Note

Estamos en proceso de actualización de la consola de comprobaciones de estado para Route 53. Durante el periodo de transición, puede seguir utilizando la consola anterior.

Seleccione la pestaña de la consola que esté utilizando.

- [New console](#)
- [Consola antigua](#)

New console

Cómo ver la latencia entre los comprobadores de estado de Route 53 y el punto de conexión

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Comprobaciones de estado.
3. Seleccione el ID vinculado para la comprobación de estado para la que desea ver las métricas. Solo puede ver los datos de latencia de las comprobaciones de estado que monitorizan el estado de un punto de conexión y para las que está habilitada la opción Latency graphs.
4. En el panel inferior, elija la pestaña Métricas.
5. Elija el intervalo de tiempo y la región geográfica de la que desea mostrar los gráficos de latencia.

Los gráficos muestran el estado del intervalo de tiempo especificado:

Tiempo de conexión TCP (solo HTTP y TCP)

El tiempo medio, en milisegundos, que han tardado los comprobadores de estado de Route 53 en la región geográfica seleccionada en establecer una conexión TCP con el punto de conexión.

Tiempo hasta el primer byte (solo HTTP y HTTPS)

El tiempo medio, en milisegundos, que han tardado los comprobadores de estado de Route 53 en la región geográfica seleccionada en recibir el primer byte de la respuesta a una solicitud HTTP o HTTPS.

Tiempo en completar el protocolo de enlace SSL (solo HTTPS)

El tiempo medio, en milisegundos, que han tardado los comprobadores de estado de Route 53 en la región geográfica seleccionada en completar el protocolo SSL/TLS.

6. Para ver una gráfica más grande y especificar una configuración diferente, elija los tres puntos ubicados en la parte superior derecha de la gráfica. Puede cambiar las opciones siguientes:

Estadística

Cambia el cálculo que realiza CloudWatch sobre los datos.

Intervalo de tiempo

Muestra el estado de una comprobación de estado durante un periodo diferente, por ejemplo, por la mañana o la semana pasada.

Periodo

Cambia el intervalo entre puntos de datos del gráfico.

Tenga en cuenta lo siguiente:

- Si acaba de crear una comprobación de estado, es posible que tenga que esperar unos minutos para que aparezcan los datos en el gráfico y para que aparezca la métrica de comprobación de estado en la lista de métricas disponibles.

- El gráfico no se actualiza por su cuenta de forma automática.

Para actualizar la pantalla, elija el icono de actualización



).

- Si se producen errores en las comprobaciones de estado por algún motivo, como tiempo de espera agotado de la conexión, Route 53 no puede medir la latencia y los datos de latencia no se mostrarán en el gráfico durante el período afectado.

Old console

Cómo ver la latencia entre los comprobadores de estado de Route 53 y el punto de conexión

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Health Checks.
3. Seleccione las filas de las comprobaciones de estado correspondientes. Solo puede ver los datos de latencia de las comprobaciones de estado que monitorizan el estado de un punto de conexión y para las que está habilitada la opción Latency graphs.
4. En el panel de abajo, elija la pestaña Latency.
5. Elija el intervalo de tiempo y la región geográfica de la que desea mostrar los gráficos de latencia.

Los gráficos muestran el estado del intervalo de tiempo especificado:

Tiempo de conexión TCP (solo HTTP y TCP)

El tiempo medio, en milisegundos, que han tardado los comprobadores de estado de Route 53 en la región geográfica seleccionada en establecer una conexión TCP con el punto de conexión.

Tiempo hasta el primer byte (solo HTTP y HTTPS)

El tiempo medio, en milisegundos, que han tardado los comprobadores de estado de Route 53 en la región geográfica seleccionada en recibir el primer byte de la respuesta a una solicitud HTTP o HTTPS.

Tiempo en completar el protocolo de enlace SSL (solo HTTPS)

El tiempo medio, en milisegundos, que han tardado los comprobadores de estado de Route 53 en la región geográfica seleccionada en completar el protocolo SSL/TLS.

Note

Si selecciona varias comprobaciones de estado, el gráfico se muestra una línea de código de color independiente para cada una de ellas.

6. Para ver un gráfico más grande y especificar diferentes ajustes, haga clic en el gráfico. Puede cambiar las opciones siguientes:

Estadística

Cambia el cálculo que realiza CloudWatch sobre los datos.

Intervalo de tiempo

Muestra el estado de una comprobación de estado durante un periodo diferente, por ejemplo, por la mañana o la semana pasada.

Periodo

Cambia el intervalo entre puntos de datos del gráfico.

Tenga en cuenta lo siguiente:

- Si acaba de crear una comprobación de estado, es posible que tenga que esperar unos minutos para que aparezcan los datos en el gráfico y para que aparezca la métrica de comprobación de estado en la lista de métricas disponibles.
- El gráfico no se actualiza por su cuenta de forma automática.
Para actualizar la pantalla, elija el icono de actualización



).

- Si se producen errores en las comprobaciones de estado por algún motivo, como tiempo de espera agotado de la conexión, Route 53 no puede medir la latencia y los datos de latencia no se mostrarán en el gráfico durante el período afectado.

Monitorear comprobaciones de estado mediante CloudWatch

Las comprobaciones de estado de Route 53 se integran con las métricas de CloudWatch para que pueda hacer lo siguiente:

- Comprobar que una comprobación de estado está configurada correctamente.
- Revisar el estado de una comprobación de estado durante un periodo de tiempo especificado.
- Configurar CloudWatch para enviar una alerta de Amazon SNS cuando el estado de una comprobación de estado sea incorrecto. Tenga en cuenta que pueden transcurrir varios minutos

entre el momento del error de la comprobación de estado y el momento en que recibe la notificación de SNS asociada.

Para obtener más información, consulte [Cómo determina Amazon Route 53 si la comprobación de estado es correcta](#).

Temas

- [Comprobación del estado de la comprobación de estado](#)
- [Visualización de alarmas de comprobación de estado](#)
- [Cómo ver métricas de comprobación de estado en la consola de CloudWatch](#)
- [Cómo crear una alarma con una notificación de SNS](#)

Comprobación del estado de la comprobación de estado

Note

Estamos en proceso de actualización de la consola de comprobaciones de estado para Route 53. Durante el periodo de transición, puede seguir utilizando la consola anterior.

Seleccione la pestaña de la consola que esté utilizando.

- [New console](#)
- [Consola antigua](#)

New console

Cómo ver el estado de una comprobación de estado

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Comprobaciones de estado.
3. Elija el ID vinculado de la comprobación de estado para la que desea ver las métricas.
4. En el panel inferior, elija la pestaña Métricas.

Los dos gráficos muestran el estado de la última hora en intervalos de un minuto:

Health check status (Estado de la comprobación de estado)

El gráfico muestra la evaluación de Route 53 del estado del punto de conexión. 1 indica estado correcto y 0 indica estado incorrecto.

Health checkers that report the endpoint healthy (%)

En las comprobaciones de estado que monitorean solo un punto de conexión, el gráfico muestra el porcentaje de comprobadores de estado de Route 53 que considera que el estado del punto de conexión seleccionado es correcto.

Cuando se deshabilita una comprobación de estado, esta métrica no está disponible.

Number of healthy child health checks

Para las comprobaciones de estado calculadas únicamente, el gráfico muestra el número de comprobaciones de estado que funcionan bien.

5. Para ver una gráfica más grande y especificar una configuración diferente, elija los tres puntos ubicados en la parte superior derecha y, a continuación, Ampliar. Puede cambiar las opciones siguientes:

Estadística

Cambia el cálculo que realiza CloudWatch sobre los datos.

Intervalo de tiempo

Muestra el estado de una comprobación de estado durante un periodo diferente, por ejemplo, por la mañana o la semana pasada.

Periodo

Cambia el intervalo entre puntos de datos del gráfico.

Tenga en cuenta lo siguiente:

- Si acaba de crear una comprobación de estado, es posible que tenga que esperar unos minutos para que aparezcan los datos en el gráfico y para que aparezca la métrica de comprobación de estado en la lista de métricas disponibles.

- El gráfico no se actualiza por su cuenta de forma automática.
Para actualizar la pantalla, elija el icono de actualización



).

Old console

Cómo ver el estado de una comprobación de estado (consola nueva)

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Health Checks.
3. Elija las filas de las comprobaciones de estado correspondientes.
4. En el panel inferior, elija la pestaña Monitoring.

Los dos gráficos muestran el estado de la última hora en intervalos de un minuto:

Health check status (Estado de la comprobación de estado)

El gráfico muestra la evaluación de Route 53 del estado del punto de conexión. 1 indica estado correcto y 0 indica estado incorrecto.

Health checkers that report the endpoint healthy (%)

En las comprobaciones de estado que monitorean solo un punto de conexión, el gráfico muestra el porcentaje de comprobadores de estado de Route 53 que considera que el estado del punto de conexión seleccionado es correcto.

Cuando se deshabilita una comprobación de estado, esta métrica no está disponible.

Number of healthy child health checks

Para las comprobaciones de estado calculadas únicamente, el gráfico muestra el número de comprobaciones de estado que funcionan bien.

Note

Si ha seleccionado varias comprobaciones de estado, el gráfico se muestra una línea de código de color independiente para cada una de ellas.

5. Para ver un gráfico más grande y especificar diferentes ajustes, haga clic en el gráfico. Puede cambiar las opciones siguientes:

Estadística

Cambia el cálculo que realiza CloudWatch sobre los datos.

Intervalo de tiempo

Muestra el estado de una comprobación de estado durante un periodo diferente, por ejemplo, por la mañana o la semana pasada.

Periodo

Cambia el intervalo entre puntos de datos del gráfico.

Tenga en cuenta lo siguiente:

- Si acaba de crear una comprobación de estado, es posible que tenga que esperar unos minutos para que aparezcan los datos en el gráfico y para que aparezca la métrica de comprobación de estado en la lista de métricas disponibles.
- El gráfico no se actualiza por su cuenta de forma automática. Para actualizar la pantalla, elija el icono de actualización



).

Visualización de alarmas de comprobación de estado

Note

Estamos en proceso de actualización de la consola de comprobaciones de estado para Route 53. Durante el periodo de transición, puede seguir utilizando la consola anterior.

Seleccione la pestaña de la consola que esté utilizando.

- [New console](#)
- [Consola antigua](#)

New console

Cómo ver el estado de alarma de CloudWatch y editar alarmas para Amazon Route 53

1. En el panel de navegación de la consola de Route 53, elija Comprobaciones de estado.
2. Elija el ID vinculado de la comprobación de estado para la que desea ver las alarmas.
3. En la página de detalles, en la parte inferior de la página, elija la pestaña Alarmas.

La lista Alarmas contiene todas las alarmas de Route 53 que ha creado para la comprobación de estado seleccionada.

La columna State muestra el estado actual de cada alarma:

OK (Correcto)

CloudWatch ha acumulado suficientes estadísticas de las comprobaciones de estado de Route 53 para determinar que el punto de conexión no cumple el umbral de alarma.

INSUFFICIENT DATA

CloudWatch no ha acumulado estadísticas suficientes para determinar si el punto de conexión cumple el umbral de alarma. Es el estado inicial de una nueva alarma. El estado de alarma también cambia a INSUFFICIENT DATA (DATOS INSUFICIENTES) si las métricas de CloudWatch no están disponibles o si elimina la comprobación de estado sin eliminar la alarma asociada.

ALARM

CloudWatch ha acumulado estadísticas suficientes de las comprobaciones de estado de Route 53 para determinar que el punto de conexión cumple el umbral de alarma y para enviar una notificación a la dirección de correo electrónico especificada.

4. Para ver una alarma en la consola de CloudWatch, que proporciona información más detallada acerca de la alarma (por ejemplo, un historial de actualizaciones de la alarma y los cambios de estado), elija el nombre vinculado de la alarma. También puede editar la alarma desde la consola de CloudWatch.
5. Para crear una nueva alarma de CloudWatch en la consola de CloudWatch, seleccione [Crear una alarma de CloudWatch](#). Para obtener más información, consulte [Buscar y crear las alarmas recomendadas](#) en la Guía del usuario de CloudWatch.

Old console

Cómo ver el estado de alarma de CloudWatch y editar alarmas para Amazon Route 53

1. En el panel de navegación de la consola de Route 53, elija Health Checks (Comprobaciones de estado).
2. Elija la fila de cualquier comprobación de estado.
3. En el panel de detalles (después de x Health Checks Selected (Comprobaciones de estado seleccionadas)), elija el icono de intercalación correcto ).

La lista CloudWatch Alarms (Alarmas de CloudWatch) contiene todas las alarmas de Route 53 que ha creado usando la cuenta de AWS actual.

La columna State muestra el estado actual de cada alarma:

OK (Correcto

CloudWatch ha acumulado suficientes estadísticas de las comprobaciones de estado de Route 53 para determinar que el punto de conexión no cumple el umbral de alarma.

INSUFFICIENT DATA

CloudWatch no ha acumulado estadísticas suficientes para determinar si el punto de conexión cumple el umbral de alarma. Es el estado inicial de una nueva alarma. El estado de alarma también cambia a INSUFFICIENT DATA (DATOS INSUFICIENTES) si las métricas de CloudWatch no están disponibles o si elimina la comprobación de estado sin eliminar la alarma asociada.

ALARM

CloudWatch ha acumulado estadísticas suficientes de las comprobaciones de estado de Route 53 para determinar que el punto de conexión cumple el umbral de alarma y para enviar una notificación a la dirección de correo electrónico especificada.

4. Para ver o editar la configuración de una alarma, elija el nombre de la alarma.
5. Para ver una alarma en la consola de CloudWatch, que proporciona información más detallada acerca de la alarma (por ejemplo, un historial de actualizaciones de la alarma y los cambios de estado), elija View (Ver) en la columna More Options (Más opciones) de la alarma.

6. Para ver todas las alarmas de CloudWatch que ha creado con la cuenta de AWS actual, incluidas las alarmas de otros servicios de AWS, elija View All CloudWatch Alarms (Ver todas las alarmas de CloudWatch).
7. Para ver todas las métricas de CloudWatch disponibles, incluidas las métricas que la cuenta de AWS actual no está utilizando en este momento, elija View All CloudWatch Metrics (Ver todas las métricas de CloudWatch).

Cómo ver métricas de comprobación de estado en la consola de CloudWatch

Para consultar las métricas de Route 53 en la consola de CloudWatch

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. Cambie la región a US East (N. Virginia) (EE. UU. Este (Norte de Virginia)). Las métricas de Route 53 no están disponibles si selecciona cualquier otra región como la actual.
3. En el panel de navegación, seleccione Métricas.
4. En la pestaña All metrics, elija Route 53.
5. Elija Health Check Metrics.
6. También puede configurar la notificación de SNS en la consola de CloudWatch. Para obtener más información, consulte [Crear alarmas recomendadas](#) en la Guía del usuario de CloudWatch.

Cómo crear una alarma con una notificación de SNS

Note

El siguiente procedimiento se aplica en forma exclusiva a la antigua consola. La nueva consola lo dirige a la consola de CloudWatch para crear alarmas. Para obtener más información, consulte [Buscar y crear las alarmas recomendadas](#) en la Guía del usuario de CloudWatch.

Cómo recibir una notificación de Amazon SNS cuando una comprobación de estado es incorrecta (consola antigua)

1. En el panel de navegación de la consola de Route 53, elija Health Checks (Comprobaciones de estado).
2. Elija la fila de la comprobación de estado correspondiente.
3. En el panel inferior, elija la pestaña Alarms.

En la tabla se enumeran las alarmas que ya ha creado para esta comprobación de estado.

4. Elija Crear alarma.
5. Especifique los siguientes valores:

Nombre de alarma

Ingrese el nombre que desea que muestre Route 53 en la columna Name (Nombre) de la pestaña Alarms (Alarmas).

Alarm description

(Opcional) Escriba una descripción de la alarma. Este valor aparece en la consola de CloudWatch.

Send notification

Elija si desea que Route 53 le envíe una notificación si el estado de la comprobación de estado activa una alarma.

Notification target (solo si "Send notification" es "Yes")

Si desea que CloudWatch envíe una notificación a un tema de SNS existente, elíjalo en la lista.

Si desea que CloudWatch envíe una notificación, pero no a un tema de SNS existente, realice una de las siguientes acciones:

- Si desea que CloudWatch envíe una notificación por correo electrónico: elija New SNS topic (Nuevo tema de SNS) y continúe con este procedimiento.
- Si desea que CloudWatch envíe una notificación por otro método: abra una nueva pestaña del navegador, vaya a la consola de Amazon SNS y cree el tema. A continuación, vuelva a la consola de Route 53, elija el nombre del nuevo tema en la lista Notification target (Destino de la notificación) y continúe con este procedimiento.

Topic name (Nombre de tema) (solo si ha elegido crear un tema de Amazon SNS)

Ingrese el nombre del nuevo tema de Amazon SNS.

Recipient email addresses (Direcciones de correo electrónico de los destinatarios) (solo si ha elegido crear un tema de Amazon SNS nuevo)

Ingrese la dirección de correo electrónico a la que desee que Route 53 envíe una notificación de SNS cuando una comprobación de estado dispare una alarma.

Alarm target

Elija el valor que desee que evalúe Route 53 para esta comprobación de estado:

- Health check status (Estado de la comprobación de estado): los comprobadores de estado de Route 53 informan de que la comprobación de estado es correcta o incorrecta
- Comprobadores de estado que informan de que el punto de conexión está en buen estado (%) (comprobaciones de estado que monitorean solo un punto de conexión): el porcentaje de comprobadores de estado de Route 53 que informan de que el estado de la comprobación de estado es correcto
- Number of healthy child health checks (Número de comprobaciones de estado secundarias correctas) (solo las comprobaciones de estado calculadas): el número de comprobaciones de estado secundarias en una comprobación de estado que informan de que el estado de la comprobación de estado es correcto
- Tiempo de conexión TCP (solo comprobaciones de estado HTTP y TCP): el tiempo en milisegundos que han tardado los comprobadores de estado de Route 53 en establecer una conexión TCP con el punto de conexión.
- Time to complete SSL handshake (Tiempo necesario para completar el protocolo SSL) (solo comprobaciones de estado HTTPS): el tiempo en milisegundos que han tardado los comprobadores de estado de Route 53 en completar el protocolo SSL/TLS
- Time to first byte (Tiempo hasta el primer byte) (solo comprobaciones de estado HTTP y HTTPS): el tiempo en milisegundos que han tardado los comprobadores de estado de Route 53 en recibir el primer byte de la respuesta a una solicitud HTTP o HTTPS

Alarm target

Para los destinos de alarma que se basan en la latencia (TCP connection time (Tiempo de conexión TCP), Time to complete SSL handshake (Tiempo necesario para completar el protocolo SSL), Time to first byte (Tiempo hasta el primer byte)), elija si desea que

CloudWatch calcule la latencia de los comprobadores de estado de Route 53 en una determinada región o en todas las regiones (Global).

Tenga en cuenta que si elige una región, Route 53 solo mide la latencia dos veces por minuto y el número de muestras será menor que si elige todas las regiones. Por consiguiente, hay más probabilidad de valores periféricos. Para evitar notificaciones de alarma falsas, le recomendamos que especifique un mayor número de períodos consecutivos en los que no debe ser correcta la comprobación de estado antes de que CloudWatch le envíe una notificación.

Fulfill condition

Utilice las siguientes opciones de configuración para determinar cuándo debe activar CloudWatch una alarma.

Alarm target	Condición recomendada	Descripción
Health check status (Estado de la comprobación de estado)	Minimum (Mínimo) < 1	Los comprobadores de estado de Route 53 informan de cuándo es incorrecto el estado del punto de conexión.

Alarm target	Condición recomendada	Descripción
Health checkers that report the endpoint healthy (%)	Average (Media) < porcentaje deseado	Comprobadores de estado que monitorean solo un punto de conexión: Route 53 considera que el estado de una comprobación de estado es incorrecto cuando menos del 18 % de los comprobadores de estado informan de que el estado es correcto. No elija Sample Count (Número de muestras) para esta métrica, ya que el rango de los números de muestras puede cambiar a medida que Route 53 agrega más regiones de comprobación de estado. Average (Promedio) siempre representará con exactitud el porcentaje de comprobadores que informan del estado de una comprobación de estado.
Number of healthy child health checks	Minimum (Mínimo) < número deseado de comprobaciones de estado secundarias correctas	La estadística Minimum devuelve el valor más conservador y representa el escenario de peor caso.
TCP connection time	Average > tiempo deseado en milisegundos	Average es un valor más coherente que otras estadísticas.
Time to complete SSL handshake	Average > tiempo deseado en milisegundos	Average es un valor más coherente que otras estadísticas.
Time to first byte	Average > tiempo deseado en milisegundos	Average es un valor más coherente que otras estadísticas.

For at least **x** consecutive periods of **y** minutes/hours/day

Especifique la cantidad de períodos consecutivos que el valor especificado debe cumplir los criterios antes de que Route 53 envíe una notificación. A continuación, especifique la duración del periodo de tiempo.

6. Al elegir Create (Crear), Amazon SNS le envía un correo electrónico con información sobre el nuevo tema de SNS.
7. En el correo electrónico, elija Confirm subscription. Debe confirmar la suscripción para comenzar a recibir notificaciones de CloudWatch.

Uso de DNS Firewall para filtrar el tráfico de DNS saliente

Con Resolver DNS Firewall, puede filtrar y regular el tráfico DNS saliente para su nube privada virtual (VPC). Para ello, cree colecciones reutilizables de reglas de filtrado en grupos de reglas de DNS Firewall, asocie los grupos de reglas a su VPC y, a continuación, monitoree la actividad en los registros y métricas de DNS Firewall. En función de la actividad, puede ajustar el comportamiento de DNS Firewall según corresponda.

El firewall de DNS proporciona protección para sus solicitudes de DNS salientes. VPCs Estas solicitudes se envían a través de VPC Resolver para la resolución de nombres de dominio. Un uso principal de las protecciones de DNS Firewall es ayudar a evitar la filtración de datos DNS. La filtración de datos DNS puede ocurrir cuando un agente malintencionado pone en peligro una instancia de aplicación en su VPC y, a continuación, utiliza la búsqueda DNS para enviar datos fuera de la VPC a un dominio que controla. Con DNS Firewall, puede monitorear y controlar los dominios que las aplicaciones pueden consultar. Puede denegar el acceso a los dominios que sabe que son malos y permitir que pasen el resto de consultas. También puede denegar el acceso a todos los dominios, excepto a aquellos en los que confía explícitamente.

También puede utilizar DNS Firewall para bloquear las solicitudes de resolución a los recursos de zonas alojadas privadas (compartidas o locales), incluidos los nombres de los puntos de enlace de VPC. También puede bloquear las solicitudes de nombres de EC2 instancias de Amazon públicas o privadas.

El firewall de DNS es una función de la resolución de VPC de Route 53 y no requiere ninguna configuración de resolución de VPC adicional para su uso.

AWS Firewall Manager es compatible con DNS Firewall

Puede usar Firewall Manager para configurar y administrar de forma centralizada las asociaciones de grupos de reglas del Firewall DNS para sus VPCs cuentas en AWS Organizations. Firewall Manager añade automáticamente las asociaciones VPCs que entran en el ámbito de aplicación de su política de Firewall Manager DNS Firewall. Para obtener más información, consulte [AWS Firewall Manager](#) la AWS WAF guía para AWS Shield Advanced desarrolladores y la guía para desarrolladores. AWS Firewall Manager

Cómo funciona DNS Firewall con AWS Network Firewall

DNS Firewall y Network Firewall ofrecen filtrado de nombres de dominio, pero para diferentes tipos de tráfico. Con DNS Firewall y Network Firewall juntos, puede configurar el filtrado basado en dominio para el tráfico de la capa de aplicación en dos rutas de red diferentes.

- El firewall de DNS proporciona filtrado para las consultas de DNS salientes que pasan por la resolución de VPC de Route 53 desde las aplicaciones incluidas en su servidor. VPCs También puede configurar DNS Firewall a fin de enviar respuestas personalizadas para las consultas a nombres de dominio bloqueados.
- Network Firewall proporciona filtrado para el tráfico de la red y de la capa de aplicación, pero no tiene visibilidad de las consultas realizadas por Route 53 VPC Resolver.

Para obtener más información sobre Network Firewall, consulte la [Guía para desarrolladores de Network Firewall](#).

Cómo funciona Resolver DNS Firewall

El firewall de DNS de Resolver le permite controlar el acceso a los sitios y bloquear las amenazas a nivel de DNS para las consultas de DNS que se envían desde su VPC a través del Resolver de VPC de Route 53. Con el firewall de DNS, usted define las reglas de filtrado de nombres de dominio en los grupos de reglas que asocia a su VPCs Puede especificar listas de nombres de dominio para permitir o bloquear, o bien reglas avanzadas de Resolver DNS Firewall que ofrecen protección contra las amenazas basadas en los túneles de DNS y los algoritmos de generación de dominios (DGA). Puede personalizar las respuestas a las consultas de DNS que bloquee. En el caso de las reglas que contienen listas de dominios, también puede refinar estas reglas para permitir determinados tipos de consultas, como los registros MX.

DNS Firewall solo filtra por el nombre de dominio. No resuelve ese nombre a una dirección IP que se va a bloquear. Además, DNS Firewall filtra el tráfico de DNS, pero no filtra otros protocolos de capa de aplicación, como HTTPS, SSH, TLS, FTP, entre otros.

Componentes y ajustes del firewall DNS de Resolver

Puede administrar DNS Firewall con los siguientes componentes y configuración centrales.

Grupo de reglas de DNS Firewall

Define una colección, con nombre y reutilizable, de reglas de DNS Firewall para filtrar consultas de DNS. Rellene el grupo de reglas con las reglas de filtrado y, a continuación, asocie el grupo de

reglas a una o más VPCs. Cuando se asocia un grupo de reglas a una VPC, se habilita el filtrado de DNS Firewall en la VPC. A continuación, cuando el Resolver de VPC recibe una consulta de DNS para una VPC que tiene un grupo de reglas asociado, el Resolver de VPC pasa la consulta al Firewall de DNS para que la filtre.

Si asocia varios grupos de reglas a una sola VPC, indicará su orden de procesamiento a través de la configuración de prioridad de cada asociación. DNS Firewall procesa grupos de reglas para una VPC a partir de la configuración de prioridad numérica más baja activada.

Para obtener más información, consulte [Reglas y grupos de reglas de DNS Firewall](#).

Regla de DNS Firewall

Define una regla de filtrado para consultas de DNS en un grupo de reglas de DNS Firewall. Cada regla especifica una lista de dominios o una protección de DNS Firewall y una acción que se debe realizar en relación con las consultas de DNS cuyos dominios coincidan con las especificaciones de dominios de la regla. Puede elegir que las consultas concordantes se acepten (solo en reglas con listas de dominios), se bloqueen, o bien que se emita una alerta sobre ellas. En las reglas con listas de dominios, también puede especificar tipos de consulta para los dominios de la lista; por ejemplo, puede bloquear o permitir un tipo de consulta MX para uno o varios dominios específicos. También se pueden definir respuestas personalizadas para las consultas bloqueadas.

Cuando se trata de reglas de DNS Firewall, solo puede bloquear las consultas coincidentes o alertar sobre ellas.

Cada regla de un grupo de reglas tiene una configuración de prioridad única en dicho grupo. DNS Firewall procesa las reglas en un grupo de reglas a partir de la configuración de prioridad numérica más baja activada.

Las reglas de DNS Firewall solo existen en el contexto del grupo de reglas en el que están definidas. No se puede reutilizar una regla ni hacer referencia a ella con independencia de su grupo de reglas.

Para obtener más información, consulte [Reglas y grupos de reglas de DNS Firewall](#).

Lista de dominios

Define una colección con nombre y reutilizable de especificaciones de dominio para su uso en el filtrado de DNS. Cada regla de un grupo de reglas requiere una lista única de dominios. Puede

optar por especificar los dominios a los que desea permitir el acceso, a los que desea denegar el acceso o una combinación de ambos. Puede crear sus propias listas de dominios y utilizar listas de dominios que se AWS administren por usted.

Para obtener más información, consulte [Listas de dominios del firewall de DNS de Resolver](#).

Configuración de redireccionamiento de dominios (solo listas de dominios)

La configuración de redireccionamiento de dominios le permite configurar una regla de DNS Firewall para inspeccionar todos los dominios de la cadena de redireccionamiento de DNS (predeterminado), como CNAME, DNAME, entre otros, o solo el primer dominio y confiar en el resto. Si decide inspeccionar toda la cadena de redireccionamiento de DNS, debe agregar los dominios subsiguientes a una lista de dominios configurada como PERMITIDA en la regla. Si decide inspeccionar toda la cadena de redireccionamiento de DNS, debe añadir los dominios subsiguientes a una lista de dominios y establecer la acción que desea que lleve a cabo la regla: PERMITIR, BLOQUEAR o ALERTAR.

Para obtener más información, consulte [Configuración de las reglas en DNS Firewall](#).

Tipo de consulta (solo listas de dominios)

La configuración del tipo de consulta le permite configurar una regla de DNS Firewall para filtrar un tipo de consulta de DNS concreto. Si no selecciona un tipo de consulta, la regla se aplica a todos los tipos de consultas de DNS. Por ejemplo, es posible que desee bloquear todos los tipos de consultas de un dominio concreto, pero permitir los registros MX.

Para obtener más información, consulte [Configuración de las reglas en DNS Firewall](#).

Protección de DNS Firewall Advanced

Detecta las consultas de DNS sospechosas en función de las firmas de amenazas conocidas en las consultas de DNS. Cada regla de un grupo de reglas requiere una configuración de protección única de DNS Firewall Advanced. Puede elegir que se proteja de lo siguiente:

- Algoritmos de generación de dominios (DGAs)

DGAs son utilizados por los atacantes para generar una gran cantidad de dominios con los que lanzar ataques de malware.

- Túneles de DNS

Los atacantes utilizan los túneles de DNS para extraer datos del cliente mediante el uso del túnel de DNS sin establecer una conexión de red con el cliente.

- Diccionario (DGA)

Los atacantes DGAs utilizan los diccionarios para generar dominios utilizando palabras del diccionario para evitar ser detectados en las comunicaciones con malware command-and-control.

En una regla de DNS Firewall Advanced, puede elegir entre bloquear las consultas que coincidan con la amenaza o alertar sobre estas. Los algoritmos de protección contra amenazas son gestionados y actualizados por AWS.

Para obtener más información, consulte [Resolver DNS Firewall Advanced](#).

Umbral de confianza (solo con protección de DNS Firewall Advanced)

El umbral de confianza para la protección contra las amenazas del DNS. Debe proporcionar este valor al crear una regla de DNS Firewall Advanced. Los valores del nivel de confianza significan lo siguiente:

- Alto: detecta solo las amenazas mejor corroboradas con una baja tasa de falsos positivos.
- Medio: proporciona un equilibrio entre la detección de amenazas y los falsos positivos.
- Bajo: proporciona la tasa de detección de amenazas más alta, pero también aumenta los falsos positivos.

Para obtener más información, consulte [Configuración de las reglas en DNS Firewall](#).

Asociación entre un grupo de reglas de DNS Firewall y una VPC

Define una protección para una VPC mediante un grupo de reglas de firewall de DNS y habilita la configuración del firewall de DNS de VPC Resolver para la VPC.

Si asocia varios grupos de reglas a una sola VPC, indicará su orden de procesamiento a través de la configuración de prioridades en las asociaciones. DNS Firewall procesa grupos de reglas para una VPC a partir de la configuración de prioridad numérica más baja activada.

Para obtener más información, consulte [Habilitar las protecciones de Resolver DNS Firewall para su VPC](#).

Configuración del firewall DNS para una VPC

Especifica cómo VPC Resolver debe gestionar las protecciones del firewall de DNS a nivel de VPC. Esta configuración está vigente siempre que tenga al menos un grupo de reglas de DNS Firewall asociado a la VPC.

Esta configuración especifica la forma en que Route 53 VPC Resolver gestiona las consultas cuando el firewall de DNS no las filtra. De forma predeterminada, si el Resolver de VPC no recibe una respuesta del firewall de DNS para una consulta, no se cierra y bloquea la consulta.

Para obtener más información, consulte [Configuración de la VPC de DNS Firewall](#).

Supervisión de las acciones del DNS Firewall

Puede utilizar Amazon CloudWatch para supervisar el número de consultas de DNS que filtran los grupos de reglas del firewall de DNS. CloudWatch recopila y procesa datos sin procesar para convertirlos en métricas legibles y prácticamente en tiempo real.

Para obtener más información, consulte [Supervisión de los grupos de reglas de Resolver DNS Firewall con Amazon CloudWatch](#).

Puede usar Amazon EventBridge, un servicio sin servidor que usa eventos para conectar los componentes de la aplicación y crear aplicaciones escalables basadas en eventos.

Para obtener más información, consulte [Administrar los eventos de Resolver DNS Firewall mediante Amazon EventBridge](#).

Cómo filtra Resolver DNS Firewall las consultas de DNS

Cuando un grupo de reglas de firewall de DNS está asociado a la resolución de VPC Route 53 de su VPC, el firewall filtra el siguiente tráfico:

- Consultas de DNS que se originan en esa VPC y que atraviesan el DNS de la VPC.
- Consultas de DNS que pasan a través de los puntos de enlace de Resolver desde recursos locales a la misma VPC que tiene DNS Firewall asociado a su solucionador.

Cuando el Firewall de DNS recibe una consulta de DNS, la filtra mediante los grupos de reglas, las reglas y otros ajustes que haya configurado y envía los resultados a VPC Resolver:

- DNS Firewall evalúa la consulta de DNS con los grupos de reglas asociados a la VPC hasta que encuentre una coincidencia o agote todos los grupos de reglas. DNS Firewall evalúa los grupos de reglas según la prioridad establecida en la asociación, comenzando por la configuración numérica más baja. Para obtener más información, consulte [Reglas y grupos de reglas de DNS Firewall](#) y [Habilitar las protecciones de Resolver DNS Firewall para su VPC](#).

- En cada grupo de reglas, DNS Firewall evalúa la consulta de DNS en relación con la lista de dominios de cada regla o con las protecciones de DNS Firewall Advanced hasta que encuentra una coincidencia o agota todas las reglas. DNS Firewall evalúa las reglas por orden de prioridad, comenzando por la configuración numérica más baja. Para obtener más información, consulte [Reglas y grupos de reglas de DNS Firewall](#).
- Cuando el firewall de DNS encuentra una coincidencia con la lista de dominios de una regla o anomalías identificadas por las protecciones de reglas avanzadas del firewall de DNS, finaliza la evaluación de la consulta y responde a VPC Resolver con el resultado. Si la acción es `Alert`, el firewall de DNS también envía una alerta a los registros configurados del Resolver de VPC. Para obtener más información, consulte [Acciones de regla en DNS Firewall](#), [Listas de dominios del firewall de DNS de Resolver](#) y [Resolver DNS Firewall Advanced](#).
- Si DNS Firewall evalúa todos los grupos de reglas sin encontrar una coincidencia, responde a la consulta de forma normal.

El solucionador de VPC enruta la consulta según la respuesta del firewall de DNS. En el improbable caso de que el firewall de DNS no responda, el solucionador de VPC aplica el modo de error del firewall de DNS configurado por la VPC. Para obtener más información, consulte [Configuración de la VPC de DNS Firewall](#).

Pasos de alto nivel para usar Resolver DNS Firewall

Para implementar el filtrado de Resolver DNS Firewall en su VPC de Amazon Virtual Private Cloud, lleve a cabo los siguientes pasos de alto nivel.

- Definir el enfoque de filtrado, las listas de dominios o las protecciones de DNS Firewall: decida cómo desea filtrar las consultas, identifique las especificaciones de dominio que necesitará y defina la lógica que utilizará para evaluar las consultas. Por ejemplo, puede que quiera permitir todas las consultas excepto las que se encuentran en una lista de dominios incorrectos conocidos. O es posible que desee hacer lo contrario y bloquearlos todos, menos una lista autorizada de dominios; a esto se le llama enfoque de jardín vallado. Puede crear y administrar sus propias listas de especificaciones de dominio aprobadas o bloqueadas y puede usar listas de dominios que se administren por usted. Para proteger el firewall de DNS, puede filtrar las consultas bloqueándolas todas o puede alertar sobre cualquier tráfico de consultas sospechoso a dominios que puedan contener anomalías asociadas a amenazas (DGA, túneles de DNS, DGA de diccionario) para comprobar la configuración del firewall de DNS. Para obtener más información, consulte [Listas de dominios del firewall de DNS de Resolver](#) y [Resolver DNS Firewall Advanced](#).

- Crear un grupo de reglas de firewall: en DNS Firewall, cree un grupo de reglas para filtrar las consultas de DNS de la VPC. Debe crear un grupo de reglas en cada región en la que desee utilizarlo. También puedes separar tu comportamiento de filtrado en más de un grupo de reglas para poder volver a usarlo en varios escenarios de filtrado según tus necesidades. VPCs Para obtener información acerca de los grupos de reglas, consulte [Reglas y grupos de reglas de DNS Firewall](#).
- Agregar y configurar las reglas: agregue una regla al grupo de reglas para cada lista de dominios y comportamiento de filtrado que desee que proporcione el grupo de reglas. Establezca la configuración de prioridades de las reglas para que se procesen en el orden correcto en el grupo de reglas, dando la prioridad más baja a la regla que desee evaluar en primer lugar. Para obtener más información acerca de las reglas, consulte [Reglas y grupos de reglas de DNS Firewall](#).
- Asociar el grupo de reglas a la VPC: para comenzar a utilizar el grupo de reglas de DNS Firewall, asícielo a la VPC. Si utiliza más de un grupo de reglas para la VPC, establezca la prioridad de cada asociación para que los grupos de reglas se procesen en el orden correcto, dando la prioridad más baja al grupo de reglas que desee evaluar en primer lugar. Para obtener más información, consulte [Administrar las asociaciones entre la VPC y el grupo de reglas de Resolver DNS Firewall](#).
- (Opcional) Cambie la configuración del firewall de la VPC: si desea que Route 53 VPC Resolver bloquee las consultas cuando el firewall de DNS no puede devolverles una respuesta, en VPC Resolver, cambie la configuración del firewall de DNS de la VPC. Para obtener más información, consulte [Configuración de la VPC de DNS Firewall](#).

Uso de grupos de reglas del firewall DNS de Resolver en varias regiones

Resolver DNS Firewall es un servicio regional, por lo que los objetos que cree en una AWS región solo están disponibles en esa región. Para usar el mismo grupo de reglas en más de una región, debe crearlo en cada región.

La AWS cuenta que creó un grupo de reglas puede compartirlo con otras AWS cuentas. Para obtener más información, consulte [Compartir los grupos de reglas de Resolver DNS Firewall entre cuentas AWS](#).

Disponibilidad regional para Resolver DNS Firewall

El firewall DNS está disponible en las siguientes ubicaciones: Regiones de AWS

- Africa (Cape Town)

- Asia-Pacífico (Hong Kong)
- Asia-Pacífico (Hyderabad)
- Asia-Pacífico (Yakarta)
- Asia-Pacífico (Malasia)
- Asia-Pacífico (Melbourne)
- Asia-Pacífico (Mumbai)
- Región Asia-Pacífico (Osaka)
- Asia-Pacífico (Seúl)
- Asia-Pacífico (Singapur)
- Asia-Pacífico (Sídney)
- Asia-Pacífico (Tailandia)
- Asia-Pacífico (Tokio)
- Región de Canadá (centro)
- Oeste de Canadá (Calgary)
- Región de Europa (Fráncfort)
- Región de Europa (Irlanda)
- Región de Europa (Londres)
- Europa (Milán)
- Región Europa (París)
- Europa (España)
- Europa (Estocolmo)
- Europa (Zúrich)
- Israel (Tel Aviv)
- México (centro)
- Middle East (Bahrain)
- Medio Oriente (EAU)
- América del Sur (São Paulo)
- Este de EE. UU. (Norte de Virginia)
- Este de EE. UU. (Ohio)

- Oeste de EE. UU. (Norte de California)
- Oeste de EE. UU. (Oregón)
- China (Pekín)
- China (Ningxia)
- AWS GovCloud (US)

Cómo empezar con Resolver DNS Firewall

La consola de DNS Firewall incluye un asistente que le guía por los siguientes pasos para comenzar a utilizar DNS Firewall:

- Cree grupos de reglas para cada conjunto de reglas que desee utilizar.
- Para cada regla, rellene la lista de dominios que desee inspeccionar. Puede crear sus propias listas de dominios y utilizar listas de dominios AWS gestionados.
- Asocie sus grupos de reglas al VPCs lugar donde desee usarlos.

Ejemplo de jardín amurallado de Resolver DNS Firewall

En este tutorial, creará un grupo de reglas que bloqueará todos los dominios menos un grupo exclusivo en el que confíe. A esto se le llama plataforma cerrada o enfoque de jardín vallado.

Configuración de un grupo de reglas de DNS Firewall mediante el asistente de la consola

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.

Seleccione DNS Firewall en el panel de navegación para abrir la página Grupos de regla de DNS Firewall en la consola de Amazon VPC. Continúe en el paso 3.

- O BIEN -

Inicie sesión en Consola de administración de AWS y abra

la consola Amazon VPC que se encuentra debajo. <https://console.aws.amazon.com/vpc/>

2. En el panel de navegación, en DNS Firewall, elija Grupos de regla.
3. En la barra de navegación, elija la región del grupo de reglas.

4. En la página Rule groups (Grupos de reglas), elija Add rule group (Agregar grupo de reglas).
5. Para el nombre del grupo de reglas, ingrese **WalledGardenExample**.

En la sección Etiquetas, puede, de forma opcional, ingresar un par de clave/valor para una etiqueta. Las etiquetas le ayudan a organizar y administrar sus recursos de AWS . Para obtener más información, consulte [Etiquetado de recursos de Amazon Route 53](#).

6. Seleccione Añadir grupo de reglas.
7. En la página de WalledGardenExampledetalles, seleccione la pestaña Reglas y, a continuación, Agregar regla.
8. En el panel Detalles de la regla, ingrese el nombre de la regla **BlockAll**.
9. En el panel Domain list (Lista de dominios), seleccione Add my own domain list (Agregar mi propia lista de dominios).
10. En Choose or create a new domain list (Elegir o crear una nueva lista de dominios), seleccione Create new domain list (Crear una nueva lista de dominios).
11. Introduzca un nombre de lista de dominios y**AllDomains**, a continuación, en el cuadro de texto Introduzca un dominio por línea, introduzca un asterisco:*
12. Para Configuración de redireccionamiento de dominio, acepte la configuración predeterminada y deje en blanco Tipo de consulta (opcional).
13. Para la Acción, seleccione BLOCK y, a continuación, deje la respuesta que se va a enviar en la configuración predeterminada de NODATA.
14. Seleccione Agregar regla. BlockAllLa regla se muestra en la pestaña Reglas de la WalledGardenExamplepágina.
15. En la WalledGardenExamplepágina, elija Agregar regla para agregar una segunda regla a su grupo de reglas.
16. En el panel Detalles de la regla, ingrese el nombre de la regla **AllowSelectDomains**.
17. En el panel Domain list (Lista de dominios), seleccione Add my own domain list (Agregar mi propia lista de dominios).
18. En Choose or create a new domain list (Elegir o crear una nueva lista de dominios), seleccione Create new domain list (Crear una nueva lista de dominios).
19. Ingrese un nombre de lista de dominios **ExampleDomains**.
20. En el cuadro de texto Ingresar un dominio por línea, en la primera línea, ingrese **example.com** y, en la segunda línea, **example.org**.

 Note

Si desea que la regla se aplique también a subdominios, tendrá que agregar esos dominios a la lista. Por ejemplo, para agregar todos los subdominios de `example.com`, agregue `*.example.com` a la lista.

21. Para Configuración de redireccionamiento de dominio, acepte la configuración predeterminada y deje en blanco Tipo de consulta (opcional).
22. Para la Acción, seleccione ALLOW.
23. Elija Add rule (Agregar regla). Ambas reglas se muestran en la pestaña Reglas de la WalledGardenExamplepágina.
24. En la pestaña Reglas de la WalledGardenExamplepágina, puede ajustar el orden de evaluación de las reglas de su grupo de reglas seleccionando el número que aparece en la columna Prioridad y escribiendo un número nuevo. DNS Firewall evalúa las reglas comenzando por la configuración de prioridad más baja, por lo que la regla con la prioridad más baja es la primera en ser evaluada. Para este ejemplo, queremos que DNS Firewall identifique y permita en primer lugar consultas de DNS para la lista de selección de dominios y, a continuación, que bloquee las consultas restantes.

Ajuste la prioridad de la regla para que AllowSelectDomainstenga una prioridad más baja.

Ahora tiene un grupo de reglas que solo permite consultas de dominio específicas. Para empezar a utilizarla, debe asociarla a la ubicación VPCs en la que desee utilizar el comportamiento de filtrado. Para obtener más información, consulte [Administrar las asociaciones entre la VPC y el grupo de reglas de Resolver DNS Firewall](#).

Ejemplo de lista de bloqueos de Resolver DNS Firewall

En este tutorial, creará un grupo de reglas que bloquea los dominios que sabe que son malintencionados. También agregará un tipo de consulta de DNS que esté permitido para los dominios de la lista de bloqueados. El grupo de reglas permite todas las demás solicitudes de DNS salientes a través del solucionador de VPC.

Configuración de una lista de bloqueo de DNS Firewall mediante el asistente de la consola

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/route53/>

Seleccione DNS Firewall en el panel de navegación para abrir la página Grupos de regla de DNS Firewall en la consola de Amazon VPC. Continúe en el paso 3.

- O BIEN -

Inicie sesión en la consola de Amazon VPC Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/vpc/>

2. En el panel de navegación, en DNS Firewall, elija Grupos de regla.
3. En la barra de navegación, elija la región del grupo de reglas.
4. En la página Rule groups (Grupos de reglas), elija Add rule group (Agregar grupo de reglas).
5. Para el nombre del grupo de reglas, ingrese **BlockListExample**.

En la sección Etiquetas, puede, de forma opcional, ingresar un par de clave/valor para una etiqueta. Las etiquetas le ayudan a organizar y administrar sus recursos de AWS . Para obtener más información, consulte [Etiquetado de recursos de Amazon Route 53](#).

6. En la página de BlockListExampledetalles, seleccione la pestaña Reglas y, a continuación, Agregar regla.
7. En el panel Detalles de la regla, ingrese el nombre de la regla **BlockList**.
8. En el panel Domain list (Lista de dominios), seleccione Add my own domain list (Agregar mi propia lista de dominios).
9. En Choose or create a new domain list (Elegir o crear una nueva lista de dominios), seleccione Create new domain list (Crear una nueva lista de dominios).
10. Ingrese un nombre de lista de dominios **MaliciousDomains** y luego, en el cuadro de texto, ingrese los dominios que desea bloquear. Por ejemplo, **example.org**. Ingrese un dominio por línea.

 Note

Si desea que la regla se aplique también a los subdominios, tendrá que agregar esos dominios a la lista. Por ejemplo, para agregar todos los subdominios de example.org, agregue ***.example.org** a la lista.

11. Para Configuración de redireccionamiento de dominio, acepte la configuración predeterminada y deje en blanco Tipo de consulta (opcional).

12. Para la acción, seleccione BLOCK (BLOCK) y, a continuación, deje la respuesta que se va a enviar en la configuración predeterminada de NODATA (NODATA).
13. Elija Add rule (Agregar regla). La regla se muestra en la pestaña Reglas de la BlockListExamplepágina
14. en la pestaña Reglas de la BlockedListExamplepágina, puede ajustar el orden de evaluación de las reglas de su grupo de reglas seleccionando el número que aparece en la columna Prioridad y escribiendo un número nuevo. DNS Firewall evalúa las reglas comenzando por la configuración de prioridad más baja, por lo que la regla con la prioridad más baja es la primera en ser evaluada.

Seleccione y ajuste la prioridad de las reglas para que BlockList se evalúe antes o después de cualquier otra regla que pueda tener. La mayoría de las veces, los dominios malintencionados conocidos deben bloquearse en primer lugar. Es decir, las reglas asociadas con ellos deben tener el número de prioridad más bajo.

15. Para agregar una regla que permita los registros MX para los BlockList dominios, en la página de BlockedListExampledetalles de la pestaña Reglas, selecciona Agregar regla.
16. En el panel Detalles de la regla, ingrese el nombre de la regla **BlockList-allowMX**.
17. En el panel Domain list (Lista de dominios), seleccione Add my own domain list (Agregar mi propia lista de dominios).
18. En Elegir o crear una nueva lista de dominios, seleccione **MaliciousDomains**.
19. Para Configuración de redireccionamiento de dominio, acepte la configuración predeterminada.
20. En la lista Tipo de consulta de DNS, seleccione MX: especifica los servidores de correo.
21. Para la acción, seleccione ALLOW (ALLOW).
22. Elija Add rule (Agregar regla).
23. En la pestaña Reglas de la BlockedListExamplepágina, puede ajustar el orden de evaluación de las reglas de su grupo de reglas seleccionando el número que aparece en la columna Prioridad y escribiendo un número nuevo. DNS Firewall evalúa las reglas comenzando por la configuración de prioridad más baja, por lo que la regla con la prioridad más baja es la primera en ser evaluada.

Seleccione y ajuste la prioridad de las reglas para que BlockList-AllowMx se evalúe antes o después de cualquier otra regla que pueda tener. Como quiere permitir las consultas MX, asegúrese de que la regla BlockList-AllowMx tenga una prioridad inferior a. BlockList

Ahora tiene un grupo de reglas que bloquea consultas de dominios malintencionados específicos; sin embargo, permite un tipo de consulta de DNS específico. Para empezar a utilizarla, asóciela al VPCs lugar en el que desee utilizar el comportamiento de filtrado. Para obtener más información, consulte [Administrar las asociaciones entre la VPC y el grupo de reglas de Resolver DNS Firewall](#).

Reglas y grupos de reglas de DNS Firewall

En esta sección se describen los ajustes que puede configurar para los grupos de reglas y reglas del Firewall de DNS, a fin de definir el comportamiento del Firewall de DNS para usted VPCs. También se describe cómo administrar la configuración de las reglas y los grupos de reglas.

Cuando los grupos de reglas estén configurados según sus preferencias, los puede usar directamente, así como compartirlos y administrarlos, entre cuentas y en toda la organización en AWS Organizations.

- Puede asociar un grupo de reglas a varios VPCs para proporcionar un comportamiento coherente en toda la organización. Para obtener información, consulte [Administrar las asociaciones entre la VPC y el grupo de reglas de Resolver DNS Firewall](#).
- Puede compartir grupos de reglas entre cuentas para obtener una administración coherente de consultas de DNS en toda la organización. Para obtener información, consulte [Compartir los grupos de reglas de Resolver DNS Firewall entre cuentas AWS](#).
- Puede usar grupos de reglas en toda su organización AWS Organizations administrándolos en AWS Firewall Manager políticas. Para obtener información sobre Firewall Manager, consulte [AWS Firewall Manager](#) la AWS WAF guía para AWS Shield Advanced desarrolladores y la guía para desarrolladores. AWS Firewall Manager

Configuración del grupo de reglas en DNS Firewall

Al crear o editar un grupo de reglas de DNS Firewall, debe especificar los siguientes valores:

Name

Un nombre único fácil de recordar que permita encontrar fácilmente un grupo de reglas en el panel.

(Opcional) Descripción

Una breve descripción que proporcione más contexto para el grupo de reglas.

Region

La AWS región que elija al crear el grupo de reglas. Un grupo de reglas creado en una región solo estará disponible en esa región. Para utilizar el mismo grupo de reglas en más de una región, debe crearlo en cada región.

Reglas

El comportamiento de filtrado del grupo de reglas está incluido en sus reglas. Para obtener información, consulte la siguiente sección.

Tags

Especifique una o más claves y los valores correspondientes. Por ejemplo, puede especificar Centro de costos en Key (Clave) y 456 en Value (Valor).

Estas son las etiquetas Administración de facturación y costos de AWS que permiten organizar su AWS factura. Para obtener más información sobre el uso de etiquetas para la asignación de costes, consulte [Uso de etiquetas de asignación de costes](#) en la Guía del usuario de AWS Billing .

Configuración de las reglas en DNS Firewall

Al crear o editar una regla de un grupo de reglas de DNS Firewall, debe especificar los siguientes valores:

Name

Un identificador único de la regla del grupo de reglas.

(Opcional) Descripción

Una breve descripción que proporciona más información acerca de la regla.

Lista de dominios

La lista de dominios que inspecciona la regla. Puede crear y administrar sus propias listas de dominios, o bien puede suscribirse a una lista de dominios que AWS administra automáticamente. Para obtener más información, consulte [Listas de dominios del firewall de DNS de Resolver](#).

Una regla puede contener una lista de dominios o una protección de DNS Firewall Advanced, pero no ambas.

Configuración de redireccionamiento de dominios (solo listas de dominios)

Puede elegir que la regla de DNS Firewall inspeccione únicamente el primer dominio o todos (de forma predeterminada) los dominios de la cadena de redireccionamiento de DNS, como CNAME, DNAME, etc. Si decide inspeccionar todos los dominios, debe añadir los dominios subsiguientes de la cadena de redireccionamiento de DNS a la lista de dominios y establecer la acción que desee que lleve a cabo la regla: ALLOW, BLOCK o ALERT. Para obtener más información, consulte [Componentes y ajustes del firewall DNS de Resolver](#).

Tipo de consulta (solo listas de dominios)

La lista de tipos de consultas de DNS que inspecciona la regla. Los siguientes valores son válidos:

- R: Devuelve una IPv4 dirección.
- AAAA: devuelve una dirección Ipv6.
- CAA: Limita la CAs posibilidad de crear SSL/TLS certificaciones para el dominio.
- CNAME: devuelve otro nombre de dominio.
- DS: registro que identifica la clave de firma del DNSSEC de una zona delegada.
- MX: especifica los servidores de correo.
- NAPTR: Regular-expression-based reescritura de nombres de dominio.
- NS: servidores de nombres autorizados.
- PTR: asigna una dirección IP a un nombre de dominio.
- SOA: registro de inicio de autoridad de la zona.
- SPF: muestra los servidores autorizados a enviar correos electrónicos desde un dominio.
- SRV: valores específicos de la aplicación que identifican a los servidores.
- TXT: verifica los remitentes de correo electrónico y los valores específicos de la aplicación.
- Un tipo de consulta que se define mediante el ID de tipo de DNS, por ejemplo, 28 para AAAA. Los valores deben definirse como TYPE **NUMBER**, donde **NUMBER** pueden estar comprendidos entre 1 y 65334, por ejemplo. TYPE28 Para obtener más información, consulte la sección [Lista de tipos de registros de DNS](#).

Puede crear un tipo de consulta por regla.

 Note

Si configuras una regla de bloqueo de firewall con la acción NXDOMAIN en el tipo de consulta igual a AAAA, esta acción no se aplicará a IPv6 las direcciones sintéticas generadas cuando esté habilitada. DNS64

Protección de DNS Firewall Advanced

Detecta las consultas de DNS sospechosas en función de las firmas de amenazas conocidas en las consultas de DNS. Puede elegir que se proteja de lo siguiente:

- Algoritmos de generación de dominios () DGAs

DGAs son utilizados por los atacantes para generar una gran cantidad de dominios con los que lanzar ataques de malware.

- Túneles de DNS

Los atacantes utilizan los túneles de DNS para extraer datos del cliente mediante el uso del túnel de DNS sin establecer una conexión de red con el cliente.

- Diccionario (DGA)

Los atacantes DGAs utilizan los diccionarios para generar dominios utilizando palabras del diccionario para evitar ser detectados en las comunicaciones con malwarecommand-and-control .

En una regla de DNS Firewall Advanced, puede elegir entre bloquear las consultas que coincidan con la amenaza o alertar sobre estas.

Para obtener más información, vea Para obtener más información, consulte [Resolver DNS Firewall Advanced](#).

Una regla puede contener una protección de DNS Firewall Advanced o una lista de dominios, pero no ambas.

Umbral de confianza (solo con DNS Firewall Advanced)

El umbral de confianza para DNS Firewall Advanced. Debe proporcionar este valor al crear una regla de DNS Firewall Advanced. Los valores del nivel de confianza significan lo siguiente:

- Alto: detecta solo las amenazas mejor corroboradas con una baja tasa de falsos positivos.

- Medio: proporciona un equilibrio entre la detección de amenazas y los falsos positivos.
- Bajo: proporciona la tasa de detección de amenazas más alta, pero también aumenta los falsos positivos.

Para obtener más información, consulte [Configuración de las reglas en DNS Firewall](#).

Action

Cómo desea que DNS Firewall gestione una consulta de DNS cuyo nombre de dominio coincida con las especificaciones de la lista de dominios de la regla. Para obtener más información, consulte [Acciones de regla en DNS Firewall](#).

Priority (Prioridad)

Configuración única de entero positivo para la regla del grupo de reglas que determina el orden de procesamiento. DNS Firewall inspecciona las consultas de DNS en las reglas de un grupo de reglas, comenzando por la configuración de prioridad numérica más baja y aumentando esta prioridad. Puede cambiar la prioridad de una regla en cualquier momento; por ejemplo, para cambiar el orden de procesamiento o dejar espacio para otras reglas.

Acciones de regla en DNS Firewall

Cuando DNS Firewall encuentra una coincidencia entre una consulta de DNS y una especificación de dominio en una regla, aplica a la consulta la acción especificada en la regla.

Se le pide que especifique una de las opciones siguientes en cada regla que cree:

- Allow— Deja de inspeccionar la consulta y deja que se complete. No está disponible para DNS Firewall Advanced.
- Alert— Deje de inspeccionar la consulta, deje que se realice y registre una alerta para la consulta en los registros de VPC Resolver de Route 53.
- Block— Interrumpa la inspección de la consulta, impida que vaya al destino previsto y registre la acción de bloqueo de la consulta en los registros de VPC Resolver de Route 53.

Responda con la respuesta de bloqueo configurada, a partir de lo siguiente:

- NODATA— Responda indicando que la consulta se ha realizado correctamente, pero no hay ninguna respuesta disponible para ella.
- NXDOMAIN— Responda indicando que el nombre de dominio de la consulta no existe.

- **OVERRIDE**— Proporcione una anulación personalizada en la respuesta. Esta opción requiere los siguientes ajustes adicionales:
 - **Record value**— El registro DNS personalizado que se devolverá en respuesta a la consulta.
 - **Record type**— El tipo de registro DNS. Esto determina el formato del valor del registro. Debe ser CNAME.
 - **Time to live in seconds**— El tiempo recomendado para que la resolución de DNS o el navegador web almacenen en caché el registro de anulación y lo utilicen en respuesta a esta consulta, si se vuelve a recibir. De forma predeterminada, es cero y el registro no se almacena en caché.

Para obtener más información acerca de la configuración de registros de consulta y el contenido, consulte [Registro de consultas de Resolver](#) y [Valores que aparecen en los registros de consultas de VPC Resolver](#).

Use Alert para probar las reglas de bloqueo

Cuando cree por primera vez una regla de bloqueo, puede probarla configurándola con la acción establecida en Alert. A continuación, puede examinar el número de consultas sobre las que avisa la regla para ver cuántas se bloquearían si establece la acción en Block.

Administración de reglas y grupos de reglas en DNS Firewall

Para administrar reglas y grupos de reglas en la consola, siga las instrucciones de esta sección.

Cuando realiza cambios en las entidades de DNS Firewall, como reglas y listas de dominios, DNS Firewall propaga los cambios en todos los lugares donde se almacenan y utilizan las entidades. Los cambios se aplican en cuestión de segundos, pero puede haber un breve período de incoherencia en el que los cambios hayan llegado en algunos lugares y en otros no. Por ejemplo, si agrega un dominio a una lista de dominios a la que hace referencia una regla de bloqueo, es posible que el nuevo dominio se bloquee brevemente en un área de la VPC pero se permita en otra. Esta incoherencia temporal puede producirse al configurar por primera vez el grupo de reglas y asociaciones de VPC, y al cambiar la configuración existente. Generalmente, las incoherencias de este tipo duran solo unos segundos.

Creación de reglas y de un grupo de reglas

Para crear un grupo de reglas y añadirle reglas, siga los pasos de este procedimiento.

Creación de un grupo de reglas y sus reglas

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.

Seleccione DNS Firewall en el panel de navegación para abrir la página Grupos de regla de DNS Firewall en la consola de Amazon VPC. Continúe en el paso 3.

- O BIEN -

Inicie sesión en la Consola de administración de AWS y abra la

la consola Amazon VPC que se encuentra debajo. <https://console.aws.amazon.com/vpc/>

2. En el panel de navegación, en DNS Firewall, elija Grupos de regla.
3. En la barra de navegación, elija la región del grupo de reglas.
4. Elija Add rule group (Agregar grupo de reglas) y, a continuación, siga las instrucciones del asistente para especificar la configuración de la regla y del grupo de reglas.

Para obtener información acerca de los valores de los grupos de reglas, consulte [Configuración del grupo de reglas en DNS Firewall](#).

Para obtener información acerca de los valores para las reglas, consulte [Configuración de las reglas en DNS Firewall](#).

Visualización y actualización de reglas y de un grupo de reglas

Utilice el siguiente procedimiento para ver los grupos de reglas y las reglas que se les han asignado. También puede actualizar el grupo de reglas y la configuración de reglas.

Visualización y actualización de un grupo de reglas

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.

Seleccione DNS Firewall en el panel de navegación para abrir la página Grupos de regla de DNS Firewall en la consola de Amazon VPC. Continúe en el paso 3.

- O BIEN -

Inicie sesión en la Consola de administración de AWS y abra la

la consola Amazon VPC que se encuentra debajo. <https://console.aws.amazon.com/vpc/>

2. En el panel de navegación, en DNS Firewall, elija Grupos de regla.
3. En la barra de navegación, elija la región del grupo de reglas.
4. Seleccione el grupo de reglas que desea ver o editar y, a continuación, elija View details (Ver detalles).
5. En la página del grupo de reglas puede ver y editar la configuración.

Para obtener información acerca de los valores de los grupos de reglas, consulte [Configuración del grupo de reglas en DNS Firewall](#).

Para obtener información acerca de los valores para las reglas, consulte [Configuración de las reglas en DNS Firewall](#).

Eliminación de un grupo de reglas

Para eliminar un grupo de reglas, realice el procedimiento siguiente.

Important

Si elimina un grupo de reglas asociado a una VPC, DNS Firewall quita la asociación y detiene las protecciones que el grupo de reglas estaba proporcionando a la VPC.

Eliminación de entidades de DNS Firewall

Cuando elimina una entidad que puede usar en DNS Firewall, como una lista de dominios que podría estar en uso en un grupo de reglas, o un grupo de reglas que podría estar asociado a una VPC, DNS Firewall verifica si la entidad se está utilizando actualmente. Si descubre que está en uso, DNS Firewall le avisa. DNS Firewall casi siempre sabe determinar si alguna entidad está en uso. No obstante, es posible que en algunos casos no consiga hacerlo. Si tiene que asegurarse de que no hay nada que esté utilizando actualmente la entidad, verifique las configuraciones de DNS Firewall antes de eliminarla. Si la entidad es una lista de dominios a la que se hace referencia, verifique que ningún grupo de reglas la esté utilizando. Si la entidad es un grupo de reglas, compruebe que no esté asociada a ninguno VPCs.

Para eliminar un grupo de reglas:

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.

Seleccione DNS Firewall en el panel de navegación para abrir la página Grupos de regla de DNS Firewall en la consola de Amazon VPC. Continúe en el paso 3.

- O BIEN -

Inicie sesión en la Consola de administración de AWS y abra la

la consola Amazon VPC que se encuentra debajo. <https://console.aws.amazon.com/vpc/>

2. En el panel de navegación, en DNS Firewall, elija Grupos de regla.
3. En la barra de navegación, elija la región del grupo de reglas.
4. Seleccione el grupo de reglas que desee eliminar y, a continuación, seleccione Eliminar y confirme la eliminación.

Listas de dominios del firewall de DNS de Resolver

Una lista de dominios es un conjunto reutilizable de especificaciones de dominio que se utiliza en una regla de DNS Firewall, dentro de un grupo de reglas. Al asociar un grupo de reglas a una VPC, DNS Firewall compara las consultas de DNS con las listas de dominios que se utilizan en las reglas. Si encuentra una coincidencia, gestiona la consulta de DNS según la acción de la regla coincidente. Para obtener más información acerca de las reglas y los grupos de reglas, consulte [Reglas y grupos de reglas de DNS Firewall](#).

Las listas de dominios le permiten separar las especificaciones de dominio explícitas de las acciones que desea realizar sobre ellas. Puede utilizar una sola lista de dominios en varias reglas; cualquier actualización que realice en la lista de dominios afectará automáticamente a todas las reglas que la utilicen.

Las listas de dominios se dividen en dos categorías principales:

- Listas de dominios gestionadas, que se AWS crean y mantienen por ti.
- Sus propias listas de dominios, que crea y mantiene por su cuenta.

En esta sección se describen los tipos de listas de dominios administrados que están disponibles y se proporciona orientación para crear y administrar sus propias listas de dominios, si así lo decide.

Listas de dominios administrados

Las listas de dominios gestionados contienen nombres de dominio asociados a actividades maliciosas u otras amenazas potenciales. AWS mantiene estas listas para permitir que los clientes de Route 53 VPC Resolver comprueben las consultas de DNS salientes de forma gratuita cuando utilizan el firewall de DNS.

Mantenerse al día del panorama de amenazas en constante cambio puede resultar lento y costoso. Las listas de dominios gestionadas pueden ahorrarle tiempo a la hora de implementar y utilizar el firewall de DNS. AWS actualiza automáticamente las listas cuando aparecen nuevas vulnerabilidades y amenazas. AWS suele recibir notificaciones de nuevas vulnerabilidades antes de que se divulguen públicamente, por lo que DNS Firewall puede implementar medidas de mitigación por usted con frecuencia antes de que se dé a conocer ampliamente una nueva amenaza.

Las listas de dominios administradas están diseñadas para ayudarlo a protegerse de las amenazas web más comunes y agregan otra capa de seguridad para las aplicaciones. Las listas de dominios AWS gestionados obtienen sus datos tanto de AWS fuentes internas como de fuentes externas [RecordedFuture](#), y se actualizan continuamente. Sin embargo, las listas de dominios AWS gestionados no pretenden sustituir a otros controles de seguridad Amazon GuardDuty, como los que se determinan en función de los AWS recursos que seleccione.

Como práctica recomendada, pruebe una lista de dominios administrados en un entorno que no sea de producción antes de usarlo en producción, con la acción de la regla establecida en `Alert`. Evalúe la regla mediante CloudWatch métricas de Amazon combinadas con solicitudes muestreadas de Resolver DNS Firewall o registros de DNS Firewall. Cuando la regla haga lo que quería, cambie la configuración de la acción según sea necesario.

Listas de dominios AWS gestionados disponibles

En esta sección se describen las listas de dominios administrados por que están disponibles actualmente. Cuando se encuentra en una región en la que se admiten estas listas, las ve en la consola cuando administra listas de dominios y cuando especifica la lista de dominios para una regla. En los registros, la lista de dominios se registra en el elemento `firewall_domain_list_id` field.

AWS proporciona las siguientes listas de dominios gestionados, en las regiones en las que están disponibles, para todos los usuarios de Resolver DNS Firewall.

- `AWSManagedDomainsMalwareDomainList`: dominios asociados al envío, alojamiento o distribución de malware.
- `AWSManagedDomainsBotnetCommandandControl`: dominios asociados al control de redes de ordenadores infectados con malware de envío de spam.
- `AWSManagedDomainsAggregateThreatList`— Dominios asociados a varias categorías de amenazas para el DNS, como el malware, el ransomware, las redes de bots, el spyware y los túneles de DNS, para ayudar a bloquear varios tipos de amenazas. `AWSManagedDomainsAggregateThreatList` incluye todos los dominios de las demás listas de dominios AWS gestionados que se indican aquí.
- `AWSManagedDomainsAmazonGuardDutyThreatList`— Dominios asociados a los hallazgos de seguridad de Amazon GuardDuty DNS. Los dominios provienen únicamente de los sistemas GuardDuty de inteligencia de amenazas de la empresa y no contienen dominios procedentes de fuentes externas de terceros. Más específicamente, actualmente esta lista solo bloquea los dominios que se generan internamente y se utilizan para realizar las siguientes detecciones en GuardDuty: `Impact:EC2/AbusedDomainRequest.Reputation`, `Impact:EC2/BitcoinDomainRequest.Reputation`, `Impact:EC2/MaliciousDomainRequest.Reputation`, `Runtime/AbusedDomainRequest.Reputation`, `Impact:Runtime/BitcoinDomainRequest.Reputation`, and `Impact:Runtime/MaliciousDomainRequest`

Para obtener más información, consulta [Búsqueda de tipos](#) en la Guía del GuardDuty usuario de Amazon.

AWS Las listas de dominios gestionados no se pueden descargar ni consultar. Para proteger la propiedad intelectual, no puedes ver ni editar las especificaciones de los dominios individuales de una lista de dominios AWS gestionados. Esta restricción también permite impedir que usuarios malintencionados diseñen amenazas que eludan específicamente las listas publicadas.

Cómo probar las listas de dominios administradas

Proporcionamos el siguiente conjunto de dominios para probar las listas de dominios administradas:

`AWSManagedDomainsBotnetCommandandControl`

- `controldomain1.botnetlist.firewall.route53resolver.us-east-1.amazonaws.com`
- `controldomain2.botnetlist.firewall.route53resolver.us-east-1.amazonaws.com`
- `controldomain3.botnetlist.firewall.route53resolver.us-east-1.amazonaws.com`

AWSManagedDomainsMalwareDomainList

- controldomain1.malwarelist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain2.malwarelist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain3.malwarelist.firewall.route53resolver.us-east-1.amazonaws.com

AWSManagedDomainsAggregateThreatList y AWSManaged DomainsAmazonGuardDutyThreatList

- controldomain1.aggregatelist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain2.aggregatelist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain3.aggregatelist.firewall.route53resolver.us-east-1.amazonaws.com

Estos dominios pasarán a ser 1.2.3.4 si no están bloqueados. Si utiliza las listas de dominios administradas en una VPC, si se consulta estos dominios, la respuesta que se obtendrá es que se ha establecido una acción de bloqueo en la regla (por ejemplo, NODATA).

Para obtener más información sobre las listas de dominios administrados, contacte con el [Centro de AWS Support](#).

En la siguiente tabla se muestra la disponibilidad regional de las listas de dominios AWS gestionados.

Disponibilidad por región de la lista de dominios administradas

Region	¿Hay disponibilidad de las listas de dominios administrados?
África (Ciudad del Cabo)	Sí
Asia-Pacífico (Hong Kong)	Sí
Asia-Pacífico (Hyderabad)	Sí
Asia-Pacífico (Yakarta)	Sí
Asia-Pacífico (Malasia)	Sí
	Sí

Region	¿Hay disponibilidad de las listas de dominios administrados?
Asia-Pacífico (Melbourne)	
Asia-Pacífico (Mumbai)	Sí
Región Asia-Pacífico (Osaka)	Sí
Asia-Pacífico (Seúl)	Sí
Asia-Pacífico (Singapur)	Sí
Asia-Pacífico (Sídney)	Sí
Asia-Pacífico (Tailandia)	Sí
Asia-Pacífico (Tokio)	Sí
Región de Canadá (centro)	Sí
Oeste de Canadá (Calgary)	Sí
Región de Europa (Fráncfort)	Sí
Región de Europa (Irlanda)	Sí
Región de Europa (Londres)	Sí
Europa (Milán)	Sí

Region	¿Hay disponibilidad de las listas de dominios administrados?
Región Europa (París)	Sí
Europa (España)	Sí
Europa (Estocolmo)	Sí
Europa (Zúrich)	Sí
Israel (Tel Aviv)	Sí
Medio Oriente (Baréin)	Sí
Medio Oriente (EAU)	Sí
América del Sur (São Paulo)	Sí
EE. UU. Este (Norte de Virginia)	Sí
EE. UU. Este (Ohio)	Sí
EE. UU Oeste (Norte de California)	Sí
Oeste de EE. UU. (Oregón)	Sí
China (Pekín)	Sí
China (Ningxia)	Sí

Region	¿Hay disponibilidad de las listas de dominios administrados?
AWS GovCloud (US)	Sí

Consideraciones adicionales de seguridad

AWS Las listas de dominios gestionados están diseñadas para ayudarle a protegerse de las amenazas web más comunes. Cuando se utilizan de acuerdo con la documentación, estas listas agregan otra capa de seguridad a sus aplicaciones. No obstante, las listas de dominios administrados por no están destinadas a reemplazar otros controles de seguridad, que vienen determinados por los recursos de AWS que seleccione. Para garantizar que sus recursos AWS estén debidamente protegidos, consulte la guía del [Modelo de responsabilidad compartida](#).

Mitigación de escenarios falsos positivos

Si encuentra escenarios de falsos positivos en reglas que utilizan listas de dominios administrados por para bloquear consultas, realice los siguientes pasos:

1. En los registros de VPC Resolver, identifique el grupo de reglas y la lista de dominios administrados que están causando el falso positivo. Para ello, busque el registro de la consulta que DNS Firewall está bloqueando y que desea permitir. La entrada de registro muestra el grupo de reglas, la acción de la regla y la lista administrada. Para obtener información acerca de los registros, consulte [Valores que aparecen en los registros de consultas de VPC Resolver](#).
2. Cree una regla en el grupo de reglas que permita de forma explícita la consulta bloqueada. Al crear la regla, puede definir su propia lista de dominios con solo la especificación de dominio que desea permitir. Siga las instrucciones para la administración de reglas y grupos de reglas en [Creación de reglas y de un grupo de reglas](#).
3. Dé prioridad a la nueva regla dentro del grupo de reglas para que se ejecute antes de la regla que utiliza la lista administrada. Para ello, asigne a la nueva regla un valor de prioridad numérica más bajo.

Cuando haya actualizado el grupo de reglas, la nueva regla permitirá de forma explícita el nombre de dominio que desea permitir antes de que se ejecute la regla de bloqueo.

Administración de sus propias listas de dominios

Puede crear sus propias listas de dominios para especificar categorías de dominios que no encuentre en las ofertas de listas de dominios administrados o para gestionarlos por su cuenta, si así lo prefiere.

Además de los procedimientos descritos en esta sección, en la consola, al crear o actualizar una regla, puede crear una lista de dominios en el contexto de la administración de reglas de Resolver DNS Firewall.

Cada especificación de dominio en la lista de dominios debe cumplir los siguientes requisitos:

- Opcionalmente, puede comenzar por * (asterisco).
- Con la excepción del asterisco inicial opcional y de un punto, como delimitador entre etiquetas, solo debe contener los siguientes caracteres: A-Z, a-z 0-9, - (guión).
- Debe tener una longitud de entre 1 y 255 caracteres.

Cuando realiza cambios en las entidades de DNS Firewall, como reglas y listas de dominios, DNS Firewall propaga los cambios en todos los lugares donde se almacenan y utilizan las entidades. Los cambios se aplican en cuestión de segundos, pero puede haber un breve período de incoherencia en el que los cambios hayan llegado en algunos lugares y en otros no. Por ejemplo, si agrega un dominio a una lista de dominios a la que hace referencia una regla de bloqueo, es posible que el nuevo dominio se bloquee brevemente en un área de la VPC pero se permita en otra. Esta incoherencia temporal puede producirse al configurar por primera vez el grupo de reglas y asociaciones de VPC, y al cambiar la configuración existente. Generalmente, las incoherencias de este tipo duran solo unos segundos.

Prueba de la lista de dominios antes de su uso en producción

Como práctica recomendada, pruebe una lista de dominios en un entorno que no sea de producción antes de usarlo en producción, con la acción de la regla establecida en Alert. Evalúe la regla con CloudWatch las métricas de Amazon y los registros de VPC Resolver. Los registros proporcionan el nombre de la lista de dominios de todas las alertas y acciones de bloqueo. Cuando la lista de dominios coincida con las consultas de DNS de acuerdo con sus preferencias, cambie la configuración de la acción de la regla según sea necesario. Para obtener información sobre CloudWatch las métricas y los registros de consultas, consulte [Supervisión de los grupos de reglas de Resolver DNS Firewall con Amazon CloudWatch](#) Valores que aparecen en los registros

[de consultas de VPC Resolver](#), y [Administración de configuraciones de registro de consultas de Resolver](#).

Incorporación de una lista de dominios

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.

Seleccione DNS Firewall en el panel de navegación para abrir la página Grupos de regla de DNS Firewall en la consola de Amazon VPC. Continúe en el paso 2.

- O BIEN -

Inicie sesión en la Consola de administración de AWS y abra la

la consola Amazon VPC que se encuentra debajo. <https://console.aws.amazon.com/vpc/>

2. En el panel de navegación, en DNS Firewall, elija Listas de dominios. En la página Domain lists (Listas de dominios), puede seleccionar y editar listas de dominios existentes y agregar las suyas propias.
3. Para agregar una lista de dominios, elija Add domain list (Agregar lista de dominios).
4. Proporcione un nombre para la lista de dominios y, a continuación, ingrese las especificaciones de dominio en el cuadro de texto, uno por línea.

Si desliza Switch to bulk upload (Cambiar a la carga masiva) a on (activado), ingrese el URI del bucket de Amazon S3 en el que haya creado una lista de dominios. Esta lista de dominios debe tener un nombre de dominio por línea.

Note

Los nombres de dominio duplicados provocarán un error en la importación masiva.

5. Elija Add domain list (Agregar lista de dominios). La página Domain lists (Listas de dominios) muestra la nueva lista de dominios.

Después de crear la lista de dominios, puede hacer referencia a ella por nombre desde las reglas de DNS Firewall.

Eliminación de entidades de DNS Firewall

Cuando elimina una entidad que puede usar en DNS Firewall, como una lista de dominios que podría estar en uso en un grupo de reglas, o un grupo de reglas que podría estar asociado a una VPC, DNS Firewall verifica si la entidad se está utilizando actualmente. Si descubre que está en uso, DNS Firewall le avisa. DNS Firewall casi siempre sabe determinar si alguna entidad está en uso. No obstante, es posible que en algunos casos no consiga hacerlo. Si tiene que asegurarse de que no hay nada que esté utilizando actualmente la entidad, verifique las configuraciones de DNS Firewall antes de eliminarla. Si la entidad es una lista de dominios a la que se hace referencia, verifique que ningún grupo de reglas la esté utilizando. Si la entidad es un grupo de reglas, compruebe que no esté asociada a ninguna VPCs.

Eliminación de una lista de dominios

1. En el panel de navegación, elija Domain lists (Listas de dominios).
2. En la barra de navegación, elija la región de la lista de dominios.
3. Seleccione la lista de dominios que desee eliminar y, a continuación, elija Eliminar y confirme la eliminación.

Resolver DNS Firewall Advanced

DNS Firewall Advanced detecta las consultas de DNS sospechosas en función de las firmas de amenazas conocidas en las consultas de DNS. Puede especificar un tipo de amenaza en una regla que utiliza en una regla de DNS Firewall, dentro de un grupo de reglas. Al asociar un grupo de reglas a una VPC, DNS Firewall compara las consultas de DNS con los dominios que se marcan en las reglas. Si encuentra una coincidencia, gestiona la consulta de DNS según la acción de la regla coincidente.

DNS Firewall Advanced identifica las firmas de amenazas del DNS sospechosas mediante la inspección de una serie de identificadores clave en la carga útil del DNS, como la marca horaria de las solicitudes, la frecuencia de las solicitudes y las respuestas, las cadenas de consulta de DNS y la longitud, el tipo o el tamaño de las consultas de DNS entrantes y salientes. Según el tipo de firma de la amenaza, puede configurar políticas para bloquear la consulta o simplemente registrarla y alertar sobre ella. Si utiliza un conjunto ampliado de identificadores de amenazas, puede protegerse contra las amenazas del DNS procedentes de fuentes de dominio que tal vez aún no estén clasificadas por las fuentes de inteligencia de amenazas mantenidas por la comunidad de seguridad en general.

En la actualidad, DNS Firewall Advanced ofrece protección contra:

- Algoritmos de generación de dominios (DGAs)

DGAs son utilizados por los atacantes para generar una gran cantidad de dominios con los que lanzar ataques de malware.

- Túneles de DNS

Los atacantes utilizan los túneles de DNS para extraer datos del cliente mediante el uso del túnel de DNS sin establecer una conexión de red con el cliente.

- Diccionario (DGA)

Los atacantes DGAs utilizan los diccionarios para generar dominios utilizando palabras del diccionario para evitar ser detectados en las comunicaciones con malware command-and-control.

Para obtener información acerca de cómo crear reglas, consulte [Creación de reglas y de un grupo de reglas](#) y [Configuración de las reglas en DNS Firewall](#).

Mitigación de escenarios falsos positivos

Si encuentra escenarios de falsos positivos en reglas que utilizan protecciones de DNS Firewall Advanced para bloquear consultas, realice los siguientes pasos:

1. En los registros de VPC Resolver, identifique el grupo de reglas y las protecciones avanzadas del firewall de DNS que están causando el falso positivo. Para ello, busque el registro de la consulta que DNS Firewall está bloqueando y que desea permitir. La entrada del registro muestra el grupo de reglas, la acción de la regla y la protección de DNS Firewall Advanced. Para obtener información acerca de los registros, consulte [Valores que aparecen en los registros de consultas de VPC Resolver](#).
2. Cree una regla en el grupo de reglas que permita de forma explícita la consulta bloqueada. Al crear la regla, puede definir su propia lista de dominios con solo la especificación de dominio que desea permitir. Siga las instrucciones para la administración de reglas y grupos de reglas en [Creación de reglas y de un grupo de reglas](#).
3. Dé prioridad a la nueva regla dentro del grupo de reglas para que se ejecute antes de la regla que utiliza la lista administrada. Para ello, asigne a la nueva regla un valor de prioridad numérica más bajo.

Cuando haya actualizado el grupo de reglas, la nueva regla permitirá de forma explícita el nombre de dominio que desea permitir antes de que se ejecute la regla de bloqueo.

Configuración de registros para DNS Firewall

Puede evaluar las reglas del firewall de DNS mediante las CloudWatch métricas de Amazon y los registros de consultas de Resolver. Los registros proporcionan el nombre de la lista de dominios de todas las alertas y acciones de bloqueo. Para obtener más información sobre Amazon CloudWatch, consulte [Supervisión de los grupos de reglas de Resolver DNS Firewall con Amazon CloudWatch](#).

Cuando habilite DNS Firewall, asócielo a una VPC y tenga habilitado el registro; `firewall_rule_group_id`, `firewall_rule_action` y `firewall_domain_list_id` son los campos específicos de DNS Firewall que se proporcionan en los registros.

Note

Los registros de consultas mostrarán los campos adicionales de DNS Firewall solo para las consultas bloqueadas por las reglas de DNS Firewall.

Para empezar a registrar las consultas de DNS filtradas por las reglas del firewall de DNS que se originan en su VPCs, realice las siguientes tareas en la consola de Amazon Route 53:

Configuración del registro de consultas de Resolver para DNS Firewall

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. Expanda el menú de la consola de Route 53. En la esquina superior izquierda de la consola, elija el icono de las tres barras horizontales ().
3. En el menú Resolver, elija Registro de consultas.
4. En el selector de regiones, elija la AWS región en la que desee crear la configuración de registro de consultas.

Debe ser la misma región en la que creó la VPCs que está asociada al firewall de DNS para la que desea registrar las consultas. Si está VPCs en varias regiones, debe crear al menos una configuración de registro de consultas para cada región.

5. Elija Configure query logging (Configuración del registro de consultas).
6. Especifique los siguientes valores:

Nombre de configuración del registro de consultas

Ingrese un nombre para la configuración del registro de consultas. El nombre aparece en la consola en la lista de configuraciones del registro de consultas. Ingrese un nombre que le ayude a encontrar esta configuración más tarde.

Destino de los registros de consulta

Elija el tipo de AWS recurso al que quiere que VPC Resolver envíe los registros de consultas. Para obtener información sobre cómo elegir entre las opciones (grupo de CloudWatch registros, depósito S3 y transmisión de entrega Firehose), consulte [AWS recursos a los que puede enviar registros de consultas de VPC Resolver](#)

Tras elegir el tipo de recurso, puede crear otro recurso de ese tipo o elegir un recurso existente creado por la AWS cuenta corriente.

Note

Solo puede elegir recursos que se hayan creado en la región de AWS que eligió en el paso 4, la región donde está creando la configuración del registro de consultas. Si decide crear un recurso nuevo, ese recurso se creará en la misma región.

VPCs para registrar consultas para

Esta configuración de registro de consultas registrará las consultas de DNS que se originen en el VPCs que elija. Marque la casilla de verificación de cada VPC de la región actual en la que desee que VPC Resolver registre las consultas y, a continuación, seleccione Elegir.

Note

La entrega de registros de VPC solo se puede habilitar una vez para un tipo de destino específico. Los registros no se pueden entregar a varios destinos del mismo tipo. Por ejemplo, los registros de VPC no se pueden entregar a dos destinos de Amazon S3.

7. Elija Configure query logging (Configuración del registro de consultas).

 Note

Debe comenzar a ver consultas de DNS realizadas por los recursos de su VPC en los registros unos minutos después de crear correctamente la configuración del registro de consultas.

Compartir los grupos de reglas de Resolver DNS Firewall entre cuentas AWS

Puede compartir grupos de reglas de DNS Firewall entre AWS cuentas. Para compartir grupos de reglas, usa AWS Resource Access Manager (AWS RAM). La consola de DNS Firewall se integra con la AWS RAM consola. Para obtener más información al respecto AWS RAM, consulte la [Guía del usuario de Resource Access Manager](#).

Tenga en cuenta lo siguiente:

Asociar grupos de reglas compartidos a VPCs

Si otra AWS cuenta ha compartido un grupo de reglas con la suya, puede asociarlo a VPCs la suya del mismo modo que asocia los grupos de reglas que ha creado. Para obtener más información, consulte [Administrar las asociaciones entre la VPC y el grupo de reglas de Resolver DNS Firewall](#).

Eliminación o anulación de uso compartido de un grupo de reglas

Si compartes un grupo de reglas con otras cuentas y, a continuación, eliminas el grupo de reglas o dejas de compartirlo, el Firewall de DNS elimina todas las asociaciones que las demás cuentas hayan creado entre el grupo de reglas y las tuyas VPCs.

Configuración máxima para grupos de reglas y asociaciones

Los grupos de reglas compartidos y sus asociaciones VPCs se incluyen en los recuentos de las cuentas con las que se comparten los grupos de reglas.

Para conocer las cuotas actuales de DNS Firewall, consulte [Cuotas en el firewall DNS de Resolver](#).

Permisos

Para compartir un grupo de reglas con otra AWS cuenta, debe tener permiso para usar la [PutFirewallRuleGroupPolicy](#) acción.

Restricciones en la AWS cuenta con la que se comparte un grupo de reglas

La cuenta con la que se comparte un grupo de reglas no puede cambiar o eliminar este grupo de reglas.

Etiquetado

Solo la cuenta que creó un grupo de reglas puede agregar, eliminar o consultar etiquetas de este grupo de reglas.

Para ver el estado actual de uso compartido de un grupo de reglas (incluida la cuenta que compartió el grupo de reglas o la cuenta con la que se comparte un grupo de reglas) y compartir grupos de reglas con otra cuenta, siga el procedimiento que se indica a continuación.

Para ver el estado de uso compartido y compartir grupos de reglas con otra AWS cuenta

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Rule groups (Grupos de reglas).
3. En la barra de navegación, elija la región en la que creó el grupo de reglas.

En la columna Sharing status (Estado de uso compartido) se muestra el estado actual de uso compartido de los grupos de reglas que ha creado la cuenta actual o que se comparten con la cuenta actual:

- No compartido: la AWS cuenta actual creó el grupo de reglas y el grupo de reglas no se comparte con ninguna otra cuenta.
 - Shared by me (Compartido por mí): la cuenta actual ha creado el grupo de reglas y lo ha compartido con una o varias cuentas.
 - Shared with me (Compartido conmigo): otra cuenta ha creado el grupo de reglas y lo ha compartido con la cuenta actual.
4. Elija el nombre del grupo de reglas cuya información de uso compartido desea mostrar o que desea compartir con otra cuenta.

En la *rule group name* página Grupo de reglas:, el valor de Propietario muestra el ID de la cuenta que creó el grupo de reglas. Es la cuenta actual a menos que el valor de Sharing status (Estado de uso compartido) sea Shared with me (Compartido conmigo). En ese caso, el propietario es la cuenta que creó el grupo de reglas y lo compartió con la cuenta actual.

5. Elija Share (Compartir) para ver información adicional o para compartir el grupo de reglas con otra cuenta. Aparece una página en la AWS RAM consola, en función del valor del estado de uso compartido:
 - Not shared (No compartido): aparece la página Create resource share (Crear recurso compartido de recursos). Para obtener más información acerca de cómo compartir el grupo de reglas con otra cuenta, unidad organizativa (OU) u organización, vaya al siguiente paso.
 - Shared by me (Compartido por mí): la página Shared resources (Recursos compartidos) muestra los grupos de reglas y otros recursos que son propiedad de la cuenta actual y que están compartidos con otras cuentas.
 - Shared with me (Compartido conmigo): la página Shared resources (Recursos compartidos) muestra los grupos de reglas y otros recursos que son propiedad de otras cuentas y que están compartidos con la cuenta actual.
6. Para compartir un grupo de reglas con otra AWS cuenta, unidad organizativa u organización, especifique los siguientes valores.

 Note

No se puede actualizar la configuración de uso compartido. Si desea cambiar cualquiera de los siguientes valores, debe volver a compartir un grupo de reglas con la nueva configuración y, a continuación, quitar la configuración de uso compartido anterior.

Description (Descripción)

Ingrese una breve descripción que le ayude a recordar por qué compartió el grupo de reglas.

Recursos

Elija la casilla de verificación correspondiente al grupo de reglas que desea compartir.

Entidades principales

Introduzca el número de AWS cuenta, el nombre de la OU o el nombre de la organización.

Tags

Especifique una o más claves y los valores correspondientes. Por ejemplo, puede especificar el centro de coste para la clave y 456 para el valor.

Estas son las etiquetas Administración de facturación y costos de AWS que permiten organizar su AWS factura; también puede utilizarlas para otros fines. Para obtener más información sobre el uso de etiquetas para la asignación de costes, consulte [Uso de etiquetas de asignación de costes](#) en la Guía del usuario de AWS Billing .

Habilitar las protecciones de Resolver DNS Firewall para su VPC

Asocie uno o más grupos de reglas a la VPC a fin de habilitar las protecciones de DNS Firewall para esta VPC. Siempre que se asocie una VPC a un grupo de reglas de firewall de DNS, el Resolver de VPC de Route 53 proporciona las siguientes protecciones de firewall de DNS:

- El solucionador de VPC enruta las consultas DNS salientes de la VPC a través del firewall de DNS y el firewall de DNS filtra las consultas mediante los grupos de reglas asociados.
- El solucionador de VPC aplica los ajustes de la configuración del firewall DNS de la VPC.

Para proporcionar protecciones de DNS Firewall a la VPC, se debe hacer lo siguiente:

- Cree y administre asociaciones entre los grupos de reglas de DNS Firewall y la VPC. Para obtener información acerca de los grupos de reglas, consulte [Reglas y grupos de reglas de DNS Firewall](#).
- Configure la forma en que desea que VPC Resolver gestione las consultas de DNS para la VPC durante un error, por ejemplo, si el firewall de DNS no proporciona una respuesta a una consulta de DNS.

Administrar las asociaciones entre la VPC y el grupo de reglas de Resolver DNS Firewall

Visualización de las asociaciones de VPC de un grupo de reglas

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.

Seleccione DNS Firewall en el panel de navegación para abrir la página Grupos de regla de DNS Firewall en la consola de Amazon VPC.

- O BIEN -

Inicie sesión en la Consola de administración de AWS y abra la

la consola Amazon VPC que se encuentra debajo. <https://console.aws.amazon.com/vpc/>

2. En el panel de navegación, en DNS Firewall, elija Grupos de regla.
3. En la barra de navegación, elija la región del grupo de reglas.
4. Seleccione el grupo de reglas que desea asociar.
5. Elija Ver detalles. Se muestra la página de grupo de reglas.
6. En la parte inferior, puede ver un área de detalles con pestañas que incluye las reglas y las asociadas. VPCs Seleccione la pestaña VPCsAsociado.

Asociación de un grupo de reglas a una VPC

1. Busque las asociaciones de VPC del grupo de reglas siguiendo las instrucciones del [procedimiento anterior](#) Visualización de las asociaciones de VPC de un grupo de reglas.
2. En la VPCs pestaña Asociada, elija Asociar VPC.
3. En el menú desplegable, busque la VPC que desea asociar al grupo de reglas. Selecciónelo y, a continuación, elija Associate (Asociar).

En la página del grupo de reglas, su VPC aparece en la pestaña VPCsAsociada. Al principio, la opción Status (Estado) notifica Updating (Actualizando). Cuando termina la asociación, el estado cambia a Complete (Completa).

Eliminación de una asociación entre un grupo de reglas y una VPC

1. Busque las asociaciones de VPC del grupo de reglas siguiendo las instrucciones del [procedimiento anterior](#) Visualización de las asociaciones de VPC de un grupo de reglas.
2. Seleccione la VPC que desee eliminar de la lista y, a continuación, elija Desasociar. Compruebe la acción y, a continuación, confírmela.

En la página del grupo de reglas, su VPC aparece en la VPCs pestaña Asociada con el estado Desasociándose. Cuando finalice la operación, DNS Firewall actualiza la lista para quitar la VPC.

Configuración de la VPC de DNS Firewall

La configuración del firewall de DNS de la VPC determina si el Resolver de VPC de Route 53 permite el paso de las consultas o las bloquea durante los errores, por ejemplo, cuando el firewall de DNS está dañado, no responde o no está disponible en la zona. El solucionador de VPC aplica la configuración del firewall de una VPC siempre que tenga uno o más grupos de reglas de firewall de DNS asociados a la VPC.

Puede configurar una VPC para que permanezca abierta o cerrada al producirse un error.

- De forma predeterminada, el modo de error está cerrado, lo que significa que VPC Resolver bloquea las consultas para las que no recibe una respuesta del firewall de DNS y envía una respuesta de SERVFAIL DNS. Este enfoque antepone la seguridad a la disponibilidad.
- Si habilitas la apertura por error, VPC Resolver permite el paso de consultas si no recibe una respuesta del firewall de DNS. Este enfoque antepone la disponibilidad a la seguridad.

Modificación de la configuración de DNS Firewall para una VPC (consola)

1. Inicie sesión en la consola de VPC Resolver Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/route53resolver/>
2. En el panel de navegación, en Resolvers, elija. VPCs
3. En la VPCspágina, localice y edite la VPC. Cambie la configuración de DNS Firewall para que permanezca abierta o cerrada al producirse un error cuando sea necesario.

Modificación del comportamiento de DNS Firewall para una VPC (API)

- Actualice la configuración del firewall de su VPC llamando [UpdateFirewallConfig](#) habilitando o deshabilitando. `FirewallFailOpen`

Puedes recuperar una lista de las configuraciones de firewall de tu VPC a través de la API llamando. [ListFirewallConfigs](#)

¿Qué son los perfiles de Amazon Route 53?

Con los perfiles de Route 53, puede aplicar y administrar configuraciones de Route 53 relacionadas con el DNS en muchas VPCs y diferentes configuraciones. Cuentas de AWS Los perfiles hacen que administrar la configuración de DNS para muchos sea tan fácil VPCs como administrarlos para una sola VPC y, cuando se actualiza un perfil, su configuración se propaga a todos los VPCs asociados al perfil. También puede compartir un perfil Cuentas de AWS en las mismas regiones utilizando. AWS RAM Los recursos que actualmente admite Route 53 y que puede asociar a un perfil son:

- Zonas alojadas privadas y la configuración especificada en ellas. Para obtener más información sobre cómo trabajar con zonas alojadas privadas, consulte [Uso de zonas alojadas privadas](#).
- Reglas de resolución, tanto de reenvío como de sistema. Para obtener más información acerca de las reglas de Resolver, consulte [Administración de reglas de reenvío](#).
- Grupos de reglas de DNS Firewall. Para obtener más información sobre los grupos de reglas de DNS Firewall, consulte [Reglas y grupos de reglas de DNS Firewall](#).
- Puntos de conexión de VPC de la interfaz Para obtener más información sobre los puntos de conexión de VPC, consulte los [puntos de conexión de VPC](#) en la Guía del usuario de Amazon VPC.
- Configuraciones de registro de consultas de VPC Resolver. Para obtener más información sobre el registro de consultas de VPC Resolver, consulte. [Registro de consultas de Resolver](#)

Algunas de las configuraciones de VPC se administran directamente en el perfil. Las configuraciones son:

- Configuración de búsqueda de DNS inverso para reglas de Resolver.
- Configuración del modo de error de DNS Firewall.
- Perfil de validación de DNSSEC.

Por ejemplo, puede habilitar la configuración del modo de error del firewall de DNS para todos los perfiles a los VPCs que esté asociado, pero conservar la configuración de validación de DNSSEC existente en la VPC.

 Important

Una vez que habilite la configuración del perfil para las configuraciones anteriores y asocie el perfil a una VPC, la configuración del perfil surtirá efecto de inmediato.

También puedes utilizarla CloudFormation para configurar una configuración de DNS coherente para los recién aprovisionados. VPCs

Puede asociar un perfil por VPC y la cantidad de recursos que puede asociar por perfil varía. Para obtener más información, consulte [Cuotas en perfiles de Route 53](#).

Cómo se prioriza la configuración del perfil de Route 53

Puede configurar la configuración y las asociaciones del DNS local para los perfiles con fines de migración u otros fines de prueba. Cuando una consulta de DNS coincide con la regla de Resolver para una zona alojada privada que está directamente asociada a la VPC y una regla de solucionador para una zona alojada privada que está asociada al perfil, la configuración de DNS local tiene prioridad. Cuando se realiza una consulta de DNS para un nombre de dominio en conflicto, gana el más específico. La siguiente tabla incluye ejemplos del orden de evaluación:

consulta DNS	Regla de perfil	Regla de VPC	Regla evaluada
example.com	example.com	example.com	VPC local
test.example.com	test.example.com	example.com	Perfil
marketing.example.com	Ninguno	marketing.example.com	VPC local

Disponibilidad de región de perfiles de Route 53

Para ver la disponibilidad regional y los puntos de conexión, consulte los [puntos de conexión del servicio para Route 53](#) en la Guía de referencia general de AWS .

Pasos de alto nivel para utilizar perfiles de Route 53

Para implementar los perfiles de Amazon Route 53 en su Amazon Virtual Private Cloud VPCs, debe realizar los siguientes pasos de alto nivel.

1. Crear un perfil vacío: el primer paso es crear un perfil vacío al que pueda asociar recursos de DNS. Para obtener más información, consulte [Creación de perfiles de Route 53](#).
2. Asocie recursos de DNS al perfil: los recursos que puede asociar actualmente a un perfil son zonas alojadas privadas, reglas de resolución, tanto de reenvío como de sistema, grupos de reglas de firewall de DNS, configuraciones de registro de consultas de VPC Resolver y puntos finales de interfaz de VPC. Para obtener más información, consulte [Asociación de grupos de reglas de DNS Firewall a un perfil de Route 53](#), [Asociación de zonas alojadas privadas a un perfil de Route 53](#), [Asociación de reglas de Resolver a un perfil de Route 53](#), [Asocie las configuraciones de registro de consultas de VPC Resolver a un perfil de Route 53](#) y [Asociación de puntos de conexión de VPC de interfaz a un perfil de Route 53](#).
3. Configure algunos de los ajustes de VPC para el perfil: algunos de los ajustes de DNS, como las zonas alojadas asociadas al perfil, se aplican inmediatamente. VPCs Para configurar la validación de DNSSEC, la búsqueda de DNS inverso de Resolver y el modo de error de DNS Firewall, puede elegir una de las siguientes opciones:
 - Para la validación de DNSSEC, puede optar por utilizar la configuración de VPC local (predeterminada), habilitar la validación o deshabilitar la validación para todos los VPCs asociados al perfil.
 - Para la configuración de búsqueda de DNS inverso de Resolver, puede habilitarla, deshabilitarla o usar las reglas autodefinidas para la VPC de forma local (predeterminada).
 - Para la configuración del modo de error de DNS Firewall, puede habilitarlo, deshabilitarlo o usar la configuración del modo de error definida para la VPC de forma local (predeterminada).

Para obtener más información, consulte [Edición de configuraciones de perfil de Route 53](#).

4. Asocie el perfil a uno o más VPCs: para empezar a usar su perfil, asícielo a uno o varios. VPCs Para obtener más información, consulte [Asocie un perfil de Route 53 a VPCs](#).

Creación de perfiles de Route 53

Para crear perfiles de Route 53, siga las instrucciones de este tema. Elija una pestaña para crear un perfil de Route 53 mediante la consola de Route 53, o AWS CLI.

- [Consola](#)
- [CLI](#)

Console

Cómo crear un perfil de Route 53

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Perfiles.
3. En la barra de navegación, elija la región en la que desee crear el perfil.
4. Introduzca un nombre para el perfil, si lo desea, añada etiquetas y elija Crear perfil.

Esto crea un perfil vacío con las configuraciones predeterminadas a las que puede asociar los recursos. Después de asociar los recursos al perfil, puede asociarlos a varios VPCs y editar la forma en que se aplican algunas de las configuraciones del Resolver al VPCs.

CLI

Puede crear un perfil ejecutando un AWS CLI comando como el siguiente y utilizando su propio valor paraname.

```
aws route53profiles create-profile --name test
```

A continuación, se muestra un ejemplo de salida luego de ejecutar el comando:

```
{
  "Profile": {
    "Arn": "arn:aws:route53profiles:us-east-1:123456789012:profile/
rp-6ffe47d5example",
    "ClientToken": "2ca1a304-32b3-4f5f-bc4c-EXAMPLE11111",
    "CreationTime": 1710850903.578,
    "Id": "rp-6ffe47d5example",
    "ModificationTime": 1710850903.578,
    "Name": "test",
    "OwnerId": "123456789012",
    "ShareStatus": "NOT_SHARED",
    "Status": "COMPLETE",
    "StatusMessage": "Created Profile"
  }
}
```

```
}
```

Para asociar los perfiles a diferentes recursos y editar las configuraciones de VPC para el perfil, consulte los siguientes procedimientos:

Temas

- [Asociación de grupos de reglas de DNS Firewall a un perfil de Route 53](#)
- [Asociación de zonas alojadas privadas a un perfil de Route 53](#)
- [Asociación de reglas de Resolver a un perfil de Route 53](#)
- [Asociación de puntos de conexión de VPC de interfaz a un perfil de Route 53](#)
- [Asocie las configuraciones de registro de consultas de VPC Resolver a un perfil de Route 53](#)
- [Edición de configuraciones de perfil de Route 53](#)
- [Asocie un perfil de Route 53 a VPCs](#)

Asociación de grupos de reglas de DNS Firewall a un perfil de Route 53

Para obtener instrucciones sobre cómo crear un grupo de reglas, consulte [Creación de reglas y de un grupo de reglas](#) y elija una pestaña para asociar los grupos de reglas de DNS Firewall a un perfil de Route 53 con la consola de Route 53, o AWS CLI.

- [Consola](#)
- [CLI](#)

Console

Cómo asociar grupos de reglas de DNS Firewall

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En la barra de navegación, elija la región en la que creó el perfil.
3. En el panel de navegación, elija Perfiles y, en la tabla Perfiles, elija el nombre vinculado del perfil con el que desee trabajar.
4. En la página <Nombre del perfil>, seleccione la pestaña Grupos de reglas de DNS Firewall y, a continuación, seleccione Asociar.

5. En la sección Grupos de reglas de DNS Firewall, puede seleccionar hasta 10 grupos de reglas que haya creado con anterioridad. Si desea asociar más de 10 grupos de reglas, utilice el APIs. Para obtener más información, consulte [AssociateResourceToProfile](#).

Para crear nuevos grupos de reglas, consulte [Creación de reglas y de un grupo de reglas](#).

6. Elija Siguiente.
7. En la página Definir prioridad, puede establecer el orden en que se procesan los grupos de reglas al hacer clic en el número de prioridad preasignado y escribir uno nuevo. Los valores permitidos para la prioridad están entre 100 y 9900.

Los grupos de reglas se evalúan comenzando por la configuración de prioridad numérica más baja y aumentando esta prioridad. Puede cambiar la prioridad de un grupo de reglas en cualquier momento; por ejemplo, para cambiar el orden de procesamiento o dejar espacio para otros grupos de reglas.

Elija Enviar.

8. El progreso de la asociación se muestra en la columna Estado del cuadro de diálogo de grupos de reglas de DNS Firewall.

CLI

Puede asociar un grupo de reglas a un perfil ejecutando un AWS CLI comando como el siguiente y utilizando sus propios valores para name profile-idresource-arn, ypriority:

```
aws route53profiles associate-resource-to-profile --name test-resource-association --profile-id rp-4987774726example --resource-arn arn:aws:route53resolver:us-east-1:123456789012:firewall-rule-group/rslvr-frg-cfe7f72example --resource-properties "{\"priority\": 102}"
```

A continuación, se muestra un ejemplo de salida luego de ejecutar el comando:

```
{
  "ProfileResourceAssociation": {
    "CreationTime": 1710851216.613,
    "Id": "rpr-001913120a7example",
    "ModificationTime": 1710851216.613,
    "Name": "test-resource-association",
    "OwnerId": "123456789012",
    "ProfileId": "rp-4987774726example",
```

```
"ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:firewall-  
rule-group/rslvr-frg-cfe7f72example",  
  "ResourceProperties": "{\"priority\":102}",  
  "ResourceType": "FIREWALL_RULE_GROUP",  
  "Status": "UPDATING",  
  "StatusMessage": "Updating the Profile to DNS Firewall rule group  
association"  
}
```

Asociación de zonas alojadas privadas a un perfil de Route 53

Para obtener instrucciones sobre cómo crear una zona alojada privada, consulte [Creación de una zona alojada privada](#) y siga los pasos descritos en este procedimiento para asociar una zona alojada privada a un perfil.

Cómo asociar zonas alojadas privadas

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En la barra de navegación, elija la región en la que creó el perfil.
3. En el panel de navegación, elija Perfiles y, en la tabla Perfiles, elija el nombre vinculado del perfil con el que desee trabajar.
4. En la página <Nombre del perfil>, seleccione la pestaña Zonas alojadas privadas y, a continuación, Asociar.
5. En la página Asociar zonas alojadas privadas puede seleccionar hasta 10 zonas alojadas privadas que haya creado con anterioridad. Si desea asociar más de 10 zonas alojadas privadas, utilice la APIs. Para obtener más información, consulte [AssociateResourceToProfile](#).

Para crear zonas alojadas privadas, consulte [Creación de una zona alojada privada](#).

6. Elija Asociar.
7. El progreso de la asociación se muestra en la columna Estado de la página Zonas alojadas privadas.

Asociación de reglas de Resolver a un perfil de Route 53

Para obtener instrucciones sobre cómo crear una regla de Resolver, consulte [Creación de reglas de reenvío](#) y siga los pasos descritos en este procedimiento para asociar las reglas de Resolver a un perfil.

Para asociar reglas de VPC Resolver

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En la barra de navegación, elija la región en la que creó el perfil.
3. En la página <Nombre del perfil>, seleccione la pestaña Reglas de Resolver y, a continuación, Asociar.
4. En la página Asociar reglas de Resolver, en la tabla Reglas de Resolver, puede seleccionar hasta 10 reglas de solucionador que haya creado con anterioridad. Si desea asociar más de 10 reglas de resolución, utilice la APIs. Para obtener más información, consulte [AssociateResourceToProfile](#).

Para crear reglas de Resolver, consulte [Creación de reglas de reenvío](#).

5. Elija Asociar.
6. El progreso de la asociación se muestra en la columna Estado de la pestaña Reglas de Resolver.

Asociación de puntos de conexión de VPC de interfaz a un perfil de Route 53

Para obtener instrucciones sobre cómo crear un punto de conexión de VPC de interfaz, consulte [Create a VPC endpoint](#) en la Guía del usuario de VPC y, a continuación, siga los pasos descritos en este procedimiento para asociar un punto de conexión de VPC a un perfil.

Cómo asociar los puntos de conexión de VPC

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/route53/>
2. En la barra de navegación, elija la región en la que creó el perfil.

3. En la página <Nombre de perfil>, seleccione la pestaña puntos de conexión de VPC y, a continuación, Asociar.
4. En la página Asociar puntos de conexión de VPC, en la tabla Puntos de conexión de VPC, puede seleccionar hasta 10 puntos de conexión que haya creado con anterioridad. Si desea asociar más de 10 puntos finales, utilice el APIs. Para obtener más información, consulte [AssociateResourceToProfile](#).

Para crear reglas de Resolver, consulte [Creación de reglas de reenvío](#).

5. Elija Asociar.
6. El progreso de la asociación se muestra en la columna Estado de la página puntos de conexión de VPC.

Asocie las configuraciones de registro de consultas de VPC Resolver a un perfil de Route 53

Para obtener instrucciones sobre cómo crear una configuración de registro de consultas de VPC Resolver, consulte y, a continuación [Configuración \(registro de consultas de VPC Resolver\)](#), elija una pestaña para asociar la configuración de VPC Resolver a un perfil de Route 53 mediante la consola de Route 53, o. AWS CLI

- [Consola](#)
- [CLI](#)

Console

Para asociar configuraciones de registro de consultas

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En la barra de navegación, elija la región en la que creó el perfil.
3. En la página del nombre del perfil, seleccione la pestaña de configuraciones del registro de consultas de Resolver y, a continuación, asocie.
4. En la página Asociar configuraciones de registro de consultas, en la tabla de configuraciones del registro de consultas de Resolver, puede seleccionar hasta tres configuraciones que haya creado anteriormente. Si desea asociar más de tres configuraciones de registro de consultas, utilice la API. Para obtener más información, consulte [AssociateResourceToProfile](#).

5. Para crear nuevas configuraciones de registro de consultas de VPC Resolver, consulte. [Configuración \(registro de consultas de VPC Resolver\)](#)
6. Elija Asociar.
7. El progreso de la asociación se muestra en la columna Estado de la pestaña de configuraciones del registro de consultas del Resolver.

CLI

Puede asociar una configuración de registro de consultas a un perfil ejecutando un AWS CLI comando como el siguiente y utilizando sus propios valores para `name` `profile-id` y `resource-arn`.

```
aws route53profiles associate-resource-to-profile --name test-resource-association --profile-id rp-4987774726example --resource-arn arn:aws:route53resolver:us-east-1:123456789012:resolver-query-log-config/rqlc-cfe7f72example
```

A continuación, se muestra un ejemplo de salida luego de ejecutar el comando:

```
{
  "ProfileResourceAssociation": {
    "CreationTime": 1710851226.613,
    "Id": "rpr-001913120b8example",
    "ModificationTime": 1710851226.613,
    "Name": "test-resource-association",
    "OwnerId": "123456789012",
    "ProfileId": "rp-4987774726example",
    "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:resolver-query-log-config/rqlc-cfe7f72example",
    "ResourceType": "RESOLVER_QUERY_LOG_CONFIG",
    "Status": "CREATING",
    "StatusMessage": "Creating rp-4987774726example to rqlc-cfe7f72example association"
  }
}
```

Edición de configuraciones de perfil de Route 53

Tras asociar los recursos a un perfil, puede editar las configuraciones de VPC predeterminadas para decidir cómo se aplican al. VPCs

Cómo editar las configuraciones de perfil

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En la barra de navegación, elija la región en la que creó el perfil.
3. En el panel de navegación, elija Perfiles y, en la tabla Perfiles, elija el nombre vinculado del perfil con el que desee trabajar.
4. En la página <Nombre de perfil>, seleccione la pestaña Configuración y, a continuación, Editar.
5. En la página Editar configuración, elija uno de los valores para la configuración de DNSSEC de VPC, la configuración de búsqueda de DNS inverso de Resolver y la configuración del modo de error de DNS Firewall.

Para obtener más información acerca de los valores, consulte [Ajustes de configuración del perfil de Route 53](#).

6. Elija Actualizar.

Ajustes de configuración del perfil de Route 53

Al momento de editar una configuración de perfil de Route 53, debe especificar los siguientes valores:

Configuración de DNSSEC

Elija uno de los valores siguientes:

- Uso de la configuración de DNSSEC de VPC local: (predeterminada)

Seleccione esta opción para que todos los dispositivos VPCs asociados a este perfil conserven su configuración de validación de DNSSEC local.

- Habilitar la validación de DNSSEC

Elija esta opción para habilitar la validación de DNSSEC en todos los archivos VPCs asociados a este perfil.

- Deshabilitar la validación de DNSSEC

Elija esta opción para deshabilitar la validación de DNSSEC en todos los VPCs que estén asociados a este perfil.

Configuración de búsqueda de DNS inverso del solucionador

Elija uno de los valores siguientes:

- Habilitado

Elija esta opción para crear reglas autodefinidas para la búsqueda inversa de DNS en todos los dominios asociados VPCs.

- No habilitado

Elija esta opción para no crear reglas autodefinidas para la búsqueda inversa de DNS en todos los dominios asociados VPCs.

- Usar reglas locales autodefinidas: predeterminada

Elija esta opción para usar la configuración de la VPC local para la búsqueda inversa de DNS para la VPC asociada. VPCs

Configuración del modo de error de DNS Firewall

Elija uno de los valores siguientes:

- Deshabilitado

Seleccione esta opción para cerrar el modo de error del firewall DNS asociado VPCs. Con esta opción, DNS Firewall bloqueará todas las consultas que no pueda evaluar correctamente.

- Enabled (Habilitado)

Seleccione esta opción para mantener abierto el modo de fallo del firewall DNS para todos los asociados VPCs. Con esta opción, DNS Firewall permitirá que las consultas continúen si no puede evaluarlas de manera adecuada.

- Usar la configuración del modo de error local: predeterminada

Elija esta opción para usar la configuración del modo de error de DNS Firewall de la VPC local.

Para obtener más información acerca de las configuraciones, consulte

- [Activar la validación de DNSSEC en Amazon Route 53](#)

- [Reglas de reenvío para consultas de DNS inversas en VPC Resolver](#)
- [Configuración de la VPC de DNS Firewall](#)

Asocie un perfil de Route 53 a VPCs

Para asociar un perfil de Route 53 a una VPC, siga las instrucciones de este tema. Elija una pestaña para asociar un perfil de Route 53 a una VPC mediante la consola de Route 53, o. AWS CLI

- [Consola](#)
- [CLI](#)

Console

Para asociar VPCs

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En la barra de navegación, elija la región en la que creó el perfil.
3. En la <Profile name>página, elija la VPCs pestaña y, a continuación, Asociar.
4. En la VPCs página Asociar, puede seleccionar hasta 10 VPCs que haya creado anteriormente. Si desea asociar más de 10 VPCs, utilice la APIs. Para obtener más información, consulte [AssociateProfile](#).
5. Elija Asociar.
6. El progreso de la asociación se muestra en la columna Estado de la VPCs página.

CLI

Puede enumerar los perfiles ejecutando un AWS CLI comando como el siguiente y utilizando sus propios valores para `nameprofile-id`, y `resource-id`:

```
aws route53profiles associate-profile --name test-association --profile-id rp-4987774726example --resource-id vpc-0af3b96b3example
```

A continuación, se muestra un ejemplo de salida luego de ejecutar el comando:

```
{  
  "ProfileResourceAssociation": {
```

```
{
  "CreationTime": 1710851216.613,
  "Id": "rpr-001913120a7example",
  "ModificationTime": 1710851216.613,
  "Name": "test-resource-association",
  "OwnerId": "123456789012",
  "ProfileId": "rp-4987774726example",
  "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:firewall-
rule-group/rslvr-frg-cfe7f72example",
  "ResourceProperties": "{\"priority\":102}",
  "ResourceType": "FIREWALL_RULE_GROUP",
  "Status": "UPDATING",
  "StatusMessage": "Updating the Profile to DNS Firewall rule group
association"
}
```

Visualización y actualización de perfiles de Amazon Route 53

Elija la pestaña de la consola para ver y editar el perfil de Route 53. Elija la pestaña CLI para AWS CLI enumerar los perfiles que le pertenecen, que usted comparte o que comparte con usted.

- [Consola](#)
- [CLI](#)

Console

Visualización y actualización de perfiles de Route 53

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Perfiles.
3. Seleccione el botón situado junto al nombre del perfil que desea ver o editar.
4. En la página <Nombre de perfil> puede ver los recursos de DNS actualmente asociados, asociar otros nuevos y editar las etiquetas y las configuraciones de VPC.

CLI

Puede enumerar los perfiles ejecutando un AWS CLI comando como el siguiente:

```
aws route53profiles list-profiles
```

A continuación, se muestra un ejemplo de salida luego de ejecutar el comando:

```
{
  "ProfileSummaries": [
    {
      "Arn": "arn:aws:route53profiles:us-east-1:123456789012:profile/
rp-4987774726example",
      "Id": "rp-4987774726example",
      "Name": "test",
      "ShareStatus": "NOT_SHARED"
    }
  ]
}
```

Para obtener información sobre un VPS concreto al que esté asociado el perfil, ejecute un comando de la AWS CLI como el siguiente y utilice su propio valor para `profile-association-id`:

```
aws route53profiles get-profile-association --profile-association-id
rrpassoc-489ce212fexample
```

A continuación, se muestra un ejemplo de salida luego de ejecutar el comando:

```
"ProfileAssociation": {
  "CreationTime": 1709338817.148,
  "Id": "rrpassoc-489ce212fexample",
  "ModificationTime": 1709338974.772,
  "Name": "test-association",
  "OwnerId": "123456789012",
  "ProfileId": "rp-4987774726example",
  "ResourceId": "vpc-0af3b96b3example",
  "Status": "COMPLETE",
  "StatusMessage": "Created Profile Association"
}
```

Eliminación de un perfil de Amazon Route 53

Elija una pestaña para eliminar un perfil de Route 53 mediante la consola de Route 53, o AWS CLI.

- [Consola](#)
- [CLI](#)

Console

Cómo eliminar un perfil de Route 53

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Perfiles.
3. Elija el botón junto al nombre del perfil que desea eliminar y, a continuación, elija Eliminar.

Important

No puede eliminar un perfil si está asociado a VPCs. Además, si el perfil se comparte con otra Cuenta de AWS persona, cualquiera a la VPCs que estén asociadas las configuraciones del perfil perderá esas configuraciones.

4. En el cuadro de diálogo Eliminar <Nombre de perfil>, escriba **confirm** y, a continuación, seleccione Eliminar.

CLI

Important

No puede eliminar un perfil si está asociado a VPCs. Además, si el perfil se comparte con otra Cuenta de AWS persona, cualquiera a la VPCs que estén asociadas las configuraciones del perfil perderá esas configuraciones.

Puede eliminar un perfil ejecutando un AWS CLI comando como el siguiente y utilizando su propio valor `paraprofile-id`:

```
aws route53profiles delete-profile --profile-id rp-6ffe47d5example
```

A continuación, se muestra un ejemplo de salida luego de ejecutar el comando:

```
{
```

```
"Profile": {
  "Arn": "arn:aws:route53profiles:us-east-1:123456789012:profile/
rp-6ffe47d5example",
  "ClientToken": "0a15fec0-05d9-4f78-bec0-EXAMPLE11111",
  "CreationTime": 1710850903.578,
  "Id": "rp-6ffe47d5example",
  "ModificationTime": 1710850903.578,
  "Name": "test",
  "OwnerId": "123456789012",
  "ShareStatus": "NOT_SHARED",
  "Status": "DELETED",
  "StatusMessage": "Deleted Profile"
}
```

Visualización y actualización de los recursos de Route 53 asociados a un perfil de Amazon Route 53

Elija la pestaña de la consola para ver las asociaciones de recursos de perfiles de Route 53 y, si lo desea, edite la prioridad del grupo de reglas de DNS Firewall. Seleccione la pestaña CLI para AWS CLI enumerar las asociaciones de recursos y ver un ejemplo de actualización de una prioridad de un grupo de reglas de firewall de DNS.

- [Consola](#)
- [CLI](#)

Console

Cómo ver y actualizar los recursos asociados a un perfil

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Perfiles.
3. En la barra de navegación, elija la región en la que creó el perfil.
4. Seleccione el botón situado junto al nombre del perfil del que desea ver o editar las asociaciones de recursos.

5. En la página <Nombre de perfil>, elija la pestaña del recurso que desee ver o editar, ya sea Grupos de reglas de DNS Firewall, Zonas alojadas privadas, Reglas de Resolver o Puntos de conexión de VPC.
6. En la página de pestañas de un recurso puede ver los nombres, el ARN y el estado de los recursos asociados. Además, puede elegir el icono de engranaje para ajustar lo que se muestra en la tabla de recursos.

En la página de pestañas Grupos de reglas de DNS Firewall también puede elegir la entrada prioritaria del grupo de reglas y editarla con un número mayor o menor. Los grupos de reglas se evalúan en orden, empezando por el número de prioridad más baja hasta el número de prioridad más alta.

CLI

Puede enumerar los recursos asociados a un perfil ejecutando un AWS CLI comando como el siguiente y utilizando su propio valor `profile-id`:

```
aws route53profiles list-profile-resource-associations --profile-id  
rp-4987774726example
```

A continuación, se muestra un ejemplo de salida luego de ejecutar el comando:

```
{  
  "ProfileResourceAssociations": [  
    {  
      "CreationTime": 1710851216.613,  
      "Id": "rpr-001913120a7example",  
      "ModificationTime": 1710851216.613,  
      "Name": "test-resource-association",  
      "OwnerId": "123456789012",  
      "ProfileId": "rp-4987774726example",  
      "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:firewall-  
rule-group/rslvr-frg-cfe7f72example",  
      "ResourceProperties": "{\"priority\":102}",  
      "ResourceType": "FIREWALL_RULE_GROUP",  
      "Status": "COMPLETE",  
      "StatusMessage": "Completed creation of Profile to DNS Firewall rule  
group association"  
    }  
  ]  
}
```

```
}
```

Puede actualizar la prioridad de un grupo de reglas del firewall de DNS asociado a un perfil ejecutando un AWS CLI comando como el siguiente y utilizando su propio valor para `profile-resource-association-id` y `--resource-properties`:

```
aws route53profiles update-profile-resource-association --profile-  
resource-association-id rpr-001913120a7example --resource-properties  
"{\"priority\": 105}"
```

A continuación, se muestra un ejemplo de salida luego de ejecutar el comando:

```
{  
  "ProfileResourceAssociation": {  
    "CreationTime": 1710851216.613,  
    "Id": "rpr-001913120a7example",  
    "ModificationTime": 1710852303.798,  
    "Name": "test-resource-association",  
    "OwnerId": "123456789012",  
    "ProfileId": "rp-4987774726example",  
    "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:firewall-  
rule-group/rslvr-frg-cfe7f72example",  
    "ResourceProperties": "{\"priority\":105}",  
    "ResourceType": "FIREWALL_RULE_GROUP",  
    "Status": "UPDATING",  
    "StatusMessage": "Updating the Profile to DNS Firewall rule group  
association"  
  }  
}
```

Desasociación de un recurso de un perfil de Amazon Route 53

Antes de eliminar un perfil, debe disociar todos los recursos del mismo.

Cómo desasociar un recurso asociado a un perfil de Route 53

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/route53/>
2. En el panel de navegación, elija Perfiles.

3. En la barra de navegación, elija la región en la que se creó el perfil del que desea desasociar un recurso.
4. Seleccione el botón situado junto al nombre del perfil del que desea desasociar un recurso.
5. En la página Nombre del perfil, elija la pestaña del recurso que desee eliminar, ya sea grupos de reglas de firewall DNS, zonas alojadas privadas, registro de consultas de Resolver, reglas de Resolver o puntos finales de VPC.
6. En la página de pestañas del recurso, elija el recurso que desee desasociar y, luego, elija Desasociar.
7. En el cuadro de diálogo Desasociar recursos escriba **confirm** y, luego, elija Desasociar.

Visualización VPCs asociada a un perfil de Amazon Route 53

Elija la pestaña de la consola para ver y editar las asociaciones entre perfiles de Route 53 y VPC. Elija la pestaña CLI AWS CLI para ver una lista de las asociaciones de perfil a VPC o para obtener información sobre una asociación específica

- [Consola](#)
- [CLI](#)

Console

Para ver las propiedades VPCs asociadas a un perfil

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Perfiles.
3. En la barra de navegación, elija la región en la que creó el perfil.
4. Seleccione el botón situado junto al nombre del perfil al que desee ver el perfil asociado VPCs.
5. En la <Profile name>página, elija la VPCs pestaña.
6. En la página de pestañas VPCs puede ver los nombres, el ARN y el estado de los asociados. VPCs

CLI

Puede enumerar a qué está asociado VPCs el perfil ejecutando un AWS CLI comando como el siguiente:

```
aws route53profiles list-profile-associations
```

A continuación, se muestra un ejemplo de salida luego de ejecutar el comando:

```
{
  "ProfileAssociations": [
    {
      "CreationTime": 1709338817.148,
      "Id": "rpassoc-489ce212fexample", {
        "ProfileAssociations": [
          {
            "CreationTime": 1709338817.148,
            "Id": "rpassoc-489ce212fexample",
            "ModificationTime": 1709338974.772,
            "Name": "test-association",
            "OwnerId": "123456789012",
            "ProfileId": "rp-4987774726example",
            "ResourceId": "vpc-0af3b96b3example",
            "Status": "COMPLETE",
            "StatusMessage": "Created Profile Association"
          }
        ]
      }
    ]
  }

  "ModificationTime": 1709338974.772,
  "Name": "test-association",
  "OwnerId": "123456789012",
  "ProfileId": "rp-4987774726example",
  "ResourceId": "vpc-0af3b96b3example",
  "Status": "COMPLETE",
  "StatusMessage": "Created Profile Association"
}
}
```

Para obtener información sobre un VPS concreto al que esté asociado el perfil, ejecute un comando de la AWS CLI como el siguiente y utilice su propio valor para `profile-association-id`:

```
aws route53profiles get-profile-association --profile-association-id  
rrpassoc-489ce212fexample
```

A continuación, se muestra un ejemplo de salida luego de ejecutar el comando:

```
"ProfileAssociation": {  
  "CreationTime": 1709338817.148,  
  "Id": "rrpassoc-489ce212fexample",  
  "ModificationTime": 1709338974.772,  
  "Name": "test-association",  
  "OwnerId": "123456789012",  
  "ProfileId": "rp-4987774726example",  
  "ResourceId": "vpc-0af3b96b3example",  
  "Status": "COMPLETE",  
  "StatusMessage": "Created Profile Association"  
}  
}
```

Desasociación de una VPC de un perfil de Amazon Route 53

Elija una pestaña para disociar un perfil de Route 53 de una VPC mediante la consola de Route 53, o. AWS CLI

- [Consola](#)
- [CLI](#)

Console

Cómo desasociar una VPC asociada a un perfil de Route 53

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/route53/>
2. En el panel de navegación, elija Perfiles.
3. En la barra de navegación, elija la región en la que se creó el perfil del que desea desasociar una VPC.
4. Seleccione el botón situado junto al nombre del perfil del que desea desasociar una VPC.
5. En la <Profile name>página, elija la VPCs pestaña.

6. En la página de VPCs pestañas del recurso, elija la VPC que desee desasociar y, a continuación, Desasocie.
7. En el cuadro de diálogo Desasociar recursos escriba **confirm** y, luego, elija Desasociar.

CLI

Puede disociar un perfil de una VPC ejecutando un AWS CLI comando como el siguiente y utilizando su propio valor para y: `profile-id` --resource-id

```
aws route53profiles disassociate-profile --profile-id  
rp-4987774726example --resource-id vpc-0af3b96b3example
```

A continuación, se muestra un ejemplo de salida luego de la ejecución del comando:

```
"ProfileAssociation": {  
  "CreationTime": 1710851336.527,  
  "Id": "rpassoc-489ce212fexample",  
  "ModificationTime": 1710851401.362,  
  "Name": "test-association",  
  "OwnerId": "123456789012",  
  "ProfileId": "rp-4987774726example",  
  "ResourceId": "vpc-0af3b96b3example",  
  "Status": "DELETING",  
  "StatusMessage": "Deleting Profile Association"  
}
```

Cómo trabajar con perfiles de Route 53 compartidos

Puede compartir un perfil con otras cuentas de la siguiente manera:

- Otorgar permisos de solo lectura, lo que significa que la otra cuenta puede asociar el perfil a su cuenta. VPCs En este caso, todos los recursos y configuraciones del DNS estarán en vigor en el servidor asociado. VPCs
- Concesión de permisos de administrador En este caso, las cuentas con el perfil compartido pueden modificar el perfil y, a continuación, asociarlo a su perfil VPCs. El propietario también puede crear permisos administrados por el cliente que se pueden usar para especificar qué acciones puede realizar la cuenta del consumidor. Para obtener más información, consulte [Permisos administrados por el cliente](#) en la Guía del usuario de AWS RAM .

Amazon Route 53 Profile se integra con AWS Resource Access Manager (AWS RAM) para permitir el uso compartido de recursos. AWS RAM es un servicio que le permite compartir algunos recursos de Route 53 con otras Cuentas de AWS o a través de ellas AWS Organizations. Con AWS RAM, puede compartir los recursos de su propiedad mediante la creación de un recurso compartido. Un uso compartido de recursos especifica los recursos que compartir y los consumidores con quienes compartirlos. Los consumidores pueden incluir lo siguiente:

- Específico Cuentas de AWS
- Una unidad organizativa dentro de su organización en AWS Organizations
- Toda su organización en AWS Organizations

Para obtener más información al respecto AWS RAM, consulte la [Guía AWS RAM del usuario](#).

En este tema se explica cómo compartir los recursos que le pertenecen y cómo utilizar los recursos que se comparten con usted.

Contenido

- [Concesión de permisos para compartir perfiles de Route 53](#)
- [Requisitos previos para compartir perfiles de Route 53](#)
- [Cómo compartir un perfil de Route 53](#)
- [Cómo dejar de compartir un perfil de Route 53 compartido](#)
- [Identificación de un perfil de Route 53 compartido](#)
- [Responsabilidades y permisos de los perfiles compartidos de Route 53](#)
- [Facturación y medición](#)
- [Cuotas de instancias](#)

Concesión de permisos para compartir perfiles de Route 53

Se requiere un conjunto mínimo de permisos para que una entidad principal de IAM comparta un perfil. Recomendamos el uso de la política de IAM `AmazonRoute53ProfilesFullAccess` administrada para garantizar que las entidades principales de IAM dispongan de los permisos necesarios para compartir y utilizar los perfiles compartidos.

Si utiliza una política de IAM personalizada, las acciones `route53profiles:GetProfilePolicy` y `route53profiles:PutProfilePolicy` son obligatorias. Estas son acciones de IAM solo de

permiso. Si a un director de IAM no se le conceden estos permisos, se producirá un error al intentar compartir el perfil mediante el AWS RAM servicio.

Requisitos previos para compartir perfiles de Route 53

- Para compartir un perfil de Route 53, debes tenerlo en tu Cuenta de AWS. Esto significa que el recurso debe asignarse o suministrarse en su cuenta. No puede compartir un perfil de Route 53 que se ha compartido con usted.
- Para compartir un perfil de Route 53 con su organización o con una unidad organizativa en AWS Organizations, debe habilitar el uso compartido con AWS Organizations. Para obtener más información, consulte [Habilitar el uso compartido con AWS Organizations](#) en la Guía del usuario de AWS RAM .

Cómo compartir un perfil de Route 53

Cuando compartes un perfil que te pertenece con otra persona Cuenta de AWS, les permites aplicar la configuración relacionada con el DNS del perfil a su perfil. VPCs Esto facilita la aplicación de configuraciones de DNS uniformes en miles de ellos VPCs con una sobrecarga de administración mínima.

Para compartir un perfil de Route 53, debe añadirlo a un recurso compartido. Un recurso compartido es un recurso de AWS RAM que le permite compartir los recursos a través de Cuentas de AWS. Un recurso compartido especifica los recursos que compartir y los consumidores con quienes se comparten. Cuando se comparte un perfil de Route 53 mediante la consola de Route 53, lo añade a un uso compartido de recurso existente. Para agregar el perfil de Route 53 a un nuevo uso compartido de recurso, primero debe crear el uso compartido del recurso mediante la [consola de AWS RAM](#).

Si forma parte de una organización AWS Organizations y está habilitado el uso compartido dentro de su organización, los consumidores de su organización tienen acceso automático al perfil compartido de Route 53. De lo contrario, los consumidores reciben una invitación para unirse al uso compartido de recursos y se les concede acceso al perfil de Route 53 compartido después de aceptar la invitación.

Puede empezar a compartir un perfil de Route 53 que sea de su propiedad en la consola de Route 53 y continuar en la AWS RAM consola.

Cómo compartir un perfil de Route 53 que sea de su propiedad mediante la consola de Route 53

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Perfiles.
3. Seleccione el perfil que desee compartir y, en la página Detalles del perfil, seleccione Compartir perfil.
4. Accederás a la AWS RAM consola, donde podrás seguir estos pasos: [Crear un recurso compartido](#) en la Guía del AWS RAM usuario.
5. Si se comparte un perfil con usted, la tabla Perfiles incluye el texto Compartido conmigo.

Si ha compartido un perfil, aparece como Compartido en la tabla de Perfiles.

Para compartir un perfil de Route 53 de tu propiedad mediante la AWS RAM consola

Consulte [Crear un recurso compartido](#) en la Guía del usuario de AWS RAM .

Para compartir un perfil de Route 53 de tu propiedad mediante el AWS CLI

Utilice el comando [create-resource-share](#).

Cómo dejar de compartir un perfil de Route 53 compartido

Cuando dejes de compartir un perfil y tengas las configuraciones de VPCs ese perfil asociadas, las perderás y, de forma predeterminada, pasarán a las configuraciones específicas de VPC.

Para dejar de compartir un perfil de Route 53 que sea de su propiedad, debe quitarlo del recurso compartido. Para ello, puede utilizar la consola de Route 53, la consola de AWS RAM o la AWS CLI.

Cómo dejar de compartir un perfil compartido de Route 53 que le pertenece mediante la consola de Route 53

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/route53/>
2. En el panel de navegación, elija Perfiles.
3. Seleccione el nombre vinculado del perfil que quiere dejar de compartir y, en la página <Nombre de perfil>, seleccione Administrar el uso compartido.

4. Accederás a la AWS RAM consola, donde podrás seguir estos pasos: [Actualizar un recurso compartido](#) en la Guía del AWS RAM usuario.

Para dejar de compartir un perfil de Route 53 compartido de tu propiedad mediante la consola AWS RAM

Consulte [Actualización de un recurso compartido](#) en la Guía del usuario de AWS RAM .

Para dejar de compartir un perfil de Route 53 compartido de tu propiedad mediante el AWS CLI

Utilice el comando [disassociate-resource-share](#).

Identificación de un perfil de Route 53 compartido

Los propietarios y consumidores pueden identificar perfiles de Route 53 compartidos mediante la consola de Route 53 y la AWS CLI.

Cómo identificar un perfil de Route 53 compartido mediante la consola de Route 53

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Perfiles.
3. Si se comparte un perfil con usted, la tabla Perfiles incluye el texto Compartido conmigo.

Si ha compartido un perfil, aparece como Compartido en la tabla de Perfiles.

Para identificar un perfil de Route 53 compartido mediante el AWS CLI

Utilice el comando [get-profile](#) o [list-profile](#). Los comandos devuelven información sobre los perfiles de Route 53 que posee y el estado de uso compartido de los perfiles de Route 53.

Responsabilidades y permisos de los perfiles compartidos de Route 53

Permisos de los propietarios

El propietario de un perfil puede ver, administrar y eliminar las asociaciones de recursos del perfil, incluidas las asociaciones de recursos creadas por las cuentas de los consumidores. El propietario puede ver y eliminar las asociaciones de VPC de las que es propietario. Además, solo el propietario

de un perfil puede eliminar un perfil de su propiedad y esto también elimina de forma automática todas las asociaciones de recursos del perfil.

Note

Debe crear un permiso administrado personalizado que incluya la acción `route53profiles:AssociateResourceToProfile`, además de las predeterminadas, para asociar cualquier recurso de las cuentas con las que se comparte el perfil, ya que la política `AWSRAMPermissionRoute53ProfileAllowAssociation` predeterminada no la incluye.

Permisos de los consumidores

El permiso predeterminado para los consumidores de un perfil compartido es de solo lectura. Con el permiso de solo lectura, pueden ver los recursos asociados y asociarlos a ellos VPCs, pero no pueden administrar las asociaciones de recursos.

El propietario también puede crear permisos gestionados por el cliente en la AWS RAM consola. Para obtener más información, consulte [Creating and using customer managed permissions](#) en la Guía del usuario de AWS RAM .

Facturación y medición

Los perfiles de Route 53 se facturan en función del número de asociaciones de VPC. El propietario del perfil es responsable de la factura de las asociaciones de VPC por parte del cliente.

Cuotas de instancias

Los propietarios y los consumidores del perfil comparten la misma cuota, excepto la cantidad de perfiles de Route 53 por cuenta en una región. Para obtener más información, consulte [Cuotas en perfiles de Route 53](#)

¿Qué es Amazon Route 53 on Outposts?

AWS Outposts es un servicio totalmente gestionado que extiende AWS las infraestructuras APIs, los servicios y las herramientas a las instalaciones del cliente. Esto permite a los clientes ejecutar AWS servicios con cargas de trabajo locales mediante las mismas interfaces de programación que en. Regiones de AWS Para obtener más información, consulte [¿Qué es? AWS Outposts](#) en la Guía AWS Outposts del usuario.

Route 53 on Outposts ofrece dos funciones:

- Un solucionador de VPC que almacena en caché todas las consultas de DNS que se originan en. AWS Outposts
- Puede configurar la conectividad híbrida entre un Outpost y un Resolver de DNS en las instalaciones mediante la implementación de puntos de conexión entrantes y salientes.

Para obtener más información, consulte [¿Qué es el solucionador de VPC Route 53?](#).

Además, Route 53 on Outposts reduce la latencia de la red permitiendo que las consultas se resuelvan dentro del Outpost en lugar de hacer el recorrido de ida y vuelta a la Región de AWS más cercana.

- Un solucionador de VPC que almacena en caché todas las consultas de DNS que se originan en. AWS Outposts
- Puede configurar la conectividad híbrida entre un Outpost y un Resolver de DNS en las instalaciones mediante la implementación de puntos de conexión entrantes y salientes.

Para obtener más información, consulte [¿Qué es el solucionador de VPC Route 53?](#).

Además, Route 53 on Outposts reduce la latencia de la red permitiendo que las consultas se resuelvan dentro del Outpost en lugar de hacer el recorrido de ida y vuelta a la Región de AWS más cercana.

Note

Si tienes una versión de los AWS Outposts racks que no es compatible con Route 53 en Outposts, AWS un equipo de cuentas recibirá una notificación y se pondrá en contacto contigo para ayudarte a actualizar. AWS Outposts

Información general de la arquitectura

Route 53 en Outposts implementa una arquitectura de DNS distribuida:

- Los registros DNS y las zonas alojadas siguen gestionados en Amazon Route 53 en la AWS región.
- La funcionalidad de resolución se extiende a su AWS Outposts rack para el procesamiento de consultas locales

Este diseño optimiza el rendimiento y la disponibilidad de las consultas y, al mismo tiempo, mantiene una administración centralizada de los registros de DNS. Los registros de DNS se siguen almacenando en la AWS región, no de forma local en el AWS Outposts rack.

Características de Amazon Route 53 on Outposts

En la siguiente tabla, se describe cómo se comparan las características de Route 53 on Outposts con las de Amazon Route 53.

Route 53 on Outposts comparado con Route 53

Característica	Disponibilidad en Route 53 on Outposts
Solucionador de VPC	Sí. El solucionador de VPC mantiene una caché local de registros para las aplicaciones alojadas en el rack de Outpost, la VPC interconectada del rack y cualquier nombre de host de Región de AWS acceso público.
Comprobaciones de estado	La cantidad de comprobaciones de estado se calculan e informan desde la Región de AWS. Si un Outpost se desconecta de la nube, los puntos de conexión no se abren y no se pueden realizar conmutaciones por error a una copia de seguridad.
Puntos de conexión de Resolver	Sí. Los puntos de conexión de Resolver en el rack del Outpost permiten que las consultas de DNS se reenvíen y reciban desde servidores de DNS en las instalaciones.

Característica	Disponibilidad en Route 53 on Outposts
	Solo el tipo de IPv4 punto final está disponible para los puntos finales.
Resolver DNS Firewall	No disponible.
Flujo de tráfico	No disponible.

Comportamiento del solucionador de VPC cuando AWS Outposts está desconectado de la VPC

Si AWS Outposts está desconectado de la Región de AWS, el Resolver de Outpost se comporta de la siguiente manera:

- Los cambios en el plano de control no están disponibles.
- Las comprobaciones de estado y la capacidad de conmutación por error de DNS no están disponibles.
- Las consultas de DNS para los recursos que están alojados localmente en los Outposts se resuelven, pero en algunos casos la respuesta puede quedar obsoleta si la dirección IP del recurso se actualizó mientras el Outpost estaba desconectado.
- Las consultas de DNS para los recursos alojados en la VPC de la región se pueden resolver. Sin embargo, no se podrá acceder a los recursos hasta que se restablezca la conexión de Outpost con Región de AWS .
- Las consultas de DNS para los recursos de DNS públicos se pueden resolver si están disponibles en la caché de VPC Resolver de Outpost.

Cómo empezar a usar VPC Resolver en AWS Outposts

Una vez que haya pedido sus AWS Outposts racks y los haya entregado, tal y como se describe aquí: [Cree](#) uno AWS Outposts en la AWS Outposts guía, podrá configurar Resolver en Outpost.

 Important

Solo la AWS cuenta propietaria del estante puede crear Resolver en Outpost. AWS Outposts
Si el AWS Outposts rack se comparte con otras cuentas, esas cuentas no pueden crear Resolver on Outpost en el rack compartido.

También puedes utilizarla APIs para gestionar Route 53 en Outposts. Para obtener más información, consulte [Acciones en Resolver on Outpost](#).

 Important

La creación de una caché de resolución de VPC en un. AWS Outposts

Una vez que te hayan entregado tus AWS Outposts estantes, puedes optar por Route 53 en Outposts.

Para configurar Resolver on Outpost

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/route53/>
2. En el panel de navegación izquierdo, expanda Resolver y, a continuación, navegue hasta Outposts.
3. En la barra de navegación, elija la región en la AWS Outposts que se encuentra.
4. En la página Resolver on Outpost, selecciona Crear resolución de VPC.
5. En la página Crear resolución de VPC:
 - En AWS OutpostsSeleccione una en la AWS Outposts que desee crear el solucionador de VPC.
 - Escriba un nombre para el solucionador de VPC en el cuadro de texto Nombre del solucionador de VPC.
 - Cuando los tipos de instancias recomendados para VPC Resolver se completen con las EC2 instancias de Amazon, elige uno.

Para obtener más información sobre los tipos de instancia, consulte [Cuotas de Resolver on Outpost](#).

- En Número de instancias, elija el número de instancias de interfaz elástica para el solucionador de VPC de VPC. El valor predeterminado es 4.

Si AWS Outposts no tienes un tipo de instancia que sea compatible con la resolución de VPC, no podrás crear una resolución de VPC.

6. Elija Crear resolución de VPC.

Puede supervisar la creación del solucionador de VPC en la página Resolver on Outpost.

Creación de puntos de conexión entrantes

Una vez que haya creado un Resolver en Outpost, puede agregar puntos de conexión entrantes y salientes para resolver las consultas de DNS que se realizan desde y hacia la red en las instalaciones.

Para configurar los puntos de conexión de entrada para Resolver on Outpost

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación izquierdo, expanda Resolver y, a continuación, navegue hasta Outposts.
3. En la barra de navegación, elija la región en la AWS Outposts que se encuentra.
4. Seleccione la casilla de verificación situada junto al solucionador de VPC que está en estado operativo y elija Ver detalles.
5. En la tabla de puntos de conexión entrantes, seleccione Crear punto de conexión entrante.
6. En la página Crear punto de conexión entrante, ingrese los valores aplicables. Para obtener más información, consulte [Valores que se especifican al crear o editar puntos de conexión de entrada en Outpost](#).
7. Seleccione Crear punto de conexión.

Valores que se especifican al crear o editar puntos de conexión de entrada en Outpost

Al crear o editar un punto de conexión de entrada, tiene que especificar los siguientes valores:

ID de Outpost

Si va a crear el punto final para un solucionador de VPC en una AWS Outposts VPC, este es el ID. AWS Outposts

Endpoint name (Nombre del punto de conexión)

Un nombre fácil de recordar que le permite encontrar fácilmente un punto de conexión de entrada en el panel.

VPC in the region-name Region (VPC en la región nombre-región)

Todas las consultas DNS entrantes de la red pasan por esta VPC hasta llegar a VPC Resolver.

Security group for this endpoint (Grupo de seguridad para este punto de conexión)

El ID de uno o varios grupos de seguridad que desea utilizar para controlar el acceso a este punto de conexión de entrada. El grupo de seguridad que especifique debe incluir una o más reglas de entrada. Las reglas de entrada deben permitir el acceso de TCP y UDP en el puerto 53. No puede cambiar este valor después de crear un punto de conexión.

Para obtener más información, consulte [Grupos de seguridad de su VPC](#) en la Guía del usuario de Amazon VPC.

Direcciones IP

Las direcciones IP que quiere asignar a los puntos de conexión de entrada. Le pedimos que especifique un mínimo de dos direcciones IP para la redundancia. Tenga en cuenta lo siguiente:

Direcciones IP e interfaces de red elásticas de Amazon VPC

Para cada combinación de zona de disponibilidad, subred y dirección IP que especifique, VPC Resolver crea una interfaz de red elástica de Amazon VPC. Para obtener información acerca del número máximo actual de consultas de DNS por segundo por cada dirección IP de un punto de conexión, consulte [Cuotas en el solucionador de VPC Route 53](#). Para obtener información acerca de los precios de cada interfaz de red elástica, consulte Amazon Route 53 en la [página de precios de Amazon Route 53](#).

Note

El punto de conexión de Resolver tiene una dirección IP privada. Estas direcciones IP no cambiarán a lo largo de la vida de un punto de conexión.

Para cada dirección IP, especifique los siguientes valores. Cada dirección IP debe estar en una zona de disponibilidad de la VPC que especificó en VPC in the region-name Region (VPC en la región nombre-región).

Zona de disponibilidad

La zona de disponibilidad por la que quiere que pasen las consultas de DNS en el recorrido hacia la VPC. La zona de disponibilidad que especifique debe estar configurada con una subred.

Subred

La subred que contiene la dirección IP a la que quiere reenviar las consultas de DNS. La subred debe tener una dirección IP disponible.

Especifique la subred de una dirección. IPv4 IPv6 no se admite.

Dirección IP

La dirección IP a la que quiere reenviar las consultas de DNS.

Elija si desea que VPC Resolver elija una dirección IP para usted de entre las direcciones IP disponibles en la subred especificada o si desea especificar la dirección IP usted mismo.

Si decide especificar la dirección IP usted mismo, introduzca una IPv4 dirección. IPv6 no se admite.

Tags

Especifique una o más claves y los valores correspondientes. Por ejemplo, puede especificar Centro de costos en Key (Clave) y 456 en Value (Valor).

Estas son las etiquetas Administración de facturación y costos de AWS que permiten organizar su AWS factura; también puede utilizarlas para otros fines. Para obtener más información sobre el uso de etiquetas para la asignación de costes, consulte [Uso de etiquetas de asignación de costes](#) en la Guía del usuario de AWS Billing .

Creación de puntos de conexión de salida

Una vez que hayas activado y configurado un solucionador de VPC, también puedes añadir puntos de enlace entrantes y salientes para resolver las consultas de DNS en tu red local.

 Note

Cuando configuras los puntos de conexión salientes, el solucionador de VPC almacena en caché las respuestas de DNS para que las consultas se puedan seguir resolviendo si tu Outpost se desconecta de la región. Si se mantiene esta caché, es posible que aumente el flujo de solicitudes de DNS a los solucionadores en las instalaciones.

Para configurar los puntos de conexión de salida para Resolver on Outpost

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/route53/>
2. En el panel de navegación izquierdo, expanda Resolver y, a continuación, navegue hasta Outposts.
3. En la barra de navegación, elija la región en la AWS Outposts que se encuentra.
4. Seleccione la marca de verificación situada junto al solucionador de VPC que está en estado operativo y elija Ver detalles.
5. En la tabla de puntos de conexión de salida, seleccione Crear punto de conexión de salida.
6. En la página Crear punto de conexión de salida, ingrese los valores aplicables. Para obtener más información, consulte [Valores que se especifican al crear o editar puntos de conexión de salida en un AWS Outposts](#).
7. Seleccione Crear punto de conexión.

Valores que se especifican al crear o editar puntos de conexión de salida en un AWS Outposts

Al crear o editar un punto de conexión de salida, tiene que especificar los siguientes valores:

ID de Outpost

Si va a crear el punto final para un solucionador de VPC en una AWS Outposts VPC, este es el ID. AWS Outposts

Endpoint name (Nombre del punto de conexión)

Un nombre fácil de recordar que le permite encontrar fácilmente un punto de conexión de salida en el panel.

VPC in the region-name Region (VPC en la región nombre-región)

Todas las consultas de DNS salientes de su VPC atraviesan esta VPC en el recorrido hacia su red.

Security group for this endpoint (Grupo de seguridad para este punto de conexión)

El ID de uno o varios grupos de seguridad que desea utilizar para controlar el acceso a esta VPC. El grupo de seguridad que especifique debe incluir una o más reglas de salida. Las reglas de salida deben permitir el acceso de TCP y UDP en el puerto que utiliza para las consultas de DNS de la red. No puede cambiar este valor después de crear un punto de conexión.

Para obtener más información, consulte [Grupos de seguridad de su VPC](#) en la Guía del usuario de Amazon VPC.

Direcciones IP

Las direcciones IP que quiere asignar a los puntos de conexión de salida. Le pedimos que especifique un mínimo de dos direcciones IP para la redundancia. Tenga en cuenta lo siguiente:

Direcciones IP e interfaces de red elásticas de Amazon VPC

Para cada combinación de zona de disponibilidad, subred y dirección IP que especifique, VPC Resolver crea una interfaz de red elástica de Amazon VPC. Para obtener información acerca del número máximo actual de consultas de DNS por segundo por cada dirección IP de un punto de conexión, consulte [Cuotas en el solucionador de VPC Route 53](#). Para obtener información acerca de los precios de cada interfaz de red elástica, consulte “Amazon Route 53” en la [página de precios de Amazon Route 53](#).

Note

El punto de conexión de Resolver tiene una dirección IP privada. Estas direcciones IP no cambiarán a lo largo de la vida de un punto de conexión.

Para cada dirección IP, especifique los siguientes valores. Cada dirección IP debe estar en una zona de disponibilidad de la VPC que especificó en VPC in the region-name Region (VPC en la región nombre-región).

Zona de disponibilidad

La zona de disponibilidad por la que quiere que pasen las consultas de DNS en el recorrido desde la VPC. La zona de disponibilidad que especifique debe estar configurada con una subred.

Subred

La subred que contiene la dirección IP desde la que quiere reenviar las consultas de DNS. La subred debe tener una dirección IP disponible.

Especifique la subred de una dirección. IPv4 IPv6 no se admite.

Dirección IP

La dirección IP que desea asignar a los puntos de conexión de salida.

Elija si desea que VPC Resolver elija una dirección IP para usted de entre las direcciones IP disponibles en la subred especificada o si desea especificar la dirección IP usted mismo.

Si decide especificar la dirección IP usted mismo, introduzca una IPv4 dirección. IPv6 no se admite.

Tags

Especifique una o más claves y los valores correspondientes. Por ejemplo, puede especificar Centro de costos en Key (Clave) y 456 en Value (Valor).

Estas son las etiquetas Administración de facturación y costos de AWS que permiten organizar su AWS factura; también puede utilizarlas para otros fines. Para obtener más información sobre el uso de etiquetas para la asignación de costes, consulte [Uso de etiquetas de asignación de costes](#) en la Guía del usuario de AWS Billing .

Creación de reglas de reenvío para los puntos de conexión de salida

También puede crear reglas de reenvío para los puntos de conexión salientes. Para obtener más información, consulte [Para crear reglas de reenvío y asociarlas a una o más VPCs](#)

Administración de Resolver on Outpost

Para administrar Resolver on Outpost, siga el procedimiento correspondiente.

Temas

- [Edición de Resolver on Outpost](#)
- [Ver el estado de Resolver on Outpost](#)
- [Eliminación de Resolver en Outpost](#)

Edición de Resolver on Outpost

Para editar un Resolver on Outpost, realice el siguiente procedimiento.

Para editar un Resolver en Outpost

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación izquierdo, expanda Resolver y, a continuación, navegue hasta Outposts.
3. En la barra de navegación, elija la región en la AWS Outposts que se encuentra.
4. Seleccione la marca de verificación situada junto al solucionador de VPC que está en estado operativo y elija Editar.
5. Puede editar la siguiente información:
 - El nombre del solucionador de VPC
 - El tipo de instancia
 - El número de instancias
6. Cuando haya terminado de editar, elija Guardar cambios.

Ver el estado de Resolver on Outpost

Para ver el estado de un punto de conexión saliente, realice el siguiente procedimiento.

Para ver el estado de un punto de conexión de entrada

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación izquierdo, expanda Resolver y, a continuación, navegue hasta Outposts.
3. En la barra de navegación, elija la región en la AWS Outposts que se encuentra.

4. Seleccione la marca de verificación situada junto al solucionador de VPC que está en estado operativo y elija Ver detalles.
5. La columna Estado de la página Resolver on Outpost contiene uno de los siguientes valores:

Creación

El Resolver on Outpost está en proceso de creación.

Operational (En funcionamiento)

El Resolver on Outpost está configurado correctamente.

Actualización

El Resolver on Outpost está actualizando los tipos de instancias.

Action needed (Acción necesaria)

Este solucionador de VPC no funciona correctamente y no se puede recuperar automáticamente. Para resolver el problema, te recomendamos que te asegures de que la instancia AWS Outposts sea compatible con Resolver en Outpost.

Eliminación

Resolver on Outpost está en proceso de borrarse.

Error de creación

No se pudo crear el Resolver en Outpost.

Error de eliminación

No se pudo eliminar el Resolver on Outpost. Para solucionar este problema, inténtalo de nuevo en unos minutos.

Eliminación de Resolver en Outpost

Note

Antes de eliminar un Resolver on Outpost, primero debe eliminar todos los puntos de conexión asociados con él.

Para eliminar un Resolver on Outpost, realice el siguiente procedimiento.

Para eliminar un Resolver on Outpost

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación izquierdo, expanda Resolver y, a continuación, navegue hasta Outposts.
3. En la barra de navegación, elija la región en la AWS Outposts que se encuentra.
4. Seleccione la casilla de verificación situada junto al solucionador de VPC que está en estado operativo y elija Eliminar.
5. En el cuadro de diálogo Eliminar VPC Resolver, introduzca **delete** en el cuadro de texto y elija Eliminar.

Administración de puntos de conexión de entrada de Resolver en Outpost

Para administrar los puntos de conexión entrantes en Resolver on Outpost, siga el procedimiento correspondiente.

Temas

- [Visualización y edición de puntos de conexión de entrada](#)
- [Visualización del estado de los puntos de conexión de entrada](#)
- [Eliminación de puntos de conexión de entrada](#)

Visualización y edición de puntos de conexión de entrada

Para ver y editar la configuración de un punto de conexión de entrada, realice el siguiente procedimiento.

Para ver y editar la configuración de un punto de conexión de entrada

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación izquierdo, expanda Resolver y, a continuación, navegue hasta Outposts.
3. En la barra de navegación, elija la región en la AWS Outposts que se encuentra.

4. Seleccione la casilla de verificación situada junto al solucionador de VPC que está en estado operativo y elija Ver detalles.
5. En la lista de puntos de conexión de entrada, elija la opción correspondiente al punto de conexión cuya configuración desea ver o editar.
6. Elija View details (Ver detalles) o Edit (Editar).

Para obtener información acerca de los valores para los puntos de conexión de entrada, consulte [Valores que se especifican al crear o editar puntos de conexión de salida en un AWS Outposts](#).

7. Si eligió Edit (Editar), escriba los valores correspondientes y elija Save (Guardar).

Visualización del estado de los puntos de conexión de entrada

Para ver el estado de un punto de conexión de entrada, realice el procedimiento siguiente.

Para ver el estado de un punto de conexión de entrada

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación izquierdo, expanda Resolver y, a continuación, navegue hasta Outposts.
3. En la barra de navegación, elija la región en la AWS Outposts que se encuentra.
4. Seleccione la casilla de verificación situada junto al solucionador de VPC que está en estado operativo y elija Ver detalles.
5. La columna Estado en la lista de puntos de conexión entrantes contiene uno de los siguientes valores:

Creación

El solucionador de VPC crea y configura una o más interfaces de red de Amazon VPC para este punto final.

Operational (En funcionamiento)

Las interfaces de red de Amazon VPC para este punto de conexión están configuradas correctamente y pueden transmitir consultas de DNS entrantes o salientes entre su red y VPC Resolver.

Actualización

El solucionador está asociando o disociando una o más interfaces de red con este punto de conexión.

Auto recovering (Recuperación automática)

El solucionador de VPC está intentando recuperar una o más de las interfaces de red asociadas a este punto final. Durante el proceso de recuperación, el punto de conexión opera con una capacidad limitada debido al límite en el número de consultas de DNS por dirección IP (por interfaz de red). Para ver el límite actual, consulte [Cuotas en el solucionador de VPC Route 53](#).

Action needed (Acción necesaria)

Este punto final está en mal estado y VPC Resolver no puede recuperarlo automáticamente. Para solucionar el problema, le recomendamos que compruebe cada dirección IP que haya asociado al punto de conexión. Para cada dirección IP que no esté disponible, añada otra dirección IP y, a continuación, elimine la dirección IP que no esté disponible. Un punto de conexión siempre debe incluir al menos dos direcciones IP. Un estado de Action needed (Acción necesaria) puede deberse a varios motivos. Estas son dos causas comunes:

- Se ha eliminado una o más interfaces de red asociadas al punto de conexión mediante Amazon VPC.
- No se pudo crear la interfaz de red por alguna razón ajena al control de VPC Resolver.

Eliminación

El solucionador está eliminando este punto de conexión y las interfaces de red asociadas.

Eliminación de puntos de conexión de entrada

Para eliminar un punto de conexión de entrada, siga el procedimiento que se indica a continuación.

Important

Si elimina un punto de enlace entrante, las consultas de DNS de su red ya no se reenvían al Resolver de VPC en la VPC que especificó en el punto de enlace.

Para eliminar un punto de conexión de entrada

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/route53/>
2. En el panel de navegación izquierdo, expanda Resolver y, a continuación, navegue hasta Outposts.
3. En la barra de navegación, elija la región en la AWS Outposts que se encuentra.
4. Seleccione la casilla de verificación situada junto al solucionador de VPC que está en estado operativo y elija Ver detalles.
5. Seleccione la casilla de verificación junto al punto de conexión que desea eliminar.
6. Elija Eliminar.
7. Para confirmar que desea eliminar el punto de conexión, escriba el nombre del punto de conexión y elija Submit (Enviar).

Administración de puntos de conexión de salida de Resolver on Outpost

Para administrar los puntos de conexión de salida en Resolver on Outposts, siga el procedimiento correspondiente.

Temas

- [Visualización y edición de puntos de conexión de salida](#)
- [Visualización del estado de los puntos de conexión de salida](#)
- [Eliminación de puntos de conexión de salida](#)

Visualización y edición de puntos de conexión de salida

Para ver y editar la configuración de un punto de conexión de salida, realice el siguiente procedimiento.

Para ver y editar la configuración de un punto de conexión de salida

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.

2. En el panel de navegación izquierdo, expanda Resolver y, a continuación, navegue hasta Outposts.
3. En la barra de navegación, elija la región en la AWS Outposts que se encuentra.
4. Seleccione la casilla de verificación situada junto al solucionador de VPC que está en estado operativo y elija Ver detalles.
5. En la lista Puntos de conexión de salida, seleccione la casilla de verificación junto al punto de conexión cuya configuración desea editar o ver.
6. Elija View details (Ver detalles) o Edit (Editar).

Para obtener información acerca de los valores de los puntos de conexión de salida, consulte [Valores que se especifican al crear o editar puntos de conexión de salida en un AWS Outposts](#).

7. Si eligió Edit (Editar), escriba los valores correspondientes y, a continuación, elija Save (Guardar).

Visualización del estado de los puntos de conexión de salida

Para ver el estado de un punto de conexión de salida, realice el procedimiento siguiente.

Para ver el estado de un punto de conexión de salida

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación izquierdo, expanda Resolver y, a continuación, navegue hasta Outposts.
3. En la barra de navegación, elija la región en la AWS Outposts que se encuentra.
4. Seleccione la casilla de verificación situada junto al solucionador de VPC que está en estado operativo y elija Ver detalles.
5. En la lista de puntos de conexión de salida, la columna Estado contiene uno de los siguientes valores:

Creación

El solucionador de VPC crea y configura una o más interfaces de red de Amazon VPC para este punto final.

Operational (En funcionamiento)

Las interfaces de red de Amazon VPC para este punto de conexión están configuradas correctamente y pueden transmitir consultas de DNS entrantes o salientes entre su red y VPC Resolver.

Actualización

El solucionador está asociando o disociando una o más interfaces de red con este punto de conexión.

Auto recovering (Recuperación automática)

El solucionador de VPC está intentando recuperar una o más de las interfaces de red asociadas a este punto final. Durante el proceso de recuperación, el punto de conexión opera con una capacidad limitada debido al límite en el número de consultas de DNS por dirección IP (por interfaz de red). Para ver el límite actual, consulte [Cuotas en el solucionador de VPC Route 53](#).

Action needed (Acción necesaria)

Este punto final está en mal estado y VPC Resolver no puede recuperarlo automáticamente. Para solucionar el problema, le recomendamos que compruebe cada dirección IP que haya asociado al punto de conexión. Para cada dirección IP que no esté disponible, añada otra dirección IP y, a continuación, elimine la dirección IP que no esté disponible. (Un punto de conexión siempre debe incluir al menos dos direcciones IP). Un estado de Action needed (Acción necesaria) puede deberse a varios motivos. Estas son dos causas comunes:

- Se ha eliminado una o más interfaces de red asociadas al punto de conexión mediante Amazon VPC.
- No se pudo crear la interfaz de red por alguna razón ajena al control de VPC Resolver.

Eliminación

El solucionador está eliminando este punto de conexión y las interfaces de red asociadas.

Eliminación de puntos de conexión de salida

Para poder eliminar un punto de conexión, primero debe eliminar las reglas que estén asociadas a una VPC.

Para eliminar un punto de conexión de salida, siga el procedimiento que se indica a continuación.

 Important

Si eliminas un endpoint de salida, VPC Resolver deja de reenviar las consultas de DNS de tu VPC a tu red para las reglas que especifican el endpoint de salida eliminado.

Para eliminar un punto de conexión de salida

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/route53/>
2. En el panel de navegación izquierdo, expanda Resolver y, a continuación, navegue hasta Outposts.
3. Seleccione la casilla de verificación situada junto al solucionador de VPC que está en estado operativo y elija Ver detalles.
4. En la lista puntos de conexión de salida, elija la opción correspondiente al punto de conexión que desea eliminar.
5. Elija Eliminar.
6. Para confirmar que desea eliminar el punto de conexión, escriba el nombre del punto de conexión y, a continuación, elija Submit (Enviar).

¿Qué es Route 53 Global Resolver?

Route 53 Global Resolver es un solucionador de DNS con acceso a Internet que proporciona una resolución de DNS fácil, segura y confiable para los clientes autorizados de su organización en ubicaciones remotas, sucursales y entornos locales. Puede resolver consultas para dominios alojados en Amazon Route 53, zonas alojadas privadas o dominios públicos en Internet y, al mismo tiempo, mantener una alta disponibilidad mediante la arquitectura anycast global. Route 53 Global Resolver lo ayuda a proteger a sus clientes de los ataques de exfiltración de datos basados en DNS mediante el filtrado de consultas a dominios potencialmente maliciosos.

Route 53 Global Resolver usa direcciones IP anycast que enrutan automáticamente las consultas de DNS a la AWS región más cercana a la ubicación de la consulta de origen para lograr una latencia y disponibilidad óptimas. Puede seleccionar las regiones desde las que su solucionador global debe proporcionar la resolución de DNS a sus clientes autorizados, configurar diferentes vistas para los clientes para la resolución de dominios públicos y privados, filtrar los dominios maliciosos y supervisar la actividad del DNS en toda su organización.

Temas

- [¿Por qué Route 53 Global Resolver?](#)
- [Conceptos y componentes clave de Route 53 Global Resolver](#)
- [Cómo funciona Route 53 Global Resolver](#)
- [Casos de uso de seguridad de DNS y horizonte dividido para Route 53 Global Resolver](#)
- [AWS servicios que se integran con Route 53 Global Resolver para mejorar la seguridad del DNS](#)
- [Cómo acceder y administrar Route 53 Global Resolver a través de AWS interfaces](#)
- [Compatible Regiones de AWS](#)
- [Configuración del acceso a la cuenta para Route 53 Global Resolver](#)
- [Tutorial: Cree su primer Route 53 Global Resolver](#)
- [Administración de vistas de DNS con Route 53 Global Resolver](#)
- [Administrar los controles de acceso con fuentes de acceso y tokens en Route 53 Global Resolver](#)
- [Protección del DNS para los clientes con Route 53 Global Resolver](#)
- [Configuración de asociaciones de zonas alojadas privadas con Route 53 Global Resolver](#)
- [Supervisión de la actividad y el rendimiento del DNS con Route 53 Global Resolver](#)
- [Solución de problemas de DNS con Route 53 Global Resolver](#)

- [Cuotas para Route 53 Global Resolver](#)

¿Por qué Route 53 Global Resolver?

Route 53 Global Resolver proporciona seguridad y filtrado de DNS centralizados para cargas de trabajo y clientes remotos e híbridos en varias ubicaciones. Independientemente de la ubicación de sus cargas de trabajo, aplicaciones o usuarios, Route 53 Global Resolver garantiza una protección de DNS uniforme sin requerir una infraestructura local compleja.

Ventajas clave para los entornos remotos e híbridos:

- Administración simplificada: configure la resolución de dominios públicos y privados mediante una única solución en lugar de administrar varios servidores DNS locales
- Seguridad de DNS unificada: aplique políticas de filtrado coherentes en todos los clientes remotos y cargas de trabajo híbridas
- Protección escalable: se escala automáticamente para gestionar las consultas de DNS de las crecientes fuerzas de trabajo remotas y las cargas de trabajo en la nube
- Infraestructura reducida: minimiza la necesidad de dispositivos de seguridad de DNS en cada ubicación remota

Para empezar, consulte:

- [the section called “Conceptos y terminología”](#)- Conceptos básicos para la implementación de la seguridad del DNS
- [the section called “Funcionamiento”](#)- Cómo protege Route 53 Global Resolver los entornos remotos e híbridos
- [the section called “Tutorial: Cree su primer Route 53 Global Resolver”](#)- Tutorial para su primera configuración de filtrado de DNS

Conceptos y componentes clave de Route 53 Global Resolver

Route 53 Global Resolver utiliza varios componentes clave que funcionan en conjunto para proporcionar una resolución de DNS de tráfico dividido, alta disponibilidad a través de una arquitectura anycast global y una seguridad de DNS integral para su organización. Comprender estos conceptos de Route 53 Global Resolver le ayuda a diseñar e implementar soluciones que permiten

un acceso sin problemas a los recursos públicos y privados, garantizan la continuidad del servicio en varias regiones y protegen contra las amenazas basadas en el DNS.

Resolución de DNS para clientes en ubicaciones locales y remotas

Para implementar Route 53 Global Resolver en sus cargas de trabajo distribuidas, ubicaciones de clientes y usuarios, configure estos componentes clave:

Resolver global

La instancia de servicio principal que proporciona resolución y filtrado de DNS para su organización en varias AWS regiones. Su solucionador global utiliza la tecnología anycast para dirigir automáticamente las consultas de DNS a la región disponible más cercana, lo que garantiza tiempos de respuesta rápidos para todos los clientes, independientemente de su ubicación.

Direcciones IP de Anycast

Dos IPv6 direcciones IPv4 OR únicas asignadas a su resolución global que usted configura en los dispositivos cliente y en los equipos de red. Estas direcciones IP anycast son las mismas en todo el mundo, lo que simplifica la configuración del DNS en todas sus ubicaciones. El direccionamiento IP Anycast permite el enrutamiento automático de las solicitudes de DNS a la resolución global más cercana, lo que optimiza los tiempos de respuesta y mejora la confiabilidad del servicio.

Vistas de DNS

Plantillas de configuración que le permiten aplicar distintas políticas de DNS a distintos grupos de clientes de la red. Utilice las vistas de DNS para implementar un DNS de horizonte dividido; por ejemplo, aplique filtros estrictos y una autenticación mediante token para las ubicaciones remotas, y utilice el acceso basado en IP y diferentes políticas de seguridad para las sucursales.

Autenticación de clientes DNS

Seleccione el método de autenticación que mejor se adapte a su implementación:

Autenticación basada en token

Proteja las conexiones DNS mediante tokens cifrados para DNS-over-HTTPS (DoH) y DNS-over-TLS (DoT). Puede generar tokens de acceso únicos para clientes individuales o grupos de dispositivos, establecer períodos de caducidad y revocar los tokens según sea necesario.

Acceda a la autenticación basada en la fuente

Controle el acceso mediante listas de direcciones IP y rangos de CIDR permitidos. Puede configurar las direcciones IP públicas o los rangos de redes de la sucursal y, a continuación, especificar qué protocolos de DNS (DNS-over-Port-53, DoT o DoH) puede usar cada ubicación en función de sus requisitos de seguridad.

Selección del protocolo DNS

Elija el protocolo DNS adecuado en función de sus necesidades de seguridad y compatibilidad:

- DNS a través del puerto 53 (Do53): utilícelo para obtener la máxima compatibilidad con la infraestructura de red existente
- DNS-over-TLS (DoT): utilícelo cuando necesite un DNS cifrado con separación de puertos dedicada para la supervisión de la red
- DNS-over-HTTPS (DoH): úselo cuando necesite eludir las restricciones de la red, ya que el tráfico aparece como HTTPS normal

Resolución de DNS de tráfico dividido

Route 53 Global Resolver permite a las organizaciones resolver sin problemas dominios públicos y privados desde cualquier ubicación, lo que elimina la necesidad de configuraciones de VPN complejas o configuraciones de DNS específicas de la región.

Resolución de DNS híbrida

La resolución de DNS híbrido permite a Route 53 Global Resolver resolver simultáneamente las consultas de usuarios y aplicaciones locales a aplicaciones privadas en AWS ellas.

Acceso a la zona privada global

El acceso a la zona privada global amplía el alcance de las zonas alojadas privadas de Amazon Route 53 más allá de los límites de la VPC. Los clientes autorizados de cualquier parte de Internet pueden resolver los nombres de dominio privados, lo que permite a los equipos distribuidos acceder a los recursos internos sin los requisitos de conectividad de red tradicionales.

Conmutación por error perfecta

La conmutación por error perfecta garantiza el acceso continuo a los recursos públicos y privados, incluso cuando AWS las regiones individuales no estén disponibles. La arquitectura anycast enruta automáticamente las consultas a las regiones en buen estado y, al mismo tiempo, mantiene un comportamiento de resolución uniforme.

Alta disponibilidad y presencia global

Route 53 Global Resolver proporciona disponibilidad de nivel empresarial a través de una arquitectura distribuida y capacidades de conmutación por error automática.

Implementación en varias regiones

La implementación multirregional distribuye las instancias de Route 53 Global Resolver en al menos 2 AWS regiones para garantizar una alta disponibilidad y permitir la conmutación por error durante las interrupciones del servicio. Puede seleccionar regiones específicas en función de sus requisitos geográficos y de conformidad.

Optimización geográfica automática

La optimización geográfica automática dirige las consultas de DNS a la AWS región disponible más cercana en función de la topología y la latencia de la red. Esto reduce los tiempos de respuesta y mejora la experiencia del usuario para las organizaciones distribuidas por todo el mundo.

Redundancia integrada

La redundancia integrada garantiza la continuidad del servicio mediante la conmutación automática por error a regiones alternativas cuando las regiones principales dejan de estar disponibles. Los clientes siguen utilizando las mismas direcciones IP de transmisión automática mientras el tráfico se redirige de forma transparente.

Resolución y reenvío de DNS

Resolución de zonas alojadas privadas

La resolución de zonas alojadas privadas permite a Route 53 Global Resolver resolver las consultas de DNS para las zonas alojadas privadas de Route 53 en todas AWS las regiones. Esto permite a los clientes autorizados resolver los dominios de las aplicaciones y los recursos alojados en Route 53 desde cualquier lugar de Internet.

DNS de horizonte dividido

El DNS de horizonte dividido proporciona diferentes respuestas de DNS en función del cliente que realiza la consulta. Route 53 Global Resolver puede resolver dominios públicos en Internet y, al mismo tiempo, resolver dominios privados, lo que proporciona un acceso perfecto a los recursos públicos y privados.

Validación de DNSSEC

La validación de DNSSEC verifica la autenticidad e integridad de las respuestas de DNS de los servidores de nombres públicos para los dominios firmados por el DNSSEC. Esta validación garantiza que las respuestas del DNS no se hayan manipulado durante la transmisión, lo que proporciona protección contra los ataques de suplantación de DNS y de envenenamiento de la caché.

Subred de clientes EDNS (ECS)

La subred de clientes de EDNS es una función opcional que reenvía la información de la subred del cliente en las consultas de DNS a servidores de nombres autorizados. Esto permite respuestas de DNS geográficas más precisas, lo que podría reducir la latencia al dirigir a los clientes a redes o servidores de entrega de contenido más cercanos. Para las conexiones DNS-over-TLS (DoT) y DNS-over-HTTPS (DoH), puede usar EDNS0 para transmitir la información de la dirección IP del cliente. Cuando ECS está activado en Global Resolver, el servicio inyecta automáticamente la IP del cliente si no se proporciona en la consulta.

Filtrado de DNS y listas de dominios

Route 53 Global Resolver proporciona un filtrado basado en dominios mediante listas de dominios administradas por AWS para bloquear o permitir dominios específicos.

Reglas de filtrado de DNS

Las reglas de filtrado de DNS definen la forma en que Route 53 Global Resolver gestiona las consultas de DNS en función de los criterios de coincidencia de dominios. Las reglas se evalúan por orden de prioridad y pueden especificar acciones (PERMITIR, BLOQUEAR o ALERTAR) para las consultas a dominios o categorías de dominios específicos.

Listas de dominios

Las listas de dominios son conjuntos de dominios que se utilizan en las reglas de filtrado. Pueden ser:

- Listas de dominios personalizadas: colecciones de dominios que usted crea y mantiene
- AWS listas de dominios gestionadas: las listas de amenazas y las categorías de contenido preconfiguradas AWS que mantienen utilizan la inteligencia sobre amenazas para identificar los dominios maliciosos. Las listas de amenazas disponibles incluyen:
 - Dominios de malware: dominios conocidos por alojar o distribuir malware

- Comando y control de botnets: dominios utilizados por las botnets para las comunicaciones de mando y control
- Correo no deseado: dominios asociados a campañas de spam y correo electrónico no deseado
- Suplantación de identidad: dominios utilizados en los ataques de suplantación de identidad para robar credenciales e información personal
- Lista de GuardDuty amenazas de Amazon: dominios identificados por la inteligencia de GuardDuty amenazas

Las categorías de contenido disponibles incluyen las redes sociales, los juegos de azar y otras categorías que ayudan a las organizaciones a controlar el acceso a tipos específicos de contenido.

Las especificaciones de dominio individuales de las listas gestionadas no se pueden ver ni editar para proteger la propiedad intelectual y mantener la eficacia de la seguridad.

Detección avanzada de amenazas de DNS

Route 53 Global Resolver utiliza un análisis algorítmico dinámico para detectar amenazas de DNS avanzadas, como la tunelización de DNS y los algoritmos de generación de dominios. A diferencia de las listas de dominios que coinciden con los dominios defectuosos conocidos, la detección algorítmica analiza los patrones de consulta del DNS en tiempo real para identificar comportamientos sospechosos.

Detección de túneles de DNS

Los atacantes utilizan los túneles de DNS para extraer datos del cliente mediante el uso del túnel de DNS sin establecer una conexión de red con el cliente.

Detección del algoritmo de generación de dominios (DGA)

Los atacantes utilizan los algoritmos de generación de dominios (DGAs) para crear un gran número de nombres de dominio para sus command-and-control servidores.

Umbrales de confianza

Cada algoritmo de detección genera una puntuación de confianza que determina la activación de la regla. Los umbrales de confianza más altos reducen los falsos positivos, pero pueden pasar

por alto los ataques sofisticados. Los umbrales más bajos aumentan la sensibilidad de detección, pero requieren un análisis de alerta adicional para filtrar los falsos positivos.

Limitaciones de acción

Solo admiten reglas avanzadas de protección contra amenazas ALERT y BLOCK acciones. Esta ALLOW acción no es compatible porque la detección algorítmica no puede clasificar definitivamente el tráfico benigno, sino que solo identifica patrones potencialmente maliciosos.

Supervisión y registro

Consulta de registros de

Los registros de consultas proporcionan información detallada sobre las consultas de DNS procesadas por Route 53 Global Resolver, incluida la IP de origen, el dominio consultado, el código de respuesta, las medidas políticas adoptadas y las marcas de tiempo. Los registros se pueden enviar a Amazon CloudWatch, Amazon Data Firehose o Amazon Simple Storage Service para su análisis y elaboración de informes de conformidad.

Formato OCSF

El formato Open Cybersecurity Schema Framework (OCSF) es un formato de registro estandarizado utilizado por Route 53 Global Resolver para los registros de consultas de DNS. Este formato proporciona datos estructurados y consistentes que se integran fácilmente con los sistemas de información de seguridad y gestión de eventos (SIEM) y otras herramientas de seguridad.

Registro de destinos

Los destinos de los registros determinan dónde se envían los registros de consultas de DNS, cada uno con características diferentes:

- Amazon Simple Storage Service: almacenamiento rentable a largo plazo ideal para el cumplimiento y el análisis de lotes. Se integra con herramientas de análisis como Amazon Athena y Amazon EMR.
- Amazon CloudWatch Logs: monitoreo y alertas en tiempo real con integración a CloudWatch las alarmas y los paneles de Amazon. Admite la información de registros para consultas ad hoc.
- Amazon Data Firehose: transmisión en tiempo real a sistemas externos con funciones de transformación de datos integradas. Admite el escalado y el almacenamiento en búfer automáticos.

Región de observabilidad

La región de observabilidad determina dónde se entregan los registros de consultas de DNS.

Cómo funciona Route 53 Global Resolver

Route 53 Global Resolver permite la resolución de DNS de tráfico dividido entre dominios públicos y privados, proporciona alta disponibilidad a través de los dos o más Regiones de AWS que elija y protege las consultas de DNS interceptando las solicitudes y aplicando políticas de filtrado de DNS. Comprender este proceso le ayuda a solucionar problemas y a optimizar su implementación en términos de rendimiento, disponibilidad y seguridad.

¿Qué ocurre cuando los clientes realizan consultas de DNS

Cuando alguien en su ubicación intenta consultar el dominio, Route 53 Global Resolver procesa su solicitud de DNS a través de varios niveles de seguridad.

El procesamiento de las consultas de DNS implica estos pasos secuenciales:

1. **Recepción de consultas:** los dispositivos cliente envían consultas de DNS a las direcciones IP anycast de Route 53 Global Resolver. El enrutamiento anycast dirige automáticamente las consultas a la región más cercana AWS .
2. **Autenticación:** Route 53 Global Resolver autentica al cliente mediante métodos de autenticación configurados (basados en token DoH/DoT o fuente de acceso IP para todos los protocolos).
3. **Evaluación de políticas:** el servicio evalúa las consultas de DNS comparándolas con las políticas de seguridad y las listas de dominios configuradas para determinar la acción adecuada (permitir, bloquear o alertar). Para las consultas dirigidas a zonas alojadas privadas, Route 53 Global Resolver comprueba si el cliente está autorizado a acceder al dominio privado según la regla de visualización de DNS administrada por el administrador antes de continuar con la resolución.
4. **Resolución:** para las consultas permitidas, Route 53 Global Resolver realiza la resolución de DNS mediante resolutores de DNS públicos o una resolución de zona alojada privada, según corresponda.
5. **Entrega de respuestas:** el servicio devuelve la respuesta de DNS al cliente y registra los detalles de la consulta para su supervisión y análisis.

Arquitectura anycast global

Route 53 Global Resolver utiliza direcciones IP anycast para proporcionar disponibilidad global y enrutamiento geográfico automático.

Route 53 Global Resolver usa direcciones IP anycast para proporcionar:

- Enrutamiento geográfico automático: las consultas de DNS se redirigen automáticamente a la AWS región más cercana para obtener un rendimiento óptimo.
- Redundancia integrada: si una región deja de estar disponible, el tráfico se transfiere automáticamente a la siguiente región más cercana.
- Direcciones IP coherentes: los clientes utilizan las mismas direcciones IP de transmisión automática independientemente de su ubicación, lo que simplifica la configuración.

Filtrado y seguridad de DNS

Route 53 Global Resolver proporciona seguridad y filtrado de DNS integrales a través de múltiples capas. El diagrama de la arquitectura de filtrado y seguridad del DNS ilustra cómo se procesan las consultas mediante las capas de autenticación, evaluación de políticas y resolución.

Route 53 Global Resolver proporciona una seguridad de DNS integral a través de:

- Filtrado basado en dominios: bloquee o permita consultas basadas en nombres de dominio mediante listas de dominios personalizadas o AWS administradas.
- Integración de la inteligencia de amenazas: aproveche la inteligencia de amenazas AWS gestionada para bloquear automáticamente los dominios maliciosos conocidos.
- Detección avanzada de amenazas: detecte y bloquee los intentos de creación de túneles en el DNS y los patrones del algoritmo de generación de dominios (DGA).
- Supervisión en tiempo real: genere alertas y registros de eventos de seguridad e infracciones de políticas.

Casos de uso de seguridad de DNS y horizonte dividido para Route 53 Global Resolver

Route 53 Global Resolver aborda tres desafíos principales del DNS para las organizaciones:

Permite dividir el tráfico entre la resolución de DNS pública y privada

Habilite el acceso global a las zonas alojadas privadas (PHZs) en Amazon Route 53 desde cualquier ubicación y, al mismo tiempo, resuelva los dominios públicos en Internet. Permita que las sucursales y ubicaciones remotas resuelvan los nombres de las aplicaciones internas sin complejas configuraciones de VPN ni reenvíos específicos de cada región. Implemente un DNS de horizonte dividido para proporcionar diferentes respuestas de DNS en función del cliente que realiza la consulta, lo que ayuda a los clientes remotos a resolver las consultas de dominios públicos y privados.

Proteja el tráfico de DNS de los ataques de exfiltración de DNS

Proteja las ubicaciones y sucursales remotas de los ataques de exfiltración de datos basados en el DNS filtrando las consultas a dominios maliciosos. Mejore la privacidad cifrando el tráfico de DNS en tránsito mediante DNS-over-HTTPS (DoH) y DNS-over-TLS (DoT) para garantizar que solo los clientes autorizados puedan acceder a sus servicios de DNS. Aplica políticas de seguridad para bloquear amenazas como los túneles de DNS y los algoritmos de generación de dominios (). DGAs Valide la autenticidad de la respuesta del DNS mediante las DNSSEC (extensiones de seguridad del sistema de nombres de dominio) para los dominios firmados por el DNSSEC a fin de protegerse contra los ataques de suplantación de DNS y de envenenamiento de la caché.

Alta disponibilidad y presencia global

Logre una alta disponibilidad mediante la implementación global y mantenga una configuración de DNS uniforme en todo el mundo desde una única interfaz de administración. Route 53 Global Resolver se ejecuta en todas las regiones que Regiones de AWS usted elija y utiliza direcciones IP anycast que dirigen automáticamente las consultas a la región disponible más cercana para lograr un rendimiento y una confiabilidad óptimos. Las empresas globales pueden configurar y administrar las políticas de DNS de forma centralizada y, al mismo tiempo, proporcionar a los clientes un conjunto único de direcciones IP que funcionan a nivel mundial con una optimización geográfica automática. La redundancia integrada garantiza la continuidad del servicio incluso si las regiones individuales dejan de estar disponibles.

Las capacidades adicionales respaldan estos casos de uso principales:

Implementación de políticas de contenido y filtrado de DNS

Controle el acceso a Internet en varias ubicaciones mediante la creación de listas de dominios personalizadas o mediante listas de dominios AWS gestionadas. Para ayudarle a implementar

políticas de filtrado y contenido de acuerdo con sus necesidades, las listas de dominios gestionadas incluyen varias categorías de amenazas al DNS que abarcan varios dominios. Configure la fuente de acceso mediante listas de IP permitidas o tokens de acceso, y configure diferentes políticas de filtrado para diferentes ubicaciones de oficinas o grupos de clientes.

Autenticación flexible para diferentes escenarios de implementación

Elija el método de autenticación que mejor se adapte a su implementación: autenticación basada en token o autenticación basada en IP mediante las listas de permisos del rango CIDR de origen.

Mantener la visibilidad y el cumplimiento

Supervisa la actividad de DNS en toda tu organización enviando los registros a Amazon CloudWatch, Firehose o Amazon Simple Storage Service. Elija una región de destino única para el almacenamiento centralizado de registros a fin de respaldar las auditorías de seguridad, los requisitos de conformidad y la investigación de amenazas.

AWS servicios que se integran con Route 53 Global Resolver para mejorar la seguridad del DNS

Route 53 Global Resolver se integra perfectamente con otros AWS servicios para proporcionar capacidades integrales de administración y seguridad del DNS. Estas integraciones mejoran la funcionalidad principal de Route 53 Global Resolver y permiten casos de uso avanzados:

Amazon Route 53

Route 53 Global Resolver se integra con Amazon Route 53 para resolver zonas alojadas privadas en todo el mundo. Para obtener más información, consulte la [Guía para desarrolladores de Amazon Route 53](#).

Amazon CloudWatch

Route 53 Global Resolver puede enviar registros de consultas a Amazon CloudWatch para su supervisión y análisis. Para obtener más información, consulta la [Guía del CloudWatch usuario de Amazon](#).

Amazon Simple Storage Service

Route 53 Global Resolver puede almacenar registros de consultas en depósitos de Amazon Simple Storage Service para su almacenamiento y análisis a largo plazo. Para obtener más información, consulte la [Guía del usuario de Amazon S3](#).

Amazon Data Firehose

Route 53 Global Resolver puede transmitir los registros de consultas a Amazon Data Firehose para su procesamiento en tiempo real. Para obtener más información, consulte la [Guía para desarrolladores de Amazon Data Firehose](#).

DNS Firewall de Route 53 Resolver

Route 53 Global Resolver complementa el firewall DNS de Route 53 Resolver al proporcionar capacidades de filtrado de DNS globales. Para obtener más información, consulte la [documentación del Firewall DNS de Route 53 Resolver](#).

AWS Global Accelerator

Route 53 Global Resolver funciona AWS Global Accelerator para proporcionar un rendimiento de red global optimizado para la resolución de DNS. Para obtener más información, consulte la [Guía para desarrolladores de AWS Global Accelerator](#).

Cómo acceder y administrar Route 53 Global Resolver a través de AWS interfaces

Route 53 Global Resolver proporciona varios métodos de acceso para adaptarse a las diferentes preferencias de administración y requisitos de automatización. Puede administrar Route 53 Global Resolver a través de estas interfaces:

Consola de administración de AWS

Consola de administración de AWS Proporciona una interfaz basada en la web para Route 53 Global Resolver. Puede usar la consola para configurar las políticas de filtrado de DNS, administrar la configuración de autenticación y monitorear los registros de consultas.

AWS Command Line Interface (AWS CLI)

AWS CLI Proporciona acceso directo a las operaciones de la API Global Resolver de Route 53. Puede usarlo AWS CLI para automatizar las tareas de Route 53 Global Resolver e integrarlas en sus scripts y flujos de trabajo.

AWS SDKs

AWS proporciona SDKs muchos lenguajes de programación. Puede usarlo SDKs para integrar la funcionalidad de Cloud Resolver en sus aplicaciones.

API de REST

Route 53 Global Resolver proporciona una API REST que puede usar para administrar mediante programación sus políticas de filtrado y resolución de DNS.

Compatible Regiones de AWS

Route 53 Global Resolver está disponible en las siguientes versiones Regiones de AWS:

- Región Este de EE. UU. (Norte de Virginia)
- Región del este de EE. UU. (Ohio)
- Región del oeste de EE. UU. (Norte de California)
- Región del oeste de EE. UU. (Oregón)
- Región de Europa (Fráncfort)
- Región de Europa (Irlanda)
- Región de Europa (Londres)
- Región de Asia-Pacífico (Bombay)
- Región de Asia-Pacífico (Singapur)
- Asia-Pacífico (Tokio)
- Región de Asia-Pacífico (Sídney)

Configuración del acceso a la cuenta para Route 53 Global Resolver

Antes de empezar a usar Route 53 Global Resolver, necesita una AWS cuenta y los permisos adecuados para acceder a los recursos de Route 53 Global Resolver. Esto incluye la creación de usuarios y roles de IAM con los permisos necesarios.

Esta sección lo guía a través de los pasos necesarios para configurar los usuarios y las funciones para acceder a Route 53 Global Resolver.

Temas

- [Inscríbase en una Cuenta de AWS](#)
- [Creación de un usuario con acceso administrativo](#)

- [Crear políticas y roles](#)
- [Consideraciones sobre la red](#)

Inscríbase en una Cuenta de AWS

Si no tiene una Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirse a una Cuenta de AWS

1. Abrir <https://portal.aws.amazon.com/billing/registro>.
2. Siga las instrucciones que se le indiquen.

Parte del procedimiento de registro consiste en recibir una llamada telefónica o mensaje de texto e indicar un código de verificación en el teclado del teléfono.

Cuando te registras en una Cuenta de AWS, Usuario raíz de la cuenta de AWS se crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar [tareas que requieren acceso de usuario raíz](#).

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. En cualquier momento, puede ver la actividad de su cuenta actual y administrarla accediendo a <https://aws.amazon.com/> y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión [Consola de administración de AWS](#) como propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

Para obtener ayuda para iniciar sesión con el usuario raíz, consulte [Iniciar sesión como usuario raíz](#) en la Guía del usuario de AWS Sign-In .

2. Active la autenticación multifactor (MFA) para el usuario raíz.

Para obtener instrucciones, consulte [Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz \(consola\)](#) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

Consulte las instrucciones en [Activar AWS IAM Identity Center](#) en la Guía del usuario de AWS IAM Identity Center .

2. En IAM Identity Center, conceda acceso administrativo a un usuario.

Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte [Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la](#) Guía del AWS IAM Identity Center usuario.

Inicio de sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, use la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte [Iniciar sesión en el portal de AWS acceso](#) en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

Para conocer las instrucciones, consulte [Create a permission set](#) en la Guía del usuario de AWS IAM Identity Center .

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

Para conocer las instrucciones, consulte [Add groups](#) en la Guía del usuario de AWS IAM Identity Center .

Crear políticas y roles

Configure los permisos de AWS Identity and Access Management (IAM) para que su equipo pueda implementar y administrar los recursos de Route 53 Global Resolver. Puede usar permisos administrativos para un acceso total o permisos de solo lectura para supervisar y ver las configuraciones.

Todas las operaciones de la API Global Resolver de Route 53 requieren los permisos de IAM adecuados. Si no tiene los permisos necesarios, las llamadas a la API devolverán errores `AccessDeniedException` (401) o `UnauthorizedException` (401).

Permisos administrativos

Si configura Route 53 Global Resolver por primera vez o administra todos los aspectos del servicio, necesitará permisos administrativos. Puede usar estas políticas AWS administradas:

- `AmazonRoute53GlobalResolverFullAccess`- Proporciona acceso completo a los recursos de Route 53 Global Resolver, incluida la creación, actualización y eliminación de resolutores globales, vistas de DNS, reglas de firewall y listas de dominios
- `AmazonRoute53FullAccess`- Necesario si planea utilizar el reenvío de zonas alojadas privadas
- `CloudWatchLogsFullAccess`- Necesario si planeas enviar registros a Amazon CloudWatch
- `AmazonS3FullAccess`- Necesario si tiene previsto importar listas de dominios de firewall desde Amazon S3 o enviar registros a Amazon S3

Permisos de solo lectura

Si solo necesita ver las configuraciones y los registros de Route 53 Global Resolver, puede usar estas políticas AWS administradas:

- `AmazonRoute53GlobalResolverReadOnlyAccess`- Proporciona acceso de solo lectura a los recursos de Route 53 Global Resolver, incluida la visualización de resoluciones globales, vistas de DNS, reglas de firewall, listas de dominios y fuentes de acceso
- `AmazonRoute53ReadOnlyAccess`- Necesario para ver las asociaciones de zonas alojadas privadas
- `CloudWatchReadOnlyAccess`- Necesario para ver los registros en Amazon CloudWatch
- `AmazonS3ReadOnlyAccess`- Necesario para ver los archivos de la lista de dominios del firewall almacenados en Amazon S3

Consideraciones sobre la red

Antes de implementar Route 53 Global Resolver, tenga en cuenta los siguientes requisitos de red:

Intervalos de IP de clientes

Esto solo es necesario cuando se utiliza la autenticación basada en la fuente de acceso.

Identifique los rangos de direcciones IP (bloques CIDR) de todos los clientes que utilizarán Route 53 Global Resolver. Los necesitará para configurar las reglas de su fuente de acceso.

Protocolos DNS

Determine qué protocolos de DNS utilizarán sus clientes:

- Do53: DNS estándar a través del puerto 53 (UDP/TCP)
- DoH: para consultas cifradas DNS-over-HTTPS
- DoT: DNS-over-TLS para consultas cifradas

Grupos de firewall y seguridad

Asegúrese de que los firewalls y grupos de seguridad de su red permitan el tráfico saliente a las direcciones IP anycast de Route 53 Global Resolver en los puertos correspondientes (53 para Do53, 443 para DoH, 853 para DoT).

Tutorial: Cree su primer Route 53 Global Resolver

Esta guía de introducción muestra los componentes básicos de Route 53 Global Resolver y, opcionalmente, cómo crear una configuración sencilla de filtrado de DNS. Este tutorial cubre los conceptos básicos, pero no incluye los requisitos de producción, como la configuración del cliente, el registro o la resolución de dominios privados.

Cuando haya terminado, dispondrá de una configuración básica de Route 53 Global Resolver que puede filtrar las consultas de DNS y bloquear los dominios maliciosos.

En las siguientes secciones se describe cómo empezar rápidamente con la seguridad y el filtrado de DNS mediante Route 53 Global Resolver.

Requisitos previos

Antes de poder usar Route 53 Global Resolver, necesita una AWS cuenta y los permisos adecuados para acceder, ver y editar los componentes de Route 53 Global Resolver. El administrador del

sistema debe completar los [the section called “Configurar el acceso a la cuenta”](#) pasos descritos y volver a este tutorial.

Paso 1: Crear un solucionador global

En primer lugar, cree una instancia de resolución global y seleccione las AWS regiones en las que funcionará.

1. Abra la consola de Route 53 Global Resolver en <https://console.aws.amazon.com/route53globalresolver/>.
2. Elija Crear un solucionador global.
3. En Nombre, introduzca un nombre descriptivo para el solucionador global.
4. En Descripción, si lo desea, introduzca una descripción.
5. En el caso de las regiones, seleccione dos o más Regiones de AWS en las que desee crear una instancia del solucionador global. Elija las regiones más cercanas a sus clientes para obtener un rendimiento óptimo.
6. Si lo desea, añada etiquetas para ayudar a organizar y administrar sus recursos.
7. Seleccione Crear resolución global.

Recibirás inmediatamente IPv4 direcciones anycast que tus clientes podrán utilizar para contactar con el solucionador. El proceso de creación del solucionador global tarda unos minutos en completarse antes de que las direcciones comiencen a funcionar.

Paso 2: Crear una vista de DNS y configurar la autenticación

Cree una vista de DNS para organizar sus clientes y configurar la autenticación mediante fuentes de acceso IP. En este tutorial se utiliza la autenticación basada en IP. También puede usar tokens de acceso para los protocolos DOH/DOT.

1. En la consola de Route 53 Global Resolver, elija su resolución global.
2. Elija Crear vista DNS.
3. En Nombre, introduce un nombre descriptivo para la vista de DNS.
4. En Descripción, si lo desea, introduzca una descripción.
5. Seleccione Crear vista DNS.
6. Una vez creada la vista DNS, selecciona Fuente de acceso y, a continuación, Crear fuente de acceso.

7. Para el bloque CIDR, introduzca el rango de direcciones IP de sus clientes (por ejemplo, 203.0.113.0/24).
8. En Protocolo, elija Do53 (DNS a través del puerto 53) para la configuración básica.
9. Elija la regla Crear fuente de acceso.

Paso 3: Configurar las reglas de filtrado de DNS (opcional)

Configure reglas básicas de filtrado de DNS para bloquear el acceso a dominios maliciosos.

1. En la vista de DNS, selecciona Reglas de firewall y luego Crear regla de firewall.
2. En Nombre, introduce un nombre descriptivo para la regla.
3. En Prioridad, introduzca 100 (los números más bajos tienen mayor prioridad).
4. En Acción, elija Bloquear.
5. Para el tipo de lista de dominios, selecciona Lista de dominios AWS gestionados.
6. En Lista de dominios gestionados, selecciona AmazonGuardDutyThreatListel comando y control de malware y botnet para bloquear los dominios maliciosos conocidos (puedes añadir otras listas gestionadas o crear listas personalizadas más adelante).
7. Selecciona Crear regla de firewall.

Paso 4: Pruebe la configuración

Compruebe que la configuración de Route 53 Global Resolver funcione correctamente.

1. Desde una máquina cliente que se encuentre dentro del rango de CIDR configurado, pruebe la resolución de DNS con las direcciones IP anycast proporcionadas por su resolución global:

```
nslookup example.com <anycast-ip-address>
```

2. Compruebe que los dominios legítimos se resuelven correctamente.
3. Compruebe que los dominios bloqueados estén filtrados correctamente. Puede crear una lista de dominios personalizada con un dominio de prueba para comprobar que las reglas del firewall funcionan correctamente. Para obtener más información sobre las listas de dominios gestionados, consulte [Listas de dominios gestionados](#).
4. Consulte la consola de Route 53 Global Resolver para ver los registros de consultas y la actividad de filtrado.

Para obtener información completa sobre los procedimientos de prueba y la solución de problemas, consulte Solución de problemas de Route 53 Global Resolver.

Paso 5: Monitorear la actividad del DNS

Configura el registro de tu actividad de DNS.

1. Elija una región de observabilidad.
2. Seleccione el destino de los registros de consultas.

Para obtener información completa sobre los procedimientos de prueba y la solución de problemas, consulte Prueba y solución de problemas del Resolver global Route 53.

Paso 6: Limpiar (opcional)

Si creó esta configuración con fines de prueba y no quiere seguir usando Route 53 Global Resolver, agote los recursos para evitar cargos continuos.

1. En la consola de Route 53 Global Resolver, elimine las reglas de firewall que haya creado.
2. Elimine cualquier regla de fuente de acceso que haya creado.
3. Elimine la vista de DNS.
4. Elimine el solucionador global.

Important

Al eliminar estos recursos, se detendrá la resolución de DNS para todos los clientes que estén configurados para usarlos. Actualice las configuraciones de sus clientes antes de eliminar la resolución o eliminar las reglas de acceso.

Siguientes pasos

Ahora que tiene una configuración básica de Route 53 Global Resolver, puede explorar funciones adicionales:

- Configure los dispositivos cliente para que usen su resolución (necesario para la producción). Actualice la configuración de DNS de su cliente para usar las direcciones IP anycast proporcionadas por su resolución global.
- Configure el registro para la supervisión y el cumplimiento (recomendado para la producción). Configure el registro en Amazon CloudWatch, Amazon S3 o Amazon Data Firehose para la supervisión y el análisis. Para obtener más información, consulte [???](#).
- Configure el reenvío de zonas alojadas privadas para los dominios internos (obligatorio si dispone de AWS recursos privados). Para obtener más información, consulte [Uso de zonas alojadas privadas](#).
- Configure la conectividad DNS cifrada mediante DNS-over-HTTPS (DoH) o DNS-over-TLS (DoT). Para obtener más información, consulte [Configuración del DNS cifrado](#).
- Cree listas de dominios personalizadas y reglas de filtrado avanzadas. Para obtener más información, consulte [Filtrado de DNS](#).

Administración de vistas de DNS con Route 53 Global Resolver

Puede administrar las operaciones continuas de Route 53 Global Resolver, incluida la actualización de las vistas de DNS para controlar qué grupos de dispositivos cliente pueden resolver en los recursos internos y qué dominios filtrar.

Administrar las vistas de DNS

Tras crear las vistas de DNS, puede actualizar su configuración, habilitarlas o deshabilitarlas y gestionar su ciclo de vida.

Crear vistas de DNS para grupos de dispositivos cliente

Una vista de DNS es una agrupación lógica que define las políticas de seguridad para un grupo de dispositivos cliente, como trabajadores remotos, dispositivos de sucursales o equipos locales. Cada vista tiene sus propios requisitos de autenticación, reglas de filtrado y asociaciones de zonas alojadas privadas.

Para crear una vista de DNS

1. Abra la consola en <https://console.aws.amazon.com/route53globalresolver/>.
2. Elija su resolución global de la lista.

3. Elija la pestaña de vistas de DNS.
4. Selecciona Crear vista de DNS.
5. En la sección de detalles de la vista de DNS:
 - a. En el caso del nombre de la vista de DNS, introduce un nombre descriptivo para la vista de DNS (hasta 128 caracteres).
 - b. (Opcional) En Descripción, introduce una descripción para la vista de DNS (255 caracteres como máximo).
6. En la sección de gestión de consultas de DNS, configura los siguientes ajustes:
 - Validación de DNSSEC: seleccione Activar o Desactivar. La validación de DNSSEC permite al Resolver global verificar la autenticidad de las respuestas de DNS.
 - Las reglas del firewall no se abren correctamente: seleccione Habilitar para permitir que las consultas continúen cuando el firewall de DNS no pueda evaluarlas o Inhabilitar para bloquear dichas consultas.
 - Subred del cliente EDNS0: seleccione Activar para mejorar la precisión de la ubicación del cliente para el enrutamiento del tráfico a los recursos cercanos y un almacenamiento en caché eficiente, o Inhabilitar para desactivar esta función.
7. Seleccione Crear vista DNS.

Tras crear la vista DNS, puede configurar los controles de acceso, las reglas de firewall y las asociaciones de zonas alojadas privadas.

Edición de vistas de DNS

Puede modificar la configuración de la vista de DNS después de la creación, incluidas las opciones de gestión de consultas de DNS y los recursos asociados.

Para editar una vista de DNS

1. En la consola, navegue hasta su resolución global.
2. Selecciona la pestaña de vistas de DNS.
3. Seleccione la vista de DNS que desee editar y elija Editar.
4. Modifique la configuración de la vista de DNS según sea necesario y seleccione Guardar cambios.

Habilitar y deshabilitar las vistas de DNS

Puede deshabilitar temporalmente una vista de DNS sin eliminarla. Cuando está deshabilitada, la resolución global deja de atender las solicitudes de los dispositivos cliente asociadas a esa vista de DNS.

Warning

Al deshabilitar una vista de DNS, se detiene inmediatamente la resolución de DNS en todos los dispositivos cliente asociados a esa vista. Asegúrese de tener configurada una resolución de DNS alternativa para los dispositivos cliente afectados.

Eliminar vistas de DNS

Para poder eliminar una vista de DNS, primero debe eliminar todos los recursos asociados, incluidas las reglas de la fuente de acceso, los tokens de acceso, las reglas de firewall y las asociaciones de zonas alojadas privadas.

Warning

La eliminación de una vista de DNS es irreversible y detendrá inmediatamente la resolución de DNS en todos los dispositivos cliente asociados a esa vista.

Administrar las asociaciones de zonas alojadas privadas

Puede ver, actualizar y eliminar las asociaciones de zonas alojadas privadas según sea necesario para controlar qué grupos de dispositivos cliente tienen acceso a los recursos internos.

Visualización de asociaciones

Para ver todas las asociaciones de zonas alojadas privadas para una vista de DNS, navegue hasta su vista de DNS y consulte la sección Zonas alojadas privadas para ver todas las zonas asociadas con su estado y los detalles de la asociación.

Actualización de las asociaciones

Para actualizar el nombre de una asociación de zona alojada privada, seleccione la asociación, elija Editar, actualice el nombre de la asociación y guarde los cambios.

Eliminar asociaciones

Al eliminar una asociación de zona alojada privada, Route 53 Global Resolver deja de usar esa zona para resolver las consultas de DNS para la vista de DNS asociada.

Warning

La eliminación de una asociación de zona alojada privada afecta inmediatamente a la resolución de DNS. Las consultas de los dominios de la zona disociada se resolverán mediante el DNS público en lugar de los registros de la zona privada.

Configurar los ajustes de las vistas de DNS en Route 53 Global Resolver

Route 53 Global Resolver le permite configurar diferentes políticas de DNS y controles de acceso para diferentes grupos de dispositivos cliente en función de sus requisitos de seguridad y necesidades de acceso. Configure políticas de DNS y controles de acceso en Route 53 Global Resolver para diferentes grupos de dispositivos cliente en función de sus requisitos de seguridad y necesidades de acceso.

Configurar los ajustes de DNS para los grupos de clientes

Cada vista de DNS tiene varios ajustes que controlan el modo en que se procesan y resuelven las consultas de DNS para los distintos grupos de dispositivos cliente.

Validación de DNSSEC

La validación de DNSSEC ayuda a garantizar que las respuestas de DNS de los dominios públicos sean auténticas y no hayan sido manipuladas. Al habilitar la validación de DNSSEC, Route 53 Global Resolver comprueba las firmas de DNSSEC y devuelve SERVFAIL para los dominios con firmas no válidas.

Considere la posibilidad de habilitar la validación de DNSSEC si:

- Su organización necesita la verificación criptográfica de las respuestas de DNS
- Desea protegerse contra los ataques de suplantación de DNS y de envenenamiento de la caché
- Tiene requisitos de conformidad que requieren la validación del DNSSEC

 Note

La validación de DNSSEC solo se aplica a los dominios públicos. Las zonas alojadas privadas utilizan sus propios mecanismos de autenticación.

Subred de clientes EDNS (ECS)

La subred de clientes de EDNS incluye información sobre la ubicación de la red del cliente en las consultas de DNS que se envían a los servidores autorizados. Esto permite que las redes de entrega de contenido y los servicios distribuidos geográficamente proporcionen respuestas adecuadas a la ubicación.

ECS puede ayudarlo a:

- Obtenga un mejor rendimiento de los servicios distribuidos geográficamente
- Mejore la precisión del enrutamiento de la red de entrega de
- Cumpla mejor con las restricciones de contenido regionales

Consideraciones de privacidad:

- ECS revela información parcial de la IP del cliente a los servidores autorizados (máximo /24 para IPv4 y /48 para IPv6)
- Tenga en cuenta los requisitos de privacidad de su organización antes de activarlos

Error al abrir el firewall

La configuración de apertura por error del firewall determina lo que ocurre cuando las reglas del firewall de DNS no se pueden evaluar debido a un deterioro del servicio o a problemas de configuración.

Desactivado (predeterminado)

Las consultas de DNS se bloquean cuando no se pueden evaluar las reglas del firewall. Esto le proporciona la máxima seguridad, pero puede afectar a la disponibilidad en caso de problemas con el servicio.

Habilitado

Se permiten las consultas de DNS cuando no se pueden evaluar las reglas del firewall. Esto da prioridad a la disponibilidad por encima de la seguridad durante los problemas de servicio.

Prácticas recomendadas para organizar los grupos de dispositivos de los clientes

Siga estas prácticas recomendadas al diseñar vistas de DNS para distintos grupos de dispositivos cliente:

Vea las estrategias de la organización

- Separe según los requisitos de seguridad: cree diferentes vistas para los dispositivos cliente con diferentes autorizaciones de seguridad o niveles de acceso
- Organice por ubicación: utilice vistas independientes para diferentes ubicaciones geográficas o segmentos de red
- Agrupar por tipo de dispositivo: cree vistas dedicadas para servidores, estaciones de trabajo, dispositivos móviles o dispositivos de IoT
- Utilice nombres descriptivos: elija nombres que indiquen claramente el propósito de la vista y los dispositivos cliente de destino

Consideraciones de seguridad

- Principio de privilegios mínimos: configure cada vista con el acceso mínimo necesario para sus dispositivos cliente
- Denegar por defecto: comience con reglas de firewall restrictivas y añada excepciones según sea necesario
- Revisión periódica: revise y actualice periódicamente las configuraciones de visualización de DNS
- Supervise el uso: utilice los registros de consultas del DNS para supervisar y analizar los patrones de uso de las vistas del DNS

Administrar los controles de acceso con fuentes de acceso y tokens en Route 53 Global Resolver

Route 53 Global Resolver proporciona dos métodos principales para controlar el acceso a los dispositivos del cliente: fuentes de acceso para la autenticación basada en IP y tokens de acceso

para la autenticación basada en token. Este capítulo cubre ambos enfoques y le ayuda a elegir el método de autenticación adecuado para su entorno e implementar controles de acceso integrales.

Temas

- [Descripción de los métodos de control de acceso en Route 53 Global Resolver](#)
- [Configurar las fuentes de acceso y las reglas de las fuentes de acceso](#)
- [Administrar los tokens de acceso para la autenticación cifrada](#)
- [Prácticas recomendadas de control de acceso y consideraciones de seguridad](#)

Descripción de los métodos de control de acceso en Route 53 Global Resolver

Route 53 Global Resolver ofrece dos métodos de autenticación distintos para controlar el acceso de los clientes a su infraestructura de DNS. Cada método sirve para diferentes casos de uso y entornos.

Fuentes de acceso basadas en IP

Las reglas de fuente de acceso se configuran para permitir o denegar las consultas de DNS en función de las direcciones IP de los clientes. Este método funciona bien en entornos con rangos de IP predecibles, como sucursales o conexiones VPN. Las fuentes de acceso admiten todos los protocolos DNS (Do53, DoT y DoH) y proporcionan una configuración sencilla para los administradores de red.

Autenticación basada en fichas

Los tokens de acceso proporcionan una autenticación segura para los protocolos DoH y DoT mediante credenciales cifradas y de tiempo limitado. Este método se adapta a los clientes móviles y a los entornos en los que las direcciones IP cambian con frecuencia. Puede renovar los tokens antes de que caduquen y ofrecen una mayor seguridad mediante el cifrado.

Tenga en cuenta estos factores a la hora de seleccionar su método de autenticación:

Elegir el método de autenticación correcto

Factor	Acceder a las fuentes	Tokens de acceso
Lo mejor para	Rangos de IP fijos, redes de oficinas, usuarios de VPN	Dispositivos móviles, trabajadores dinámicos IPs y remotos
Nivel de seguridad	Basado en la red, se basa en la confianza de IP	Credenciales cifradas, por tiempo limitado
Complejidad de administración	Administración sencilla del rango de IP	Ciclo de vida y distribución de los tokens
Compatibilidad del protocolo	Do53, DoT, DoH	Solo DoT, DoH

Puede utilizar ambos métodos simultáneamente para crear una seguridad por capas. Por ejemplo, utilice las fuentes de acceso para las redes de oficinas y los tokens para los trabajadores remotos.

Configurar las fuentes de acceso y las reglas de las fuentes de acceso

Las fuentes de acceso controlan el acceso de los clientes en función de las direcciones IP. Usted crea reglas de fuentes de acceso que especifican qué rangos de IP pueden consultar su infraestructura de DNS y qué protocolos pueden usar.

Crear reglas de fuente de acceso

Siga estos pasos para crear una regla de fuente de acceso que permita que rangos de IP específicos consulten su infraestructura de DNS.

1. Abra la consola de Route 53 Global Resolver y navegue hasta la vista de DNS.
2. En la sección Fuente de acceso, selecciona Crear regla de fuente de acceso.
3. En Nombre, introduzca un nombre descriptivo que identifique el propósito de esta regla, como `office-network ovpn-users`.
4. Para el rango de direcciones IP, especifique las direcciones IP a las que deben tener acceso. Puede usar la notación CIDR para los rangos de IP: `192.168.1.0/24` o direcciones IP individuales: `203.0.113.5/32`.

5. En Protocolo, seleccione los protocolos DNS a los que se aplica esta regla:

- Do53: puerto de DNS estándar UDP/TCP (puerto 53)
- DoT: DNS sobre TLS (puerto 853)
- DoH: DNS a través de HTTPS (puerto 443)

6. Elija Crear regla de fuente de acceso.

Los dispositivos cliente de los rangos de IP especificados ahora pueden consultar su infraestructura de DNS mediante los protocolos seleccionados.

Comprender la evaluación y la prioridad de las reglas

Route 53 Global Resolver evalúa las reglas de la fuente de acceso al identificar la vista correcta que se debe usar.

- Las reglas se procesan desde los rangos de IP más específicos hasta los menos específicos, donde prevalece la regla de coincidencia más específica.
- Si ninguna regla coincide, la solicitud se deniega de forma predeterminada.

Pruebe la configuración de la fuente de acceso consultando desde diferentes direcciones IP para asegurarse de que las reglas funcionan según lo esperado.

Administrar los tokens de acceso para la autenticación cifrada

Los tokens de acceso proporcionan una autenticación cifrada para los protocolos DoH y DoT. A diferencia de las fuentes de acceso basadas en IP, los tokens funcionan independientemente de la ubicación del cliente y ofrecen una mayor seguridad mediante los controles de cifrado y caducidad.

Creación de tokens de acceso

Siga estos pasos para crear tokens de acceso para autenticar los dispositivos cliente que utilizan los protocolos DoH o DoT.

1. Abra la consola de Route 53 Global Resolver y navegue hasta la vista de DNS.
2. En la sección Fuente de acceso, selecciona Crear token de acceso.
3. En Nombre, introduce un nombre descriptivo que identifique el propósito del token, como `mobile-devices oremote-workers-q4`.

4. En Expiración, defina cuándo debe caducar el token. Recomendamos 90 días o menos por motivos de seguridad. Ten en cuenta tus capacidades de distribución y renovación de los tokens a la hora de establecer el período de caducidad.
5. Selecciona Crear token de acceso.
6. Distribuya el token de forma segura a los dispositivos de sus clientes mediante los canales de comunicación seguros de su organización.

Configuración de los dispositivos cliente con tokens de acceso

Configure los dispositivos cliente para que usen tokens de acceso para la autenticación con su infraestructura de Route 53 Global Resolver.

Configuración de DoH

Para configurar DoH con tokens de acceso, necesita el nombre DNS o las direcciones IP del solucionador global:

1. Utilice la GetGlobalResolver API para recuperar los detalles de conectividad de su resolución.
2. Anote las `ipv4Addresses` (por ejemplo, 3.3.3.3, 3.3.3.4) y (por ejemplo, `dnsName a1bc234567890a.route53globalresolver.global.on.aws`).
3. Incluya el token como parámetro de URL en el punto final del DoH con el nombre DNS:

```
https://a1bc234567890a.route53globalresolver.global.on.aws/dns-query?token=<token-value>
```

`<token-value>` Sustitúyalo por el token real que generaste.

Configuración DoT

Para las consultas DoT con tokens de acceso, incluya el token en una opción EDNS0 con las siguientes especificaciones:

- Código de opción: `0xffa0`
- Datos de opción: el token de acceso en formato de cadena

La implementación específica depende del software de su cliente DoT y de cómo gestione las opciones de EDNS0.

Gestión del ciclo de vida del token

Gestione la caducidad y la renovación de los tokens para mantener un acceso seguro a los dispositivos de sus clientes.

- Supervise las fechas de caducidad: haga un seguimiento de las fechas de caducidad de los tokens y planifique las renovaciones con antelación.
- Renueve antes de que caduquen: cree nuevos tokens antes de que caduquen los antiguos para evitar la interrupción del servicio.
- Rota las fichas con regularidad: sustituye las fichas periódicamente incluso antes de que caduquen para mejorar la seguridad.
- Revoca las fichas comprometidas: elimina las fichas inmediatamente si sospechas que están comprometidas.

Considere la posibilidad de implementar procesos automatizados de renovación de tokens para despliegues grandes a fin de reducir la sobrecarga administrativa.

Ejemplos de configuración de plataformas

Utilice estos ejemplos específicos de la plataforma para configurar los dispositivos cliente con los identificadores de acceso y los detalles de conexión de Route 53 Global Resolver.

Configuración de Windows

Siga estos pasos para configurar los clientes de Windows para que usen DoH con los tokens de acceso mediante el comando netsh.

1. Abre la línea de comandos como administrador.
2. Habilite la configuración global de DoH:

```
netsh dns add global doh=yes
```

3. Registre los servidores del DoH con tokens de acceso. Sustituya los valores de ejemplo por los detalles reales de la resolución:

```
netsh dns add encryption server=3.3.3.3 dohtemplate=https://  
a1bc234567890a.route53globalresolver.global.on.aws/dns-query?token=<your-token>  
autoupgrade=yes
```

```
netsh dns add encryption server=3.3.3.4 dohtemplate=https://  
a1bc234567890a.route53globalresolver.global.on.aws/dns-query?token=<your-token>  
autoupgrade=yes
```

4. Vacía la caché de DNS:

```
ipconfig /flushdns
```

5. Verifique la configuración:

```
netsh dns show global
```

Configuración de macOS

Siga estos pasos para configurar los clientes de macOS mediante un perfil de configuración móvil para DoH con tokens de acceso.

Cree un perfil de configuración móvil con la siguiente estructura:

```
<?xml version="1.0" encoding="UTF-8"?>  
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/  
PropertyList-1.0.dtd">  
<plist version="1.0">  
<dict>  
  <key>PayloadContent</key>  
  <array>  
    <dict>  
      <key>DNSSettings</key>  
      <dict>  
        <key>DNSProtocol</key>  
        <string>HTTPS</string>  
        <key>ServerAddresses</key>  
        <array>  
          <string>3.3.3.3</string>  
          <string>3.3.3.4</string>  
        </array>  
        <key>ServerURL</key>  
        <string>https://a1bc234567890a.route53globalresolver.global.on.aws/dns-query?  
token=<your-token></string>  
      </dict>  
      <key>PayloadType</key>  
      <string>com.apple.dnsSettings.managed</string>
```

```
</dict>
</array>
</dict>
</plist>
```

Instale el perfil en Configuración del sistema > Administración de dispositivos.

Prácticas recomendadas de control de acceso y consideraciones de seguridad

Siga estas prácticas recomendadas para mantener controles de acceso seguros y efectivos para su infraestructura de Route 53 Global Resolver.

Prácticas recomendadas de seguridad

Implemente estas medidas de seguridad para proteger su infraestructura de DNS:

- Utilice la autenticación por capas: combine las fuentes de acceso para redes confiables con tokens para los usuarios de dispositivos móviles. Este enfoque proporciona una defensa en profundidad y se adapta a diferentes escenarios de clientes.
- Implemente el acceso con privilegios mínimos: conceda acceso solo a los rangos de IP y protocolos que los clientes realmente necesiten. Evite reglas de origen de acceso demasiado amplias que podrían exponer su infraestructura a un uso no autorizado.
- Cambie las fichas con regularidad: sustituya las fichas de acceso de forma regular, incluso antes de que caduquen. Esta práctica limita el impacto de las fichas comprometidas y mantiene la higiene de la seguridad.
- Supervise los patrones de acceso: revise los registros de consultas del DNS para identificar patrones de acceso inusuales o posibles problemas de seguridad. Configura alertas para consultas desde rangos de IP inesperados o si utilizas tokens caducados.

Prácticas operativas recomendadas

Siga estas prácticas operativas para mantener controles de acceso confiables:

- Documente su estrategia de control de acceso: lleve una documentación clara sobre qué fuentes de acceso y tokens sirven a qué grupos de clientes.
- Pruebe los controles de acceso con regularidad: compruebe que las reglas y los tokens de las fuentes de acceso funcionan correctamente desde diferentes ubicaciones y escenarios de clientes.

- Planifique la renovación de los tokens: establezca procesos para distribuir los nuevos tokens antes de que caduquen los antiguos para evitar interrupciones en el servicio.
- Revise los controles de acceso periódicamente: elimine las reglas de origen de acceso no utilizadas y los tokens caducados para mantener una configuración limpia.

Protección del DNS para los clientes con Route 53 Global Resolver

En las siguientes secciones se describe cómo crear reglas para proteger las consultas de DNS realizadas por sus clientes.

Temas

- [Configure y administre las reglas del firewall de DNS](#)
- [Listas de dominios gestionados para Route 53 Global Resolver](#)
- [Crea listas de dominios para bloquear o permitir](#)
- [Firewall de DNS: protecciones avanzadas](#)
- [Administre las políticas de seguridad de DNS en Route 53 Global Resolver](#)

Configure y administre las reglas del firewall de DNS

Creación y visualización de reglas de firewall

Las reglas de firewall definen la forma en que Route 53 Global Resolver gestiona las consultas de DNS en función de las listas de dominios, las listas de dominios gestionados, las categorías de contenido o la protección avanzada contra amenazas. Cada regla especifica una prioridad, los dominios de destino y la acción que se debe realizar.

Prácticas recomendadas para la prioridad de las reglas:

- Utilice la prioridad 100-999 para las reglas de autorización de alta prioridad (dominios de confianza)
- Utilice la prioridad 1000-4999 para las reglas de bloqueo (amenazas conocidas)
- Utilice la prioridad 5000-9999 para las reglas de alerta (supervisión y análisis)
- Deje brechas entre las prioridades para permitir la inserción de reglas en el futuro

Para crear una regla de firewall de DNS

1. En la consola de Route 53 Global Resolver, navegue hasta la vista de DNS.
2. Seleccione la pestaña de reglas del firewall.
3. Seleccione Crear regla de firewall.
4. En la sección de detalles de la regla:
 - a. En Nombre de la regla, introduzca un nombre descriptivo para la regla (hasta 128 caracteres).
 - b. (Opcional) En Descripción de la regla, introduzca una descripción para la regla (255 caracteres como máximo).
5. En la sección Configuración de la regla, elija el tipo de configuración de la regla:
 - Listas de dominios gestionadas por el cliente: utilice una lista de dominios que usted cree y administre
 - AWS listas de dominios gestionados: utilice listas de dominios proporcionadas por Amazon que pueda utilizar
 - Protecciones avanzadas de DNS Firewall: elija entre una gama de protecciones administradas y especifique un umbral de confianza
6. En Acción de regla, elija la acción que se realizará cuando la regla coincida:
 - Permitir: la consulta de DNS está resuelta
 - Alerta: permite la consulta de DNS pero crea una alerta
 - Bloquear: la consulta de DNS está bloqueada
7. Seleccione Crear regla de firewall.

Utilice el siguiente procedimiento para ver las reglas que se les han asignado. También puede actualizar la regla y su configuración.

Para ver y actualizar una regla

1. En la consola de Route 53 Global Resolver, navegue hasta la vista DNS.
2. Seleccione la pestaña de reglas del firewall de DNS.
3. Elija la regla que desee ver o editar y, a continuación, seleccione Editar.
4. En la página de reglas, puede ver y editar la configuración.

Para obtener información acerca de los valores para las reglas, consulte [the section called “Configuración de las reglas en DNS Firewall”](#).

Para eliminar una regla

1. En la consola de Route 53 Global Resolver, navegue hasta la vista DNS.
2. Seleccione la pestaña de reglas del firewall de DNS.
3. Elija la regla que desee eliminar, elija Eliminar y confirme la eliminación.

Configuración de las reglas en DNS Firewall

Al crear o editar una regla de firewall de DNS en la vista de DNS, se especifican los siguientes valores:

Name

Un identificador único para la regla en la vista de DNS.

(Opcional) Descripción

Una breve descripción que proporciona más información acerca de la regla.

Lista de dominios

La lista de dominios que inspecciona la regla. Puedes crear y administrar tu propia lista de dominios o puedes suscribirte a una lista de dominios que se AWS administre por ti.

Una regla puede contener una lista de dominios o una protección de DNS Firewall Advanced, pero no ambas.

Tipo de consulta (solo listas de dominios)

La lista de tipos de consultas de DNS que inspecciona la regla. Los siguientes valores son válidos:

- R: Devuelve una IPv4 dirección.
- AAAA: devuelve una dirección Ipv6.
- CAA: Limita la CAs posibilidad de crear SSL/TLS certificaciones para el dominio.
- CNAME: devuelve otro nombre de dominio.
- DS: registro que identifica la clave de firma del DNSSEC de una zona delegada.
- MX: especifica los servidores de correo.
- NAPTR: Regular-expression-based reescritura de nombres de dominio.
- NS: servidores de nombres autorizados.
- PTR: asigna una dirección IP a un nombre de dominio.
- SOA: registro de inicio de autoridad de la zona.

- SPF: muestra los servidores autorizados a enviar correos electrónicos desde un dominio.
- SRV: valores específicos de la aplicación que identifican a los servidores.
- TXT: verifica los remitentes de correo electrónico y los valores específicos de la aplicación.

Un tipo de consulta que se define mediante el ID de tipo de DNS, por ejemplo, 28 para AAAA. Los valores deben definirse como TYPENUMBER, donde NUMBER pueden estar comprendidos entre 1 y 65334, por ejemplo. TYPE28 Para obtener más información, consulte la sección [Lista de tipos de registros de DNS](#).

Puede crear un tipo de consulta por regla.

Protección de DNS Firewall Advanced

Detecta las consultas de DNS sospechosas en función de las firmas de amenazas conocidas en las consultas de DNS. Puede elegir que se proteja de lo siguiente:

- Algoritmos de generación de dominios () DGAs

DGAs son utilizados por los atacantes para generar una gran cantidad de dominios con los que lanzar ataques de malware.

- Túneles de DNS

Los atacantes utilizan los túneles de DNS para extraer datos del cliente mediante el uso del túnel de DNS sin establecer una conexión de red con el cliente.

En una regla de DNS Firewall Advanced, puede elegir entre bloquear las consultas que coincidan con la amenaza o alertar sobre estas.

Para obtener más información, consulte Protecciones avanzadas de DNS Firewall.

Una regla puede contener una protección de DNS Firewall Advanced o una lista de dominios, pero no ambas.

Umbral de confianza (solo con DNS Firewall Advanced)

El umbral de confianza para DNS Firewall Advanced. Debe proporcionar este valor al crear una regla de DNS Firewall Advanced. Los valores del nivel de confianza significan lo siguiente:

- Alto: detecta solo las amenazas mejor corroboradas con una baja tasa de falsos positivos.
- Medio: proporciona un equilibrio entre la detección de amenazas y los falsos positivos.
- Bajo: proporciona la tasa de detección de amenazas más alta, pero también aumenta los falsos positivos.

Para obtener más información, consulte Configuración de reglas en el Firewall de DNS.

Action

Cómo desea que DNS Firewall gestione una consulta de DNS cuyo nombre de dominio coincida con las especificaciones de la lista de dominios de la regla. Para obtener más información, consulte [the section called “Acciones de regla en DNS Firewall”](#).

Priority (Prioridad)

Configuración única de enteros positivos para la regla en la vista DNS que determina el orden de procesamiento. El firewall de DNS inspecciona las consultas de DNS según las reglas de una vista de DNS, empezando por la configuración de prioridad numérica más baja y subiendo. Puede cambiar la prioridad de una regla en cualquier momento; por ejemplo, para cambiar el orden de procesamiento o dejar espacio para otras reglas.

Acciones de regla en DNS Firewall

Cuando DNS Firewall encuentra una coincidencia entre una consulta de DNS y una especificación de dominio en una regla, aplica a la consulta la acción especificada en la regla.

Se le pide que especifique una de las opciones siguientes en cada regla que cree:

- Permitir: deja de inspeccionar la consulta y deja que se complete. No está disponible para DNS Firewall Advanced.
- Alerta: deje de inspeccionar la consulta, deje que se realice y registre una alerta para la consulta en los registros de Route 53 Resolver.
- Bloquear: interrumpa la inspección de la consulta, impida que vaya al destino previsto y registre la acción de bloqueo de la consulta en los registros de Route 53 Resolver.

Responda con la respuesta de bloqueo configurada, a partir de lo siguiente:

- NODATA: responde indicando que la consulta se ha realizado correctamente, pero no hay ninguna respuesta disponible para ella.
- NXDOMAIN: responde indicando que el nombre de dominio de la consulta no existe.
- Anulación: proporciona una anulación personalizada en la respuesta. Esta opción requiere los siguientes ajustes adicionales:
 - Valor de registro: el registro DNS personalizado que se va a devolver en respuesta a la consulta.

- Tipo de registro: el tipo de registro DNS. Esto determina el formato del valor del registro. Debe ser CNAME.
- Tiempo de vida en segundos: tiempo recomendado para que la resolución de DNS o el navegador web almacenen en caché el registro de anulación y lo utilicen en respuesta a esta consulta, si se vuelve a recibir. De forma predeterminada, es cero y el registro no se almacena en caché.

Listas de dominios gestionados para Route 53 Global Resolver

Las listas de dominios gestionados contienen nombres de dominio asociados a actividades maliciosas u otras amenazas potenciales. AWS mantiene estas listas para permitir que los clientes de Route 53 Global Resolver comprueben las consultas de DNS enlazadas a Internet cuando utilizan el Firewall de DNS.

Mantenerse al día del panorama de amenazas en constante cambio puede resultar lento y costoso. Las listas de dominios administradas pueden ahorrarle tiempo al implementar y usar el firewall de DNS en Global Resolver. AWS actualiza automáticamente las listas cuando aparecen nuevas vulnerabilidades y amenazas.

Las listas de dominios gestionados se clasifican en las categorías de amenazas y contenido, diseñadas para ayudarle a protegerse de las amenazas web más comunes y, además, bloquear la resolución de consultas a dominios que no son de dominio safe-for-work.

Como práctica recomendada, pruebe una lista de dominios administrados en un entorno que no sea de producción antes de usarlo en producción, con la acción de la regla establecida en `Alert`. Evalúe la regla mediante CloudWatch métricas de Amazon combinadas con solicitudes muestreadas de DNS Firewall o registros de Global Resolver. Cuando la regla haga lo que quería, cambie la configuración de la acción según sea necesario.

Listas de dominios AWS gestionados disponibles

En esta sección se describen las listas de dominios gestionados que están disponibles actualmente para Global Resolver. AWS proporciona las siguientes listas de dominios gestionados, para todos los usuarios de Global Resolver, clasificadas por amenaza o tipo de contenido.

Categorías de amenazas

Malware

Botnet/Comando y Control

Lista agregada de amenazas

Lista de GuardDuty amenazas de Amazon

Phishing

No deseado

Categorías de contenido

Violencia y discurso de odio

Para niños

Anuncios online

Ciencia

Familia y paternidad

Pets

Búsqueda de empleo y carrera

Religión

Lifestyle

Hogar y jardín

Actividades delictivas e ilegales

Deportes y recreación

Vehículos

Servicios financieros

Bienes inmuebles

Pasatiempos e intereses

Travel

Comida y gastronomía

Gobierno y asuntos legales

Educación

Moda

Estado

Compras

Contenido para adultos y adultos

Tecnología e Internet

Negocios y economía

Noticias

Motores de búsqueda y portales

Arte y cultura

Entretenimiento

Militar

Redes sociales

Evitación de poderes

Redirigir

Correo electrónico

Traducción

Abuso infantil

Aborto

Apuestas

Hackeando

Marihuana

Cryptocurrency

Citas

Inteligencia Artificial y Machine Learning

Dominios estacionados

Dirección IP privada

Las listas de dominios administrados no se pueden descargar ni explorar. Para proteger la propiedad intelectual, no puede ver ni editar las especificaciones de los dominios individuales en las listas de dominios gestionados. Esta restricción también permite impedir que usuarios malintencionados diseñen amenazas que eludan específicamente las listas publicadas.

Crea listas de dominios para bloquear o permitir

Puede crear sus propias listas de dominios para especificar categorías de dominios que no encuentre en las ofertas de listas de dominios administrados o para gestionarlos por su cuenta, si así lo prefiere.

Además de los procedimientos descritos en esta sección, en la consola puede crear una lista de dominios en el contexto de la administración de reglas del firewall de DNS, al crear o actualizar una regla.

Cada especificación de dominio en la lista de dominios debe cumplir los siguientes requisitos:

- Opcionalmente, puede comenzar por * (asterisco).
- Con la excepción del asterisco inicial opcional y de un punto, como delimitadores entre etiquetas solo se debe contener los siguientes caracteres: A-Z, a-z, 0-9 y - (guion).

- Debe tener una longitud de entre 1 y 255 caracteres.

Para crear una lista de dominios

1. En la consola de Route 53 Global Resolver, navegue hasta su Global Resolver.
2. Seleccione la pestaña de listas de dominios.
3. Seleccione Crear lista de dominios.
4. Proporcione un nombre y una descripción opcional para tu lista de dominios, junto con las etiquetas, y seleccione Crear lista de dominios.
5. Una vez creada y operativa, puedes empezar a añadir dominios a tu lista de dominios seleccionando Añadir dominios.
6. Si decide cargar una lista de dominios de un bucket de Amazon S3, introduzca el URI del bucket de Amazon S3 en el que creó la lista de dominios. Esta lista de dominios debe tener un nombre de dominio por línea.
7. De lo contrario, introduce las especificaciones de tu dominio en el cuadro de texto, una por línea.
8. Seleccione Añadir dominios.

Para eliminar una lista de dominios

1. En la consola de Route 53 Global Resolver, navegue hasta su Global Resolver.
2. Seleccione la pestaña de listas de dominios.
3. Seleccione la lista de dominios que desea eliminar y, a continuación, elija Delete (Eliminar) y confirme la eliminación.

Firewall de DNS: protecciones avanzadas

DNS Firewall Advanced detecta las consultas de DNS sospechosas en función de las firmas de amenazas conocidas en las consultas de DNS. Puede especificar un tipo de amenaza en una regla que utilice en una regla de firewall de DNS asociada a una vista de DNS.

DNS Firewall Advanced identifica las firmas de amenazas del DNS sospechosas mediante la inspección de una serie de identificadores clave en la carga útil del DNS, como la marca horaria de las solicitudes, la frecuencia de las solicitudes y las respuestas, las cadenas de consulta de DNS y la longitud, el tipo o el tamaño de las consultas de DNS entrantes y salientes. Según el tipo de firma de la amenaza, puede configurar políticas para bloquear la consulta o simplemente registrarla y alertar

sobre ella. Si utiliza un conjunto ampliado de identificadores de amenazas, puede protegerse contra las amenazas del DNS procedentes de fuentes de dominio que tal vez aún no estén clasificadas por las fuentes de inteligencia de amenazas mantenidas por la comunidad de seguridad en general.

En la actualidad, DNS Firewall Advanced ofrece protección contra:

- Algoritmos de generación de dominios (DGAs)

DGAs son utilizados por los atacantes para generar una gran cantidad de dominios con los que lanzar ataques de malware.

- Túneles de DNS

Los atacantes utilizan los túneles de DNS para extraer datos del cliente mediante el uso del túnel de DNS sin establecer una conexión de red con el cliente.

Para obtener información sobre cómo crear reglas, consulte [the section called “Configure y administre las reglas del firewall de DNS”](#).

Mitigación de escenarios falsos positivos

Si encuentra escenarios de falsos positivos en reglas que utilizan protecciones de DNS Firewall Advanced para bloquear consultas, realice los siguientes pasos:

1. En los registros de Global Resolver, identifique la regla y las protecciones avanzadas del firewall de DNS que están causando el falso positivo. Para ello, busque el registro de la consulta que DNS Firewall está bloqueando y que desea permitir. El registro incluye la vista de DNS, la regla, la acción de la regla y la protección avanzada del firewall de DNS.
2. Cree una nueva regla en la vista DNS que permita de forma explícita el acceso a la consulta bloqueada. Al crear la regla, puede definir su propia lista de dominios con solo la especificación de dominio que desea permitir. Siga las instrucciones para la administración de reglas que se encuentran en [the section called “Configure y administre las reglas del firewall de DNS”](#).
3. Priorice la nueva regla dentro de la regla para que se ejecute antes que la regla que usa la lista administrada. Para ello, asigne a la nueva regla un valor de prioridad numérica más bajo.

Cuando hayas actualizado las reglas, la nueva regla permitirá explícitamente el nombre de dominio que desees permitir antes de que se ejecute la regla de bloqueo.

Administre las políticas de seguridad de DNS en Route 53 Global Resolver

Administrar los solucionadores globales

Tras crear un solucionador global, puede ver sus detalles, editar su configuración y gestionar los recursos asociados desde la página Resolvers globales.

Ver los detalles del solucionador

La página Global Resolvers muestra una lista de todos sus resolutores con información clave, como el nombre de la resolución, las regiones implementadas, las vistas de DNS asociadas, la región de observabilidad y el estado operativo.

Edición de resolutores globales

Puede modificar el nombre y la descripción del solucionador después de crearlo. No puede modificar las regiones en las que se despliega un solucionador global después de su creación.

Administrar las reglas de firewall

Tras crear las reglas de firewall, puede modificar su prioridad, actualizar su configuración o eliminarlas según sea necesario.

Prioridad de las reglas y orden de evaluación

Las reglas del firewall se evalúan por orden de prioridad, procesándose primero los números más bajos. Cuando una consulta coincide con varias reglas, solo se aplica la acción de la primera regla coincidente.

Actualización de las reglas del firewall

Puede actualizar la mayoría de los aspectos de una regla de firewall después de crearla, incluidos sus dominios de prioridad, acción y destino.

Configuración de asociaciones de zonas alojadas privadas con Route 53 Global Resolver

El Resolver global de Route 53 le permite resolver los registros asociados a sus zonas alojadas privadas de Route 53 de sus clientes autorizados. Puede asociar las zonas alojadas privadas de Route 53 a la vista de DNS que sus clientes autorizados con la vista de DNS pueden resolver.

Temas

- [Administre las asociaciones de zonas alojadas privadas con Route 53 Global Resolver](#)

Administre las asociaciones de zonas alojadas privadas con Route 53 Global Resolver

Creación de zonas alojadas privadas para aplicaciones internas

Antes de poder asociar una zona alojada privada a una vista de DNS, primero debe crear la zona mediante la consola o la API de Amazon Route 53.

Para crear una zona alojada privada

1. Abra la consola de Amazon Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Zonas alojadas.
3. Elija Crear zona alojada.
4. En Nombre de dominio, introduzca el nombre de dominio de su zona privada (por ejemplo, `internal.example.com`).
5. En la lista Tipo, elija Zona alojada privada.
6. VPCs Para asociarlo a la zona alojada, elija el VPCs que desee asociar a la zona alojada. Si lo desea, puede usar la operación de `CreateHostedZone` API para omitir la introducción de un valor, ya que en su lugar asociará la zona con Route 53 Global Resolver.
7. Elija Crear zona alojada.

Después de crear la zona alojada privada, añada los registros DNS que necesite para sus servicios internos.

Asociar zonas alojadas privadas a vistas de DNS

Para permitir que Route 53 Global Resolver resuelva las consultas de su zona alojada privada, debe asociar la zona a una o más vistas de DNS.

Para asociar una zona alojada privada a una vista de DNS

1. En la consola del Resolver global de Route 53, navegue hasta el solucionador global.
2. Elija la vista de DNS a la que desee asociar la zona alojada privada.

3. En la sección Zonas alojadas privadas, selecciona Asociar zona alojada.
4. En Zona alojada, selecciona la zona alojada privada que deseas asociar.
5. En Nombre de la asociación, introduzca un nombre descriptivo para esta asociación.
6. Elija Asociar zona hospedada.

El proceso de asociación suele tardar unos minutos en completarse. Una vez completado, Route 53 Global Resolver utilizará los registros de la zona alojada privada para responder a las consultas de DNS de los dispositivos cliente asociadas a la vista de DNS.

Supervisión de la actividad y el rendimiento del DNS con Route 53 Global Resolver

Route 53 Global Resolver proporciona una visibilidad completa de la actividad del DNS en toda su organización, lo que le permite identificar las amenazas de seguridad, analizar el comportamiento de los dispositivos del cliente y mantener el cumplimiento. En este capítulo se describen las herramientas de supervisión disponibles y los procedimientos detallados para configurar la supervisión del DNS, configurar los destinos de registro y analizar los datos del DNS a fin de investigar las amenazas y optimizar el rendimiento.

AWS proporciona las siguientes herramientas de supervisión para ayudarle a mantener un servicio de DNS seguro y fiable:

- Amazon CloudWatch rastrea los volúmenes de consultas de DNS, los tiempos de respuesta y los eventos de seguridad en tiempo real. Cree paneles para monitorear el rendimiento del DNS en todas las ubicaciones y configure alarmas que le notifiquen cuando el volumen de consultas aumente o los tiempos de respuesta aumenten según lo especificado. Para Route 53 Global Resolver, puede supervisar los volúmenes de consultas, los tiempos de respuesta y la actividad de filtrado. Para obtener más información, consulta la [Guía del CloudWatch usuario de Amazon](#).
- Amazon CloudWatch Logs le permite supervisar, almacenar y acceder a sus archivos de registro desde EC2 instancias de Amazon y otras fuentes. CloudTrail Route 53 Global Resolver puede entregar los registros de consultas de DNS directamente a CloudWatch los registros para su monitoreo y análisis en tiempo real. También se pueden archivar los datos del registro en un almacenamiento de larga duración. Para obtener más información, consulta la [Guía del usuario CloudWatch de Amazon Logs](#).
- Amazon se EventBridge puede utilizar para automatizar sus AWS servicios y responder automáticamente a los eventos del sistema, como los problemas de disponibilidad de las

aplicaciones o los cambios de recursos. Los eventos de AWS los servicios se entregan EventBridge prácticamente en tiempo real. Puede crear reglas sencillas para indicar qué eventos le resultan de interés, así como qué acciones automatizadas se van a realizar cuando un evento cumple una de las reglas. Para obtener más información, consulta la [Guía EventBridge del usuario de Amazon](#).

- AWS CloudTrail captura las llamadas a la API y los eventos relacionados realizados por su AWS cuenta o en su nombre y entrega los archivos de registro a un bucket de Amazon S3 que especifique. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. Para obtener más información, consulte la [Guía del usuario de AWS CloudTrail](#).

Temas

- [Obtenga visibilidad de la actividad de DNS con Route 53 Global Resolver](#)
- [Configure la supervisión y el registro de DNS con Route 53 Global Resolver](#)

Obtenga visibilidad de la actividad de DNS con Route 53 Global Resolver

Route 53 Global Resolver ofrece capacidades integrales de registro de consultas de DNS para monitorear la actividad de los dispositivos del cliente e identificar las amenazas de seguridad. Habilite el registro de consultas de DNS en Route 53 Global Resolver para ver a qué sitios web acceden los dispositivos cliente, identificar posibles amenazas de seguridad y analizar los patrones de resolución de DNS. Los registros recopilan información completa sobre cada consulta, incluidas las políticas de seguridad que se aplicaron.

¿Qué información se captura en los registros de DNS

Cada entrada del registro de consultas de DNS proporciona información detallada sobre la actividad de los dispositivos del cliente y la aplicación de las políticas de seguridad:

- Información de consulta: nombre de dominio, tipo de consulta, clase de consulta y protocolo utilizado
- Información del dispositivo del cliente: dirección IP de origen, vista de DNS y método de autenticación
- Información de respuesta: código de respuesta, registros de respuestas y tiempo de respuesta
- Acciones de seguridad: coincidencias de las reglas del firewall, resultados de la detección de amenazas y medidas adoptadas

- Metadatos: fecha y hora, identificador de resolución global, región e información de rastreo

Formato OCSF para la integración de la seguridad

Los registros de consultas del DNS utilizan el Open Cybersecurity Schema Framework (OCSF), que proporciona un formato estandarizado para los datos de eventos de seguridad. Este formato permite:

- Análisis estandarizado: esquema coherente en diferentes herramientas de seguridad
- Interoperabilidad mejorada: fácil integración con SIEM y plataformas de análisis
- Correlación mejorada: capacidad de correlacionar los eventos del DNS con otros datos de seguridad
- Compatibilidad futura: Support para los requisitos de análisis de seguridad en evolución

Ejemplos de formatos de registro OCSF

Los registros de consultas de DNS de Route 53 Global Resolver siguen la estructura del esquema OCSF y proporcionan información detallada sobre cada consulta, respuesta y acción de seguridad de DNS. Los siguientes ejemplos muestran el formato de registro de las consultas permitidas y denegadas.

Registro DNS de Route 53 Global Resolver: ejemplo de acceso permitido

En este ejemplo, se muestra una consulta de DNS que se permitió mediante reglas de firewall. El registro incluye detalles de consultas, información de respuesta y datos de enriquecimiento con identificadores específicos de Route 53 Global Resolver.

```
{
  "action_id": 1,
  "action_name": "Allowed",
  "activity_id": 6,
  "activity_name": "Traffic",
  "category_name": "Network Activity",
  "category_uid": 4,
  "class_name": "DNS Activity",
  "class_uid": 4003,
  "cloud": {
    "provider": "AWS",
    "region": "us-east-1",
    "account": {
      "uid": "123456789012"
```

```
    }
  },
  "connection_info": {
    "direction": "Inbound",
    "direction_id": 1,
    "protocol_name": "udp",
    "protocol_num": 17,
    "protocol_ver": "",
    "uid": "db21d1739ddb423a"
  },
  "duration": 1,
  "end_time": 1761358379996,
  "answers": [{
    "rdata": "3.3.3.3",
    "type": "A",
    "class": "IN",
    "ttl": 300
  },
  {
    "rdata": "3.3.3.4",
    "type": "A",
    "class": "IN",
    "ttl": 300
  }
],
  "src_endpoint": {
    "ip": "3.3.3.1",
    "port": 56576
  },
  "enrichments": [{
    "name": "global-resolver",
    "value": "gr-a1b2c3d4fexample",
    "data": {
      "dns_view_id": "dnsv-a1b2c3d4fexample",
      "firewall_rule_id": "fr-a1b2c3d4fexample",
      "token_id": "t-a1b2c3d4fexample",
      "token_name": "device-123456",
      "token_expiration": "1789419206",
    }
  }
],
  "message": "",
  "metadata": {
    "version": "1.2.0",
    "product": {
      "name": "Global Resolver",
```

```
        "vendor_name": "AWS",
        "feature": {
            "name": "DNS"
        }
    },
    "query": {
        "hostname": "example.com.",
        "class": "IN",
        "type": "A",
        "opcode": "Query",
        "opcode_id": 0
    },
    "query_time": 1761358379995,
    "rcode": "NOERROR",
    "rcode_id": 0,
    "response_time": 1761358379995,
    "severity": "Informational",
    "severity_id": 1,
    "src_endpoint": {
        "ip": "3.3.3.3",
        "port": 28276
    },
    "start_time": 1761358379995,
    "status": "Success",
    "status_id": 1,
    "time": 1761358379995,
    "type_name": "DNS Activity: Traffic",
    "type_uid": 400306
}
```

Registro DNS de Route 53 Global Resolver: ejemplo de acceso denegado

En este ejemplo, se muestra una consulta de DNS que estaba bloqueada por las reglas del firewall. El registro incluye la acción de denegación, una matriz de respuestas vacía y el código de respuesta REFUSED que indica que la consulta no se ha procesado.

```
{
    "action_id": 2,
    "action_name": "Denied",
    "activity_id": 6,
    "activity_name": "Traffic",
    "category_name": "Network Activity",
```



```
"category_uid": 4,
"class_name": "DNS Activity",
"class_uid": 4003,
"cloud": {
  "provider": "AWS",
  "region": "us-west-2",
  "account": {
    "uid": "123456789012"
  }
},
"connection_info": {
  "direction": "Inbound",
  "direction_id": 1,
  "protocol_name": "tcp",
  "protocol_num": 6,
  "protocol_ver_id": 4,
  "uid": "9fdc6fbc09794d5e"
},
"duration": 1,
"end_time": 1761358379996,
"answers": [],
"src_endpoint": {
  "ip": "3.3.3.3",
  "port": 28276
},
"enrichments": [
  {
    "name": "global-resolver",
    "value": "gr-a1b2c3d4fexample",
    "data": {
      "dns_view_id": "dnsv-a1b2c3d4fexample",
      "firewall_rule_id": "fr-a1b2c3d4fexample",
      "token_id": "t-a1b2c3d4fexample",
      "token_name": "device-123456",
      "token_expiration": "1789419206",
    }
  }
],
"message": "",
"metadata": {
  "version": "1.2.0",
  "product": {
    "name": "Global Resolver",
    "vendor_name": "AWS",
```

```
        "feature": {
            "name": "DNS"
        }
    },
    "query": {
        "hostname": "example.com.",
        "class": "IN",
        "type": "A",
        "opcode": "Query",
        "opcode_id": 0
    },
    "query_time": 1761358379995,
    "rcode": "REFUSED",
    "rcode_id": 5,
    "response_time": 1761358379995,
    "severity": "Informational",
    "severity_id": 1,
    "start_time": 1761358379995,
    "status": "Failure",
    "status_id": 1,
    "time": 1761358379995,
    "type_name": "DNS Activity: Traffic",
    "type_uid": 400306
}
```

Configure la supervisión y el registro de DNS con Route 53 Global Resolver

Configure la supervisión de DNS en Route 53 Global Resolver para capturar información detallada sobre las consultas, respuestas y acciones de seguridad de DNS. En esta sección se describen los pasos para configurar los destinos de registro y las herramientas de supervisión.

Configuración de la región de observabilidad

Antes de configurar el registro de DNS, debe establecer una región de observabilidad en la que se almacenarán los registros y las métricas. Esta región determina dónde se procesan y almacenan los datos de monitoreo.

1. Abra la consola de Route 53 Global Resolver en <https://console.aws.amazon.com/route53globalresolver/>.
2. En el panel de navegación, seleccione Configuración.

3. En la sección Región de observabilidad, elija Establecer región.
4. Seleccione la AWS región en la que desea almacenar los datos de monitoreo y, a continuación, elija Establecer región.

Después de configurar la región de observabilidad, puede configurar los destinos de entrega de registros en esa región.

Solución de problemas de DNS con Route 53 Global Resolver

Route 53 Global Resolver ofrece capacidades integrales de resolución de DNS, pero en ocasiones es posible que necesite solucionar problemas de conectividad, rendimiento o configuración. Utilice registros de DNS, datos de supervisión y técnicas de diagnóstico para identificar y resolver los problemas que afectan a la resolución de DNS de los dispositivos cliente con Route 53 Global Resolver. Este capítulo proporciona enfoques sistemáticos para solucionar problemas comunes de DNS y optimizar el rendimiento.

Temas

- [Diagnosticque problemas de conectividad de DNS con Route 53 Global Resolver](#)
- [Resuelva los problemas de rendimiento de DNS con Route 53 Global Resolver](#)
- [Solucionar problemas de configuración en Route 53 Global Resolver](#)
- [Solución de problemas de acceso a los recursos internos](#)

Diagnosticque problemas de conectividad de DNS con Route 53 Global Resolver

Route 53 Global Resolver proporciona una resolución de DNS fiable, pero en ocasiones pueden producirse problemas de conectividad debido a problemas de configuración, autenticación o red. Cuando los dispositivos cliente no puedan resolver los nombres de dominio con Route 53 Global Resolver, utilice estos enfoques sistemáticos para identificar y resolver los problemas de conectividad.

Los dispositivos cliente no pueden resolver dominios

Siga estos pasos para diagnosticar los errores de resolución:

1. Compruebe que las consultas lleguen al solucionador global

- Compruebe los registros de consultas de DNS para ver si hay consultas desde la dirección IP del dispositivo cliente afectado
 - Confirme que el dispositivo cliente esté configurado con las direcciones IP anycast correctas
 - Pruebe la conectividad de red del dispositivo cliente al anycast IPs
2. Compruebe la autenticación del dispositivo cliente
- Compruebe que el dispositivo cliente esté autenticado en la vista de DNS correcta
 - Compruebe las reglas de la fuente de acceso para ver la dirección IP o el bloque CIDR del dispositivo cliente
 - Confirme que los tokens de acceso sean válidos y no hayan caducado (para la autenticación basada en tokens)
3. Revise las reglas del firewall
- Compruebe si las reglas del firewall bloquean las consultas
 - Revise la prioridad de las reglas y asegúrese de que las reglas de permiso tengan mayor prioridad que las reglas de bloqueo
 - Compruebe la configuración del comportamiento de apertura por error del firewall
4. Confirme las asociaciones de visualización de DNS
- Compruebe las asociaciones de zonas alojadas privadas para los dominios internos
 - Compruebe que existan registros DNS en las zonas alojadas privadas asociadas
 - Asegúrese de que los nombres de dominio de las consultas coincidan exactamente con los nombres de las zonas

Fallos de resolución intermitentes

En el caso de problemas de resolución de DNS esporádicos, investigue estas posibles causas:

Problemas de autenticación

- Compruebe los patrones de caducidad y renovación de los tokens de acceso
- Revise los registros de autenticación para ver si hay intentos de autenticación fallidos
- Compruebe la sincronización del reloj del dispositivo cliente para validar el token

Conectividad de red

- Supervise los cambios en la ruta de la red o los problemas de enrutamiento
- Compruebe si hay cambios en la configuración del firewall o del dispositivo NAT

- Verifique el enrutamiento uniforme de anycast a la región más cercana

Estado de los servicios

- Consulte AWS Service Health Dashboard para ver si hay problemas con Route 53 Global Resolver
- Revise CloudWatch las métricas para ver si hay picos en la tasa de errores
- Supervise el estado de la asociación de zonas alojadas privadas

Resolución pública inesperada

Cuando las consultas se resuelven en un DNS público en lugar de en zonas alojadas privadas:

1. Compruebe la configuración de la zona alojada privada

- Confirme que la zona alojada privada contiene los registros DNS esperados
- Compruebe que los nombres de los registros coincidan exactamente con el dominio consultado
- Compruebe que los tipos de registro coincidan con el tipo de consulta (A, AAAA, CNAME, etc.)

2. Compruebe las asociaciones de vistas de DNS

- Compruebe que la zona alojada privada esté asociada a la vista de DNS correcta
- Confirme que el dispositivo cliente esté autenticado en la vista de DNS
- Compruebe el estado de la asociación en la consola

3. Revise las reglas del firewall

- Compruebe si hay reglas de firewall que puedan bloquear las consultas a zonas privadas
- Compruebe el orden y la prioridad de la evaluación de las reglas
- Revise los registros de consultas de DNS para ver las acciones del firewall

Resuelva los problemas de rendimiento de DNS con Route 53 Global Resolver

El Resolver global Route 53 está diseñado para ofrecer un rendimiento óptimo con una arquitectura anycast global, pero varios factores pueden afectar a la velocidad de resolución del DNS. Solucione la lentitud de la resolución de DNS y optimice los tiempos de respuesta a las consultas para mejorar el rendimiento de los dispositivos cliente con Route 53 Global Resolver.

Resolución de DNS lenta

Para diagnosticar y resolver los tiempos de respuesta lentos del DNS:

1. Analice los tiempos de respuesta a las consultas

- Utilice los registros de consultas de DNS para identificar las consultas con tiempos de respuesta elevados
- Compare los tiempos de respuesta en distintos dominios y tipos de consultas
- Supervisa las tendencias del tiempo de respuesta a lo largo del tiempo

2. Compruebe si hay grandes volúmenes de consultas

- Supervise CloudWatch las métricas para detectar los picos de volumen de consultas
- Identifique los dispositivos cliente o las vistas de DNS que generan un número excesivo de consultas
- Busque patrones de consulta que puedan indicar errores de configuración

3. Revise el rendimiento de la memoria caché

- Analice las tasas de aciertos de la caché de los dominios consultados con frecuencia
- Revise la configuración de TTL para los registros de DNS
- Considere la posibilidad de ajustar los valores de TTL en función de los patrones de consulta

4. Compruebe la selección óptima de la región

- Asegúrese de que las regiones de resolución globales estén cerca de las ubicaciones de los dispositivos del cliente
- Supervise el enrutamiento de anycast para confirmar que las consultas lleguen a la región más cercana
- Considere la posibilidad de añadir regiones si los dispositivos del cliente están geográficamente distantes

Estrategias de optimización del rendimiento

Utilice estas estrategias para optimizar el rendimiento del DNS:

Optimización de la caché

- Ajuste los valores TTL en función de los patrones de consulta y la frecuencia de los cambios
- Utilícelo más largo TTLs para registros estables y más corto TTLs para registros que cambien con frecuencia

- Controle las tasas de aciertos de la caché y TTLs ajústelas

Optimización de la región

- Implemente un sistema de resolución global en las regiones más cercanas a las concentraciones de dispositivos de los clientes
- Supervise los patrones de enrutamiento de consultas y los tiempos de respuesta por región
- Considere la posibilidad de añadir regiones para una mejor cobertura geográfica

Optimización de protocolos

- Elija los protocolos de DNS adecuados en función de los requisitos de seguridad y rendimiento
- Considere la DNS-over-HTTPS opción (DoH) para las conexiones cifradas con ventajas de almacenamiento en caché
- Utilice DNS-over-TLS (DoT) para conexiones cifradas con una sobrecarga más baja

Optimización de reglas

- Revise y optimice la prioridad y la complejidad de las reglas de firewall
- Coloque las reglas que coinciden con frecuencia en un orden más alto de prioridad
- Simplifique las condiciones de reglas complejas siempre que sea posible

Solucionar problemas de configuración en Route 53 Global Resolver

Route 53 Global Resolver ofrece amplias opciones de configuración para las vistas de DNS, la autenticación y las reglas de firewall, lo que a veces puede provocar conflictos o discrepancias de configuración. Identifique y resuelva los problemas de configuración comunes de Route 53 Global Resolver que afectan a la resolución de DNS.

Problemas de autenticación

Problemas y soluciones de autenticación comunes:

No coinciden las reglas de la fuente de acceso

- Compruebe que las direcciones IP del dispositivo cliente coincidan con los bloques CIDR configurados
- Compruebe si los dispositivos NAT o proxy cambian las direcciones IP de origen
- Asegúrese de que las reglas de la fuente de acceso cubran todos los rangos de IP esperados de los dispositivos cliente

Fallos de autenticación de los tokens

- Compruebe que los tokens estén configurados correctamente en los dispositivos cliente
- Compruebe las fechas de caducidad y los procesos de renovación de los tokens
- Asegúrese de que los relojes de los dispositivos del cliente estén sincronizados para la validación de los tokens

Discordancias de protocolo

- Compruebe que los dispositivos cliente utilizan los protocolos permitidos por las reglas de Access Source
- Compruebe que las configuraciones de DoH y DoT coincidan con los protocolos de token
- Asegúrese de que las reglas del firewall no bloqueen los protocolos necesarios

Problemas de configuración de visualización de DNS

Problemas comunes de configuración de visualización de DNS:

Asociaciones de visualización de DNS incorrectas

- Compruebe que los dispositivos cliente estén autenticados en la vista de DNS deseada
- Compruebe que las zonas alojadas privadas estén asociadas a las vistas de DNS correctas
- Revise las reglas de firewall aplicadas a cada vista de DNS

Conflictos de configuración de DNS

- Revise la configuración de validación de DNSSEC para comprobar su compatibilidad con los dispositivos cliente
- Compruebe la configuración de la subred del cliente de EDNS para garantizar el equilibrio entre privacidad y rendimiento
- Compruebe que el comportamiento de apertura por error del firewall se ajuste a los requisitos de seguridad

Problemas con las reglas del firewall

Problemas comunes de configuración de las reglas de firewall:

Conflictos de prioridad de reglas

- Revise el orden de evaluación de las reglas y asegúrese de que la asignación de prioridades sea correcta

- Compruebe si las reglas de bloque tienen una prioridad superior a la prevista para las reglas de autorización
- Pruebe los cambios en las reglas en un entorno controlado antes del despliegue en producción

La lista de dominios no coincide

- Compruebe las especificaciones de los dominios en las listas de dominios personalizadas
- Compruebe los patrones de caracteres comodín para ver si la sintaxis y la cobertura son correctas
- Asegúrese de que las listas de dominios estén actualizadas y sincronizadas

Solución de problemas de acceso a los recursos internos

Problemas y soluciones comunes a la hora de gestionar el acceso a los recursos internos:

Los dispositivos cliente no se resuelven en los registros de la zona privada

- Compruebe que la zona alojada privada esté asociada a la vista de DNS correcta
- Compruebe que el dispositivo cliente esté autenticado en la vista de DNS correcta
- Asegúrese de que el nombre de dominio de la consulta coincida exactamente con el nombre de la zona
- Compruebe que los registros DNS existan en la zona alojada privada

Fallos de resolución intermitentes

- Compruebe el estado de la asociación en la consola
- Revise los registros de consultas de DNS para ver si hay patrones de error
- Verificar la conectividad de red entre Route 53 Global Resolver y Amazon Route 53

Resolución pública inesperada

- Confirme que la zona alojada privada contiene los registros esperados
- Compruebe si hay reglas de firewall que puedan estar bloqueando la consulta
- Compruebe que la consulta proviene de un dispositivo cliente asociado a la vista de DNS

Cuotas para Route 53 Global Resolver

Su AWS cuenta tiene cuotas predeterminadas, anteriormente denominadas límites, para cada AWS servicio. A menos que se indique lo contrario, cada cuota es específica de la región de . Puede solicitar el aumento de algunas cuotas, pero otras no se pueden aumentar.

Para ver las cuotas de Route 53 Global Resolver, abra la [consola Service Quotas](#). En el panel de navegación, elija AWS servicios y seleccione Route 53 Global Resolver.

Para solicitar un aumento de cuota, consulte [Solicitud de aumento de cuota](#) en la Guía del usuario de Service Quotas. Si la cuota aún no se encuentra disponible en Service Quotas, utilice el [formulario de aumento del límite](#).

Su AWS cuenta tiene las siguientes cuotas relacionadas con Route 53 Global Resolver.

Cuotas flexibles

En la siguiente tabla se describen las cuotas en Route 53 Global Resolver que se pueden aumentar. Para obtener información sobre cómo cambiar las cuotas, consulte [Solicitar un aumento de cuota](#) en la Guía del usuario de Service Quotas.

En el caso de algunos clientes, la cuota de la cuenta podría ser inferior a las cuotas anunciados. Si cree que ha encontrado un error de límite de recursos superado erróneamente, utilice la consola de Service Quotas para [solicitar aumentos de cuota](#).

Recurso	Cuota predeterminada	Ajustable
Resolvedores globales por cuenta	2	Sí
Vistas de DNS por solucionador global	5	Sí
Vistas de DNS por cuenta	50	Sí
Listas de dominios por cuenta	1 000	Sí
Dominios por lista de dominios	100 000	Sí
Dominios de un archivo importado de S3	10 000	Sí
Número de dominios en todas las reglas de firewall	1 000 000	Sí

Recurso	Cuota predeterminada	Ajustable
Reglas de firewall por vista de DNS	100	Sí
Tokens de acceso por resolución global	5 000	Sí
Fuentes de acceso por resolución global	1 000	Sí
Tamaño CIDR de las fuentes de acceso por resolución global	65.000	No
Zonas alojadas privadas por vista de DNS	1 000	Sí

Cuotas invariables

En la siguiente tabla se describen las cuotas en Route 53 Global Resolver que no se pueden aumentar.

Recurso u operación	Cuota
Configuraciones de entrega de registros por (resolución global, tipo de destino, región)	1

Creación de recursos de resolución de VPC de Amazon Route 53 y Route 53 con AWS CloudFormation

Amazon Route 53 y Route 53 VPC Resolver están integrados con AWS CloudFormation un servicio que le ayuda a modelar y configurar sus AWS recursos para que pueda dedicar menos tiempo a crear y administrar sus recursos e infraestructura. Cree una plantilla que describa todos los AWS recursos que desee y los CloudFormation aprovisiona y configura automáticamente.

Cuando la utilice CloudFormation, podrá reutilizar la plantilla para configurar los recursos de Route 53 y VPC Resolver de forma coherente y repetida. Describa sus recursos una vez y, a continuación, aprovisiona los mismos recursos una y otra vez en varias Cuentas de AWS regiones.

Route 53, VPC Resolver y plantillas CloudFormation

[Para aprovisionar y configurar recursos para Route 53, VPC Resolver y servicios relacionados, debe comprender CloudFormation las plantillas.](#) Las plantillas son archivos de texto con formato JSON o YAML. Estas plantillas describen los recursos que desea aprovisionar en sus CloudFormation pilas. Si no estás familiarizado con JSON o YAML, puedes usar CloudFormation Designer para ayudarte a empezar con CloudFormation las plantillas. Para obtener más información, consulta [¿Qué es CloudFormation Designer?](#) en la Guía AWS CloudFormation del usuario.

Route 53 admite la creación de los siguientes tipos de recursos en CloudFormation:

- `AWS::Route53::DNSSEC`
- `AWS::Route53::HealthCheck`
- `AWS::Route53::HostedZone`
- `AWS::Route53::KeySigningKey`
- `AWS::Route53::RecordSet`
- `AWS::Route53::RecordSetGroup`

Para obtener más información, incluidos ejemplos de plantillas JSON y YAML para estos recursos, consulte la [referencia del tipo de recurso de Amazon Route 53](#) en la Guía del usuario de AWS CloudFormation .

El solucionador de VPC admite la creación de los siguientes tipos de recursos en: CloudFormation

- `AWS::Route53Resolver::FirewallDomainList`
- `AWS::Route53Resolver::FirewallDomainList`
- `AWS::Route53Resolver::FirewallRuleGroupAssociation`
- `AWS::Route53Resolver::ResolverDNSSECConfig`
- `AWS::Route53Resolver::ResolverEndpoint`
- `AWS::Route53Resolver::ResolverQueryLoggingConfig`
- `AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation`
- `AWS::Route53Resolver::ResolverRule`
- `AWS::Route53Resolver::ResolverRuleAssociation`

Para obtener más información, incluidos ejemplos de plantillas JSON y YAML para los recursos de VPC Resolver, consulte la referencia sobre el [tipo de recurso de VPC Resolver de Route 53](#) en la Guía del usuario.AWS CloudFormation

Prácticas recomendadas para Route 53 y CloudFormation

Cuando CloudFormation los utilices para administrar los recursos de Route 53, sigue estas prácticas recomendadas para evitar problemas comunes y garantizar una implementación confiable.

Nociones generales sobre la consistencia final

Route 53 utiliza un modelo de consistencia final para los cambios de DNS. Esto puede afectar a las operaciones de CloudFormation , especialmente durante las reversiones y los cambios rápidos y sucesivos.

Important

Cuando se CloudFormation intenta revertir los cambios en los registros de DNS, la reversión puede fallar debido al eventual modelo de coherencia de Route 53. Si CloudFormation intenta volver a crear un registro que se ha eliminado recientemente, pero que parece que sigue existiendo debido a una posible coherencia, es posible que se produzcan `InvalidChangeBatch` errores que hagan que el DNS no funcione correctamente.

Cómo minimizar los problemas relacionados con la consistencia final:

- Planifique los cambios con cuidado: evite realizar cambios rápidos y sucesivos en los mismos registros de DNS.
- Pruebe primero por fuera del entorno de producción: pruebe siempre los cambios de DNS en los entornos de desarrollo antes de aplicarlos a la producción.
- Supervise las implementaciones: observe de cerca los eventos de la CloudFormation pila durante las implementaciones relacionadas con el DNS. Para obtener orientación sobre la supervisión, consulte [Monitoreo de Amazon Route 53](#).
- Tenga preparados los procedimientos de reversión: prepare los procedimientos de recuperación manual en caso de que las reversiones automáticas fallen.

Orden y lógica de los registros de DNS IDs

Al crear varios registros DNS en CloudFormation, tenga cuidado con el orden de los registros y la asignación de identificadores lógicos.

Warning

Si define los registros DNS en matrices o listas dentro de la CloudFormation plantilla, la inserción de nuevos registros en el centro de la lista puede provocar que se reasignen CloudFormation los registros lógicos IDs a los existentes. Esto desencadena la sustitución de registros, lo que puede provocar interrupciones en el servicio y errores de reversión.

Prácticas recomendadas para la administración de registros de DNS:

- Utilice una lógica explícita IDs: asigne siempre una lógica explícita y significativa IDs a los registros de DNS en lugar de confiar en los índices de matriz. Para obtener más información sobre la CloudFormation lógica IDs, consulte la [estructura de la sección Recursos](#) de la Guía del AWS CloudFormation usuario
- Anexe nuevos registros: cuando añada nuevos registros de DNS a las listas existentes, anéxeles al final en lugar de insertarlos en el medio.
- Agrupe los registros relacionados: considere utilizar `AWS::Route53::RecordSetGroup` para administrar los registros relacionados en conjunto. Para obtener más información, consulte [AWS::Route53::RecordSetAgrupar](#) en la Guía AWS CloudFormation del usuario.
- Revise los conjuntos de cambios: revise siempre los conjuntos de cambios de CloudFormation antes de la implementación para identificar sustituciones inesperadas de registros. Para obtener

más información, consulte [Actualización de pilas con conjuntos de cambios](#) en la Guía del usuario de AWS CloudFormation .

Gestión de los errores de reversión

Si se produce un CloudFormation error en la reversión debido a problemas relacionados con el DNS, es posible que tengas que realizar una recuperación manual.

Cómo efectuar una recuperación manual cuando fallan las reversiones de DNS

1. Identifique los registros de DNS fallidos revisando los eventos de la CloudFormation pila y los registros de las zonas alojadas de Route 53
2. Cree o actualice manualmente los registros de DNS que faltan a través de la consola o la API de Route 53. Para obtener información acerca de la creación de registros, consulte [Uso de registros](#).
3. Una vez que se restablezca el DNS, actualice la CloudFormation plantilla para que coincida con el estado actual
4. Implemente la plantilla corregida para CloudFormation volver a sincronizarla con los recursos reales

Cómo evitar errores de reversión:

- Evite hacer cambios que puedan provocar la sustitución de registros de DNS durante los períodos de tráfico intenso.
- Implemente comprobaciones de estado y monitoreo para detectar rápidamente problemas de DNS. Para obtener más información sobre las comprobaciones de estado, consulte [Creación y actualización de comprobaciones de estado](#).
- Considere la posibilidad de utilizar estrategias de implementación azul/verde para los cambios críticos en el DNS. Para obtener más información sobre las prácticas recomendadas para la implementación, consulte [Prácticas recomendadas de Amazon Route 53](#).
- Documente los procedimientos de emergencia para la recuperación manual del DNS.

Obtenga más información sobre CloudFormation

Para obtener más información CloudFormation, consulte los siguientes recursos:

- [AWS CloudFormation](#)
- [AWS CloudFormation Guía del usuario](#)
- [CloudFormation Referencia de la API](#)
- [AWS CloudFormation Guía del usuario de la interfaz de línea de comandos](#)

Ejemplos de código de Route 53 con SDK de AWS

Los siguientes ejemplos de código muestran cómo utilizar Route 53 con un kit de desarrollo de software (SDK) de AWS.

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte [Uso de Route 53 con un AWS SDK](#). En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Ejemplos de código

- [Ejemplos de código para Route 53 usando AWS SDKs](#)
 - [Ejemplos básicos de uso de Route 53 AWS SDKs](#)
 - [Acciones para Route 53 mediante AWS SDKs](#)
 - [Utilizar ChangeResourceRecordSets con una CLI](#)
 - [Utilizar CreateHostedZone con una CLI](#)
 - [Utilizar DeleteHostedZone con una CLI](#)
 - [Utilizar GetHostedZone con una CLI](#)
 - [Úselo ListHostedZones con un AWS SDK o CLI](#)
 - [Utilizar ListHostedZonesByName con una CLI](#)
 - [Utilizar ListQueryLoggingConfigs con una CLI](#)
 - [Ejemplos de código para el registro de dominios de Route 53 mediante AWS SDKs](#)
 - [Ejemplos básicos del registro de dominios de Route 53 mediante AWS SDKs](#)
 - [Registro de dominio de Introducción a Route 53](#)
 - [Conozca los conceptos básicos del registro de dominios de Route 53 con un AWS SDK](#)
 - [Acciones para el registro de dominios de Route 53 mediante AWS SDKs](#)
 - [Úselo CheckDomainAvailability con un AWS SDK o CLI](#)
 - [Úselo CheckDomainTransferability con un AWS SDK o CLI](#)
 - [Úselo GetDomainDetail con un AWS SDK o CLI](#)
 - [Úselo GetDomainSuggestions con un AWS SDK o CLI](#)
 - [Úselo GetOperationDetail con un AWS SDK o CLI](#)
 - [Úselo ListDomains con un AWS SDK o CLI](#)
 - [Úselo ListOperations con un AWS SDK o CLI](#)

- [ListPricesÚselo con un AWS SDK](#)
- [Úselo RegisterDomain con un AWS SDK o CLI](#)
- [Úselo ViewBilling con un AWS SDK o CLI](#)

Ejemplos de código para Route 53 usando AWS SDKs

Los siguientes ejemplos de código muestran cómo usar Route 53 con un kit de desarrollo de AWS software (SDK).

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte [Uso de Route 53 con un AWS SDK](#). En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Ejemplos de código

- [Ejemplos básicos de uso de Route 53 AWS SDKs](#)
 - [Acciones para Route 53 mediante AWS SDKs](#)
 - [Utilizar ChangeResourceRecordSets con una CLI](#)
 - [Utilizar CreateHostedZone con una CLI](#)
 - [Utilizar DeleteHostedZone con una CLI](#)
 - [Utilizar GetHostedZone con una CLI](#)
 - [Úselo ListHostedZones con un AWS SDK o CLI](#)
 - [Utilizar ListHostedZonesByName con una CLI](#)
 - [Utilizar ListQueryLoggingConfigs con una CLI](#)

Ejemplos básicos de uso de Route 53 AWS SDKs

Los siguientes ejemplos de código muestran cómo utilizar los conceptos básicos de Amazon Route 53 con AWS SDKs.

Ejemplos

- [Acciones para Route 53 mediante AWS SDKs](#)

- [Utilizar ChangeResourceRecordSets con una CLI](#)
- [Utilizar CreateHostedZone con una CLI](#)
- [Utilizar DeleteHostedZone con una CLI](#)
- [Utilizar GetHostedZone con una CLI](#)
- [Úselo ListHostedZones con un AWS SDK o CLI](#)
- [Utilizar ListHostedZonesByName con una CLI](#)
- [Utilizar ListQueryLoggingConfigs con una CLI](#)

Acciones para Route 53 mediante AWS SDKs

Los siguientes ejemplos de código muestran cómo realizar acciones individuales de Route 53 con AWS SDKs. Cada ejemplo incluye un enlace a GitHub, donde puede encontrar instrucciones para configurar y ejecutar el código.

Los siguientes ejemplos incluyen solo las acciones que se utilizan con mayor frecuencia. Para ver una lista completa, consulte la [Referencia de la API de Amazon Route 53](#).

Ejemplos

- [Utilizar ChangeResourceRecordSets con una CLI](#)
- [Utilizar CreateHostedZone con una CLI](#)
- [Utilizar DeleteHostedZone con una CLI](#)
- [Utilizar GetHostedZone con una CLI](#)
- [Úselo ListHostedZones con un AWS SDK o CLI](#)
- [Utilizar ListHostedZonesByName con una CLI](#)
- [Utilizar ListQueryLoggingConfigs con una CLI](#)

Utilizar **ChangeResourceRecordSets** con una CLI

Los siguientes ejemplos de código muestran cómo utilizar ChangeResourceRecordSets.

CLI

AWS CLI

Cómo crear, actualizar o eliminar un conjunto de registros de recursos

El siguiente comando `change-resource-record-sets` crea un conjunto de registros de recursos mediante `hosted-zone-id` `Z1R8UBAEXAMPLE` y la configuración con formato JSON del archivo `C:\awscli\route53\change-resource-record-sets.json`:

```
aws route53 change-resource-record-sets --hosted-zone-id Z1R8UBAEXAMPLE --change-batch file://C:\awscli\route53\change-resource-record-sets.json
```

Para obtener más información, consulte `POST ChangeResourceRecordSets` en la referencia de la API de Amazon Route 53.

La configuración del archivo JSON depende del tipo de conjunto de registros de recursos que quiera crear:

BasicWeightedAliasWeighted AliasLatencyLatency AliasFailoverFailover Alias

Sintaxis básica:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "TTL": time to live in seconds,
        "ResourceRecords": [
          {
            "Value": "applicable value for the record type"
          },
          {...}
        ]
      }
    },
    {...}
  ]
}
```

Sintaxis ponderada:

```
{
  "Comment": "optional comment about the changes in this change batch request",
```

```

"Changes": [
  {
    "Action": "CREATE"|"DELETE"|"UPSERT",
    "ResourceRecordSet": {
      "Name": "DNS domain name",
      "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
      "SetIdentifier": "unique description for this resource record set",
      "Weight": value between 0 and 255,
      "TTL": time to live in seconds,
      "ResourceRecords": [
        {
          "Value": "applicable value for the record type"
        },
        {...}
      ],
      "HealthCheckId": "optional ID of an Amazon Route 53 health check"
    }
  },
  {...}
]
}

```

Sintaxis de alias:

```

{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution,
Amazon S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53
hosted zone",
          "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
bucket, Elastic Load Balancing load balancer, or another resource record set in
this hosted zone",
          "EvaluateTargetHealth": true|false
        },
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    }
  ]
}

```

```
    },
    {...}
  ]
}
```

Sintaxis de alias ponderada:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Weight": value between 0 and 255,
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution,
Amazon S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53
hosted zone",
          "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
bucket, Elastic Load Balancing load balancer, or another resource record set in
this hosted zone",
          "EvaluateTargetHealth": true|false
        },
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

Sintaxis de latencia:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
```

```

    "SetIdentifier": "unique description for this resource record set",
    "Region": "Amazon EC2 region name",
    "TTL": time to live in seconds,
    "ResourceRecords": [
      {
        "Value": "applicable value for the record type"
      },
      {...}
    ],
    "HealthCheckId": "optional ID of an Amazon Route 53 health check"
  }
},
{...}
]
}

```

Sintaxis de alias de latencia:

```

{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Region": "Amazon EC2 region name",
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution,
Amazon S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53
hosted zone",
          "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
bucket, Elastic Load Balancing load balancer, or another resource record set in
this hosted zone",
          "EvaluateTargetHealth": true|false
        },
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}

```

Sintaxis de conmutación por error:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Failover": "PRIMARY" | "SECONDARY",
        "TTL": time to live in seconds,
        "ResourceRecords": [
          {
            "Value": "applicable value for the record type"
          },
          {...}
        ],
        "HealthCheckId": "ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

Sintaxis del alias de conmutación por error:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Failover": "PRIMARY" | "SECONDARY",
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution,
Amazon S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53
hosted zone",

```



```

        "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
        bucket, Elastic Load Balancing load balancer, or another resource record set in
        this hosted zone",
        "EvaluateTargetHealth": true|false
    },
    "HealthCheckId": "optional ID of an Amazon Route 53 health check"
}
},
{...}
]
}

```

- Para obtener más información sobre la API, consulte [ChangeResourceRecordSets](#) la Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: en este ejemplo, se crea un registro A para `www.example.com` y se cambia el registro A de `test.example.com` de `192.0.2.3` a `192.0.2.1`. Tenga en cuenta que los valores de los registros de tipo TXT modificados deben estar entre comillas dobles. Consulte la documentación de Amazon Route 53 para obtener más información. Puede usar el `Get-R53Change` cmdlet para sondear y determinar cuándo se han completado los cambios.

```

$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "TXT"
$change1.ResourceRecordSet.TTL = 600
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="item 1 item 2 item 3"})

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "DELETE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "test.example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.TTL = 600
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.3"})

$change3 = New-Object Amazon.Route53.Model.Change

```

```

$change3.Action = "CREATE"
$change3.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change3.ResourceRecordSet.Name = "test.example.com"
$change3.ResourceRecordSet.Type = "A"
$change3.ResourceRecordSet.TTL = 600
$change3.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.1"})

$params = @{
    HostedZoneId="Z1PA6795UKMFR9"
    ChangeBatch_Comment="This change batch creates a TXT record for www.example.com.
    and changes the A record for test.example.com. from 192.0.2.3 to 192.0.2.1."
    ChangeBatch_Change=$change1,$change2,$change3
}

Edit-R53ResourceRecordSet @params

```

Ejemplo 2: en este ejemplo, se muestra cómo crear conjuntos de registros de recursos de alias. “Z22222222” es el ID de la zona alojada de Amazon Route 53 en la que crea el conjunto de registros de recursos de alias. “example.com” es el vértice de zona para el que desea crear un alias y “www.example.com” es un subdominio para el que también debe crear un alias. «Z11111» es un ejemplo de un ID de zona alojada para el balanceador de cargas y «example-load-balancer-11.us-east-1.elb.amazonaws.com» es un ejemplo de un nombre de dominio de balanceador de carga con el que Amazon Route 53 responde a las consultas de example.com y www.example.com. Consulte la documentación de Amazon Route 53 para obtener más información. Puede usar el cmdlet para sondear y determinar cuándo se han completado los cambios. Get-R53Change

```

$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.AliasTarget = New-Object
    Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet

```

```

$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.AliasTarget = New-Object
    Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z11111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $false

$params = @{
    HostedZoneId="Z2222222222"
    ChangeBatch_Comment="This change batch creates two alias resource record sets,
    one for the zone apex, example.com, and one for www.example.com, that both point
    to example-load-balancer-1111111111.us-east-1.elb.amazonaws.com."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params

```

Ejemplo 3: en este ejemplo, se crean dos registros A para `www.example.com`. Una cuarta parte de las veces ($1/(1+3)$), Amazon Route 53 responde a las consultas de `www.example.com` con los dos valores del primer conjunto de registros de recursos (192.0.2.9 y 192.0.2.10). Tres cuartas partes de las veces ($3/(1+3)$), Amazon Route 53 responde a las consultas de `www.example.com` con los dos valores del segundo conjunto de registros de recursos (192.0.2.11 y 192.0.2.12). Consulte la documentación de Amazon Route 53 para obtener más información. Puede usar el `Get-R53Change` cmdlet para sondear y determinar cuándo se han completado los cambios.

```

$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "Rack 2, Positions 4 and 5"
$change1.ResourceRecordSet.Weight = 1
$change1.ResourceRecordSet.TTL = 600
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.9"})
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.10"})

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet

```

```

$change2.ResourceRecordSet.Name = "www.example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "Rack 5, Positions 1 and 2"
$change2.ResourceRecordSet.Weight = 3
$change2.ResourceRecordSet.TTL = 600
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.11"})
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.12"})

$params = @{
    HostedZoneId="Z1PA6795UKMFR9"
    ChangeBatch_Comment="This change creates two weighted resource record sets,
    each of which has two values."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params

```

Ejemplo 4: en este ejemplo se muestra cómo crear conjuntos de registros de recursos de alias ponderados suponiendo que example.com es el dominio para el que desea crear conjuntos de registros de recursos de alias ponderados. SetIdentifier diferencia los dos conjuntos de registros de recursos de alias ponderados entre sí. Este elemento es obligatorio porque los elementos Nombre y Tipo tienen los mismos valores para ambos conjuntos de registros de recursos. Los valores Z333311111 y Z33333333333333 son ejemplos de zonas alojadas para el balanceador de cargas ELB especificadas IDs por el valor de. DNSName example-load-balancer-222222222.us-east-1.elb.amazonaws.com y -4444444444.us-east-1.elb.amazonaws.com example-load-balancer son ejemplos de dominios de Elastic Load Balancing desde los que Amazon Route 53 responde a las consultas de example.com. Consulte la documentación de Amazon Route 53 para obtener más información. Puede usar el cmdlet para sondear y determinar cuándo Get-R53Change se han completado los cambios.

```

$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "1"
$change1.ResourceRecordSet.Weight = 3
$change1.ResourceRecordSet.AliasTarget = New-Object
    Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"

```

```

$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-222222222.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "2"
$change2.ResourceRecordSet.Weight = 1
$change2.ResourceRecordSet.AliasTarget = New-Object
    Amazon.Route53.Model.AliasTarget
$change2.ResourceRecordSet.AliasTarget.HostedZoneId = "Z3333333333333333"
$change2.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-444444444.us-east-1.elb.amazonaws.com."
$change2.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $false

$params = @{
    HostedZoneId="Z55555555555"
    ChangeBatch_Comment="This change batch creates two weighted alias resource
        record sets. Amazon Route 53 responds to queries for example.com with the first
        ELB domain 3/4ths of the times and the second one 1/4th of the time."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params

```

Ejemplo 5: en este ejemplo, se crean dos conjuntos de registros de recursos de alias de latencia: uno para un equilibrador de carga ELB en la región Oeste de EE. UU. (Oregón) (us-west-2) y otro para un equilibrador de carga en la región Asia Pacífico (Singapur) (ap-southeast-1). Consulte la documentación de Amazon Route 53 para obtener más información. Puede usar el Get-R53Change cmdlet para sondear y determinar cuándo se han completado los cambios.

```

$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "Oregon load balancer 1"
$change1.ResourceRecordSet.Region = us-west-2

```

```

$change1.ResourceRecordSet.AliasTarget = New-Object
    Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z11111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-2222222222.us-west-2.elb.amazonaws.com"
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "Singapore load balancer 1"
$change2.ResourceRecordSet.Region = ap-southeast-1
$change2.ResourceRecordSet.AliasTarget = New-Object
    Amazon.Route53.Model.AliasTarget
$change2.ResourceRecordSet.AliasTarget.HostedZoneId = "Z22222222222222"
$change2.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.ap-southeast-1.elb.amazonaws.com"
$change2.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$params = @{
    HostedZoneId="Z555555555555"
    ChangeBatch_Comment="This change batch creates two latency resource
record sets, one for the US West (Oregon) region and one for the Asia Pacific
(Singapore) region."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params

```

- Para obtener más información sobre la API, consulte la referencia [ChangeResourceRecordSets](#) de Herramientas de AWS para PowerShell cmdlets (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: en este ejemplo, se crea un registro A para `www.example.com` y se cambia el registro A de `test.example.com` de `192.0.2.3` a `192.0.2.1`. Tenga en cuenta que los valores de los registros de tipo TXT modificados deben estar entre comillas dobles. Consulte la documentación de Amazon Route 53 para obtener más información. Puede usar el `Get-R53Change` cmdlet para sondear y determinar cuándo se han completado los cambios.

```
$change1 = New-Object Amazon.Route53.Model.Change
```

```

$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "TXT"
$change1.ResourceRecordSet.TTL = 600
$change1.ResourceRecordSet.ResourceRecords = @()
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="item 1 item 2 item 3"})

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "DELETE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "test.example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.TTL = 600
$change2.ResourceRecordSet.ResourceRecords = @()
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.3"})

$change3 = New-Object Amazon.Route53.Model.Change
$change3.Action = "CREATE"
$change3.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change3.ResourceRecordSet.Name = "test.example.com"
$change3.ResourceRecordSet.Type = "A"
$change3.ResourceRecordSet.TTL = 600
$change3.ResourceRecordSet.ResourceRecords = @()
$change3.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.1"})

$params = @{
    HostedZoneId="Z1PA6795UKMFR9"
    ChangeBatch_Comment="This change batch creates a TXT record for www.example.com.
    and changes the A record for test.example.com. from 192.0.2.3 to 192.0.2.1."
    ChangeBatch_Change=$change1,$change2,$change3
}

Edit-R53ResourceRecordSet @params

```

Ejemplo 2: en este ejemplo, se muestra cómo crear conjuntos de registros de recursos de alias. “Z222222222” es el ID de la zona alojada de Amazon Route 53 en la que crea el conjunto de registros de recursos de alias. “example.com” es el vértice de zona para el que desea crear un alias y “www.example.com” es un subdominio para el que también debe crear un alias. «Z11111» es un ejemplo de un ID de zona alojada para el balanceador de cargas y «example-load-balancer-11.us-east-1.elb.amazonaws.com» es un ejemplo de un nombre de dominio de balanceador de carga con el que Amazon Route 53 responde a las consultas

de example.com y www.example.com. Consulte la documentación de Amazon Route 53 para obtener más información. Puede usar el cmdlet para sondear y determinar cuándo se han completado los cambios. `Get-R53Change`

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.AliasTarget = New-Object
    Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.AliasTarget = New-Object
    Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $false

$params = @{
    HostedZoneId="Z222222222"
    ChangeBatch_Comment="This change batch creates two alias resource record sets,
    one for the zone apex, example.com, and one for www.example.com, that both point
    to example-load-balancer-1111111111.us-east-1.elb.amazonaws.com."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params
```

Ejemplo 3: en este ejemplo, se crean dos registros A para www.example.com. Una cuarta parte de las veces ($1/(1+3)$), Amazon Route 53 responde a las consultas de www.example.com con los dos valores del primer conjunto de registros de recursos (192.0.2.9 y 192.0.2.10). Tres cuartas partes de las veces ($3/(1+3)$), Amazon Route 53 responde a las

consultas de `www.example.com` con los dos valores del segundo conjunto de registros de recursos (192.0.2.11 y 192.0.2.12). Consulte la documentación de Amazon Route 53 para obtener más información. Puede usar el `Get-R53Change` cmdlet para sondear y determinar cuándo se han completado los cambios.

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "Rack 2, Positions 4 and 5"
$change1.ResourceRecordSet.Weight = 1
$change1.ResourceRecordSet.TTL = 600
$change1.ResourceRecordSet.ResourceRecords = @()
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.9"})
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.10"})

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "www.example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "Rack 5, Positions 1 and 2"
$change2.ResourceRecordSet.Weight = 3
$change2.ResourceRecordSet.TTL = 600
$change2.ResourceRecordSet.ResourceRecords = @()
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.11"})
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.12"})

$params = @{
    HostedZoneId="Z1PA6795UKMFR9"
    ChangeBatch_Comment="This change creates two weighted resource record sets,
    each of which has two values."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params
```

Ejemplo 4: en este ejemplo se muestra cómo crear conjuntos de registros de recursos de alias ponderados suponiendo que `example.com` es el dominio para el que desea crear conjuntos de registros de recursos de alias ponderados. `SetIdentifier` diferencia los dos conjuntos de registros de recursos de alias ponderados entre sí. Este elemento es obligatorio

porque los elementos Nombre y Tipo tienen los mismos valores para ambos conjuntos de registros de recursos. Los valores Z333311111 y Z3333333333333 son ejemplos de zonas alojadas para el balanceador de cargas ELB especificadas IDs por el valor de. DNSName example-load-balancer-222222222.us-east-1.elb.amazonaws.com y -4444444444.us-east-1.elb.amazonaws.com example-load-balancer son ejemplos de dominios de Elastic Load Balancing desde los que Amazon Route 53 responde a las consultas de example.com. Consulte la documentación de Amazon Route 53 para obtener más información. Puede usar el cmdlet para sondear y determinar cuándo Get-R53Change se han completado los cambios.

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "1"
$change1.ResourceRecordSet.Weight = 3
$change1.ResourceRecordSet.AliasTarget = New-Object
    Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-222222222.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "2"
$change2.ResourceRecordSet.Weight = 1
$change2.ResourceRecordSet.AliasTarget = New-Object
    Amazon.Route53.Model.AliasTarget
$change2.ResourceRecordSet.AliasTarget.HostedZoneId = "Z3333333333333"
$change2.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-4444444444.us-east-1.elb.amazonaws.com."
$change2.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $false

$params = @{
    HostedZoneId="Z5555555555"
    ChangeBatch_Comment="This change batch creates two weighted alias resource
record sets. Amazon Route 53 responds to queries for example.com with the first
ELB domain 3/4ths of the times and the second one 1/4th of the time."
```

```

    ChangeBatch_Change=$change1,$change2
}

```

```
Edit-R53ResourceRecordSet @params
```

Ejemplo 5: en este ejemplo, se crean dos conjuntos de registros de recursos de alias de latencia: uno para un equilibrador de carga ELB en la región Oeste de EE. UU. (Oregón) (us-west-2) y otro para un equilibrador de carga en la región Asia Pacífico (Singapur) (ap-southeast-1). Consulte la documentación de Amazon Route 53 para obtener más información. Puede usar el Get-R53Change cmdlet para sondear y determinar cuándo se han completado los cambios.

```

$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "Oregon load balancer 1"
$change1.ResourceRecordSet.Region = us-west-2
$change1.ResourceRecordSet.AliasTarget = New-Object
    Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z11111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-222222222.us-west-2.elb.amazonaws.com"
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "Singapore load balancer 1"
$change2.ResourceRecordSet.Region = ap-southeast-1
$change2.ResourceRecordSet.AliasTarget = New-Object
    Amazon.Route53.Model.AliasTarget
$change2.ResourceRecordSet.AliasTarget.HostedZoneId = "Z22222222222222"
$change2.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.ap-southeast-1.elb.amazonaws.com"
$change2.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$params = @{
    HostedZoneId="Z55555555555"

```

```
ChangeBatch_Comment="This change batch creates two latency resource
record sets, one for the US West (Oregon) region and one for the Asia Pacific
(Singapore) region."
ChangeBatch_Change=$change1,$change2
}
```

Edit-R53ResourceRecordSet @params

- Para obtener más información sobre la API, consulte la referencia [ChangeResourceRecordSets](#) de Herramientas de AWS para PowerShell cmdlets (V5).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. [Uso de Route 53 con un AWS SDK](#) En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Utilizar **CreateHostedZone** con una CLI

Los siguientes ejemplos de código muestran cómo utilizar CreateHostedZone.

CLI

AWS CLI

Para crear una zona alojada

El siguiente comando `create-hosted-zone` agrega una zona alojada denominada `example.com` mediante la referencia de intermediario `2014-04-01-18:47`. El comentario opcional incluye un espacio, por lo que debe escribirse entre comillas:

```
aws route53 create-hosted-zone --name example.com --caller-
reference 2014-04-01-18:47 --hosted-zone-config Comment="command-line version"
```

Para obtener más información, consulte [Working with Hosted Zones](#) en la Guía para desarrolladores de Amazon Route 53.

- Para obtener más información sobre la API, consulte [CreateHostedZone](#) la Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: crea una nueva zona alojada llamada “example.com”, asociada a un conjunto de delegación reutilizable. Tenga en cuenta que debe proporcionar un valor para el CallerReference parámetro de modo que las solicitudes se tengan que volver a intentar si es necesario sin correr el riesgo de ejecutar la operación dos veces. Como la zona alojada se crea en una VPC, es privada automáticamente y no se debe establecer el parámetro - HostedZoneConfig _PrivateZone .

```
$params = @{
    Name="example.com"
    CallerReference="myUniqueIdentifier"
    HostedZoneConfig_Comment="This is my first hosted zone"
    DelegationSetId="NZ8X2CISAMPLE"
    VPC_VPCId="vpc-1a2b3c4d"
    VPC_VPCRegion="us-east-1"
}

New-R53HostedZone @params
```

- Para obtener más información sobre la API, consulte [CreateHostedZone](#) la referencia de Herramientas de AWS para PowerShell cmdlets (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: crea una nueva zona alojada llamada “example.com”, asociada a un conjunto de delegación reutilizable. Tenga en cuenta que debe proporcionar un valor para el CallerReference parámetro de modo que las solicitudes se tengan que volver a intentar si es necesario sin correr el riesgo de ejecutar la operación dos veces. Como la zona alojada se crea en una VPC, es privada automáticamente y no se debe establecer el parámetro - HostedZoneConfig _PrivateZone .

```
$params = @{
    Name="example.com"
    CallerReference="myUniqueIdentifier"
    HostedZoneConfig_Comment="This is my first hosted zone"
    DelegationSetId="NZ8X2CISAMPLE"
    VPC_VPCId="vpc-1a2b3c4d"
    VPC_VPCRegion="us-east-1"
}
```

```
New-R53HostedZone @params
```

- Para obtener más información sobre la API, consulte [CreateHostedZone Herramientas de AWS para PowerShell](#) Cmdlet Reference (V5).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. [Uso de Route 53 con un AWS SDK](#) En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Utilizar **DeleteHostedZone** con una CLI

Los siguientes ejemplos de código muestran cómo utilizar DeleteHostedZone.

CLI

AWS CLI

Cómo eliminar una zona alojada

El siguiente comando `delete-hosted-zone` elimina la zona alojada con el `id` `Z36KTIQEXAMPLE`:

```
aws route53 delete-hosted-zone --id Z36KTIQEXAMPLE
```

- Para obtener más información sobre la API, consulte [DeleteHostedZone](#) la Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: se elimina la zona alojada con el ID especificado. Antes de continuar con el comando, se le solicitará que lo confirme, a menos que añada el parámetro `-Force` switch.

```
Remove-R53HostedZone -Id Z1PA6795UKMFR9
```

- Para obtener más información sobre la API, consulte [DeleteHostedZone Herramientas de AWS para PowerShell](#) Cmdlet Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: se elimina la zona alojada con el ID especificado. Antes de continuar con el comando, se le solicitará que lo confirme, a menos que añada el parámetro `-Force switch`.

```
Remove-R53HostedZone -Id Z1PA6795UKMFR9
```

- Para obtener más información sobre la API, consulte [DeleteHostedZone](#) la referencia de Herramientas de AWS para PowerShell cmdlets (V5).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. [Uso de Route 53 con un AWS SDK](#) En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Utilizar **GetHostedZone** con una CLI

Los siguientes ejemplos de código muestran cómo utilizar `GetHostedZone`.

CLI

AWS CLI

Cómo obtener información acerca de una zona alojada

El siguiente comando `get-hosted-zone` obtiene información sobre la zona alojada con un id `Z1R8UBAEXAMPLE`:

```
aws route53 get-hosted-zone --id Z1R8UBAEXAMPLE
```

- Para obtener más información sobre la API, consulte [GetHostedZone](#) la Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: Devuelve los detalles de la zona alojada con el ID `PJN98 FT9 Z1D633`.

```
Get-R53HostedZone -Id Z1D633PJN98FT9
```

- Para obtener información sobre la API, consulte Herramientas de AWS para PowerShell Cmdlet [GetHostedZoneReference](#) (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: Devuelve los detalles de la zona alojada con el ID PJN98 FT9 Z1D633.

```
Get-R53HostedZone -Id Z1D633PJN98FT9
```

- Para obtener más información sobre la API, consulte Herramientas de AWS para PowerShell Cmdlet [GetHostedZoneReference](#) (V5).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. [Uso de Route 53 con un AWS SDK](#) En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **ListHostedZones** con un AWS SDK o CLI

Los siguientes ejemplos de código muestran cómo utilizar ListHostedZones.

CLI

AWS CLI

Para enumerar las zonas alojadas asociadas a la AWS cuenta corriente

El siguiente `list-hosted-zones` comando muestra información resumida sobre las primeras 100 zonas alojadas asociadas a la AWS cuenta actual. :

```
aws route53 list-hosted-zones
```

Si tiene más de 100 zonas alojadas o si desea enumerarlas en grupos de menos de 100, incluya el parámetro `--max-items`. Por ejemplo, para enumerar las zonas alojadas, utilice el siguiente comando:

```
aws route53 list-hosted-zones --max-items 1
```

Para ver información sobre la siguiente zona alojada, tome el valor de `NextToken` de la respuesta al comando anterior e inclúyalo en el parámetro `--starting-token`, por ejemplo:


```
aws route53 list-hosted-zones --max-items 1 --starting-token Z3M3LMPEXAMPLE
```

- Para obtener más información sobre la API, consulte [ListHostedZones](#) la Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: se muestra todas las zonas alojadas públicas y privadas.

```
Get-R53HostedZoneList
```

Ejemplo 2: Muestra todas las zonas alojadas asociadas al conjunto de delegación reutilizable que tiene el ID NZ8 X2CISAMPLE

```
Get-R53HostedZoneList -DelegationSetId NZ8X2CISAMPLE
```

- Para obtener información sobre la API, consulte Herramientas de AWS para PowerShell Cmdlet [ListHostedZones](#)Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: se muestra todas las zonas alojadas públicas y privadas.

```
Get-R53HostedZoneList
```

Ejemplo 2: Muestra todas las zonas alojadas asociadas al conjunto de delegación reutilizable que tiene el ID NZ8 X2CISAMPLE

```
Get-R53HostedZoneList -DelegationSetId NZ8X2CISAMPLE
```

- Para obtener más información sobre la API, consulte Herramientas de AWS para PowerShell Cmdlet [ListHostedZones](#)Reference (V5).

Rust

SDK para Rust

Note

Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
async fn show_host_info(client: &aws_sdk_route53::Client) -> Result<(),
aws_sdk_route53::Error> {
    let hosted_zone_count = client.get_hosted_zone_count().send().await?;

    println!(
        "Number of hosted zones in region : {}",
        hosted_zone_count.hosted_zone_count(),
    );

    let hosted_zones = client.list_hosted_zones().send().await?;

    println!("Zones:");

    for hz in hosted_zones.hosted_zones() {
        let zone_name = hz.name();
        let zone_id = hz.id();

        println!(" ID : {}", zone_id);
        println!(" Name : {}", zone_name);
        println!();
    }

    Ok(())
}
```

- Para obtener más información sobre la API, consulta [ListHostedZones](#) la referencia sobre la API de AWS SDK para Rust.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte [Uso de Route 53 con un AWS SDK](#). En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Utilizar **ListHostedZonesByName** con una CLI

Los siguientes ejemplos de código muestran cómo utilizar ListHostedZonesByName.

CLI

AWS CLI

En el siguiente comando se enumeran hasta 100 zonas alojadas ordenadas por nombre de dominio:

```
aws route53 list-hosted-zones-by-name
```

Salida:

```
{
  "HostedZones": [
    {
      "ResourceRecordSetCount": 2,
      "CallerReference": "test20150527-2",
      "Config": {
        "Comment": "test2",
        "PrivateZone": false
      },
      "Id": "/hostedzone/Z119WBBTVP5WFX",
      "Name": "2.example.com."
    },
    {
      "ResourceRecordSetCount": 2,
      "CallerReference": "test20150527-1",
      "Config": {
        "Comment": "test",
        "PrivateZone": false
      },
      "Id": "/hostedzone/Z3P5QSUBK4P0TI",
      "Name": "www.example.com."
    }
  ],
}
```

```
"IsTruncated": false,  
"MaxItems": "100"  
}
```

En el siguiente comando se muestran las zonas alojadas ordenadas por nombre, empezando por `www.example.com`:

```
aws route53 list-hosted-zones-by-name --dns-name www.example.com
```

Salida:

```
{  
  "HostedZones": [  
    {  
      "ResourceRecordSetCount": 2,  
      "CallerReference": "mwunderl20150527-1",  
      "Config": {  
        "Comment": "test",  
        "PrivateZone": false  
      },  
      "Id": "/hostedzone/Z3P5QSUBK4P0TI",  
      "Name": "www.example.com."  
    },  
  ],  
  "DNSName": "www.example.com",  
  "IsTruncated": false,  
  "MaxItems": "100"  
}
```

- Para obtener más información sobre la API, consulte [ListHostedZonesByName](#) la Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: se devuelve todas las zonas alojadas públicas y privadas según el orden de la secuencia clasificación ASCII por nombre de dominio.

```
Get-R53HostedZonesByName
```

Ejemplo 2: se devuelve las zonas alojadas públicas y privadas, según el orden de la secuencia clasificación ASCII por nombre de dominio, empezando por el nombre de DNS especificado.

```
Get-R53HostedZonesByName -DnsName example2.com
```

- Para obtener más información sobre la API, consulte [ListHostedZonesByName](#) [Herramientas de AWS para PowerShell](#) Cmdlet Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: se devuelve todas las zonas alojadas públicas y privadas según el orden de la secuencia clasificación ASCII por nombre de dominio.

```
Get-R53HostedZonesByName
```

Ejemplo 2: se devuelve las zonas alojadas públicas y privadas, según el orden de la secuencia clasificación ASCII por nombre de dominio, empezando por el nombre de DNS especificado.

```
Get-R53HostedZonesByName -DnsName example2.com
```

- Para obtener más información sobre la API, consulte [ListHostedZonesByName](#) la referencia de Herramientas de AWS para PowerShell cmdlets (V5).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. [Uso de Route 53 con un AWS SDK](#) En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Utilizar **ListQueryLoggingConfigs** con una CLI

Los siguientes ejemplos de código muestran cómo utilizar ListQueryLoggingConfigs.

CLI

AWS CLI

Cómo enumerar las configuraciones de registro de consultas

En el siguiente `list-query-logging-configs` ejemplo, se muestra información sobre las primeras 100 configuraciones de registro de consultas de su AWS cuenta, para la zona alojada `Z10X3WQEXAMPLE`.

```
aws route53 list-query-logging-configs \
  --hosted-zone-id Z10X3WQEXAMPLE
```

Salida:

```
{
  "QueryLoggingConfigs": [
    {
      "Id": "964ff34e-ae03-4f06-80a2-9683cexample",
      "HostedZoneId": "Z10X3WQEXAMPLE",
      "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-group:/aws/route53/example.com:*"
    }
  ]
}
```

Para obtener más información, consulte [Logging DNS queries](#) en la Guía para desarrolladores de Amazon Route 53.

- Para obtener más información sobre la API, consulta [ListQueryLoggingConfigs](#) la Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: este ejemplo devuelve todas las configuraciones para el registro de consultas de DNS asociadas a la Cuenta de AWS actual.

```
Get-R53QueryLoggingConfigList
```

Salida:

Id	HostedZoneId	CloudWatchLogsLogGroupArn
--	-----	-----
59b0fa33-4fea-4471-a88c-926476aaa40d	Z385PDS6EAAAZR	arn:aws:logs:us-east-1:111111111112:log-group:/aws/route53/example1.com:*

```
ee528e95-4e03-4fdc-9d28-9e24ddaaa063 Z94SJHBV1AAAAZ arn:aws:logs:us-
east-1:111111111112:log-group:/aws/route53/example2.com:*
e38dddda-ceb6-45c1-8cb7-f0ae56aaaa2b Z3MEQ8T7AAA1BF arn:aws:logs:us-
east-1:111111111112:log-group:/aws/route53/example3.com:*
```

- Para obtener más información sobre la API, consulte [ListQueryLoggingConfigs](#) [Herramientas de AWS para PowerShell](#) Cmdlet Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: este ejemplo devuelve todas las configuraciones para el registro de consultas de DNS asociadas a la Cuenta de AWS actual.

```
Get-R53QueryLoggingConfigList
```

Salida:

Id	HostedZoneId	CloudWatchLogsLogGroupArn
--	-----	-----
59b0fa33-4fea-4471-a88c-926476aaa40d	Z385PDS6EAAAZR	arn:aws:logs:us-east-1:111111111112:log-group:/aws/route53/example1.com:*
ee528e95-4e03-4fdc-9d28-9e24ddaaa063	Z94SJHBV1AAAAZ	arn:aws:logs:us-east-1:111111111112:log-group:/aws/route53/example2.com:*
e38dddda-ceb6-45c1-8cb7-f0ae56aaaa2b	Z3MEQ8T7AAA1BF	arn:aws:logs:us-east-1:111111111112:log-group:/aws/route53/example3.com:*

- Para obtener más información sobre la API, consulte [ListQueryLoggingConfigs](#) la referencia de Herramientas de AWS para PowerShell cmdlets (V5).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. [Uso de Route 53 con un AWS SDK](#) En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Ejemplos de código para el registro de dominios de Route 53 mediante AWS SDKs

Los siguientes ejemplos de código muestran cómo usar el registro de dominios de Route 53 con un kit de desarrollo de AWS software (SDK).

Los conceptos básicos son ejemplos de código que muestran cómo realizar las operaciones esenciales dentro de un servicio.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte [Uso de Route 53 con un AWS SDK](#). En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Introducción

Registro de dominio de Introducción a Route 53

En los siguientes ejemplos de código se muestra cómo empezar a utilizar el registro de dominio de Route 53.

.NET

SDK para .NET

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
public static class HelloRoute53Domains
{
    static async Task Main(string[] args)
    {
        // Use the AWS .NET Core Setup package to set up dependency injection for
        // the Amazon Route 53 domain registration service.
        // Use your AWS profile name, or leave it blank to use the default
        // profile.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonRoute53Domains>()
            ).Build();
```



```
// Now the client is available for injection.
var route53Client =
host.Services.GetRequiredService<IAmazonRoute53Domains>();

// You can use await and any of the async methods to get a response.
var response = await route53Client.ListPricesAsync(new ListPricesRequest
{ Tld = "com" });
Console.WriteLine($"Hello Amazon Route 53 Domains! Following are prices
for .com domain operations:");
var comPrices = response.Prices.FirstOrDefault();
if (comPrices != null)
{
    Console.WriteLine($"Registration:
{comPrices.RegistrationPrice?.Price} {comPrices.RegistrationPrice?.Currency}");
    Console.WriteLine($"Renewal: {comPrices.RenewalPrice?.Price}
{comPrices.RenewalPrice?.Currency}");
}
}
```

- Para obtener más información sobre la API, consulta [ListPrices](#) la Referencia AWS SDK para .NET de la API.

Java

SDK para Java 2.x

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.route53domains.Route53DomainsClient;
import software.amazon.awssdk.services.route53.model.Route53Exception;
import software.amazon.awssdk.services.route53domains.model.DomainPrice;
import software.amazon.awssdk.services.route53domains.model.ListPricesRequest;
import software.amazon.awssdk.services.route53domains.model.ListPricesResponse;
import java.util.List;
```

```
/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-started.html
 *
 * This Java code examples performs the following operation:
 *
 * 1. Invokes ListPrices for at least one domain type, such as the "com" type
 * and displays the prices for Registration and Renewal.
 */
public class HelloRoute53 {
    public static final String DASHES = new String(new char[80]).replace("\0",
    "-");

    public static void main(String[] args) {
        final String usage = "\n" +
            "Usage:\n" +
            "    <hostedZoneId> \n\n" +
            "Where:\n" +
            "    hostedZoneId - The id value of an existing hosted zone. \n";

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String domainType = args[0];
        Region region = Region.US_EAST_1;
        Route53DomainsClient route53DomainsClient =
Route53DomainsClient.builder()
            .region(region)
            .build();

        System.out.println(DASHES);
        System.out.println("Invokes ListPrices for at least one domain type.");
        listPrices(route53DomainsClient, domainType);
        System.out.println(DASHES);
    }
}
```

```

    public static void listPrices(Route53DomainsClient route53DomainsClient,
String domainType) {
        try {
            ListPricesRequest pricesRequest = ListPricesRequest.builder()
                .maxItems(10)
                .tld(domainType)
                .build();

            ListPricesResponse response =
route53DomainsClient.listPrices(pricesRequest);
            List<DomainPrice> prices = response.prices();
            for (DomainPrice pr : prices) {
                System.out.println("Name: " + pr.name());
                System.out.println(
                    "Registration: " + pr.registrationPrice().price() + " " +
pr.registrationPrice().currency());
                System.out.println("Renewal: " + pr.renewalPrice().price() + " "
+ pr.renewalPrice().currency());
                System.out.println("Transfer: " + pr.transferPrice().price() + "
" + pr.transferPrice().currency());
                System.out.println("Transfer: " + pr.transferPrice().price() + "
" + pr.transferPrice().currency());
                System.out.println("Change Ownership: " +
pr.changeOwnershipPrice().price() + " "
                    + pr.changeOwnershipPrice().currency());
                System.out.println(
                    "Restoration: " + pr.restorationPrice().price() + " " +
pr.restorationPrice().currency());
                System.out.println(" ");
            }

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
}

```

- Para obtener más información sobre la API, consulta [ListPrices](#) la Referencia AWS SDK for Java 2.x de la API.

Kotlin

SDK para Kotlin

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
/**
 * Before running this Kotlin code example, set up your development environment,
 * including your credentials.
 *
 * For more information, see the following documentation topic:
 * https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html
 */
suspend fun main(args: Array<String>) {
    val usage = """
        Usage:
            <domainType>

        Where:
            domainType - The domain type (for example, com).
    """

    if (args.size != 1) {
        println(usage)
        exitProcess(0)
    }

    val domainType = args[0]
    println("Invokes ListPrices using a Paginated method.")
    listPricesPaginated(domainType)
}

suspend fun listPricesPaginated(domainType: String) {
    val pricesRequest =
        ListPricesRequest {
            maxItems = 10
            tld = domainType
        }
}
```

```

    }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
    { route53DomainsClient ->
        route53DomainsClient
            .listPricesPaginated(pricesRequest)
            .transform { it.prices?.forEach { obj -> emit(obj) } }
            .collect { pr ->
                println("Registration: ${pr.registrationPrice}
${pr.registrationPrice?.currency}")
                println("Renewal: ${pr.renewalPrice?.price}
${pr.renewalPrice?.currency}")
                println("Transfer: ${pr.transferPrice?.price}
${pr.transferPrice?.currency}")
                println("Restoration: ${pr.restorationPrice?.price}
${pr.restorationPrice?.currency}")
            }
    }
}

```

- Para obtener más información sobre la API, consulta [ListPrices](#) la referencia sobre el AWS SDK para la API de Kotlin.

Ejemplos de código

- [Ejemplos básicos del registro de dominios de Route 53 mediante AWS SDKs](#)
 - [Registro de dominio de Introducción a Route 53](#)
 - [Conozca los conceptos básicos del registro de dominios de Route 53 con un AWS SDK](#)
 - [Acciones para el registro de dominios de Route 53 mediante AWS SDKs](#)
 - [Úselo CheckDomainAvailability con un AWS SDK o CLI](#)
 - [Úselo CheckDomainTransferability con un AWS SDK o CLI](#)
 - [Úselo GetDomainDetail con un AWS SDK o CLI](#)
 - [Úselo GetDomainSuggestions con un AWS SDK o CLI](#)
 - [Úselo GetOperationDetail con un AWS SDK o CLI](#)
 - [Úselo ListDomains con un AWS SDK o CLI](#)
 - [Úselo ListOperations con un AWS SDK o CLI](#)
 - [ListPricesÚselo con un AWS SDK](#)

- [Úselo RegisterDomain con un AWS SDK o CLI](#)
- [Úselo ViewBilling con un AWS SDK o CLI](#)

Ejemplos básicos del registro de dominios de Route 53 mediante AWS SDKs

Los siguientes ejemplos de código muestran cómo usar los conceptos básicos de Amazon Route 53 domain registration with AWS SDKs.

Ejemplos

- [Registro de dominio de Introducción a Route 53](#)
- [Conozca los conceptos básicos del registro de dominios de Route 53 con un AWS SDK](#)
- [Acciones para el registro de dominios de Route 53 mediante AWS SDKs](#)
 - [Úselo CheckDomainAvailability con un AWS SDK o CLI](#)
 - [Úselo CheckDomainTransferability con un AWS SDK o CLI](#)
 - [Úselo GetDomainDetail con un AWS SDK o CLI](#)
 - [Úselo GetDomainSuggestions con un AWS SDK o CLI](#)
 - [Úselo GetOperationDetail con un AWS SDK o CLI](#)
 - [Úselo ListDomains con un AWS SDK o CLI](#)
 - [Úselo ListOperations con un AWS SDK o CLI](#)
 - [ListPricesÚselo con un AWS SDK](#)
 - [Úselo RegisterDomain con un AWS SDK o CLI](#)
 - [Úselo ViewBilling con un AWS SDK o CLI](#)

Registro de dominio de Introducción a Route 53

En los siguientes ejemplos de código se muestra cómo empezar a utilizar el registro de dominio de Route 53.

.NET

SDK para .NET

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
public static class HelloRoute53Domains
{
    static async Task Main(string[] args)
    {
        // Use the AWS .NET Core Setup package to set up dependency injection for
        // the Amazon Route 53 domain registration service.
        // Use your AWS profile name, or leave it blank to use the default
        // profile.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonRoute53Domains>()
            ).Build();

        // Now the client is available for injection.
        var route53Client =
            host.Services.GetRequiredService<IAmazonRoute53Domains>();

        // You can use await and any of the async methods to get a response.
        var response = await route53Client.ListPricesAsync(new ListPricesRequest
        { Tld = "com" });
        Console.WriteLine($"Hello Amazon Route 53 Domains! Following are prices
        for .com domain operations:");
        var comPrices = response.Prices.FirstOrDefault();
        if (comPrices != null)
        {
            Console.WriteLine($"Registration:
            {comPrices.RegistrationPrice?.Price} {comPrices.RegistrationPrice?.Currency}");
            Console.WriteLine($"Renewal: {comPrices.RenewalPrice?.Price}
            {comPrices.RenewalPrice?.Currency}");
        }
    }
}
```

```
}
```

- Para obtener más información sobre la API, consulta [ListPrices](#) la Referencia AWS SDK para .NET de la API.

Java

SDK para Java 2.x

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.route53domains.Route53DomainsClient;
import software.amazon.awssdk.services.route53.model.Route53Exception;
import software.amazon.awssdk.services.route53domains.model.DomainPrice;
import software.amazon.awssdk.services.route53domains.model.ListPricesRequest;
import software.amazon.awssdk.services.route53domains.model.ListPricesResponse;
import java.util.List;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
 * started.html
 *
 * This Java code examples performs the following operation:
 *
 * 1. Invokes ListPrices for at least one domain type, such as the "com" type
 * and displays the prices for Registration and Renewal.
 */
public class HelloRoute53 {
```



```
public static final String DASHES = new String(new char[80]).replace("\0",
"-");

public static void main(String[] args) {
    final String usage = "\n" +
        "Usage:\n" +
        "    <hostedZoneId> \n\n" +
        "Where:\n" +
        "    hostedZoneId - The id value of an existing hosted zone. \n";

    if (args.length != 1) {
        System.out.println(usage);
        System.exit(1);
    }

    String domainType = args[0];
    Region region = Region.US_EAST_1;
    Route53DomainsClient route53DomainsClient =
Route53DomainsClient.builder()
        .region(region)
        .build();

    System.out.println(DASHES);
    System.out.println("Invokes ListPrices for at least one domain type.");
    listPrices(route53DomainsClient, domainType);
    System.out.println(DASHES);
}

public static void listPrices(Route53DomainsClient route53DomainsClient,
String domainType) {
    try {
        ListPricesRequest pricesRequest = ListPricesRequest.builder()
            .maxItems(10)
            .tld(domainType)
            .build();

        ListPricesResponse response =
route53DomainsClient.listPrices(pricesRequest);
        List<DomainPrice> prices = response.prices();
        for (DomainPrice pr : prices) {
            System.out.println("Name: " + pr.name());
            System.out.println(
                "Registration: " + pr.registrationPrice().price() + " " +
pr.registrationPrice().currency());
        }
    }
}
```

```

        System.out.println("Renewal: " + pr.renewalPrice().price() + " "
+ pr.renewalPrice().currency());
        System.out.println("Transfer: " + pr.transferPrice().price() + "
" + pr.transferPrice().currency());
        System.out.println("Transfer: " + pr.transferPrice().price() + "
" + pr.transferPrice().currency());
        System.out.println("Change Ownership: " +
pr.changeOwnershipPrice().price() + " "
+ pr.changeOwnershipPrice().currency());
        System.out.println(
            "Restoration: " + pr.restorationPrice().price() + " " +
pr.restorationPrice().currency());
        System.out.println(" ");
    }

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

```

- Para obtener más información sobre la API, consulta [ListPrices](#) la Referencia AWS SDK for Java 2.x de la API.

Kotlin

SDK para Kotlin

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
/**
```

```
Before running this Kotlin code example, set up your development environment,
including your credentials.
```

For more information, see the following documentation topic:

<https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html>

```
*/
suspend fun main(args: Array<String>) {
    val usage = """
        Usage:
            <domainType>

        Where:
            domainType - The domain type (for example, com).
    """

    if (args.size != 1) {
        println(usage)
        exitProcess(0)
    }

    val domainType = args[0]
    println("Invokes ListPrices using a Paginated method.")
    listPricesPaginated(domainType)
}

suspend fun listPricesPaginated(domainType: String) {
    val pricesRequest =
        ListPricesRequest {
            maxItems = 10
            tld = domainType
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
    { route53DomainsClient ->
        route53DomainsClient
            .listPricesPaginated(pricesRequest)
            .transform { it.prices?.forEach { obj -> emit(obj) } }
            .collect { pr ->
                println("Registration: ${pr.registrationPrice}
${pr.registrationPrice?.currency}")
                println("Renewal: ${pr.renewalPrice?.price}
${pr.renewalPrice?.currency}")
                println("Transfer: ${pr.transferPrice?.price}
${pr.transferPrice?.currency}")
                println("Restoration: ${pr.restorationPrice?.price}
${pr.restorationPrice?.currency}")
            }
    }
}
```

```
}  
}
```

- Para obtener más información sobre la API, consulta [ListPrices](#) la referencia sobre el AWS SDK para la API de Kotlin.

Para ver una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulta [Uso de Route 53 con un AWS SDK](#). En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Conozca los conceptos básicos del registro de dominios de Route 53 con un AWS SDK

En el siguiente ejemplo de código, se muestra cómo:

- Enumere los dominios actuales y las operaciones del año pasado.
- Consulte la facturación del año pasado y los precios de los tipos de dominio.
- Obtención de sugerencias de dominios.
- Compruebe la disponibilidad y la transferibilidad del dominio.
- Si lo desea, solicite el registro de un dominio.
- Obtención de información de una operación.
- Si lo desea, obtenga información del dominio.

.NET

SDK para .NET

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

Ejecutar un escenario interactivo en un símbolo del sistema.

```
public static class Route53DomainScenario
{
    /*
        Before running this .NET code example, set up your development environment,
        including your credentials.

        This .NET example performs the following tasks:
        1. List current domains.
        2. List operations in the past year.
        3. View billing for the account in the past year.
        4. View prices for domain types.
        5. Get domain suggestions.
        6. Check domain availability.
        7. Check domain transferability.
        8. Optionally, request a domain registration.
        9. Get an operation detail.
        10. Optionally, get a domain detail.
    */

    private static Route53Wrapper _route53Wrapper = null!;
    private static IConfiguration _configuration = null!;

    static async Task Main(string[] args)
    {
        // Set up dependency injection for the Amazon service.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureLogging(logging =>
                logging.AddFilter("System", LogLevel.Debug)
                    .AddFilter<DebugLoggerProvider>("Microsoft",
LogLevel.Information)
                    .AddFilter<ConsoleLoggerProvider>("Microsoft",
LogLevel.Trace))
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonRoute53Domains>()
                    .AddTransient<Route53Wrapper>()
                )
            .Build();

        _configuration = new ConfigurationBuilder()
            .SetBasePath(Directory.GetCurrentDirectory())
            .AddJsonFile("settings.json") // Load settings from .json file.
            .AddJsonFile("settings.local.json",
                true) // Optionally, load local settings.
            .Build();
    }
}
```

```
var logger = LoggerFactory.Create(builder =>
{
    builder.AddConsole();
}).CreateLogger(typeof(Route53DomainScenario));

_route53Wrapper = host.Services.GetRequiredService<Route53Wrapper>();

Console.WriteLine(new string('-', 80));
Console.WriteLine("Welcome to the Amazon Route 53 domains example
scenario.");
Console.WriteLine(new string('-', 80));

try
{
    await ListDomains();
    await ListOperations();
    await ListBillingRecords();
    await ListPrices();
    await ListDomainSuggestions();
    await CheckDomainAvailability();
    await CheckDomainTransferability();
    var operationId = await RequestDomainRegistration();
    await GetOperationalDetail(operationId);
    await GetDomainDetails();
}
catch (Exception ex)
{
    logger.LogError(ex, "There was a problem executing the scenario.");
}

Console.WriteLine(new string('-', 80));
Console.WriteLine("The Amazon Route 53 domains example scenario is
complete.");
Console.WriteLine(new string('-', 80));
}

/// <summary>
/// List account registered domains.
/// </summary>
/// <returns>Async task.</returns>
private static async Task ListDomains()
{
    Console.WriteLine(new string('-', 80));
```

```
        Console.WriteLine($"1. List account domains.");
        var domains = await _route53Wrapper.ListDomains();
        for (int i = 0; i < domains.Count; i++)
        {
            Console.WriteLine($"\\t{i + 1}. {domains[i].DomainName}");
        }

        if (!domains.Any())
        {
            Console.WriteLine("\\tNo domains found in this account.");
        }

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List domain operations in the past year.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task ListOperations()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"2. List account domain operations in the past
year.");
        var operations = await _route53Wrapper.ListOperations(
            DateTime.Today.AddYears(-1));
        for (int i = 0; i < operations.Count; i++)
        {
            Console.WriteLine($"\\tOperation Id: {operations[i].OperationId}");
            Console.WriteLine($"\\tStatus: {operations[i].Status}");
            Console.WriteLine($"\\tDate: {operations[i].SubmittedDate}");
        }
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List billing in the past year.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task ListBillingRecords()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"3. View billing for the account in the past year.");
        var billingRecords = await _route53Wrapper.ViewBilling(
```

```

        DateTime.Today.AddYears(-1),
        DateTime.Today);
    for (int i = 0; i < billingRecords.Count; i++)
    {
        Console.WriteLine($"\\tBill Date:
{billingRecords[i].BillDate.ToShortDateString()}");
        Console.WriteLine($"\\tOperation: {billingRecords[i].Operation}");
        Console.WriteLine($"\\tPrice: {billingRecords[i].Price}");
    }
    if (!billingRecords.Any())
    {
        Console.WriteLine("\\tNo billing records found in this account for the
past year.");
    }
    Console.WriteLine(new string('-', 80));
}

/// <summary>
/// List prices for a few domain types.
/// </summary>
/// <returns>Async task.</returns>
private static async Task ListPrices()
{
    Console.WriteLine(new string('-', 80));
    Console.WriteLine($"4. View prices for domain types.");
    var domainTypes = new List<string> { "net", "com", "org", "co" };

    var prices = await _route53Wrapper.ListPrices(domainTypes);
    foreach (var pr in prices)
    {
        Console.WriteLine($"\\tName: {pr.Name}");
        Console.WriteLine($"\\tRegistration: {pr.RegistrationPrice?.Price}
{pr.RegistrationPrice?.Currency}");
        Console.WriteLine($"\\tRenewal: {pr.RenewalPrice?.Price}
{pr.RenewalPrice?.Currency}");
        Console.WriteLine($"\\tTransfer: {pr.TransferPrice?.Price}
{pr.TransferPrice?.Currency}");
        Console.WriteLine($"\\tChange Ownership:
{pr.ChangeOwnershipPrice?.Price} {pr.ChangeOwnershipPrice?.Currency}");
        Console.WriteLine($"\\tRestoration: {pr.RestorationPrice?.Price}
{pr.RestorationPrice?.Currency}");
        Console.WriteLine();
    }
    Console.WriteLine(new string('-', 80));
}

```



```
}

/// <summary>
/// List domain suggestions for a domain name.
/// </summary>
/// <returns>Async task.</returns>
private static async Task ListDomainSuggestions()
{
    Console.WriteLine(new string('-', 80));
    Console.WriteLine($"5. Get domain suggestions.");
    string? domainName = null;
    while (domainName == null || string.IsNullOrEmpty(domainName))
    {
        Console.WriteLine($"Enter a domain name to get available domain
suggestions.");
        domainName = Console.ReadLine();
    }

    var suggestions = await _route53Wrapper.GetDomainSuggestions(domainName,
true, 5);
    foreach (var suggestion in suggestions)
    {
        Console.WriteLine($"\\tSuggestion Name: {suggestion.DomainName}");
        Console.WriteLine($"\\tAvailability: {suggestion.Availability}");
    }
    Console.WriteLine(new string('-', 80));
}

/// <summary>
/// Check availability for a domain name.
/// </summary>
/// <returns>Async task.</returns>
private static async Task CheckDomainAvailability()
{
    Console.WriteLine(new string('-', 80));
    Console.WriteLine($"6. Check domain availability.");
    string? domainName = null;
    while (domainName == null || string.IsNullOrEmpty(domainName))
    {
        Console.WriteLine($"Enter a domain name to check domain
availability.");
        domainName = Console.ReadLine();
    }
}
```

```
        var availability = await
_route53Wrapper.CheckDomainAvailability(domainName);
        Console.WriteLine($"\\tAvailability: {availability}");
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Check transferability for a domain name.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task CheckDomainTransferability()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"7. Check domain transferability.");
        string? domainName = null;
        while (domainName == null || string.IsNullOrEmpty(domainName))
        {
            Console.WriteLine($"Enter a domain name to check domain
transferability.");
            domainName = Console.ReadLine();
        }

        var transferability = await
_route53Wrapper.CheckDomainTransferability(domainName);
        Console.WriteLine($"\\tTransferability: {transferability}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Check transferability for a domain name.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task<string?> RequestDomainRegistration()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"8. Optionally, request a domain registration.");

        Console.WriteLine($"\\tNote: This example uses domain request settings in
settings.json.");
        Console.WriteLine($"\\tTo change the domain registration settings, set the
values in that file.");
        Console.WriteLine($"\\tRemember, registering an actual domain will incur
an account billing cost.");
    }
}
```

```

        Console.WriteLine($"\\tWould you like to begin a domain registration? (y/
n)");
        var ynResponse = Console.ReadLine();
        if (ynResponse != null && ynResponse.Equals("y",
StringComparison.InvariantCultureIgnoreCase))
        {
            string domainName = _configuration["DomainName"];
            ContactDetail contact = new ContactDetail();
            contact.CountryCode =
CountryCode.FindValue(_configuration["Contact:CountryCode"]);
            contact.ContactType =
ContactType.FindValue(_configuration["Contact:ContactType"]);

            _configuration.GetSection("Contact").Bind(contact);

            var operationId = await _route53Wrapper.RegisterDomain(
                domainName,
                Convert.ToBoolean(_configuration["AutoRenew"]),
                Convert.ToInt32(_configuration["DurationInYears"]),
                contact);
            if (operationId != null)
            {
                Console.WriteLine(
                    $"\\tRegistration requested. Operation Id: {operationId}");
            }

            return operationId;
        }

        Console.WriteLine(new string('-', 80));
        return null;
    }

    /// <summary>
    /// Get details for an operation.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task GetOperationalDetail(string? operationId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"9. Get an operation detail.");

        var operationDetails =
            await _route53Wrapper.GetOperationDetail(operationId);
    }

```

```

        Console.WriteLine(operationDetails);

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Optionally, get details for a registered domain.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task<string?> GetDomainDetails()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"10. Get details on a domain.");

        Console.WriteLine($"\\tNote: you must have a registered domain to get
details.");
        Console.WriteLine($"\\tWould you like to get domain details? (y/n)");
        var ynResponse = Console.ReadLine();
        if (ynResponse != null && ynResponse.Equals("y",
StringComparison.InvariantCultureIgnoreCase))
        {
            string? domainName = null;
            while (domainName == null)
            {
                Console.WriteLine($"\\tEnter a domain name to get details.");
                domainName = Console.ReadLine();
            }

            var domainDetails = await
_route53Wrapper.GetDomainDetail(domainName);
            Console.WriteLine(domainDetails);
        }

        Console.WriteLine(new string('-', 80));
        return null;
    }
}

```

Métodos envolventes que se utilizan en situaciones para acciones de registro de dominio de Route 53.

```
public class Route53Wrapper
{
    private readonly IAmazonRoute53Domains _amazonRoute53Domains;
    private readonly ILogger<Route53Wrapper> _logger;
    public Route53Wrapper(IAmazonRoute53Domains amazonRoute53Domains,
        ILogger<Route53Wrapper> logger)
    {
        _amazonRoute53Domains = amazonRoute53Domains;
        _logger = logger;
    }

    /// <summary>
    /// List prices for domain type operations.
    /// </summary>
    /// <param name="domainTypes">Domain types to include in the results.</param>
    /// <returns>The list of domain prices.</returns>
    public async Task<List<DomainPrice>> ListPrices(List<string> domainTypes)
    {
        var results = new List<DomainPrice>();
        var paginatePrices = _amazonRoute53Domains.Paginators.ListPrices(new
        ListPricesRequest());
        // Get the entire list using the paginator.
        await foreach (var prices in paginatePrices.Prices)
        {
            results.Add(prices);
        }
        return results.Where(p => domainTypes.Contains(p.Name)).ToList();
    }

    /// <summary>
    /// Check the availability of a domain name.
    /// </summary>
    /// <param name="domain">The domain to check for availability.</param>
    /// <returns>An availability result string.</returns>
    public async Task<string> CheckDomainAvailability(string domain)
    {
        var result = await _amazonRoute53Domains.CheckDomainAvailabilityAsync(
            new CheckDomainAvailabilityRequest
            {
                DomainName = domain
            })
    }
}
```

```
        }
    );
    return result.Availability.Value;
}

/// <summary>
/// Check the transferability of a domain name.
/// </summary>
/// <param name="domain">The domain to check for transferability.</param>
/// <returns>A transferability result string.</returns>
public async Task<string> CheckDomainTransferability(string domain)
{
    var result = await _amazonRoute53Domains.CheckDomainTransferabilityAsync(
        new CheckDomainTransferabilityRequest
        {
            DomainName = domain
        }
    );
    return result.Transferability.Transferable.Value;
}

/// <summary>
/// Get a list of suggestions for a given domain.
/// </summary>
/// <param name="domain">The domain to check for suggestions.</param>
/// <param name="onlyAvailable">If true, only returns available domains.</
param>
/// <param name="suggestionCount">The number of suggestions to return.
Defaults to the max of 50.</param>
/// <returns>A collection of domain suggestions.</returns>
public async Task<List<DomainSuggestion>> GetDomainSuggestions(string domain,
    bool onlyAvailable, int suggestionCount = 50)
{
    var result = await _amazonRoute53Domains.GetDomainSuggestionsAsync(
        new GetDomainSuggestionsRequest
        {
            DomainName = domain,
            OnlyAvailable = onlyAvailable,
            SuggestionCount = suggestionCount
        }
    );
    return result.SuggestionsList;
}
```

```

    }

    /// <summary>
    /// Get details for a domain action operation.
    /// </summary>
    /// <param name="operationId">The operational Id.</param>
    /// <returns>A string describing the operational details.</returns>
    public async Task<string> GetOperationDetail(string? operationId)
    {
        if (operationId == null)
            return "Unable to get operational details because ID is null.";
        try
        {
            var operationDetails =
                await _amazonRoute53Domains.GetOperationDetailAsync(
                    new GetOperationDetailRequest
                    {
                        OperationId = operationId
                    }
                );

            var details = $"\\tOperation {operationId}:\\n" +
                $"\\tFor domain {operationDetails.DomainName} on
{operationDetails.SubmittedDate.ToShortDateString()}\\n" +
                $"\\tMessage is {operationDetails.Message}.\\n" +
                $"\\tStatus is {operationDetails.Status}.\\n";

            return details;
        }
        catch (AmazonRoute53DomainsException ex)
        {
            return $"Unable to get operation details. Here's why: {ex.Message}.";
        }
    }

    /// <summary>
    /// Initiate a domain registration request.
    /// </summary>
    /// <param name="contact">Contact details.</param>
    /// <param name="domainName">The domain name to register.</param>
    /// <param name="autoRenew">True if the domain should automatically renew.</
param>

```

```
    /// <param name="duration">The duration in years for the domain
    registration.</param>
    /// <returns>The operation Id.</returns>
    public async Task<string?> RegisterDomain(string domainName, bool autoRenew,
    int duration, ContactDetail contact)
    {
        // This example uses the same contact information for admin, registrant,
    and tech contacts.
        try
        {
            var result = await _amazonRoute53Domains.RegisterDomainAsync(
                new RegisterDomainRequest()
                {
                    AdminContact = contact,
                    RegistrantContact = contact,
                    TechContact = contact,
                    DomainName = domainName,
                    AutoRenew = autoRenew,
                    DurationInYears = duration,
                    PrivacyProtectAdminContact = false,
                    PrivacyProtectRegistrantContact = false,
                    PrivacyProtectTechContact = false
                }
            );
            return result.OperationId;
        }
        catch (InvalidInputException)
        {
            _logger.LogInformation($"Unable to request registration for domain
    {domainName}");
            return null;
        }
    }

    /// <summary>
    /// View billing records for the account between a start and end date.
    /// </summary>
    /// <param name="startDate">The start date for billing results.</param>
    /// <param name="endDate">The end date for billing results.</param>
    /// <returns>A collection of billing records.</returns>
    public async Task<List<BillingRecord>> ViewBilling(DateTime startDate,
    DateTime endDate)
    {
```



```
var results = new List<BillingRecord>();
var paginateBilling = _amazonRoute53Domains.Paginators.ViewBilling(
    new ViewBillingRequest()
    {
        Start = startDate,
        End = endDate
    });

// Get the entire list using the paginator.
await foreach (var billingRecords in paginateBilling.BillingRecords)
{
    results.Add(billingRecords);
}
return results;
}

/// <summary>
/// List the domains for the account.
/// </summary>
/// <returns>A collection of domain summary records.</returns>
public async Task<List<DomainSummary>> ListDomains()
{
    var results = new List<DomainSummary>();
    var paginateDomains = _amazonRoute53Domains.Paginators.ListDomains(
        new ListDomainsRequest());

    // Get the entire list using the paginator.
    await foreach (var domain in paginateDomains.Domains)
    {
        results.Add(domain);
    }
    return results;
}

/// <summary>
/// List operations for the account that are submitted after a specified
date.
/// </summary>
/// <returns>A collection of operation summary records.</returns>
public async Task<List<OperationSummary>> ListOperations(DateTime
submittedSince)
{
```

```
var results = new List<OperationSummary>();
var paginateOperations = _amazonRoute53Domains.Paginators.ListOperations(
    new ListOperationsRequest()
    {
        SubmittedSince = submittedSince
    });

// Get the entire list using the paginator.
await foreach (var operations in paginateOperations.Operations)
{
    results.Add(operations);
}
return results;
}

/// <summary>
/// Get details for a domain.
/// </summary>
/// <returns>A string with detail information about the domain.</returns>
public async Task<string> GetDomainDetail(string domainName)
{
    try
    {
        var result = await _amazonRoute53Domains.GetDomainDetailAsync(
            new GetDomainDetailRequest()
            {
                DomainName = domainName
            });
        var details = $"{result.DomainName}: \n" +
            $"{result.CreatedOn} \n" +
            $"{result.CreationDate.ToShortDateString()} \n" +
            $"{result.AdminContact.Email} \n" +
            $"{result.AutoRenew} \n";

        return details;
    }
    catch (InvalidInputException)
    {
        return $"Domain {domainName} was not found in your account.";
    }
}
}
```

- Para obtener información sobre la API, consulte los siguientes temas en la referencia de la API de AWS SDK para .NET .
 - [CheckDomainAvailability](#)
 - [CheckDomainTransferability](#)
 - [GetDomainDetail](#)
 - [GetDomainSuggestions](#)
 - [GetOperationDetail](#)
 - [ListDomains](#)
 - [ListOperations](#)
 - [ListPrices](#)
 - [RegisterDomain](#)
 - [ViewBilling](#)

Java

SDK para Java 2.x

Note

Hay más información GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
 * started.html
 *
 * This example uses pagination methods where applicable. For example, to list
 * domains, the
 * listDomainsPaginator method is used. For more information about pagination,
```

```

* see the following documentation topic:
*
* https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/
pagination.html
*
* This Java code example performs the following operations:
*
* 1. List current domains.
* 2. List operations in the past year.
* 3. View billing for the account in the past year.
* 4. View prices for domain types.
* 5. Get domain suggestions.
* 6. Check domain availability.
* 7. Check domain transferability.
* 8. Request a domain registration.
* 9. Get operation details.
* 10. Optionally, get domain details.
*/

public class Route53Scenario {
    public static final String DASHES = new String(new char[80]).replace("\0",
"-");

    public static void main(String[] args) {
        final String usage = ""

            Usage:
                <domainType> <phoneNumber> <email> <domainSuggestion>
<firstName> <lastName> <city>

            Where:
                domainType - The domain type (for example, com).\s
                phoneNumber - The phone number to use (for example,
+91.9966564xxx)      email - The email address to use.      domainSuggestion -
The domain suggestion (for example, findmy.accountants).\s
                firstName - The first name to use to register a domain.\s
                lastName - The last name to use to register a domain.\s
                city - the city to use to register a domain.\s
                """;

        if (args.length != 7) {
            System.out.println(usage);
            System.exit(1);
        }
    }
}

```

```
String domainType = args[0];
String phoneNumber = args[1];
String email = args[2];
String domainSuggestion = args[3];
String firstName = args[4];
String lastName = args[5];
String city = args[6];
Region region = Region.US_EAST_1;
Route53DomainsClient route53DomainsClient =
Route53DomainsClient.builder()
    .region(region)
    .build();

System.out.println(DASHES);
System.out.println("Welcome to the Amazon Route 53 domains example
scenario.");
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("1. List current domains.");
listDomains(route53DomainsClient);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("2. List operations in the past year.");
listOperations(route53DomainsClient);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("3. View billing for the account in the past year.");
listBillingRecords(route53DomainsClient);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("4. View prices for domain types.");
listPrices(route53DomainsClient, domainType);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("5. Get domain suggestions.");
listDomainSuggestions(route53DomainsClient, domainSuggestion);
System.out.println(DASHES);
```

```
        System.out.println(DASHES);
        System.out.println("6. Check domain availability.");
        checkDomainAvailability(route53DomainsClient, domainSuggestion);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("7. Check domain transferability.");
        checkDomainTransferability(route53DomainsClient, domainSuggestion);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("8. Request a domain registration.");
        String opId = requestDomainRegistration(route53DomainsClient,
            domainSuggestion, phoneNumber, email, firstName,
            lastName, city);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("9. Get operation details.");
        getOperationalDetail(route53DomainsClient, opId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("10. Get domain details.");
        System.out.println("Note: You must have a registered domain to get
details.");
        System.out.println("Otherwise, an exception is thrown that states ");
        System.out.println("Domain xxxxxxxx not found in xxxxxxxx account.");
        getDomainDetails(route53DomainsClient, domainSuggestion);
        System.out.println(DASHES);
    }

    public static void getDomainDetails(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
        try {
            GetDomainDetailRequest detailRequest =
GetDomainDetailRequest.builder()
                .domainName(domainSuggestion)
                .build();

            GetDomainDetailResponse response =
route53DomainsClient.getDomainDetail(detailRequest);
            System.out.println("The contact first name is " +
response.registrantContact().firstName());
```

```
        System.out.println("The contact last name is " +
response.registrantContact().lastName());
        System.out.println("The contact org name is " +
response.registrantContact().organizationName());

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static void getOperationalDetail(Route53DomainsClient
route53DomainsClient, String operationId) {
    try {
        GetOperationDetailRequest detailRequest =
GetOperationDetailRequest.builder()
            .operationId(operationId)
            .build();

        GetOperationDetailResponse response =
route53DomainsClient.getOperationDetail(detailRequest);
        System.out.println("Operation detail message is " +
response.message());

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static String requestDomainRegistration(Route53DomainsClient
route53DomainsClient,
        String domainSuggestion,
        String phoneNumber,
        String email,
        String firstName,
        String lastName,
        String city) {

    try {
        ContactDetail contactDetail = ContactDetail.builder()
            .contactType(ContactType.COMPANY)
            .state("LA")
            .countryCode(CountryCode.IN)
```

```
        .email(email)
        .firstName(firstName)
        .lastName(lastName)
        .city(city)
        .phoneNumber(phoneNumber)
        .organizationName("My Org")
        .addressLine1("My Address")
        .zipCode("123 123")
        .build();

    RegisterDomainRequest domainRequest = RegisterDomainRequest.builder()
        .adminContact(contactDetail)
        .registrantContact(contactDetail)
        .techContact(contactDetail)
        .domainName(domainSuggestion)
        .autoRenew(true)
        .durationInYears(1)
        .build();

    RegisterDomainResponse response =
route53DomainsClient.registerDomain(domainRequest);
    System.out.println("Registration requested. Operation Id: " +
response.operationId());
    return response.operationId();

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
    return "";
}

public static void checkDomainTransferability(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
    try {
        CheckDomainTransferabilityRequest transferabilityRequest =
CheckDomainTransferabilityRequest.builder()
            .domainName(domainSuggestion)
            .build();

        CheckDomainTransferabilityResponse response = route53DomainsClient
            .checkDomainTransferability(transferabilityRequest);
        System.out.println("Transferability: " +
response.transferability().transferable().toString());
    }
```



```
        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void checkDomainAvailability(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
        try {
            CheckDomainAvailabilityRequest availabilityRequest =
CheckDomainAvailabilityRequest.builder()
                .domainName(domainSuggestion)
                .build();

            CheckDomainAvailabilityResponse response = route53DomainsClient
                .checkDomainAvailability(availabilityRequest);
            System.out.println(domainSuggestion + " is " +
response.availability().toString());

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void listDomainSuggestions(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
        try {
            GetDomainSuggestionsRequest suggestionsRequest =
GetDomainSuggestionsRequest.builder()
                .domainName(domainSuggestion)
                .suggestionCount(5)
                .onlyAvailable(true)
                .build();

            GetDomainSuggestionsResponse response =
route53DomainsClient.getDomainSuggestions(suggestionsRequest);
            List<DomainSuggestion> suggestions = response.suggestionsList();
            for (DomainSuggestion suggestion : suggestions) {
                System.out.println("Suggestion Name: " +
suggestion.domainName());
                System.out.println("Availability: " + suggestion.availability());
                System.out.println(" ");
            }
        }
    }
}
```

```

    }

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static void listPrices(Route53DomainsClient route53DomainsClient,
String domainType) {
    try {
        ListPricesRequest pricesRequest = ListPricesRequest.builder()
            .tld(domainType)
            .build();

        ListPricesIterable listRes =
route53DomainsClient.listPricesPaginator(pricesRequest);
        listRes.stream()
            .flatMap(r -> r.prices().stream())
            .forEach(content -> System.out.println(" Name: " +
content.name() +
                " Registration: " +
content.registrationPrice().price() + " "
                + content.registrationPrice().currency() +
                " Renewal: " + content.renewalPrice().price() + " " +
content.renewalPrice().currency()));

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static void listBillingRecords(Route53DomainsClient
route53DomainsClient) {
    try {
        Date currentDate = new Date();
        LocalDateTime localDateTime =
currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime();
        ZoneOffset zoneOffset = ZoneOffset.of("+01:00");
        LocalDateTime localDateTime2 = localDateTime.minusYears(1);
        Instant myStartTime = localDateTime2.toInstant(zoneOffset);
        Instant myEndTime = localDateTime.toInstant(zoneOffset);
    }
}

```

```
ViewBillingRequest viewBillingRequest = ViewBillingRequest.builder()
    .start(myStartTime)
    .end(myEndTime)
    .build();

ViewBillingIterable listRes =
route53DomainsClient.viewBillingPaginator(viewBillingRequest);
listRes.stream()
    .flatMap(r -> r.billingRecords().stream())
    .forEach(content -> System.out.println(" Bill Date:: " +
content.billDate() +
        " Operation: " + content.operationAsString() +
        " Price: " + content.price()));

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static void listOperations(Route53DomainsClient route53DomainsClient)
{
    try {
        Date currentDate = new Date();
        LocalDateTime localDateTime =
currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime();
        ZoneOffset zoneOffset = ZoneOffset.of("+01:00");
        localDateTime = localDateTime.minusYears(1);
        Instant myTime = localDateTime.toInstant(zoneOffset);

        ListOperationsRequest operationsRequest =
ListOperationsRequest.builder()
            .submittedSince(myTime)
            .build();

        ListOperationsIterable listRes =
route53DomainsClient.listOperationsPaginator(operationsRequest);
        listRes.stream()
            .flatMap(r -> r.operations().stream())
            .forEach(content -> System.out.println(" Operation Id: " +
content.operationId() +
                " Status: " + content.statusAsString() +
                " Date: " + content.submittedDate()));
    }
```

```
        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void listDomains(Route53DomainsClient route53DomainsClient) {
        try {
            ListDomainsIterable listRes =
route53DomainsClient.listDomainsPaginator();
            listRes.stream()
                .flatMap(r -> r.domains().stream())
                .forEach(content -> System.out.println("The domain name is "
+ content.domainName()));

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
}
```

- Para obtener detalles sobre la API, consulte los siguientes temas en la Referencia de la API de AWS SDK for Java 2.x .
 - [CheckDomainAvailability](#)
 - [CheckDomainTransferability](#)
 - [GetDomainDetail](#)
 - [GetDomainSuggestions](#)
 - [GetOperationDetail](#)
 - [ListDomains](#)
 - [ListOperations](#)
 - [ListPrices](#)
 - [RegisterDomain](#)
 - [ViewBilling](#)

Kotlin

SDK para Kotlin

Note

Hay más información GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
/**
Before running this Kotlin code example, set up your development environment,
including your credentials.

For more information, see the following documentation topic:
https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html

This Kotlin code example performs the following operations:

1. List current domains.
2. List operations in the past year.
3. View billing for the account in the past year.
4. View prices for domain types.
5. Get domain suggestions.
6. Check domain availability.
7. Check domain transferability.
8. Request a domain registration.
9. Get operation details.
10. Optionally, get domain details.
*/

val DASHES: String = String(CharArray(80)).replace("\u0000", "-")

suspend fun main(args: Array<String>) {
    val usage = """
        Usage:
            <domainType> <phoneNumber> <email> <domainSuggestion> <firstName>
            <lastName> <city>
        Where:
            domainType - The domain type (for example, com).
```

```
        phoneNumber - The phone number to use (for example, +1.2065550100)

        email - The email address to use.
        domainSuggestion - The domain suggestion (for example,
findmy.example).
        firstName - The first name to use to register a domain.
        lastName - The last name to use to register a domain.
        city - The city to use to register a domain.
    ""

    if (args.size != 7) {
        println(usage)
        exitProcess(1)
    }

    val domainType = args[0]
    val phoneNumber = args[1]
    val email = args[2]
    val domainSuggestion = args[3]
    val firstName = args[4]
    val lastName = args[5]
    val city = args[6]

    println(DASHES)
    println("Welcome to the Amazon Route 53 domains example scenario.")
    println(DASHES)

    println(DASHES)
    println("1. List current domains.")
    listDomains()
    println(DASHES)

    println(DASHES)
    println("2. List operations in the past year.")
    listOperations()
    println(DASHES)

    println(DASHES)
    println("3. View billing for the account in the past year.")
    listBillingRecords()
    println(DASHES)

    println(DASHES)
    println("4. View prices for domain types.")
```

```
listAllPrices(domainType)
println(DASHES)

println(DASHES)
println("5. Get domain suggestions.")
listDomainSuggestions(domainSuggestion)
println(DASHES)

println(DASHES)
println("6. Check domain availability.")
checkDomainAvailability(domainSuggestion)
println(DASHES)

println(DASHES)
println("7. Check domain transferability.")
checkDomainTransferability(domainSuggestion)
println(DASHES)

println(DASHES)
println("8. Request a domain registration.")
val opId = requestDomainRegistration(domainSuggestion, phoneNumber, email,
firstName, lastName, city)
println(DASHES)

println(DASHES)
println("9. Get operation details.")
getOperationalDetail(opId)
println(DASHES)

println(DASHES)
println("10. Get domain details.")
println("Note: You must have a registered domain to get details.")
println("Otherwise an exception is thrown that states ")
println("Domain xxxxxxxx not found in xxxxxxxx account.")
getDomainDetails(domainSuggestion)
println(DASHES)
}

suspend fun getDomainDetails(domainSuggestion: String?) {
    val detailRequest =
        GetDomainDetailRequest {
            domainName = domainSuggestion
        }
}
```

```
Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
{ route53DomainsClient ->
    val response = route53DomainsClient.getDomainDetail(detailRequest)
    println("The contact first name is
    ${response.registrantContact?.firstName}")
    println("The contact last name is
    ${response.registrantContact?.lastName}")
    println("The contact org name is
    ${response.registrantContact?.organizationName}")
    }
}

suspend fun getOperationalDetail(opId: String?) {
    val detailRequest =
        GetOperationDetailRequest {
            operationId = opId
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
    { route53DomainsClient ->
        val response = route53DomainsClient.getOperationDetail(detailRequest)
        println("Operation detail message is ${response.message}")
    }
}

suspend fun requestDomainRegistration(
    domainSuggestion: String?,
    phoneNumberVal: String?,
    emailVal: String?,
    firstNameVal: String?,
    lastNameVal: String?,
    cityVal: String?,
): String? {
    val contactDetail =
        ContactDetail {
            contactType = ContactType.Company
            state = "LA"
            countryCode = CountryCode.In
            email = emailVal
            firstName = firstNameVal
            lastName = lastNameVal
            city = cityVal
            phoneNumber = phoneNumberVal
            organizationName = "My Org"
            addressLine1 = "My Address"
        }
}
```



```
        zipCode = "123 123"
    }

    val domainRequest =
        RegisterDomainRequest {
            adminContact = contactDetail
            registrantContact = contactDetail
            techContact = contactDetail
            domainName = domainSuggestion
            autoRenew = true
            durationInYears = 1
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
{ route53DomainsClient ->
    val response = route53DomainsClient.registerDomain(domainRequest)
    println("Registration requested. Operation Id: ${response.operationId}")
    return response.operationId
}

suspend fun checkDomainTransferability(domainSuggestion: String?) {
    val transferabilityRequest =
        CheckDomainTransferabilityRequest {
            domainName = domainSuggestion
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
{ route53DomainsClient ->
    val response =
route53DomainsClient.checkDomainTransferability(transferabilityRequest)
    println("Transferability: ${response.transferability?.transferable}")
}
}

suspend fun checkDomainAvailability(domainSuggestion: String) {
    val availabilityRequest =
        CheckDomainAvailabilityRequest {
            domainName = domainSuggestion
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
{ route53DomainsClient ->
    val response =
route53DomainsClient.checkDomainAvailability(availabilityRequest)
    println("$domainSuggestion is ${response.availability}")
}
```

```
    }  
  }  
  
suspend fun listDomainSuggestions(domainSuggestion: String?) {  
    val suggestionsRequest =  
        GetDomainSuggestionsRequest {  
            domainName = domainSuggestion  
            suggestionCount = 5  
            onlyAvailable = true  
        }  
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use  
{ route53DomainsClient ->  
        val response =  
            route53DomainsClient.getDomainSuggestions(suggestionsRequest)  
            response.suggestionsList?.forEach { suggestion ->  
                println("Suggestion Name: ${suggestion.domainName}")  
                println("Availability: ${suggestion.availability}")  
                println(" ")  
            }  
        }  
    }  
}  
  
suspend fun listAllPrices(domainType: String?) {  
    val pricesRequest =  
        ListPricesRequest {  
            tld = domainType  
        }  
  
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use  
{ route53DomainsClient ->  
        route53DomainsClient  
            .listPricesPaginated(pricesRequest)  
            .transform { it.prices?.forEach { obj -> emit(obj) } }  
            .collect { pr ->  
                println("Registration: ${pr.registrationPrice}  
${pr.registrationPrice?.currency}")  
                println("Renewal: ${pr.renewalPrice?.price}  
${pr.renewalPrice?.currency}")  
                println("Transfer: ${pr.transferPrice?.price}  
${pr.transferPrice?.currency}")  
                println("Restoration: ${pr.restorationPrice?.price}  
${pr.restorationPrice?.currency}")  
            }  
        }  
    }  
}
```

```
}

suspend fun listBillingRecords() {
    val currentDate = Date()
    val localDateTime =
        currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime()
    val zoneOffset = ZoneOffset.of("+01:00")
    val localDateTime2 = localDateTime.minusYears(1)
    val myStartTime = localDateTime2.toInstant(zoneOffset)
    val myEndTime = localDateTime.toInstant(zoneOffset)
    val timeStart: Instant? = myStartTime?.let { Instant(it) }
    val timeEnd: Instant? = myEndTime?.let { Instant(it) }

    val viewBillingRequest =
        ViewBillingRequest {
            start = timeStart
            end = timeEnd
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
    { route53DomainsClient ->
        route53DomainsClient
            .viewBillingPaginated(viewBillingRequest)
            .transform { it.billingRecords?.forEach { obj -> emit(obj) } }
            .collect { billing ->
                println("Bill Date: ${billing.billDate}")
                println("Operation: ${billing.operation}")
                println("Price: ${billing.price}")
            }
    }
}

suspend fun listOperations() {
    val currentDate = Date()
    var localDateTime =
        currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime()
    val zoneOffset = ZoneOffset.of("+01:00")
    localDateTime = localDateTime.minusYears(1)
    val myTime: java.time.Instant? = localDateTime.toInstant(zoneOffset)
    val time2: Instant? = myTime?.let { Instant(it) }
    val operationsRequest =
        ListOperationsRequest {
            submittedSince = time2
        }
}
```

```
Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
{ route53DomainsClient ->
    route53DomainsClient
        .listOperationsPaginated(operationsRequest)
        .transform { it.operations?.forEach { obj -> emit(obj) } }
        .collect { content ->
            println("Operation Id: ${content.operationId}")
            println("Status: ${content.status}")
            println("Date: ${content.submittedDate}")
        }
    }
}

suspend fun listDomains() {
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
    { route53DomainsClient ->
        route53DomainsClient
            .listDomainsPaginated(ListDomainsRequest {})
            .transform { it.domains?.forEach { obj -> emit(obj) } }
            .collect { content ->
                println("The domain name is ${content.domainName}")
            }
        }
    }
}
```

- Para obtener detalles sobre la API, consulte los siguientes temas en la Referencia de la API de AWS SDK para Kotlin.
 - [CheckDomainAvailability](#)
 - [CheckDomainTransferability](#)
 - [GetDomainDetail](#)
 - [GetDomainSuggestions](#)
 - [GetOperationDetail](#)
 - [ListDomains](#)
 - [ListOperations](#)
 - [ListPrices](#)
 - [RegisterDomain](#)
 - [ViewBilling](#)

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte [Uso de Route 53 con un AWS SDK](#). En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Acciones para el registro de dominios de Route 53 mediante AWS SDKs

Los siguientes ejemplos de código muestran cómo realizar acciones individuales de registro de dominios de Route 53 con AWS SDKs. Cada ejemplo incluye un enlace a GitHub, donde puede encontrar instrucciones para configurar y ejecutar el código.

Los siguientes ejemplos incluyen solo las acciones que se utilizan con mayor frecuencia. Para ver una lista completa, consulte la [Referencia de la API de Amazon Route 53 domain registration](#).

Ejemplos

- [Úselo CheckDomainAvailability con un AWS SDK o CLI](#)
- [Úselo CheckDomainTransferability con un AWS SDK o CLI](#)
- [Úselo GetDomainDetail con un AWS SDK o CLI](#)
- [Úselo GetDomainSuggestions con un AWS SDK o CLI](#)
- [Úselo GetOperationDetail con un AWS SDK o CLI](#)
- [Úselo ListDomains con un AWS SDK o CLI](#)
- [Úselo ListOperations con un AWS SDK o CLI](#)
- [ListPricesÚselo con un AWS SDK](#)
- [Úselo RegisterDomain con un AWS SDK o CLI](#)
- [Úselo ViewBilling con un AWS SDK o CLI](#)

Úselo **CheckDomainAvailability** con un AWS SDK o CLI

Los siguientes ejemplos de código muestran cómo utilizar CheckDomainAvailability.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- [Conceptos básicos](#)

.NET

SDK para .NET

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
/// <summary>
/// Check the availability of a domain name.
/// </summary>
/// <param name="domain">The domain to check for availability.</param>
/// <returns>An availability result string.</returns>
public async Task<string> CheckDomainAvailability(string domain)
{
    var result = await _amazonRoute53Domains.CheckDomainAvailabilityAsync(
        new CheckDomainAvailabilityRequest
        {
            DomainName = domain
        }
    );
    return result.Availability.Value;
}
```

- Para obtener más información sobre la API, consulta [CheckDomainAvailability](#) la Referencia AWS SDK para .NET de la API.

CLI

AWS CLI

Para determinar si se puede registrar un nombre de dominio con Route 53

El siguiente comando `check-domain-availability` devuelve información sobre si el nombre de dominio `example.com` está disponible para registrarse utilizando Route 53.

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains check-domain-availability \  
  --region us-east-1 \  
  --domain-name example.com
```

Salida:

```
{  
  "Availability": "UNAVAILABLE"  
}
```

Route 53 admite una gran cantidad de dominios de nivel superior (TLDs), como `.com` y `.jp`, pero no admitimos todos los disponibles TLDs. Si comprueba la disponibilidad de un dominio y Route 53 no admite el TLD, `check-domain-availability` devuelve el siguiente mensaje.

```
An error occurred (UnsupportedTLD) when calling the CheckDomainAvailability  
operation: <top-level domain> tld is not supported.
```

Para obtener una lista de los TLDs que puede utilizar al registrar un dominio en Route 53, consulte [Dominios que puede registrar en Amazon Route 53](#) en la Guía para desarrolladores de Amazon Route 53. Para obtener más información sobre el uso de Route 53 para registrar un dominio, consulte [Registering a New Domain](#) en la Guía para desarrolladores de Amazon Route 53.

- Para obtener más información sobre la API, consulte [CheckDomainAvailability](#) la Referencia de AWS CLI comandos.

Java

SDK para Java 2.x

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
public static void checkDomainAvailability(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
    try {
        CheckDomainAvailabilityRequest availabilityRequest =
        CheckDomainAvailabilityRequest.builder()
            .domainName(domainSuggestion)
            .build();

        CheckDomainAvailabilityResponse response = route53DomainsClient
            .checkDomainAvailability(availabilityRequest);
        System.out.println(domainSuggestion + " is " +
        response.availability().toString());

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

- Para obtener más información sobre la API, consulta [CheckDomainAvailability](#) la Referencia AWS SDK for Java 2.x de la API.

Kotlin

SDK para Kotlin

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
suspend fun checkDomainAvailability(domainSuggestion: String) {
    val availabilityRequest =
        CheckDomainAvailabilityRequest {
            domainName = domainSuggestion
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
    { route53DomainsClient ->
```



```
        val response =  
            route53DomainsClient.checkDomainAvailability(availabilityRequest)  
            println("$domainSuggestion is ${response.availability}")  
        }  
    }
```

- Para obtener más información sobre la API, consulta [CheckDomainAvailability](#) la referencia sobre el AWS SDK para la API de Kotlin.

Para ver una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulta [Uso de Route 53 con un AWS SDK](#). En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **CheckDomainTransferability** con un AWS SDK o CLI

Los siguientes ejemplos de código muestran cómo utilizar CheckDomainTransferability.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- [Conceptos básicos](#)

.NET

SDK para .NET

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
/// <summary>  
/// Check the transferability of a domain name.  
/// </summary>  
/// <param name="domain">The domain to check for transferability.</param>  
/// <returns>A transferability result string.</returns>  
public async Task<string> CheckDomainTransferability(string domain)
```

```
{
    var result = await _amazonRoute53Domains.CheckDomainTransferabilityAsync(
        new CheckDomainTransferabilityRequest
        {
            DomainName = domain
        }
    );
    return result.Transferability.Transferable.Value;
}
```

- Para obtener más información sobre la API, consulta [CheckDomainTransferability](#) la Referencia AWS SDK para .NET de la API.

CLI

AWS CLI

Para determinar si un dominio puede transferirse a Route 53

El siguiente comando `check-domain-transferability` devuelve información sobre si se puede transferir el nombre de dominio `example.com` a Route 53.

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains check-domain-transferability \
    --region us-east-1 \
    --domain-name example.com
```

Salida:

```
{
  "Transferability": {
    "Transferable": "UNTRANSFERABLE"
  }
}
```

Para obtener más información, consulte [Transferring Registration for a Domain to Amazon Route 53](#) en la Guía para desarrolladores de Amazon Route 53.

- Para obtener más información sobre la API, consulta [CheckDomainTransferability](#) la Referencia de AWS CLI comandos.

Java

SDK para Java 2.x

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
public static void checkDomainTransferability(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
    try {
        CheckDomainTransferabilityRequest transferabilityRequest =
        CheckDomainTransferabilityRequest.builder()
            .domainName(domainSuggestion)
            .build();

        CheckDomainTransferabilityResponse response = route53DomainsClient
            .checkDomainTransferability(transferabilityRequest);
        System.out.println("Transferability: " +
        response.transferability().transferable().toString());

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

- Para obtener más información sobre la API, consulta [CheckDomainTransferability](#) la Referencia AWS SDK for Java 2.x de la API.

Kotlin

SDK para Kotlin

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
suspend fun checkDomainTransferability(domainSuggestion: String?) {  
    val transferabilityRequest =  
        CheckDomainTransferabilityRequest {  
            domainName = domainSuggestion  
        }  
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use  
{ route53DomainsClient ->  
    val response =  
        route53DomainsClient.checkDomainTransferability(transferabilityRequest)  
    println("Transferability: ${response.transferability?.transferable}")  
    }  
}
```

- Para obtener más información sobre la API, consulta [CheckDomainTransferability](#) la referencia sobre el AWS SDK para la API de Kotlin.

Para ver una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulta [Uso de Route 53 con un AWS SDK](#). En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **GetDomainDetail** con un AWS SDK o CLI

Los siguientes ejemplos de código muestran cómo utilizar `GetDomainDetail`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- [Conceptos básicos](#)

.NET

SDK para .NET

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
/// <summary>
/// Get details for a domain.
/// </summary>
/// <returns>A string with detail information about the domain.</returns>
public async Task<string> GetDomainDetail(string domainName)
{
    try
    {
        var result = await _amazonRoute53Domains.GetDomainDetailAsync(
            new GetDomainDetailRequest()
            {
                DomainName = domainName
            });
        var details = $"\\tDomain {domainName}:\\n" +
            $"\\tCreated on
{result.CreationDate.ToShortDateString()}\\.\\n" +
            $"\\tAdmin contact is {result.AdminContact.Email}\\n" +
            $"\\tAuto-renew is {result.AutoRenew}\\n";

        return details;
    }
    catch (InvalidInputException)
    {
        return $"Domain {domainName} was not found in your account.";
    }
}
```

- Para obtener más información sobre la API, consulta [GetDomainDetail](#) la Referencia AWS SDK para .NET de la API.

CLI

AWS CLI

Para obtener información detallada acerca de un dominio específico

El siguiente comando `get-domain-detail` muestra información detallada sobre el dominio especificado.

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains get-domain-detail \
  --region us-east-1 \
  --domain-name example.com
```

Salida:

```
{
  "DomainName": "example.com",
  "Nameservers": [
    {
      "Name": "ns-2048.awsdns-64.com",
      "GlueIps": []
    },
    {
      "Name": "ns-2049.awsdns-65.net",
      "GlueIps": []
    },
    {
      "Name": "ns-2050.awsdns-66.org",
      "GlueIps": []
    },
    {
      "Name": "ns-2051.awsdns-67.co.uk",
      "GlueIps": []
    }
  ],
  "AutoRenew": true,
  "AdminContact": {
    "FirstName": "Saanvi",
    "LastName": "Sarkar",
    "ContactType": "COMPANY",
```

```
    "OrganizationName": "Example",
    "AddressLine1": "123 Main Street",
    "City": "Anytown",
    "State": "WA",
    "CountryCode": "US",
    "ZipCode": "98101",
    "PhoneNumber": "+1.8005551212",
    "Email": "ssarkar@example.com",
    "ExtraParams": []
  },
  "RegistrantContact": {
    "FirstName": "Alejandro",
    "LastName": "Rosalez",
    "ContactType": "COMPANY",
    "OrganizationName": "Example",
    "AddressLine1": "123 Main Street",
    "City": "Anytown",
    "State": "WA",
    "CountryCode": "US",
    "ZipCode": "98101",
    "PhoneNumber": "+1.8005551212",
    "Email": "arosalez@example.com",
    "ExtraParams": []
  },
  "TechContact": {
    "FirstName": "Wang",
    "LastName": "Xiulan",
    "ContactType": "COMPANY",
    "OrganizationName": "Example",
    "AddressLine1": "123 Main Street",
    "City": "Anytown",
    "State": "WA",
    "CountryCode": "US",
    "ZipCode": "98101",
    "PhoneNumber": "+1.8005551212",
    "Email": "wxiulan@example.com",
    "ExtraParams": []
  },
  "AdminPrivacy": true,
  "RegistrantPrivacy": true,
  "TechPrivacy": true,
  "RegistrarName": "Amazon Registrar, Inc.",
  "WhoIsServer": "whois.registrar.amazon",
  "RegistrarUrl": "http://registrar.amazon.com",
```

```
"AbuseContactEmail": "abuse@registrar.amazon.com",
"AbuseContactPhone": "+1.2062661000",
"CreationDate": 1444934889.601,
"ExpirationDate": 1602787689.0,
"StatusList": [
    "clientTransferProhibited"
]
}
```

- Para obtener más información sobre la API, consulta [GetDomainDetail](#) la Referencia de AWS CLI comandos.

Java

SDK para Java 2.x

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
public static void getDomainDetails(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
    try {
        GetDomainDetailRequest detailRequest =
        GetDomainDetailRequest.builder()
            .domainName(domainSuggestion)
            .build();

        GetDomainDetailResponse response =
        route53DomainsClient.getDomainDetail(detailRequest);
        System.out.println("The contact first name is " +
        response.registrantContact().firstName());
        System.out.println("The contact last name is " +
        response.registrantContact().lastName());
        System.out.println("The contact org name is " +
        response.registrantContact().organizationName());

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
    }
}
```



```
        System.exit(1);
    }
}
```

- Para obtener más información sobre la API, consulta [GetDomainDetail](#) la Referencia AWS SDK for Java 2.x de la API.

Kotlin

SDK para Kotlin

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
suspend fun getDomainDetails(domainSuggestion: String?) {
    val detailRequest =
        GetDomainDetailRequest {
            domainName = domainSuggestion
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
    { route53DomainsClient ->
        val response = route53DomainsClient.getDomainDetail(detailRequest)
        println("The contact first name is
        ${response.registrantContact?.firstName}")
        println("The contact last name is
        ${response.registrantContact?.lastName}")
        println("The contact org name is
        ${response.registrantContact?.organizationName}")
    }
}
```

- Para obtener más información sobre la API, consulta [GetDomainDetail](#) la referencia sobre el AWS SDK para la API de Kotlin.

Para ver una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulta [Uso de Route 53 con un AWS SDK](#). En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **GetDomainSuggestions** con un AWS SDK o CLI

Los siguientes ejemplos de código muestran cómo utilizar GetDomainSuggestions.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- [Conceptos básicos](#)

.NET

SDK para .NET

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
/// <summary>
/// Get a list of suggestions for a given domain.
/// </summary>
/// <param name="domain">The domain to check for suggestions.</param>
/// <param name="onlyAvailable">If true, only returns available domains.</
param>
/// <param name="suggestionCount">The number of suggestions to return.
Defaults to the max of 50.</param>
/// <returns>A collection of domain suggestions.</returns>
public async Task<List<DomainSuggestion>> GetDomainSuggestions(string domain,
bool onlyAvailable, int suggestionCount = 50)
{
    var result = await _amazonRoute53Domains.GetDomainSuggestionsAsync(
        new GetDomainSuggestionsRequest
        {
            DomainName = domain,
            OnlyAvailable = onlyAvailable,
```

```

        SuggestionCount = suggestionCount
    }
};
return result.SuggestionsList;
}

```

- Para obtener más información sobre la API, consulta [GetDomainSuggestions](#) la Referencia AWS SDK para .NET de la API.

CLI

AWS CLI

Para obtener una lista de los nombres de dominio sugeridos

El siguiente comando `get-domain-suggestions` muestra una lista de los nombres de dominio sugeridos en función del nombre de dominio `example.com`. La respuesta incluye solo los nombres de dominio que están disponibles. Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```

aws route53domains get-domain-suggestions \
  --region us-east-1 \
  --domain-name example.com \
  --suggestion-count 10 \
  --only-available

```

Salida:

```

{
  "SuggestionsList": [
    {
      "DomainName": "egzaampal.com",
      "Availability": "AVAILABLE"
    },
    {
      "DomainName": "examplelaw.com",
      "Availability": "AVAILABLE"
    },
    {

```

```
        "DomainName": "examplehouse.net",
        "Availability": "AVAILABLE"
    },
    {
        "DomainName": "homeexample.net",
        "Availability": "AVAILABLE"
    },
    {
        "DomainName": "examplelist.com",
        "Availability": "AVAILABLE"
    },
    {
        "DomainName": "examplenews.net",
        "Availability": "AVAILABLE"
    },
    {
        "DomainName": "officeexample.com",
        "Availability": "AVAILABLE"
    },
    {
        "DomainName": "exampleworld.com",
        "Availability": "AVAILABLE"
    },
    {
        "DomainName": "exampleart.com",
        "Availability": "AVAILABLE"
    }
  ]
}
```

- Para obtener más información sobre la API, consulta [GetDomainSuggestions](#) la Referencia de AWS CLI comandos.

Java

SDK para Java 2.x

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
public static void listDomainSuggestions(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
    try {
        GetDomainSuggestionsRequest suggestionsRequest =
        GetDomainSuggestionsRequest.builder()
            .domainName(domainSuggestion)
            .suggestionCount(5)
            .onlyAvailable(true)
            .build();

        GetDomainSuggestionsResponse response =
        route53DomainsClient.getDomainSuggestions(suggestionsRequest);
        List<DomainSuggestion> suggestions = response.suggestionsList();
        for (DomainSuggestion suggestion : suggestions) {
            System.out.println("Suggestion Name: " +
            suggestion.domainName());
            System.out.println("Availability: " + suggestion.availability());
            System.out.println(" ");
        }

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

- Para obtener más información sobre la API, consulta [GetDomainSuggestions](#) la Referencia AWS SDK for Java 2.x de la API.

Kotlin

SDK para Kotlin

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
suspend fun listDomainSuggestions(domainSuggestion: String?) {
```

```
val suggestionsRequest =
    GetDomainSuggestionsRequest {
        domainName = domainSuggestion
        suggestionCount = 5
        onlyAvailable = true
    }
Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
{ route53DomainsClient ->
    val response =
route53DomainsClient.getDomainSuggestions(suggestionsRequest)
    response.suggestionsList?.forEach { suggestion ->
        println("Suggestion Name: ${suggestion.domainName}")
        println("Availability: ${suggestion.availability}")
        println(" ")
    }
}
}
```

- Para obtener más información sobre la API, consulta [GetDomainSuggestions](#) la referencia sobre el AWS SDK para la API de Kotlin.

Para ver una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulta [Uso de Route 53 con un AWS SDK](#). En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **GetOperationDetail** con un AWS SDK o CLI

Los siguientes ejemplos de código muestran cómo utilizar `GetOperationDetail`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- [Conceptos básicos](#)

.NET

SDK para .NET

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
/// <summary>
/// Get details for a domain action operation.
/// </summary>
/// <param name="operationId">The operational Id.</param>
/// <returns>A string describing the operational details.</returns>
public async Task<string> GetOperationDetail(string? operationId)
{
    if (operationId == null)
        return "Unable to get operational details because ID is null.";
    try
    {
        var operationDetails =
            await _amazonRoute53Domains.GetOperationDetailAsync(
                new GetOperationDetailRequest
                {
                    OperationId = operationId
                }
            );

        var details = $"\\tOperation {operationId}:\\n" +
            $"\\tFor domain {operationDetails.DomainName} on"
            + $"{operationDetails.SubmittedDate.ToShortDateString()}\\n" +
            $"\\tMessage is {operationDetails.Message}\\n" +
            $"\\tStatus is {operationDetails.Status}\\n";

        return details;
    }
    catch (AmazonRoute53DomainsException ex)
    {
        return $"Unable to get operation details. Here's why: {ex.Message}.";
    }
}
```

```
}
```

- Para obtener más información sobre la API, consulta [GetOperationDetail](#) la Referencia AWS SDK para .NET de la API.

CLI

AWS CLI

Para obtener el estado actual de una operación

Algunas operaciones de registro de dominio funcionan de forma asíncrona y devuelven una respuesta antes de que finalicen. Estas operaciones devuelven un ID de operación que puede usar para obtener el estado actual. El siguiente comando `get-operation-detail` devuelve el estado de la operación especificada.

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains get-operation-detail \  
  --region us-east-1 \  
  --operation-id edbd8d63-7fe7-4343-9bc5-54033example
```

Salida:

```
{  
  "OperationId": "edbd8d63-7fe7-4343-9bc5-54033example",  
  "Status": "SUCCESSFUL",  
  "DomainName": "example.com",  
  "Type": "DOMAIN_LOCK",  
  "SubmittedDate": 1573749367.864  
}
```

- Para obtener más información sobre la API, consulta [GetOperationDetail](#) la Referencia de AWS CLI comandos.

Java

SDK para Java 2.x

Note

Hay más información al respecto en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
public static void getOperationalDetail(Route53DomainsClient
route53DomainsClient, String operationId) {
    try {
        GetOperationDetailRequest detailRequest =
        GetOperationDetailRequest.builder()
            .operationId(operationId)
            .build();

        GetOperationDetailResponse response =
        route53DomainsClient.getOperationDetail(detailRequest);
        System.out.println("Operation detail message is " +
        response.message());

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

- Para obtener más información sobre la API, consulta [GetOperationDetail](#) la Referencia AWS SDK for Java 2.x de la API.

Kotlin

SDK para Kotlin

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
suspend fun getOperationalDetail(opId: String?) {  
    val detailRequest =  
        GetOperationDetailRequest {  
            operationId = opId  
        }  
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use  
{ route53DomainsClient ->  
    val response = route53DomainsClient.getOperationDetail(detailRequest)  
    println("Operation detail message is ${response.message}")  
    }  
}
```

- Para obtener más información sobre la API, consulta [GetOperationDetail](#) la referencia sobre el AWS SDK para la API de Kotlin.

Para ver una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulta [Uso de Route 53 con un AWS SDK](#). En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **ListDomains** con un AWS SDK o CLI

Los siguientes ejemplos de código muestran cómo utilizar ListDomains.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- [Conceptos básicos](#)

.NET

SDK para .NET

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
/// <summary>
/// List the domains for the account.
/// </summary>
/// <returns>A collection of domain summary records.</returns>
public async Task<List<DomainSummary>> ListDomains()
{
    var results = new List<DomainSummary>();
    var paginateDomains = _amazonRoute53Domains.Paginators.ListDomains(
        new ListDomainsRequest());

    // Get the entire list using the paginator.
    await foreach (var domain in paginateDomains.Domains)
    {
        results.Add(domain);
    }
    return results;
}
```

- Para obtener más información sobre la API, consulta [ListDomains](#) la Referencia AWS SDK para .NET de la API.

CLI

AWS CLI

Para ver una lista de los dominios que están registrados en la AWS cuenta corriente

El siguiente `list-domains` comando muestra información resumida sobre los dominios que están registrados en la AWS cuenta actual.

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains list-domains
  --region us-east-1
```

Salida:

```
{
  "Domains": [
    {
      "DomainName": "example.com",
      "AutoRenew": true,
      "TransferLock": true,
      "Expiry": 1602712345.0
    },
    {
      "DomainName": "example.net",
      "AutoRenew": true,
      "TransferLock": true,
      "Expiry": 1602723456.0
    },
    {
      "DomainName": "example.org",
      "AutoRenew": true,
      "TransferLock": true,
      "Expiry": 1602734567.0
    }
  ]
}
```

- Para obtener más información sobre la API, consulte [ListDomains](#) la Referencia de AWS CLI comandos.

Java

SDK para Java 2.x

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
public static void listDomains(Route53DomainsClient route53DomainsClient) {
    try {
        ListDomainsIterable listRes =
            route53DomainsClient.listDomainsPaginator();
        listRes.stream()
            .flatMap(r -> r.domains().stream())
            .forEach(content -> System.out.println("The domain name is "
+ content.domainName()));
    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

- Para obtener más información sobre la API, consulta [ListDomains](#) la Referencia AWS SDK for Java 2.x de la API.

Kotlin

SDK para Kotlin

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
suspend fun listDomains() {
```

```
Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
{ route53DomainsClient ->
    route53DomainsClient
        .listDomainsPaginated(ListDomainsRequest {})
        .transform { it.domains?.forEach { obj -> emit(obj) } }
        .collect { content ->
            println("The domain name is ${content.domainName}")
        }
    }
}
```

- Para obtener más información sobre la API, consulta [ListDomains](#) la referencia sobre el AWS SDK para la API de Kotlin.

Para ver una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulta [Uso de Route 53 con un AWS SDK](#). En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **ListOperations** con un AWS SDK o CLI

Los siguientes ejemplos de código muestran cómo utilizar ListOperations.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- [Conceptos básicos](#)

.NET

SDK para .NET

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
/// <summary>
```

```
/// List operations for the account that are submitted after a specified
date.
/// </summary>
/// <returns>A collection of operation summary records.</returns>
public async Task<List<OperationSummary>> ListOperations(DateTime
submittedSince)
{
    var results = new List<OperationSummary>();
    var paginateOperations = _amazonRoute53Domains.Paginators.ListOperations(
        new ListOperationsRequest()
        {
            SubmittedSince = submittedSince
        });

    // Get the entire list using the paginator.
    await foreach (var operations in paginateOperations.Operations)
    {
        results.Add(operations);
    }
    return results;
}
```

- Para obtener más información sobre la API, consulta [ListOperations](#) la Referencia AWS SDK para .NET de la API.

CLI

AWS CLI

Para enumerar el estado de las operaciones que devuelven un ID de operación

Algunas operaciones de registro de dominios se ejecutan de forma asíncrona y devuelven una respuesta antes de que finalicen. Estas operaciones devuelven un ID de operación que puede usar para obtener el estado actual. El siguiente comando `list-operations` enumera información resumida, incluido el estado, sobre las operaciones actuales de registro de dominio.

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains list-operations
```

```
--region us-east-1
```

Salida:

```
{
  "Operations": [
    {
      "OperationId": "aab9822f-1da0-4bf3-8a15-fd4e0example",
      "Status": "SUCCESSFUL",
      "Type": "DOMAIN_LOCK",
      "SubmittedDate": 1455321739.986
    },
    {
      "OperationId": "c24379ed-76be-42f8-bdad-9379bexample",
      "Status": "SUCCESSFUL",
      "Type": "UPDATE_NAMESERVER",
      "SubmittedDate": 1468960475.109
    },
    {
      "OperationId": "f47e1297-ef9e-4c2b-ae1e-a5fcbexample",
      "Status": "SUCCESSFUL",
      "Type": "RENEW_DOMAIN",
      "SubmittedDate": 1473561835.943
    },
    {
      "OperationId": "75584f23-b15f-459e-aed7-dc6f5example",
      "Status": "SUCCESSFUL",
      "Type": "UPDATE_DOMAIN_CONTACT",
      "SubmittedDate": 1547501003.41
    }
  ]
}
```

El resultado incluye todas las operaciones que devuelven un identificador de operación y que ha realizado en todos los dominios que haya registrado alguna vez con la AWS cuenta corriente. Si desea obtener solo las operaciones que envió después de una fecha específica, puede incluir el parámetro `submitted-since` y especificar una fecha en formato Unix y en hora universal coordinada (UTC). El siguiente comando obtiene el estado de todas las operaciones que se enviaron después de las 00.00 h UTC del 1 de enero de 2020.

```
aws route53domains list-operations \
```


--submitted-since **1577836800**

- Para obtener más información sobre la API, consulte [ListOperations](#) la Referencia de AWS CLI comandos.

Java

SDK para Java 2.x

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
public static void listOperations(Route53DomainsClient route53DomainsClient)
{
    try {
        Date currentDate = new Date();
        LocalDateTime localDateTime =
currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime();
        ZoneOffset zoneOffset = ZoneOffset.of("+01:00");
        localDateTime = localDateTime.minusYears(1);
        Instant myTime = localDateTime.toInstant(zoneOffset);

        ListOperationsRequest operationsRequest =
ListOperationsRequest.builder()
            .submittedSince(myTime)
            .build();

        ListOperationsIterable listRes =
route53DomainsClient.listOperationsPaginator(operationsRequest);
        listRes.stream()
            .flatMap(r -> r.operations().stream())
            .forEach(content -> System.out.println(" Operation Id: " +
content.operationId() +
                " Status: " + content.statusAsString() +
                " Date: " + content.submittedDate()));

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
    }
}
```

```
        System.exit(1);
    }
}
```

- Para obtener más información sobre la API, consulta [ListOperations](#) la Referencia AWS SDK for Java 2.x de la API.

Kotlin

SDK para Kotlin

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
suspend fun listOperations() {
    val currentDate = Date()
    var localDateTime =
        currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime()
    val zoneOffset = ZoneOffset.of("+01:00")
    localDateTime = localDateTime.minusYears(1)
    val myTime: java.time.Instant? = localDateTime.toInstant(zoneOffset)
    val time2: Instant? = myTime?.let { Instant(it) }
    val operationsRequest =
        ListOperationsRequest {
            submittedSince = time2
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
    { route53DomainsClient ->
        route53DomainsClient
            .listOperationsPaginated(operationsRequest)
            .transform { it.operations?.forEach { obj -> emit(obj) } }
            .collect { content ->
                println("Operation Id: ${content.operationId}")
                println("Status: ${content.status}")
                println("Date: ${content.submittedDate}")
            }
    }
```

```
}  
}
```

- Para obtener más información sobre la API, consulta [ListOperations](#) la referencia sobre el AWS SDK para la API de Kotlin.

Para ver una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulta [Uso de Route 53 con un AWS SDK](#). En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

ListPricesÚselo con un AWS SDK

Los siguientes ejemplos de código muestran cómo utilizar ListPrices.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- [Conceptos básicos](#)

.NET

SDK para .NET

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
/// <summary>  
/// List prices for domain type operations.  
/// </summary>  
/// <param name="domainTypes">Domain types to include in the results.</param>  
/// <returns>The list of domain prices.</returns>  
public async Task<List<DomainPrice>> ListPrices(List<string> domainTypes)  
{  
    var results = new List<DomainPrice>();
```

```

    var paginatePrices = _amazonRoute53Domains.Paginators.ListPrices(new
ListPricesRequest());
    // Get the entire list using the paginator.
    await foreach (var prices in paginatePrices.Prices)
    {
        results.Add(prices);
    }
    return results.Where(p => domainTypes.Contains(p.Name)).ToList();
}

```

- Para obtener más información sobre la API, consulta [ListPrices](#) la Referencia AWS SDK para .NET de la API.

Java

SDK para Java 2.x

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```

public static void listPrices(Route53DomainsClient route53DomainsClient,
String domainType) {
    try {
        ListPricesRequest pricesRequest = ListPricesRequest.builder()
            .tld(domainType)
            .build();

        ListPricesIterable listRes =
route53DomainsClient.listPricesPaginator(pricesRequest);
        listRes.stream()
            .flatMap(r -> r.prices().stream())
            .forEach(content -> System.out.println(" Name: " +
content.name() +
                " Registration: " +
content.registrationPrice().price() + " "
                + content.registrationPrice().currency() +

```

```

        " Renewal: " + content.renewalPrice().price() + " " +
        content.renewalPrice().currency());

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

```

- Para obtener más información sobre la API, consulta [ListPrices](#) la Referencia AWS SDK for Java 2.x de la API.

Kotlin

SDK para Kotlin

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```

suspend fun listAllPrices(domainType: String?) {
    val pricesRequest =
        ListPricesRequest {
            tld = domainType
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
    { route53DomainsClient ->
        route53DomainsClient
            .listPricesPaginated(pricesRequest)
            .transform { it.prices?.forEach { obj -> emit(obj) } }
            .collect { pr ->
                println("Registration: ${pr.registrationPrice}
                ${pr.registrationPrice?.currency}")
                println("Renewal: ${pr.renewalPrice?.price}
                ${pr.renewalPrice?.currency}")
                println("Transfer: ${pr.transferPrice?.price}
                ${pr.transferPrice?.currency}")
            }
    }
}

```

```
        println("Restoration: ${pr.restorationPrice?.price}
        ${pr.restorationPrice?.currency}")
    }
}
```

- Para obtener más información sobre la API, consulta [ListPrices](#) la referencia sobre el AWS SDK para la API de Kotlin.

Para ver una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulta [Uso de Route 53 con un AWS SDK](#). En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **RegisterDomain** con un AWS SDK o CLI

Los siguientes ejemplos de código muestran cómo utilizar RegisterDomain.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- [Conceptos básicos](#)

.NET

SDK para .NET

 Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
/// <summary>
/// Initiate a domain registration request.
/// </summary>
/// <param name="contact">Contact details.</param>
/// <param name="domainName">The domain name to register.</param>
```

```

    /// <param name="autoRenew">True if the domain should automatically renew.</
param>
    /// <param name="duration">The duration in years for the domain
registration.</param>
    /// <returns>The operation Id.</returns>
    public async Task<string?> RegisterDomain(string domainName, bool autoRenew,
int duration, ContactDetail contact)
    {
        // This example uses the same contact information for admin, registrant,
and tech contacts.
        try
        {
            var result = await _amazonRoute53Domains.RegisterDomainAsync(
                new RegisterDomainRequest()
                {
                    AdminContact = contact,
                    RegistrantContact = contact,
                    TechContact = contact,
                    DomainName = domainName,
                    AutoRenew = autoRenew,
                    DurationInYears = duration,
                    PrivacyProtectAdminContact = false,
                    PrivacyProtectRegistrantContact = false,
                    PrivacyProtectTechContact = false
                }
            );
            return result.OperationId;
        }
        catch (InvalidInputException)
        {
            _logger.LogInformation($"Unable to request registration for domain
{domainName}");
            return null;
        }
    }
}

```

- Para obtener más información sobre la API, consulta [RegisterDomain](#) la Referencia AWS SDK para .NET de la API.

CLI

AWS CLI

Para registrar un dominio

El siguiente comando `register-domain` registra un dominio y recupera todos los valores de los parámetros de un archivo con formato JSON.

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains register-domain \  
  --region us-east-1 \  
  --cli-input-json file://register-domain.json
```

Contenido de `register-domain.json`:

```
{  
  "DomainName": "example.com",  
  "DurationInYears": 1,  
  "AutoRenew": true,  
  "AdminContact": {  
    "FirstName": "Martha",  
    "LastName": "Rivera",  
    "ContactType": "PERSON",  
    "OrganizationName": "Example",  
    "AddressLine1": "1 Main Street",  
    "City": "Anytown",  
    "State": "WA",  
    "CountryCode": "US",  
    "ZipCode": "98101",  
    "PhoneNumber": "+1.8005551212",  
    "Email": "mriviera@example.com"  
  },  
  "RegistrantContact": {  
    "FirstName": "Li",  
    "LastName": "Juan",  
    "ContactType": "PERSON",  
    "OrganizationName": "Example",  
    "AddressLine1": "1 Main Street",  
    "City": "Anytown",
```



```
    "State": "WA",
    "CountryCode": "US",
    "ZipCode": "98101",
    "PhoneNumber": "+1.8005551212",
    "Email": "ljuan@example.com"
  },
  "TechContact": {
    "FirstName": "Mateo",
    "LastName": "Jackson",
    "ContactType": "PERSON",
    "OrganizationName": "Example",
    "AddressLine1": "1 Main Street",
    "City": "Anytown",
    "State": "WA",
    "CountryCode": "US",
    "ZipCode": "98101",
    "PhoneNumber": "+1.8005551212",
    "Email": "mjackson@example.com"
  },
  "PrivacyProtectAdminContact": true,
  "PrivacyProtectRegistrantContact": true,
  "PrivacyProtectTechContact": true
}
```

Salida:

```
{
  "OperationId": "b114c44a-9330-47d1-a6e8-a0b11example"
}
```

Para confirmar que la operación se ha realizado correctamente, puede ejecutar `get-operation-detail`. Para obtener más información, consulte [get-operation-detail](#).

Para obtener más información, consulte [Registering a New Domain](#) en la Guía para desarrolladores de Amazon Route 53.

Para obtener información sobre los dominios de nivel superior (TLDs) que requieren valores `ExtraParams` y cuáles son los valores válidos, consulte la referencia de [ExtraParam](#) la API de Amazon Route 53.

- Para obtener más información sobre la API, consulte [RegisterDomain](#) la Referencia de AWS CLI comandos.

Java

SDK para Java 2.x

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
public static String requestDomainRegistration(Route53DomainsClient
route53DomainsClient,
    String domainSuggestion,
    String phoneNumber,
    String email,
    String firstName,
    String lastName,
    String city) {

    try {
        ContactDetail contactDetail = ContactDetail.builder()
            .contactType(ContactType.COMPANY)
            .state("LA")
            .countryCode(CountryCode.IN)
            .email(email)
            .firstName(firstName)
            .lastName(lastName)
            .city(city)
            .phoneNumber(phoneNumber)
            .organizationName("My Org")
            .addressLine1("My Address")
            .zipCode("123 123")
            .build();

        RegisterDomainRequest domainRequest = RegisterDomainRequest.builder()
            .adminContact(contactDetail)
            .registrantContact(contactDetail)
            .techContact(contactDetail)
            .domainName(domainSuggestion)
            .autoRenew(true)
            .durationInYears(1)
            .build();
```

```
        RegisterDomainResponse response =
route53DomainsClient.registerDomain(domainRequest);
        System.out.println("Registration requested. Operation Id: " +
response.operationId());
        return response.operationId();

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
    return "";
}
```

- Para obtener más información sobre la API, consulta [RegisterDomain](#) la Referencia AWS SDK for Java 2.x de la API.

Kotlin

SDK para Kotlin

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
suspend fun requestDomainRegistration(
    domainSuggestion: String?,
    phoneNumberVal: String?,
    emailVal: String?,
    firstNameVal: String?,
    lastNameVal: String?,
    cityVal: String?,
): String? {
    val contactDetail =
        ContactDetail {
            contactType = ContactType.Company
            state = "LA"
            countryCode = CountryCode.In
```

```

        email = emailVal
        firstName = firstNameVal
        lastName = lastNameVal
        city = cityVal
        phoneNumber = phoneNumberVal
        organizationName = "My Org"
        addressLine1 = "My Address"
        zipCode = "123 123"
    }

    val domainRequest =
        RegisterDomainRequest {
            adminContact = contactDetail
            registrantContact = contactDetail
            techContact = contactDetail
            domainName = domainSuggestion
            autoRenew = true
            durationInYears = 1
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
    { route53DomainsClient ->
        val response = route53DomainsClient.registerDomain(domainRequest)
        println("Registration requested. Operation Id: ${response.operationId}")
        return response.operationId
    }
}

```

- Para obtener más información sobre la API, consulta [RegisterDomain](#) la referencia sobre el AWS SDK para la API de Kotlin.

Para ver una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulta [Uso de Route 53 con un AWS SDK](#). En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **ViewBilling** con un AWS SDK o CLI

Los siguientes ejemplos de código muestran cómo utilizar ViewBilling.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- [Conceptos básicos](#)

.NET

SDK para .NET

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
/// <summary>
/// View billing records for the account between a start and end date.
/// </summary>
/// <param name="startDate">The start date for billing results.</param>
/// <param name="endDate">The end date for billing results.</param>
/// <returns>A collection of billing records.</returns>
public async Task<List<BillingRecord>> ViewBilling(DateTime startDate,
DateTime endDate)
{
    var results = new List<BillingRecord>();
    var paginateBilling = _amazonRoute53Domains.Paginators.ViewBilling(
        new ViewBillingRequest()
        {
            Start = startDate,
            End = endDate
        });

    // Get the entire list using the paginator.
    await foreach (var billingRecords in paginateBilling.BillingRecords)
    {
        results.Add(billingRecords);
    }
    return results;
}
```

- Para obtener más información sobre la API, consulta [ViewBilling](#) la Referencia AWS SDK para .NET de la API.

CLI

AWS CLI

Para obtener la información de facturación de los cargos de registro de dominio de la AWS cuenta corriente

El siguiente comando `view-billing` devuelve todos los registros de facturación relacionados con el dominio de la cuenta actual durante el período comprendido entre el 1 de enero de 2018 (1514764800 en horario Unix) y la medianoche del 31 de diciembre de 2019 (1577836800 en horario Unix).

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains view-billing \
  --region us-east-1 \
  --start-time 1514764800 \
  --end-time 1577836800
```

Salida:

```
{
  "BillingRecords": [
    {
      "DomainName": "example.com",
      "Operation": "RENEW_DOMAIN",
      "InvoiceId": "149962827",
      "BillDate": 1536618063.181,
      "Price": 12.0
    },
    {
      "DomainName": "example.com",
      "Operation": "RENEW_DOMAIN",
      "InvoiceId": "290913289",
      "BillDate": 1568162630.884,
      "Price": 12.0
    }
  ]
}
```

Para obtener más información, consulte [ViewBilling](#) la referencia de la API de Amazon Route 53.

- Para obtener más información sobre la API, consulte [ViewBilling](#) la Referencia de AWS CLI comandos.

Java

SDK para Java 2.x

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
public static void listBillingRecords(Route53DomainsClient
route53DomainsClient) {
    try {
        Date currentDate = new Date();
        LocalDateTime localDateTime =
currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime();
        ZoneOffset zoneOffset = ZoneOffset.of("+01:00");
        LocalDateTime localDateTime2 = localDateTime.minusYears(1);
        Instant myStartTime = localDateTime2.toInstant(zoneOffset);
        Instant myEndTime = localDateTime.toInstant(zoneOffset);

        ViewBillingRequest viewBillingRequest = ViewBillingRequest.builder()
            .start(myStartTime)
            .end(myEndTime)
            .build();

        ViewBillingIterable listRes =
route53DomainsClient.viewBillingPaginator(viewBillingRequest);
        listRes.stream()
            .flatMap(r -> r.billingRecords().stream())
            .forEach(content -> System.out.println(" Bill Date:: " +
content.billDate() +
                " Operation: " + content.operationAsString() +
                " Price: " + content.price()));
    } catch (Route53Exception e) {
```

```
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

- Para obtener más información sobre la API, consulta [ViewBilling](#) la Referencia AWS SDK for Java 2.x de la API.

Kotlin

SDK para Kotlin

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
suspend fun listBillingRecords() {
    val currentDate = Date()
    val localDateTime =
        currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime()
    val zoneOffset = ZoneOffset.of("+01:00")
    val localDateTime2 = localDateTime.minusYears(1)
    val myStartTime = localDateTime2.toInstant(zoneOffset)
    val myEndTime = localDateTime.toInstant(zoneOffset)
    val timeStart: Instant? = myStartTime?.let { Instant(it) }
    val timeEnd: Instant? = myEndTime?.let { Instant(it) }

    val viewBillingRequest =
        ViewBillingRequest {
            start = timeStart
            end = timeEnd
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
    { route53DomainsClient ->
        route53DomainsClient
            .viewBillingPaginated(viewBillingRequest)
            .transform { it.billingRecords?.forEach { obj -> emit(obj) } }
```



```
        .collect { billing ->
            println("Bill Date: ${billing.billDate}")
            println("Operation: ${billing.operation}")
            println("Price: ${billing.price}")
        }
    }
}
```

- Para obtener más información sobre la API, consulta [ViewBilling](#) la referencia sobre el AWS SDK para la API de Kotlin.

Para ver una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulta [Uso de Route 53 con un AWS SDK](#). En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Seguridad en Amazon Route 53

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El [modelo de responsabilidad compartida](#) la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores independientes prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los [programas de conformidad de AWS](#). Para obtener más información sobre los programas de conformidad de Amazon Route 53, consulte [Servicios de AWS en el ámbito del programa de conformidad](#).
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos vigentes.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Route 53. En los siguientes temas, se le mostrará cómo configurar Route 53 para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a usar otros AWS servicios que lo ayudan a monitorear y proteger sus recursos de Route 53.

Temas

- [Protección de datos en Route 53](#)
- [Identity and Access Management en Amazon Route 53](#)
- [Registro y monitoreo en Amazon Route 53](#)
- [Validación de la conformidad en Amazon Route 53](#)
- [Resiliencia en Amazon Route 53](#)
- [Seguridad de la infraestructura en Amazon Route 53](#)

Protección de datos en Route 53

El [modelo de](#) se aplica a protección de datos en Amazon Route 53. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las [Preguntas frecuentes sobre la privacidad de datos](#). Para obtener información sobre la protección de datos en Europa, consulta la publicación de blog sobre el [Modelo de responsabilidad compartida de AWS y RGPD](#) en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Se utiliza SSL/TLS para comunicarse con AWS los recursos. Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte [Cómo trabajar con CloudTrail senderos](#) en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulta [Estándar de procesamiento de la información federal \(FIPS\) 140-3](#).

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con Route 53 u otro dispositivo Servicios de AWS mediante la consola, la API o. AWS CLI AWS SDKs Cualquier dato que introduzca

en etiquetas o campos de formato libre utilizados para los nombres se pueden emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Protección contra registros de delegación colgantes en Route 53

Con Route 53, un cliente puede crear una zona alojada, como `example.com`, para alojar sus registros DNS. Cada zona alojada incluye un “conjunto de delegación”, que es un conjunto de cuatro servidores de nombres que un cliente puede usar para configurar los registros NS en el dominio principal. Estos registros NS se pueden denominar “registros NS de delegación” o “registros de delegación”.

Para que la zona alojada de Route 53 `example.com` adquiera autoridad, el propietario legítimo del dominio `example.com` debe configurar los registros de delegación en su dominio principal “.com” a través del registrador de dominios. En los casos en que un cliente pierde el acceso a los cuatro servidores de nombres configurados en el dominio principal, por ejemplo, porque se elimina la zona alojada asociada, se corre el riesgo de que un atacante pueda aprovecharlos. Esto se conoce como riesgo de “registros de delegación colgantes”.

Route 53 protege contra el riesgo de registros de delegación colgantes en caso de que se elimine una zona alojada. Tras la eliminación, si está en proceso la creación de una nueva zona alojada con el mismo nombre de dominio, Route 53 comprobará si los registros de delegación que apuntan a la zona alojada eliminada siguen presentes en el dominio principal. Si lo están, Route 53 evitará que se asignen servidores de nombres superpuestos. Este escenario 1 se muestra en los siguientes ejemplos.

Sin embargo, existen otros riesgos en materia de registros de delegación colgantes, contra los que Route 53 no puede protegerse, como se detalla en los escenarios 2 y 3 de los siguientes ejemplos. Para protegerse contra este conjunto más amplio de riesgos, asegúrese de que los registros NS principales coincidan con la delegación establecida para la zona alojada de Route 53. Puede encontrar el conjunto de delegación de una zona alojada a través de la consola de Route 53 o AWS CLI. Para obtener más información, consulte [Descripción de registros](#) o [get-hosted-zone](#).

Además, la habilitación de la firma de DNSSEC para una zona alojada de Route 53 puede servir como otra capa de protección más allá de las prácticas recomendadas mencionadas con anterioridad. El DNSSEC autentica que las respuestas de DNS provienen de la fuente autorizada, lo que protege contra el riesgo de forma eficaz. Para obtener más información, consulte [Configuración de la firma de DNSSEC en Amazon Route 53](#).

Ejemplos

En los siguientes ejemplos, asumimos que tiene un dominio `example.com` y su dominio secundario, `child.example.com`. Explicaremos cómo, en varios escenarios, se pueden crear registros de delegación colgantes, cómo Route 53 protege su dominio contra el abuso y cómo mitigar de manera eficaz los riesgos asociados a los registros de delegación colgantes.

Escenario 1:

En la zona alojada principal, se crean `child.example.com` con cuatro servidores de nombres: `<ns1>`, `<ns2>`, `<ns3>` y `<ns4>`. La delegación se configura correctamente en la zona alojada `example.com` y se crean registros NS de delegación para `child.example.com` con cuatro servidores de nombres: `<ns1>`, `<ns2>`, `<ns3>` y `<ns4>`. Cuando la zona alojada `child.example.com` se elimina sin eliminar los registros NS de delegación en `example.com`, Route 53 protege a `child.example.com` contra el riesgo de que se produzcan registros de delegación colgantes, ya que impide que `<ns1>`, `<ns2>`, `<ns3>` y `<ns4>` se asignen a zonas alojadas recién creadas con el mismo nombre de dominio.

Escenario 2:

Similar al escenario 1, pero esta vez se eliminan la zona alojada secundaria y los registros NS de delegación en la zona alojada `example.com`. Sin embargo, se vuelven a agregar los registros NS de delegación `<ns1>`, `<ns2>`, `<ns3>` y `<ns4>` sin crear una zona alojada secundaria. Aquí, `<ns1>`, `<ns2>`, `<ns3>` y `<ns4>` son registros de delegación colgantes porque Route 53 elimina la retención, que impedía que `<ns1>`, `<ns2>`, `<ns3>` y `<ns4>` se asignaran y ahora permitirá que las zonas alojadas recién creadas utilicen los servidores de nombres mencionados con anterioridad. Para mitigar el riesgo, elimine `<ns1>`, `<ns2>`, `<ns3>` y `<ns4>` de los registros de delegación y vuelva a agregarlos solo una vez que se haya creado la zona alojada secundaria.

Situación 3:

En este escenario, se crea un conjunto de delegación reutilizable de Route 53 con servidores de nombres `<ns1>`, `<ns2>`, `<ns3>` y `<ns4>`. A continuación, delega el dominio `example.com` a estos servidores de nombres en el dominio principal `.com`. Sin embargo, aún no se ha creado la zona alojada para `example.com` en el conjunto de delegación reutilizable. Aquí, `<ns1>`, `<ns2>`, `<ns3>` y `<ns4>` son registros de delegación colgantes. Para mitigar el riesgo, cree la zona alojada mediante el conjunto de delegación reutilizable con servidores de nombres `<ns1>`, `<ns2>`, `<ns3>` y `<ns4>`.

Identity and Access Management en Amazon Route 53

Para realizar cualquier operación en los recursos de Amazon Route 53, como registrar un dominio o actualizar un registro, AWS Identity and Access Management (IAM) requiere que autentiques que eres un usuario aprobado AWS . Si está utilizando la consola de Route 53, debe autenticar su identidad proporcionando su nombre de usuario y contraseña de AWS .

Tras autenticar su identidad, IAM controla su acceso AWS comprobando que tiene permisos para realizar operaciones y acceder a los recursos. Si es un administrador de la cuenta, puede utilizar IAM para controlar el acceso de otros usuarios a los recursos que están asociados a dicha cuenta.

En este capítulo se explica cómo utilizar [IAM](#) y Route 53 para ayudar a proteger sus recursos.

Temas

- [Autenticación con identidades](#)
- [Control de acceso](#)
- [Información general sobre la administración de los permisos de acceso a los recursos de Amazon Route 53](#)
- [Uso de políticas basadas en identidad \(políticas de IAM\) para Amazon Route 53](#)
- [Usar roles vinculados a servicios en Amazon Route 53 Resolver](#)
- [AWS políticas gestionadas para Amazon Route 53](#)
- [Uso de condiciones de las políticas de IAM para control de acceso preciso](#)
- [Permisos de la API de Amazon Route 53: referencia de acciones, recursos y condiciones](#)

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe autenticarse como usuario de Usuario raíz de la cuenta de AWS IAM o asumir una función de IAM.

Puede iniciar sesión como una identidad federada con las credenciales de una fuente de identidad, como AWS IAM Identity Center (IAM Identity Center), la autenticación de inicio de sesión único o las credenciales. Google/Facebook Para obtener más información sobre el inicio de sesión, consulte [Cómo iniciar sesión en la Cuenta de AWS](#) en la Guía del usuario de AWS Sign-In .

Para el acceso programático, AWS proporciona un SDK y una CLI para firmar criptográficamente las solicitudes. Para obtener más información, consulte [AWS Signature Version 4 para solicitudes de API](#) en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear un Cuenta de AWS, se comienza con una identidad de inicio de sesión denominada usuario Cuenta de AWS raíz que tiene acceso completo a todos Servicios de AWS los recursos. Recomendamos encarecidamente que no utilice el usuario raíz para las tareas cotidianas. Para ver las tareas que requieren credenciales de usuario raíz, consulte [Tareas que requieren credenciales de usuario raíz](#) en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio empresarial, del proveedor de identidades web o al Directory Service que se accede Servicios de AWS mediante credenciales de una fuente de identidad. Las identidades federadas asumen roles que proporcionan credenciales temporales.

Para una administración de acceso centralizada, recomendamos AWS IAM Identity Center. Para obtener más información, consulte [¿Qué es el Centro de identidades de IAM?](#) en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un [usuario de IAM](#) es una identidad con permisos específicos para una sola persona o aplicación. Recomendamos utilizar credenciales temporales en lugar de usuarios de IAM con credenciales a largo plazo. Para obtener más información, consulte [Exigir a los usuarios humanos que utilicen la federación con un proveedor de identidad para acceder AWS mediante credenciales temporales](#) en la Guía del usuario de IAM.

Un [grupo de IAM](#) especifica un conjunto de usuarios de IAM y facilita la administración de los permisos para grupos grandes de usuarios. Para obtener más información, consulte [Casos de uso para usuarios de IAM](#) en la Guía del usuario de IAM.

Roles de IAM

Un [rol de IAM](#) es una identidad con permisos específicos que proporciona credenciales temporales. Puede asumir un rol [cambiando de un rol de usuario a uno de IAM \(consola\)](#) o llamando a una AWS CLI operación de AWS API. Para obtener más información, consulte [Métodos para asumir un rol](#) en la Guía del usuario de IAM.

Las funciones de IAM son útiles para el acceso de usuarios federados, los permisos de usuario de IAM temporales, el acceso entre cuentas, el acceso entre servicios y las aplicaciones que se ejecutan en Amazon. EC2 Para obtener más información, consulte [Acceso a recursos entre cuentas en IAM](#) en la Guía del usuario de IAM.

Control de acceso

Para crear, actualizar, eliminar o enumerar recursos de Amazon Route 53, necesita permiso para realizar la operación y obtener acceso a los recursos correspondientes.

En las secciones siguientes, se describe cómo administrar los permisos de Route 53. Recomendamos que lea primero la información general.

Información general sobre la administración de los permisos de acceso a los recursos de Amazon Route 53

Cada AWS recurso es propiedad de una AWS cuenta y los permisos para crear un recurso o acceder a él se rigen por las políticas de permisos.

Note

Un administrador de la cuenta (o usuario administrador) es un usuario que cuenta con privilegios de administrador. Para obtener más información acerca de los administradores, consulte [Prácticas recomendadas de IAM](#) en la Guía del usuario de IAM.

Al conceder permisos, puede decidir a quién concederlos, los recursos para los que los concede y las acciones que se les permiten realizar.

Los usuarios necesitan acceso programático si quieren interactuar con personas AWS ajenas a. Consola de administración de AWS La forma de conceder el acceso programático depende del tipo de usuario que acceda. AWS

Para conceder acceso programático a los usuarios, elija una de las siguientes opciones.

¿Qué usuario necesita acceso programático?	Para	Mediante
IAM	(Recomendado) Utilice las credenciales de la consola como credenciales temporales para firmar las solicitudes programáticas dirigidas al AWS CLI AWS SDKs, o. AWS APIs	Siga las instrucciones de la interfaz que desea utilizar: • Para ello AWS CLI, consulte Iniciar sesión para el desarrollo AWS local en la Guía del AWS Command Line Interface usuario. • Para ello AWS SDKs, consulte Iniciar sesión para el desarrollo AWS local en la Guía de referencia de AWS SDKs and Tools.
Identidad del personal (Usuarios administrados en el IAM Identity Center)	Utilice credenciales temporales para firmar las solicitudes programáticas dirigidas al AWS CLI, AWS SDKs, o AWS APIs.	Siga las instrucciones de la interfaz que desea utilizar: • Para ello AWS CLI, consulte Configuración del AWS CLI uso AWS IAM Identity Center en la Guía del AWS Command Line Interface usuario. • Para AWS SDKs ver las herramientas y AWS APIs, consulte la autenticación del Centro de Identidad de IAM en la Guía de referencia de herramientas AWS SDKs y herramientas.
IAM	Utilice credenciales temporales para firmar las solicitudes programáticas dirigidas al	Siga las instrucciones de Uso de credenciales temporales

¿Qué usuario necesita acceso programático?	Para	Mediante
	AWS CLI AWS SDKs, o. AWS APIs	con AWS recursos de la Guía del usuario de IAM.
IAM	(No recomendado) Utilice credenciales de larga duración para firmar las solicitudes programáticas dirigidas al AWS CLI, AWS SDKs, o. AWS APIs	Siga las instrucciones de la interfaz que desea utilizar: • Para ello AWS CLI, consulte Autenticación con credenciales de usuario de IAM en la Guía del AWS Command Line Interface usuario. • Para obtener AWS SDKs información sobre las herramientas, consulte Autenticarse con credenciales de larga duración en la Guía de referencia de herramientas AWS SDKs y herramientas. • Para ello AWS APIs, consulte Administrar las claves de acceso para los usuarios de IAM en la Guía del usuario de IAM.

Temas

- [ARNs para los recursos de Amazon Route 53](#)
- [Titularidad de los recursos](#)
- [Administración del acceso a los recursos](#)
- [Especificar elementos de políticas: recursos, acciones, efectos y entidades principales](#)
- [Especificación de las condiciones de una política](#)

ARNs para los recursos de Amazon Route 53

Amazon Route 53 admite una serie de tipos de recursos para DNS, comprobación de estado y registro de dominios. En una política, puede conceder o denegar el acceso a los siguientes recursos utilizando * para el ARN:

- Comprobaciones de estado
- Zonas alojadas
- Conjuntos de delegación reutilizables
- Estado de un lote de cambios del conjunto de registros de recursos (solo API)
- Políticas de tráfico (flujo de tráfico)
- Instancias de políticas de tráfico (flujo de tráfico)

No todos los recursos de Route 53 admiten permisos. No se puede conceder ni denegar el acceso a los siguientes recursos:

- Dominios
- Registros individuales
- Etiquetas de dominios
- Etiquetas de comprobaciones de estado
- Etiquetas de zonas hospedadas

Route 53 ofrece acciones de la API para trabajar con cada uno de estos tipos de recursos. Para obtener más información, consulte la [referencia de API de Amazon Route 53](#). Para consultar una lista de acciones y el ARN a especificar para conceder o denegar permisos para ejecutar cada acción, visite [Permisos de la API de Amazon Route 53: referencia de acciones, recursos y condiciones](#).

Titularidad de los recursos

Una AWS cuenta es propietaria de los recursos que se crean en la cuenta, independientemente de quién los haya creado. En concreto, el propietario del recurso es la AWS cuenta de la entidad principal (es decir, la cuenta raíz o un rol de IAM) que autentica la solicitud de creación del recurso.

Los siguientes ejemplos ilustran cómo funciona:

- Si utilizas las credenciales de la cuenta raíz de tu AWS cuenta para crear una zona alojada, tu AWS cuenta es la propietaria del recurso.

- Si crea un usuario en su AWS cuenta y concede permisos para crear una zona alojada a ese usuario, el usuario podrá crear una zona alojada. No obstante, su cuenta de AWS, a la que pertenece el usuario, es la propietaria del recurso de la zona alojada.
- Si crea un rol de IAM en su AWS cuenta con permisos para crear una zona alojada, cualquier persona que pueda asumir el rol podrá crear una zona alojada. Su AWS cuenta, a la que pertenece el rol, es propietaria del recurso de la zona alojada.

Administración del acceso a los recursos

Una política de permisos especifica quién tiene acceso a qué. En esta sección se explican las opciones para crear políticas de permisos para Amazon Route 53. Para obtener más información sobre la sintaxis y las descripciones de la política de IAM, consulte la [Referencia de política de IAM de AWS](#) en la Guía del usuario de IAM.

Las políticas adjuntadas a una identidad de IAM se denominan políticas basadas en identidad (políticas de IAM) y las políticas adjuntadas a un recurso se denominan políticas basadas en recursos. Route 53 solo admite políticas basadas en identidad (políticas de IAM).

Temas

- [Políticas basadas en identidades \(políticas de IAM\)](#)
- [Políticas basadas en recursos](#)

Políticas basadas en identidades (políticas de IAM)

Puede asociar políticas a identidades de IAM. Por ejemplo, puede hacer lo siguiente:

- Adjuntar una política de permisos a un usuario o grupo de su cuenta: un administrador de la cuenta puede utilizar una política de permisos asociada a un usuario determinado para concederle permisos para crear recursos de Amazon Route 53.
- Adjunte una política de permisos a un rol (otorgue permisos para varias cuentas): puede conceder permiso para realizar acciones de Route 53 a un usuario creado por otra AWS cuenta. Para ello, asocie una política de permisos a un rol de IAM y, a continuación, permita al usuario de la otra cuenta asumir el rol. En el siguiente ejemplo se explica cómo este proceso funciona para dos cuentas, A y B, de AWS :
 1. El administrador de la cuenta A crea un rol de IAM y asocia a dicho rol una política que concede permisos de creación o acceso a recursos propiedad de la cuenta A.

2. El administrador de la cuenta A asocia una política de confianza al rol. La política de confianza identifica la cuenta B como la entidad principal, que puede asumir el rol.
3. El administrador de la cuenta B puede entonces delegar permisos para asumir el rol a usuarios o grupos de la cuenta B. Esto permite a los usuarios de la cuenta B crear u obtener acceso a recursos de la cuenta A.

Para obtener más información sobre cómo delegar permisos a los usuarios de otra AWS cuenta, consulte [Gestión del acceso](#) en la Guía del usuario de IAM.

La siguiente política de ejemplo permite a un usuario realizar la acción `CreateHostedZone` a fin de crear una zona alojada pública para cualquier cuenta de AWS :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "route53:CreateHostedZone"
      ],
      "Resource": "*"
    }
  ]
}
```

Si desea que la política también se aplique a las zonas alojadas privadas, debe conceder permisos para usar la `AssociateVPCWithHostedZone` acción de Route 53 y dos EC2 acciones de Amazon `DescribeVpcs` y `DescribeRegion`, como se muestra en el siguiente ejemplo:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
        "Action": [
            "route53:CreateHostedZone",
            "route53:AssociateVPCWithHostedZone"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeVpcs",
            "ec2:DescribeRegions"
        ],
        "Resource": "*"
    }
]
```

Para obtener más información acerca de cómo adjuntar políticas a identidades de Route 53, consulte [Uso de políticas basadas en identidad \(políticas de IAM\) para Amazon Route 53](#). Para obtener más información acerca de los usuarios, los grupos, los roles y los permisos, consulte [Identidades \(usuarios, grupos y roles\)](#) en la Guía del usuario de IAM.

Políticas basadas en recursos

Otros servicios, como Amazon S3, permiten también adjuntar políticas de permisos a recursos. Por ejemplo, puede asociar una política a un bucket de S3 para administrar los permisos de acceso a dicho bucket. Amazon Route 53 no admite adjuntar políticas a recursos.

Especificar elementos de políticas: recursos, acciones, efectos y entidades principales

Amazon Route 53 incluye acciones de API (consulte la [Referencia de la API de Amazon Route 53](#)) que puede usar en cada recurso de Route 53 (consulte [ARNs para los recursos de Amazon Route 53](#)). Puede conceder a un usuario o un usuario federado permisos para realizar alguna de estas acciones o todas ellas. Tenga en cuenta que algunas acciones de la API, como el registro de un dominio, requieren permisos para realizar más de una acción.

A continuación, se indican los elementos básicos de la política:

- **Recurso:** use un Nombre de recurso de Amazon (ARN) para identificar el recurso al que se aplica la política. Para obtener más información, consulte [ARNs para los recursos de Amazon Route 53](#).

- **Acción:** utilice palabras clave de acción para identificar las operaciones del recurso que desea permitir o denegar. Por ejemplo, en función del elemento `Effect` especificado, el permiso `route53:CreateHostedZone` permite o deniega a un usuario la capacidad de realizar la acción `CreateHostedZone` de Route 53.
- **Efecto:** especifique el efecto (permitir o denegar) cuando un usuario intente realizar la acción en el recurso especificado. Si no concede acceso de forma explícita a una acción, el acceso se deniega implícitamente. También puede denegar explícitamente el acceso a un recurso para asegurarse de que un usuario no pueda obtener acceso a él, aunque otra política le conceda acceso.
- **Entidad principal:** en las políticas basadas en identidades (políticas de IAM), el usuario al que se asocia esta política es la entidad principal implícita. Para las políticas basadas en recursos, debe especificar el usuario, la cuenta, el servicio u otra entidad que desee que reciba permisos (se aplica solo a las políticas basadas en recursos). Route 53 no admite políticas basadas en recursos.

Para obtener más información sobre la sintaxis y descripciones de las políticas de IAM, consulte la [Referencia de políticas de IAM de AWS](#) en la Guía del usuario de IAM.

Para ver una lista de con todas las operaciones de la API de Route 53 y los recursos a los que se aplican, consulte [Permisos de la API de Amazon Route 53: referencia de acciones, recursos y condiciones](#).

Especificación de las condiciones de una política

Al conceder permisos, puede utilizar el lenguaje de la política de IAM para especificar las condiciones en las que se debe aplicar una política. Por ejemplo, es posible que desee que solo se aplique una política después de una fecha específica. Para obtener más información acerca de cómo especificar condiciones en un lenguaje de la política, consulte [Elementos de la política de JSON de IAM: Condición](#) en la Guía del usuario de IAM.

Cómo expresar condiciones, se usan claves de condición predefinidas. No hay claves de condición específicas para Route 53. Sin embargo, hay claves condicionales AWS amplias que puede utilizar según sea necesario. Para obtener una lista completa de las teclas AWS anchas, consulte [las claves disponibles para las condiciones](#) en la Guía del usuario de IAM.

Uso de políticas basadas en identidad (políticas de IAM) para Amazon Route 53

En este tema se ofrecen ejemplos de políticas basadas en identidad que muestran cómo un administrador de una cuenta puede adjuntar políticas de permisos a identidades de IAM y, de ese modo, conceder permisos para realizar operaciones en recursos de Amazon Route 53.

Important

Le recomendamos que consulte primero los temas de introducción en los que se explican los conceptos básicos y las opciones disponibles para administrar el acceso a sus recursos de Route 53. Para obtener más información, consulte [Información general sobre la administración de los permisos de acceso a los recursos de Amazon Route 53](#).

Note

Al conceder acceso, la zona alojada y Amazon VPC deben pertenecer a la misma partición. Una partición es un grupo de Regiones de AWS. Cada una Cuenta de AWS tiene el alcance de una partición.

Las siguientes son las particiones admitidas:

- aws - Regiones de AWS
- aws-cn - Regiones de China
- aws-us-gov - AWS GovCloud (US) Region

Para obtener más información, consulte [Administración de acceso](#) y [puntos de conexión y cuotas de Amazon Route 53](#) en la Referencia general de AWS .

Temas

- [Permisos necesarios para usar la consola de Amazon Route 53](#)
- [Permisos de ejemplo para el propietario de un registro de dominio](#)
- [Permisos de clave administrados por el cliente de Route 53 necesarios para firmar DNSSEC](#)
- [Ejemplos de políticas administradas por el cliente](#)

El ejemplo siguiente muestra una política de permisos. El Sid o ID de instrucción es opcional:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowPublicHostedZonePermissions",
      "Effect": "Allow",
      "Action": [
        "route53:CreateHostedZone",
        "route53:UpdateHostedZoneComment",
        "route53:GetHostedZone",
        "route53:ListHostedZones",
        "route53>DeleteHostedZone",
        "route53:ChangeResourceRecordSets",
        "route53:ListResourceRecordSets",
        "route53:GetHostedZoneCount",
        "route53:ListHostedZonesByName"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowHealthCheckPermissions",
      "Effect": "Allow",
      "Action": [
        "route53:CreateHealthCheck",
        "route53:UpdateHealthCheck",
        "route53:GetHealthCheck",
        "route53:ListHealthChecks",
        "route53>DeleteHealthCheck",
        "route53:GetCheckerIpRanges",
        "route53:GetHealthCheckCount",
        "route53:GetHealthCheckStatus",
        "route53:GetHealthCheckLastFailureReason"
      ],
      "Resource": "*"
    }
  ]
}
```

La política incluye dos instrucciones:

- La primera instrucción concede permisos para las acciones necesarias para crear y administrar zonas hospedadas públicas y sus registros. El carácter comodín (*) del nombre del recurso de Amazon (ARN) permite el acceso a todas las zonas alojadas que son propiedad de la AWS cuenta corriente.
- La segunda instrucción concede permisos para todas las acciones necesarias para crear y administrar comprobaciones de estado.

Para consultar una lista de acciones y el ARN a especificar para conceder o denegar permisos para ejecutar cada acción, visite [Permisos de la API de Amazon Route 53: referencia de acciones, recursos y condiciones](#).

Permisos necesarios para usar la consola de Amazon Route 53

Para conceder acceso total a la consola de Amazon Route 53, debe conceder los permisos en la siguiente política de permisos:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "route53:*",
        "route53domains:*",
        "tag:*",
        "ssm:GetParametersByPath",
        "cloudfront:ListDistributions",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticbeanstalk:DescribeEnvironments",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation",
        "s3:GetBucketWebsite",
        "ec2:DescribeRegions",
        "ec2:DescribeVpcs",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
```

```

        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:ModifyNetworkInterfaceAttribute",
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:CreateTopic",
        "kms:ListAliases",
        "kms:DescribeKey",
        "kms:CreateKey",
        "kms:CreateAlias",
        "kms:Sign",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:GetMetricStatistics"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "apigateway:GET",
    "Resource": "arn:aws:apigateway:*::/domainnames"
  }
]
}

```

Aquí se explica por qué son necesarios los permisos:

route53:*

Le permite realizar todas las acciones de Route 53 salvo las siguientes:

- Cree y actualice registros de alias para los que el valor de Alias Target sea una CloudFront distribución, un balanceador de cargas ELB, un entorno de Elastic Beanstalk o un bucket de Amazon S3. (Con estos permisos, puede crear registros de alias en los que el valor de Alias Target (Destino del alias) es otro registro de la misma zona alojada).
- Trabajar con zonas alojadas privadas.
- Trabajar con dominios.

- Cree, elimine y visualice las alarmas. CloudWatch
- Renderice CloudWatch las métricas en la consola de Route 53.

route53domains:*

Le permite trabajar con dominios.

Important

Si muestra las acciones de `route53` individualmente, debe incluir `route53:CreateHostedZone` para trabajar con dominios. Al registrar un dominio, se crea una zona alojada al mismo tiempo, por lo que una política que incluya permisos para registrar dominios también requiere permiso para crear zonas alojadas.

Para el registro de dominios, Route 53 no permite conceder o denegar permisos a recursos específicos.

route53resolver:*

Le permite trabajar con Route 53 VPC Resolver.

ssm:GetParametersByPath

Le permite buscar regiones disponibles públicamente cuando crean nuevos registros de alias, zonas alojadas privadas y comprobaciones de estado.

cloudfront:ListDistributions

Permite crear y actualizar registros de alias para los que el valor de Alias Target es una CloudFront distribución.

Estos permisos no son necesarios si no está utilizando la consola de Route 53. Route 53 solo lo utiliza para obtener la lista de distribuciones que muestra en la consola.

elasticloadbalancing:DescribeLoadBalancers

Le permite crear y actualizar registros de alias en los que el valor de Alias Target (Destino del alias) es un balanceador de carga de ELB.

Estos permisos no son necesarios si no está utilizando la consola de Route 53. Route 53 solo lo utiliza para obtener la lista de balanceadores de carga que muestra en la consola.

elasticbeanstalk:DescribeEnvironments

Le permite crear y actualizar registros de alias en los que el valor de Alias Target (Destino del alias) es un entorno de Elastic Beanstalk.

Estos permisos no son necesarios si no está utilizando la consola de Route 53. Route 53 solo lo utiliza para obtener la lista de entornos que muestra en la consola.

s3:ListAllMyBuckets, s3:GetBucketLocation, y s3:GetBucketWebsite

Le permite crear y actualizar registros de alias en los que el valor de Alias Target (Destino del alias) es un bucket de Amazon S3. (Puede crear un alias para un bucket de Amazon S3 solo si el bucket está configurado como el punto de conexión de un sitio web; s3:GetBucketWebsite obtiene la información de configuración necesaria).

Estos permisos no son necesarios si no está utilizando la consola de Route 53. Route 53 solo lo utiliza para obtener la lista de buckets que muestra en la consola.

ec2:DescribeVpcs y ec2:DescribeRegions

Le permite trabajar con zonas hospedadas privadas.

Todos los permisos de **ec2** mostrados

Le permite trabajar con Route 53 VPC Resolver.

sns:ListTopics, sns:ListSubscriptionsByTopic, sns:CreateTopic, cloudwatch:DescribeAlarms, cloudwatch:PutMetricAlarm, cloudwatch:DeleteAlarms

Le permite crear, eliminar y ver CloudWatch las alarmas.

cloudwatch:GetMetricStatistics

Le permite crear controles de estado CloudWatch métricos.

Estos permisos no son necesarios si no está utilizando la consola de Route 53. Route 53 solo lo utiliza para obtener las estadísticas que muestra en la consola.

apigateway:GET

Le permite crear y actualizar registros de alias en los que el valor de Alias Target (Destino del alias) es una API de Amazon API Gateway.

Este permiso no es necesario si no está utilizando la consola de Route 53. Route 53 solo lo usa para obtener una lista APIs que se mostrará en la consola.

kms : *

Le permite trabajar con él AWS KMS para habilitar la firma de DNSSEC.

Permisos de ejemplo para el propietario de un registro de dominio

Con los permisos de conjuntos de registros de recursos, puede establecer permisos granulares que limiten lo que el AWS usuario puede actualizar o modificar. Para obtener más información, consulte [Uso de condiciones de las políticas de IAM para control de acceso preciso](#).

En algunos casos, el propietario de una zona alojada podría ser el responsable de la administración general de la misma, mientras que otra persona de la organización es responsable de un subconjunto de esas tareas. El propietario de una zona alojada que haya habilitado la firma con DNSSEC, por ejemplo, podría querer crear una política de IAM que incluya el permiso para que otra persona añada y elimine registros del conjunto de recursos (RRs) en la zona alojada, entre otras tareas. Los permisos específicos que el propietario de una zona alojada elija habilitar para un propietario de registro u otras personas dependerán de la política de su organización.

A continuación se muestra un ejemplo de política de IAM que permite al propietario de un registro realizar modificaciones en las políticas de tráfico y realizar RRs comprobaciones de estado. El propietario de un registro con esta política no puede realizar operaciones de nivel de zona, tales como crear o eliminar una zona, activar o desactivar el registro de consultas, crear o eliminar un conjunto de delegación reutilizable o cambiar la configuración de DNSSEC.

```
{
  "Sid": "Do not allow zone-level modification ",
  "Effect": "Allow",
  "Action": [
    "route53:ChangeResourceRecordSets",
    "route53:CreateTrafficPolicy",
    "route53>DeleteTrafficPolicy",
    "route53:CreateTrafficPolicyInstance",
    "route53:CreateTrafficPolicyVersion",
    "route53:UpdateTrafficPolicyInstance",
    "route53:UpdateTrafficPolicyComment",
    "route53>DeleteTrafficPolicyInstance",
    "route53:CreateHealthCheck",
    "route53:UpdateHealthCheck",
    "route53>DeleteHealthCheck",
    "route53:List*",
  ]
}
```

```

    "route53:Get*"
  ],
  "Resource": [
    "*"
  ]
}

```

Permisos de clave administrados por el cliente de Route 53 necesarios para firmar DNSSEC

Al habilitar la firma DNSSEC para Route 53, Route 53 crea una clave de firma de claves (KSK) basada en una clave administrada por el cliente en (). AWS Key Management Service AWS KMS Puede usar una clave administrada por el cliente que admita la firma DNSSEC o crear una. Route 53 debe tener permiso para acceder a la clave administrada por el cliente a fin de que pueda crear la KSK automáticamente.

Para permitir que Route 53 acceda a la clave administrada por el cliente, asegúrese de que la política de clave administrada por el cliente incluya las siguientes instrucciones:

```

{
    "Sid": "Allow Route 53 DNSSEC Service",
    "Effect": "Allow",
    "Principal": {
        "Service": "dnssec-route53.amazonaws.com"
    },
    "Action": ["kms:DescribeKey",
        "kms:GetPublicKey",
        "kms:Sign"],
    "Resource": "*"
  },
  {
    "Sid": "Allow Route 53 DNSSEC to CreateGrant",
    "Effect": "Allow",
    "Principal": {
        "Service": "dnssec-route53.amazonaws.com"
    },
    "Action": ["kms:CreateGrant"],
    "Resource": "*",
    "Condition": {
        "Bool": {
            "kms:GrantIsForAWSResource": true
        }
    }
  }
}

```

```
    }
}
```

El problema del suplente confuso es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. Para protegerse AWS KMS de ello, si lo desea, puede limitar los permisos que un servicio tiene a un recurso en una política basada en recursos proporcionando una combinación de condiciones `aws:SourceAccount` y `aws:SourceArn` (ambas o una). `aws:SourceAccount` es el identificador de AWS cuenta del propietario de una zona alojada. `aws:SourceArn` es un ARN de una zona alojada.

A continuación se muestran dos ejemplos de permisos que puede agregar:

```
{
  "Sid": "Allow Route 53 DNSSEC Service",
  ...
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": "111122223333"
    },
    "ArnEquals": {
      "aws:SourceArn": "arn:aws:route53::hostedzone/HOSTED_ZONE_ID"
    }
  }
},
```

- O -

```
{
  "Sid": "Allow Route 53 DNSSEC Service",
  ...
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": ["1111-2222-3333", "4444-5555-6666"]
    },
    "ArnLike": {
      "aws:SourceArn": "arn:aws:route53::hostedzone/*"
    }
  }
}
```



```
},
```

Para obtener más información, consulte [El problema del suplente confuso](#) en la Guía del usuario de IAM.

Ejemplos de políticas administradas por el cliente

Puede crear sus propias políticas de IAM personalizadas con el fin de conceder permisos para realizar acciones de Route 53. Puede asociar estas políticas personalizadas a los grupos de IAM que requieran los permisos especificados. Estas políticas funcionan cuando se utiliza la API de Route 53 AWS SDKs, la o la AWS CLI. A continuación se muestran algunos ejemplos de permisos para algunos casos de uso comunes. Para ver la política que concede a un usuario acceso total a Route 53, consulte [Permisos necesarios para usar la consola de Amazon Route 53](#).

Ejemplos

- [Ejemplo 1: Permitir acceso de lectura a todas las zonas hospedadas](#)
- [Ejemplo 2: Permitir la creación y eliminación de zonas hospedadas](#)
- [Ejemplo 3: Permitir acceso completo a todos los dominios \(solo zonas hospedadas públicas\)](#)
- [Ejemplo 4: Permitir la creación de puntos finales de VPC Resolver de Route 53 entrantes y salientes](#)

Ejemplo 1: Permitir acceso de lectura a todas las zonas hospedadas

La siguiente política de permisos concede al usuario permisos para mostrar todas las zonas hospedadas y ver todos los registros de una zona alojada.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "route53:GetHostedZone",
        "route53:ListResourceRecordSets"
      ],
      "Resource": "*"
    }
  ],
}
```

```
{
  "Effect": "Allow",
  "Action": ["route53:ListHostedZones"],
  "Resource": "*"
}
```

Ejemplo 2: Permitir la creación y eliminación de zonas hospedadas

La siguiente política de permisos permite a los usuarios crear y eliminar zonas hospedadas, así como realizar un seguimiento del progreso del cambio.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["route53:CreateHostedZone"],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": ["route53>DeleteHostedZone"],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": ["route53:GetChange"],
      "Resource": "*"
    }
  ]
}
```

Ejemplo 3: Permitir acceso completo a todos los dominios (solo zonas hospedadas públicas)

La siguiente política de permisos permite a los usuarios realizar todas las acciones en los registros de dominios, incluidos los permisos para registrar dominios y crear zonas hospedadas.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "route53domains:*",
        "route53:CreateHostedZone"
      ],
      "Resource": "*"
    }
  ]
}
```

Al registrar un dominio, se crea una zona alojada al mismo tiempo, por lo que una política que incluya permisos para registrar dominios también requiere permisos para crear zonas alojadas. (Para el registro de dominios, Route 53 no permite conceder permisos a recursos específicos).

Para obtener información sobre los permisos necesarios para trabajar con zonas hospedadas, consulte [Permisos necesarios para usar la consola de Amazon Route 53](#).

Ejemplo 4: Permitir la creación de puntos finales de VPC Resolver de Route 53 entrantes y salientes

La siguiente política de permisos permite a los usuarios utilizar la consola de Route 53 para crear puntos de enlace de entrada y salida de Resolver.

Algunos de estos permisos solo son necesarios para crear puntos de enlace en la consola. Puede omitir estos permisos si desea conceder permisos solo para crear puntos de enlace de entrada y salida mediante programación:

- `route53resolver:ListResolverEndpoints` permite a los usuarios ver la lista de puntos de enlace de entrada o salida para que puedan verificar que se ha creado un puntos de conexión.
- `DescribeAvailabilityZones` es necesario para mostrar una lista de zonas de disponibilidad.
- `DescribeVpcs` necesario para mostrar una lista de VPCs

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "route53resolver:CreateResolverEndpoint",
        "route53resolver:ListResolverEndpoints",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource": "*"
    }
  ]
}
```

Usar roles vinculados a servicios en Amazon Route 53 Resolver

[El solucionador de VPC de Route 53 utiliza funciones vinculadas al AWS Identity and Access Management servicio \(IAM\)](#). Un rol vinculado a un servicio es un tipo único de rol de IAM que está

vinculado directamente a VPC Resolver. VPC Resolver predefine las funciones vinculadas al servicio e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Una función vinculada a un servicio facilita la configuración de VPC Resolver, ya que no es necesario añadir manualmente los permisos necesarios. VPC Resolver define los permisos de sus funciones vinculadas a servicios y, a menos que se defina lo contrario, solo VPC Resolver puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda asociar a ninguna otra entidad de IAM.

Solo puede eliminar un rol vinculado a servicios después de eliminar los recursos relacionados. Esto protege sus recursos de VPC Resolver porque no puede eliminar el permiso de acceso a los recursos de forma inadvertida.

Para obtener información sobre otros servicios que admiten roles vinculados a servicios, consulte [Servicios de AWS que funcionan con IAM](#) y busque los servicios que muestran Yes (Sí) en la columna Service-Linked Role (Rol vinculado a un servicio). Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Temas

- [Permisos de roles vinculados a servicios para VPC Resolver](#)
- [Creación de un rol vinculado a un servicio para el solucionador de VPC](#)
- [Edición de un rol vinculado a un servicio para VPC Resolver](#)
- [Eliminar un rol vinculado a un servicio para el solucionador de VPC](#)
- [Regiones compatibles con las funciones vinculadas al servicio de resolución de VPC](#)

Permisos de roles vinculados a servicios para VPC Resolver

VPC Resolver utiliza la función **AWSServiceRoleForRoute53Resolver** vinculada al servicio para entregar los registros de consultas en su nombre.

La política de permisos de roles permite a VPC Resolver realizar las siguientes acciones en sus recursos:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs>DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "s3:GetBucketPolicy"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

```
}  
]  
}
```

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte [Permisos de roles vinculados a servicios](#) en la Guía del usuario de IAM.

Creación de un rol vinculado a un servicio para el solucionador de VPC

No necesita crear manualmente un rol vinculado a servicios. Al crear una asociación de configuración del registro de consultas de resolución en la consola, la o la AWS CLI AWS API de Amazon Route 53, VPC Resolver crea el rol vinculado al servicio por usted.

Important

Este rol vinculado a servicios puede aparecer en su cuenta si se ha completado una acción en otro servicio que utilice las características compatibles con este rol. Además, si utilizaba el servicio VPC Resolver antes del 12 de agosto de 2020, cuando comenzó a admitir funciones vinculadas a servicios, VPC Resolver creó la función en su cuenta. `AWSServiceRoleForRoute53Resolver` Para obtener más información, consulte [Un nuevo rol ha aparecido en mi cuenta de IAM](#).

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al crear una asociación de configuración del registro de consultas de Resolver, el rol vinculado a un servicio `AWSServiceRoleForRoute53Resolver` se crea de nuevo automáticamente.

Edición de un rol vinculado a un servicio para VPC Resolver

El solucionador de VPC no permite editar el rol vinculado al `AWSServiceRoleForRoute53Resolver` servicio. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte [Edición de un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Eliminar un rol vinculado a un servicio para el solucionador de VPC

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. Así no tendrá una entidad no utilizada que no se supervise ni mantenga de forma activa. Sin embargo, debe limpiar los recursos de su rol vinculado al servicio antes de eliminarlo manualmente.

Note

Si el servicio de resolución de VPC utiliza el rol al intentar eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos de VPC Resolver utilizados por el

AWSServiceRoleForRoute53Resolver

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. Expanda el menú de la consola de Route 53. En la esquina superior izquierda de la consola, elija el icono de las tres barras horizontales ().
3. En el menú Resolver, elija Registro de consultas.
4. Seleccione la casilla de verificación situada junto al nombre de la configuración del registro de consultas y, a continuación, elija Delete (Eliminar).
5. En el cuadro de texto Delete query logging configuration (Eliminar la configuración del registro de consultas), seleccione Stop logging queries (Detener el registro de consultas).

Esto desasociará la configuración de la VPC. También puede desasociar la configuración del registro de consultas mediante programación. Para obtener más información, consulte [disassociate-resolver-query-log-config](#).

6. Después de que las consultas de registro se hayan detenido, de forma opcional puede escribir **delete** en el campo y elegir Delete (Eliminar) para eliminar la configuración del registro de consultas. No obstante, esta acción no es necesaria para eliminar los recursos que utiliza **AWSServiceRoleForRoute53Resolver**.

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al `AWSServiceRoleForRoute53Resolver` servicio. Para obtener más información, consulte [Eliminación de un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Regiones compatibles con las funciones vinculadas al servicio de resolución de VPC

VPC Resolver no admite el uso de funciones vinculadas a servicios en todas las regiones en las que el servicio está disponible. Puede usar el rol `AWSServiceRoleForRoute53Resolver` en las siguientes regiones.

Nombre de la región	Identidad de la región	Support en VPC Resolver
Este de EE. UU. (Norte de Virginia)	us-east-1	Sí
Este de EE. UU. (Ohio)	us-east-2	Sí
Oeste de EE. UU. (Norte de California)	us-west-1	Sí
Oeste de EE. UU. (Oregón)	us-west-2	Sí
Asia-Pacífico (Mumbai)	ap-south-1	Sí
Asia-Pacífico (Osaka)	ap-northeast-3	Sí
Asia-Pacífico (Seúl)	ap-northeast-2	Sí
Asia-Pacífico (Singapur)	ap-southeast-1	Sí
Asia-Pacífico (Sídney)	ap-southeast-2	Sí
Asia-Pacífico (Tokio)	ap-northeast-1	Sí
Canadá (centro)	ca-central-1	Sí
Europa (Fráncfort)	eu-central-1	Sí
Europa (Irlanda)	eu-west-1	Sí
Europa (Londres)	eu-west-2	Sí

Nombre de la región	Identidad de la región	Support en VPC Resolver
Europa (París)	eu-west-3	Sí
América del Sur (São Paulo)	sa-east-1	Sí
China (Pekín)	cn-north-1	Sí
China (Ningxia)	cn-northwest-1	Sí
AWS GovCloud (US)	us-gov-east-1	Sí
AWS GovCloud (US)	us-gov-west-1	Sí

AWS políticas gestionadas para Amazon Route 53

Una política AWS administrada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir [políticas administradas por el cliente](#) específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte [Políticas administradas por AWS](#) en la Guía del usuario de IAM.

AWS política gestionada: AmazonRoute 53 FullAccess

Puede asociar la política AmazonRoute53FullAccess a las identidades de IAM.

Esta política otorga acceso total a los recursos de Route 53, incluidos el registro de dominios y la comprobación del estado, pero excluye VPC Resolver.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `route53:*`: le permite realizar todas las acciones de Route 53, salvo las siguientes:
 - Cree y actualice registros de alias para los que el valor de Alias Target sea una CloudFront distribución, un balanceador de cargas ELB, un entorno de Elastic Beanstalk o un bucket de Amazon S3. (Con estos permisos, puede crear registros de alias en los que el valor de Alias Target (Destino del alias) es otro registro de la misma zona alojada).
 - Trabajar con zonas alojadas privadas.
 - Trabajar con dominios.
 - Cree, elimine y visualice las alarmas. CloudWatch
 - Renderice CloudWatch las métricas en la consola de Route 53.
- `route53domains:*`: le permite trabajar con dominios.
- `cloudfront:ListDistributions`— Permite crear y actualizar registros de alias para los que el valor de Alias Target es una CloudFront distribución.

Este permiso no es necesario si no está utilizando la consola de Route 53. Route 53 solo lo utiliza para obtener la lista de distribuciones que muestra en la consola.

- `cloudfront:GetDistributionTenantByDomain`— Se utiliza para buscar las distribuciones de CloudFront varios usuarios, lo que permite crear y actualizar registros de alias para los que el valor de Alias Target es un CloudFront arrendatario de distribución.
- `cloudfront:GetConnectionGroup`— Se utiliza para buscar las distribuciones de CloudFront varios inquilinos y así poder crear y actualizar registros de alias para los que el valor de Alias Target es un arrendatario de distribución. CloudFront
- `cloudwatch:DescribeAlarms`— Junto con `sns:ListTopics` y `sns:ListSubscriptionsByTopic`, permite crear, eliminar y ver las alarmas. CloudWatch
- `cloudwatch:GetMetricStatistics`— Permite crear controles de estado CloudWatch métricos.

Estos permisos no son necesarios si no está utilizando la consola de Route 53. Route 53 solo lo utiliza para obtener las estadísticas que muestra en la consola.

- `cloudwatch:GetMetricData`— Le permite mostrar el estado de las métricas de sus controles de CloudWatch estado.
- `ec2:DescribeVpcs`— Le permite mostrar una lista de VPCs.

- `ec2:DescribeVpcEndpoints`: le permite mostrar una lista de puntos de enlace de VPC.
- `ec2:DescribeRegions`: le permite mostrar una lista de zonas de disponibilidad.
- `elasticloadbalancing:DescribeLoadBalancers`: le permite crear y actualizar registros de alias en los que el valor de Alias Target (Destino del alias) es un balanceador de carga de Elastic Load Balancing.

Estos permisos no son necesarios si no está utilizando la consola de Route 53. Route 53 solo lo utiliza para obtener la lista de balanceadores de carga que muestra en la consola.

- `elasticbeanstalk:DescribeEnvironments`: le permite crear y actualizar registros de alias en los que el valor de Alias Target (Destino del alias) es un entorno de Elastic Beanstalk.

Estos permisos no son necesarios si no está utilizando la consola de Route 53. Route 53 solo lo utiliza para obtener la lista de entornos que muestra en la consola.

- `es:ListDomainNames`— Te permite mostrar los nombres de todos los dominios de Amazon OpenSearch Service que son propiedad del usuario actual en la región activa.
- `es:DescribeDomains`— Le permite obtener la configuración de dominio para los dominios de Amazon OpenSearch Service especificados.
- `lightsail:GetContainerServices`— Le permite utilizar los servicios de contenedores de Lightsail para crear y actualizar registros de alias para los que el valor de Alias Target es un dominio de Lightsail.
- `s3:ListBucket`, `s3:GetBucketLocation` y `s3:GetBucketWebsite`: le permiten crear y actualizar registros de alias en los que el valor de Alias Target (Destino del alias) es un bucket de Amazon S3. (Puede crear un alias para un bucket de Amazon S3 solo si el bucket está configurado como el punto de conexión de un sitio web; `s3:GetBucketWebsite` obtiene la información de configuración necesaria).

Estos permisos no son necesarios si no está utilizando la consola de Route 53. Route 53 solo lo utiliza para obtener la lista de buckets que se van a mostrar en la consola.

- `sns:ListTopics`, `sns:ListSubscriptionsByTopic`, `cloudwatch:DescribeAlarms` — Le permiten crear, eliminar y ver las alarmas. CloudWatch
- `tag:GetResources`: le permite mostrar las etiquetas de sus recursos. Por ejemplo, los nombres de sus comprobaciones de estado.
- `apigateway:GET`: le permite crear y actualizar registros de alias en los que el valor de Alias Target (Destino del alias) es una API de Amazon API Gateway.

Para obtener más información acerca de los permisos, consulte [Permisos de la API de Amazon Route 53: referencia de acciones, recursos y condiciones](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "route53:*",
        "route53domains:*",
        "cloudfront:ListDistributions",
        "cloudfront:GetDistributionTenantByDomain",
        "cloudfront:GetConnectionGroup",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRegions",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticbeanstalk:DescribeEnvironments",
        "es:ListDomainNames",
        "es:DescribeDomains",
        "lightsail:GetContainerServices",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketWebsite",
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "tag:GetResources"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "apigateway:GET",
      "Resource": "arn:aws:apigateway:*::/domainnames"
    }
  ]
}
```

```
}
```

AWS política gestionada: AmazonRoute 53 ReadOnlyAccess

Puede asociar la política AmazonRoute53ReadOnlyAccess a las identidades de IAM.

Esta política otorga acceso de solo lectura a los recursos de Route 53, incluidos el registro de dominios y la comprobación del estado, pero excluye VPC Resolver.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `route53:Get*`: obtiene los recursos de Route 53.
- `route53:List*`: muestra los recursos de Route 53.
- `route53:TestDNSAnswer`: obtiene el valor que Route 53 devuelve como respuesta a una solicitud de DNS.

Para obtener más información acerca de los permisos, consulte [Permisos de la API de Amazon Route 53: referencia de acciones, recursos y condiciones](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "route53:Get*",
        "route53:List*",
        "route53:TestDNSAnswer"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

AWS política administrada: 53 AmazonRoute DomainsFullAccess

Puede asociar la política AmazonRoute53DomainsFullAccess a las identidades de IAM.

Esta política concede acceso completo a los recursos de registro de dominios de Route 53.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `route53:CreateHostedZone`: le permite crear una zona alojada de Route 53.
- `route53domains:*`: le permite registrar nombres de dominio y realizar operaciones relacionadas.

Para obtener más información acerca de los permisos, consulte [Permisos de la API de Amazon Route 53: referencia de acciones, recursos y condiciones](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "route53:CreateHostedZone",
        "route53domains:*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

AWS política gestionada: AmazonRoute 53 DomainsReadOnlyAccess

Puede asociar la política AmazonRoute53DomainsReadOnlyAccess a las identidades de IAM.

Esta política concede acceso de solo lectura a los recursos de registro de dominios de Route 53.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `route53domains:Get*`: le permite recuperar una lista de dominios de Route 53.
- `route53domains:List*`: le permite mostrar una lista de dominios de Route 53.

Para obtener más información acerca de los permisos, consulte [Permisos de la API de Amazon Route 53: referencia de acciones, recursos y condiciones](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "route53domains:Get*",
        "route53domains:List*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

AWS política gestionada: AmazonRoute 53 ResolverFullAccess

Puede asociar la política AmazonRoute53ResolverFullAccess a las identidades de IAM.

Esta política otorga acceso total a los recursos de VPC Resolver de Route 53.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `route53resolver:*`— Le permite crear y administrar los recursos de VPC Resolver en la consola de Route 53.

- `ec2:DescribeSubnets`: le permite mostrar una lista de las subredes de Amazon VPC.
- `ec2:CreateNetworkInterface`, `ec2>DeleteNetworkInterface`, y `ec2:ModifyNetworkInterfaceAttribute`: le permiten crear, modificar y eliminar interfaces de red.
- `ec2:DescribeNetworkInterfaces`: le permite mostrar una lista de interfaces de red.
- `ec2:DescribeSecurityGroups`: le permite mostrar una lista de todos los grupos de seguridad.
- `ec2:DescribeVpcs`— Permite mostrar una lista de VPCs.
- `ec2:DescribeAvailabilityZones`: le permite mostrar una lista de las zonas que hay disponibles.

Para obtener más información acerca de los permisos, consulte [Permisos de la API de Amazon Route 53: referencia de acciones, recursos y condiciones](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AmazonRoute53ResolverFullAccess",
      "Effect": "Allow",
      "Action": [
        "route53resolver:*",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```



```
}
```

AWS política gestionada: AmazonRoute 53 ResolverReadOnlyAccess

Puede asociar la política AmazonRoute53ResolverReadOnlyAccess a las identidades de IAM.

Esta política otorga acceso de solo lectura a los recursos de VPC Resolver de Route 53.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `route53resolver:Get*`— Obtiene los recursos de VPC Resolver.
- `route53resolver:List*`— Le permite mostrar una lista de recursos de VPC Resolver.
- `ec2:DescribeNetworkInterfaces`: le permite mostrar una lista de interfaces de red.
- `ec2:DescribeSecurityGroups`: le permite mostrar una lista de todos los grupos de seguridad.

Para obtener más información sobre los permisos, consulte [Permisos de la API de Amazon Route 53: referencia de acciones, recursos y condiciones](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AmazonRoute53ResolverReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "route53resolver:Get*",
        "route53resolver:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

```
}  
]  
}
```

AWS política gestionada: Route53 ResolverServiceRolePolicy

No puede asociar Route53ResolverServiceRolePolicy a sus entidades IAM. Esta política se adjunta a una función vinculada a un servicio que permite a Route 53 VPC Resolver acceder a los AWS servicios y recursos que VPC Resolver utiliza o administra. Para obtener más información, consulte [Usar roles vinculados a servicios en Amazon Route 53 Resolver](#).

AWS política administrada: 53 AmazonRoute ProfilesFullAccess

Puede asociar la política AmazonRoute53ProfilesReadOnlyAccess a las identidades de IAM.

Esta política concede acceso completo a los recursos de perfil de Amazon Route 53.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- route53profiles: le permite crear y administrar recursos de perfil en la consola de Route 53.
- ec2— Permite a los directores obtener información sobre VPCs.

Para obtener más información acerca de los permisos, consulte [Permisos de la API de Amazon Route 53: referencia de acciones, recursos y condiciones](#).

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "AmazonRoute53ProfilesFullAccess",  
      "Effect": "Allow",  
      "Action": [  
        "route53profiles:AssociateProfile",  
        "route53profiles:AssociateResourceToProfile",  
        "route53profiles:CreateProfile",
```

```

        "route53profiles:DeleteProfile",
        "route53profiles:DisassociateProfile",
        "route53profiles:DisassociateResourceFromProfile",
        "route53profiles:UpdateProfileResourceAssociation",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:GetProfilePolicy",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:PutProfilePolicy",
        "route53profiles:ListTagsForResource",
        "route53profiles:TagResource",
        "route53profiles:UntagResource",
        "route53resolver:GetFirewallConfig",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverRule",
        "ec2:DescribeVpcs",
        "route53:GetHostedZone"
    ],
    "Resource": [
        "*"
    ]
}
]
}

```

AWS política gestionada: 53 AmazonRoute ProfilesReadOnlyAccess

Puede asociar la política AmazonRoute53ProfilesReadOnlyAccess a las identidades de IAM.

Esta política concede acceso de solo lectura a los recursos de perfil de Amazon Route 53.

Detalles de los permisos

Para obtener más información acerca de los permisos, consulte [Permisos de la API de Amazon Route 53: referencia de acciones, recursos y condiciones](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AmazonRoute53ProfilesReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:GetProfilePolicy",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:GetFirewallConfig",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverQueryLogConfig"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Route 53 actualiza las políticas AWS gestionadas

Vea los detalles sobre las actualizaciones de las políticas AWS administradas de Route 53 desde que este servicio comenzó a rastrear estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la [página de historial de documentos](#) de Route 53.

Cambio	Descripción	Fecha
AmazonRoute53 FullAccess — Política actualizada	Agrega permisos para <code>cloudwatch:GetMetricData</code> , <code>tag:GetResources</code> , <code>es:ListDomainNames</code> , <code>es:DescribeDomains</code> , <code>cloudfront:GetDistributionTenantByDomain</code> , <code>cloudfront:GetConnectionGroup</code> y <code>lightsail:GetContainerServices</code> . Estos permisos le permiten obtener hasta 500 métricas de chequeos de CloudWatch estado, hasta 100 nombres de chequeos de estado, obtener la configuración de dominio para los dominios de Amazon OpenSearch Service especificados y enumerar los nombres de todos los dominios de Amazon OpenSearch Service propiedad del usuario actual en la región activa, obtener las distribuciones CloudFront multiusuario y obtener los servicios de contenedores de Lightsail.	1 de junio de 2025
AmazonRoute53 ProfilesFullAccess — Política actualizada	Agrega permisos para <code>GetProfilePolicy</code> y <code>PutProfilePolicy</code> . Estas son acciones de IAM solo de	27 de agosto de 2024

Cambio	Descripción	Fecha
	permiso. Si a un director de IAM no se le conceden estos permisos, se producirá un error al intentar compartir el perfil mediante el AWS RAM servicio.	
AmazonRoute53 ProfilesReadOnlyAccess — Política actualizada	Agrega permisos para <code>GetProfilePolicy</code> . Esta es una acción de IAM que solo requiere permisos. Si a un director de IAM no se le ha concedido este permiso, se producirá un error al intentar acceder a la política del perfil mediante el AWS RAM servicio.	27 de agosto de 2024
AmazonRoute53 ResolverFullAccess — Política actualizada	Se agregó un ID de instrucción (Sid) para identificar, de forma exclusiva, la política.	5 de agosto de 2024
AmazonRoute53 ResolverReadOnlyAccess — Política actualizada	Se agregó un ID de instrucción (Sid) para identificar, de forma exclusiva, la política.	5 de agosto de 2024
AmazonRoute53 — Nueva política ProfilesFullAccess	Amazon Route 53 agregó una nueva política para permitir acceso completo a los recursos de perfil de Amazon Route 53.	22 de abril de 2024

Cambio	Descripción	Fecha
AmazonRoute53 ProfilesReadOnlyAccess — Nueva política	Amazon Route 53 agregó una nueva política para permitir acceso de solo lectura a los recursos de perfil de Amazon Route 53.	22 de abril de 2024
Ruta 53 ResolverServiceRolePolicy — Nueva política	Amazon Route 53 agregó una nueva política asociada a un rol vinculado a un servicio que permite a VPC Resolver acceder a los AWS servicios y recursos que Resolver utiliza o administra.	14 de julio de 2021
AmazonRoute53 — Nueva política ResolverReadOnlyAccess	Amazon Route 53 agregó una nueva política para permitir el acceso de solo lectura a los recursos de VPC Resolver.	14 de julio de 2021
AmazonRoute53 — Nueva política ResolverFullAccess	Amazon Route 53 agregó una nueva política para permitir el acceso total a los recursos de VPC Resolver.	14 de julio de 2021
AmazonRoute53 DomainsReadOnlyAccess — Nueva política	Amazon Route 53 agregó una nueva política para permitir acceso de solo lectura a los recursos de dominios de Route 53.	14 de julio de 2021
AmazonRoute53 DomainsFullAccess — Nueva política	Amazon Route 53 agregó una nueva política para permitir acceso completo a los recursos de dominios de Route 53.	14 de julio de 2021

Cambio	Descripción	Fecha
AmazonRoute53 ReadOnlyAccess — Nueva política	Amazon Route 53 agregó una nueva política para permitir acceso de solo lectura a los recursos de Route 53.	14 de julio de 2021
AmazonRoute53 FullAccess — Nueva política	Amazon Route 53 agregó una nueva política para permitir acceso completo a los recursos de Route 53.	14 de julio de 2021
Route 53 comenzó el seguimiento de los cambios	Route 53 comenzó a rastrear los cambios en sus políticas AWS administradas.	14 de julio de 2021

Uso de condiciones de las políticas de IAM para control de acceso preciso

En Route 53, puede especificar las condiciones al conceder permisos utilizando la política de IAM (consulte [Control de acceso](#)). Por ejemplo, puede hacer lo siguiente:

- Conceda permisos para permitir el acceso a un único conjunto de registros de recursos.
- Conceda permisos para que los usuarios puedan acceder a todos los conjuntos de registros de recursos de un tipo de registro de DNS específico en una zona alojada, por ejemplo, los registros A y AAAA.
- Conceda permisos para que los usuarios puedan acceder a un conjunto de registros de recursos en el que su nombre contenga una cadena específica.
- Otorgue permisos para que los usuarios puedan realizar solo un subconjunto de CREATE | UPSERT | DELETE las acciones en la consola de Route 53 o cuando usen la API. [ChangeResourceRecordSets](#)
- Otorgue permisos para permitir a los usuarios asociar o disociar zonas alojadas privadas de una VPC determinada.
- Otorgue permisos para permitir a los usuarios enumerar las zonas alojadas asociadas a una VPC determinada.
- Otorgue permisos para permitir a los usuarios acceder a crear una nueva zona alojada privada y asociarla a una VPC determinada.

- Otorgue permisos para permitir a los usuarios crear o eliminar una autorización de asociación de VPC.

También puede crear permisos que combinen cualquiera de los permisos granulares.

Normalización de los valores clave de la condición de Route 53

Los valores que ingrese para las condiciones de la política deben formatearse o normalizarse de la siguiente manera:

Para **route53:ChangeResourceRecordSetsNormalizedRecordNames**:

- Todas las letras deben estar en minúsculas.
- El nombre de DNS debe estar sin el punto final.
- Los caracteres que no sean a-z, 0-9, - (guion), _ (guion bajo) y . (punto, como delimitador entre etiquetas) deben utilizar códigos de escape con el formato \código octal de tres dígitos. Por ejemplo, \052 es el código octal del carácter *.

Para **route53:ChangeResourceRecordSetsActions**, el valor puede ser cualquiera de los siguientes y debe estar en mayúscula:

- CREATE
- UPSERT
- DELETE

Para **route53:ChangeResourceRecordSetsRecordTypes**:

- El valor debe estar en mayúsculas y puede ser cualquiera de los tipos de registro de DNS compatibles con Route 53. Para obtener más información, consulte [Tipos de registros de DNS admitidos](#).

Para **route53:VPCs**:

- El formato del valor debe ser VPCId=<vpc-id>, VPCRegion=<region>.
- El valor de <vpc-id> y <region> debe expresarse en letras minúsculas, como VPCId=vpc-123abc y VPCRegion=us-east-1.

- Las claves de contexto y los valores distinguen entre mayúsculas y minúsculas.

 Important

Para que sus permisos permitan o restrinjan las acciones que quiera, debe seguir estas convenciones. Esta clave de condición solo VPCId acepta los VPCRegion elementos; por ejemplo, no se admiten otros AWS recursos. Cuenta de AWS

Puede utilizar [Access Analyzer](#) o [Policy Simulator](#) de la Guía del usuario de IAM para validar que la política conceda o restrinja los permisos según lo previsto. Para validar los permisos, también puede aplicar una política de IAM a un usuario o rol de prueba para llevar a cabo las operaciones de Route 53.

Especificación de condiciones: uso de claves de condición

AWS proporciona un conjunto de claves de condición AWS predefinidas (claves de condición generales) para todos los AWS servicios que admiten la IAM para el control de acceso. Por ejemplo, puede usar la clave de condición `aws:SourceIp` para comprobar la dirección IP del solicitante antes de permitir que se lleve a cabo cualquier acción. Para obtener más información y una lista con las claves generales de AWS, consulte [Available Keys for Conditions](#) (Claves disponibles para las condiciones) en la Guía del usuario de IAM.

 Note

Route 53 no admite claves de condición basadas en etiquetas.

En la siguiente tabla se muestran las claves de condición específicas del servicio Route 53 que se aplican a Route 53.

Clave de condición de Route 53	Operaciones de la API	Tipo de valor	Description (Descripción)
route53:ChangeReso		Multivalor	Representa una lista de nombres de registros DNS incluidos en la solicitud de. ChangeRes

Clave de condición de Route 53	Operaciones de la API	Tipo de valor	Description (Descripción)
sourceRecordSetsNormalizedRecordNames	ChangeResourceRecordSets		sourceRecordSets Para obtener el comportamiento esperado, los nombres de DNS de la política de IAM se deben normalizar de la siguiente manera: • Todas las letras deben estar en minúsculas. • El nombre de DNS debe estar sin el punto final. • Los caracteres que no sean de la A a la Z, del 0 al 9, - (guion), _ (guion bajo) y . (punto, como delimitador entre etiquetas) deben utilizar códigos de escape con el formato \código octal de tres dígitos.
route53:ChangeResourceRecordTypes	ChangeResourceRecordSets	Multivalor	Representa una lista de tipos de registros de DNS en la solicitud de ChangeResourceRecordSets . ChangeResourceRecordTypes puede ser cualquiera de los tipos de registros de DNS compatibles con Route 53. Para obtener más información, consulte Tipos de registros de DNS admitidos. En la política, todo se debe escribir en mayúsculas.

Clave de condición de Route 53	Operaciones de la API	Tipo de valor	Description (Descripción)
route53:ChangeResourceRecordSetsActions	ChangeResourceRecordSets	Multivalor	Representa una lista de acciones en la solicitud de ChangeResourceRecordSets . ChangeResourceRecordSetsActions puede ser cualquiera de los siguientes valores (debe estar en mayúscula): • CREATE • UPSERT • DELETE

Clave de condición de Route 53	Operaciones de la API	Tipo de valor	Description (Descripción)
route53:VPCs	Asociado VPCWith HostedZone Disociar VPCFrom HostedZone ListHostedZonesByVPC CreateHostedZone Crear autorización VPCAssociation Eliminar VPCAssociation autorización	Multivalor	Representa una lista de VPCs en la solicitud de AssociateVPCWithHostedZone, DisassociateVPCFromHostedZone, ListHostedZonesByVPC, CreateHostedZone, CreateVPCAssociationAuthorization, y DeleteVPCAssociationAuthorization, con el formato de "VPCId=<vpc-id>, VPCRegion = <region>

Ejemplos de políticas: uso de condiciones para el acceso preciso

Cada uno de los ejemplos de esta sección establece en la cláusula Effect el valor Allow y especifica solamente las acciones, los recursos y los parámetros que se permiten. Únicamente se permite el acceso a aquello que se indica explícitamente en la política de IAM.

En algunos casos, se pueden modificar estas políticas de tal forma que se basen en la denegación (en cuyo caso, se establecería la cláusula Effect en Allow y se invertiría toda la lógica de la política). Sin embargo, recomendamos evitar el uso de políticas basadas en la denegación, ya que son

difíciles de escribir correctamente en comparación con las políticas basadas el permiso. Esto es especialmente cierto para Route 53 debido a la normalización del texto que se requiere.

Concesión de permisos que limitan el acceso a los registros de DNS con nombres específicos

La siguiente política de permisos otorga permisos que permiten acciones de `ChangeResourceRecordSets` en la zona alojada `Z12345` para `ejemplo.com.` y `marketing.ejemplo.com.` Utiliza la clave de condición `route53:ChangeResourceRecordSetsNormalizedRecordNames` para limitar las acciones del usuario solo en los registros que coincidan con los nombres especificados.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "route53:ChangeResourceRecordSets",
      "Resource": "arn:aws:route53::hostedzone/Z111111122222233333",
      "Condition": {
        "ForAllValues:StringEquals": {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames":
            ["example.com", "marketing.example.com"]
        }
      }
    }
  ]
}
```

`ForAllValues:StringEquals` es un operador de condición de IAM que se aplica a claves con varios valores. La condición de la política anterior permitirá la operación solo cuando todos los cambios en `ChangeResourceRecordSets` tengan el nombre de DNS `example.com`. Para obtener más información, consulte [IAM condition operators](#) (Operadores de condición de IAM) y [IAM condition with multiple keys or values](#) (Condición de IAM con varias claves o valores) en la Guía del usuario de IAM.

Para implementar el permiso que hace coincidir nombres con ciertos sufijos, puede usar el comodín de IAM (*) en la política con el operador de condición `StringLike` o `StringNotLike`.

La siguiente política permitirá la operación cuando todos los cambios en la operación `ChangeResourceRecordSets` tengan nombres de DNS que terminen en “-beta.example.com”.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "route53:ChangeResourceRecordSets",
      "Resource": "arn:aws:route53::hostedzone/Z1111111222222333333",
      "Condition": {
        "ForAllValues:StringLike": {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames":
            ["*-beta.example.com"]
        }
      }
    }
  ]
}
```

 Note

El comodín de IAM no es el mismo que el comodín del nombre de dominio. Consulte el siguiente ejemplo para saber cómo utilizar el comodín con un nombre de dominio.

Concesión de permisos que limiten el acceso a los registros de DNS que coincidan con un nombre de dominio que tenga un comodín

La siguiente política de permisos concede permisos que autorizan acciones `ChangeResourceRecordSets` en la zona alojada Z12345 para example.com. Utiliza la clave de condición `route53:ChangeResourceRecordSetsNormalizedRecordNames` para limitar las acciones del usuario solo a los registros que coincidan con *.example.com.

JSON

```
{
```

```

    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": "route53:ChangeResourceRecordSets",
        "Resource": "arn:aws:route53::hostedzone/Z1111111222222333333",
        "Condition": {
          "ForAllValues:StringEquals": {
            "route53:ChangeResourceRecordSetsNormalizedRecordNames": ["\
\052.example.com"]
          }
        }
      }
    ]
  }

```

\052 es el código octal del carácter * del nombre de DNS, y \ en \052 es un carácter de escape que significa \\ para seguir la sintaxis JSON.

Concesión de permisos que limiten el acceso a los registros de DNS específicos

La siguiente política de permisos concede permisos que autorizan acciones

ChangeResourceRecordSets en la zona alojada Z12345 para example.com. Utiliza la combinación de tres claves de condición para limitar las acciones del usuario y permitir solo la creación o edición de registros de DNS con un nombre y un tipo de DNS determinados.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "route53:ChangeResourceRecordSets",
      "Resource": "arn:aws:route53::hostedzone/Z1111111222222333333",
      "Condition": {
        "ForAllValues:StringEquals": {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames":
["example.com"],
          "route53:ChangeResourceRecordSetsRecordTypes": ["MX"],

```



```

    "route53:ChangeResourceRecordSetsActions": ["CREATE",
    "UPSERT"]
  }
}

```

Concesión de permisos que limiten el acceso a la creación y edición solo de los tipos de registros de DNS especificados

La siguiente política de permisos concede permisos que autorizan acciones `ChangeResourceRecordSets` en la zona alojada `Z12345` para `example.com`. Utiliza la clave de condición `route53:ChangeResourceRecordSetsRecordTypes` para limitar las acciones del usuario solo en los registros que coincidan con los tipos especificados (A y AAAA).

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "route53:ChangeResourceRecordSets",
      "Resource": "arn:aws:route53::hostedzone/Z11111112222222333333",
      "Condition": {
        "ForAllValues:StringEquals": {
          "route53:ChangeResourceRecordSetsRecordTypes": ["A", "AAAA"]
        }
      }
    }
  ]
}

```

Otorgamiento de permisos que especifiquen la VPC en la que la entidad principal de IAM puede operar

La siguiente política de permisos otorga permisos que permiten acciones `AssociateVPCWithHostedZone`, `DisassociateVPCFromHostedZone`,

ListHostedZonesByVPC, CreateHostedZone, CreateVPCAssociationAuthorization y DeleteVPCAssociationAuthorization en la VPC especificada por el vpc-id.

 Important

El formato del valor de condición debe ser VPCId=<vpc-id>,VPCRegion=<region>. Si especifica un ARN de VPC en el valor de condición, la clave de condición no surtirá efecto.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "route53:*"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringLike": {
          "route53:VPCs": [
            "VPCId=<vpc-id>,VPCRegion=<region>"
          ]
        }
      }
    },
    {
      "Sid": "Statement2",
      "Effect": "Allow",
      "Action": "ec2:DescribeVpcs",
      "Resource": "*"
    }
  ]
}
```

Permisos de la API de Amazon Route 53: referencia de acciones, recursos y condiciones

Al configurar [Control de acceso](#) y redactar una política de permisos que pueda adjuntar a una identidad de IAM (políticas basadas en la identidad), puede utilizar las listas de acciones, recursos y claves de condición para [Route 53, acciones, recursos y claves de condición para los dominios de Route 53, acciones, recursos y claves de condición para VPC Resolver, y las claves de condición, recursos y acciones para los perfiles de Amazon Route 53 permiten compartir la configuración de DNS con VPCs](#) la referencia de autorización de servicio. Las páginas incluyen cada acción de la API de Amazon Route 53, las acciones a las que debe conceder permisos de acceso y el AWS recurso al que debe conceder acceso. Las acciones se especifican en el campo Action de la política y el valor del recurso se especifica en el campo Resource de la política.

Puede usar claves AWS de condición generales en sus políticas de Route 53 para expresar las condiciones. Para obtener una lista completa de las claves AWS anchas, consulta las [claves disponibles](#) en la Guía del usuario de IAM.

Note

Al conceder acceso, la zona alojada y Amazon VPC deben pertenecer a la misma partición. Una partición es un grupo de. Regiones de AWS Cada una Cuenta de AWS tiene el alcance de una partición.

Las siguientes son las particiones admitidas:

- aws - Regiones de AWS
- aws-cn - Regiones de China
- aws-us-gov - AWS GovCloud (US) Region

Para obtener más información, consulte [Administración de acceso](#) en la Referencia general de AWS .

Note

Para especificar una acción, use el prefijo correspondiente (route53, route53domains o route53resolver) seguido del nombre de operación de API, por ejemplo:

- `route53:CreateHostedZone`
- `route53domains:RegisterDomain`
- `route53resolver:CreateResolverEndpoint`

Registro y monitoreo en Amazon Route 53

Amazon Route 53 proporciona el registro de consultas de DNS y la posibilidad de monitorear sus recursos con comprobaciones de estado. Además, Route 53 se integra con otros AWS servicios para proporcionar registros y monitoreo adicionales:

Registrar consultas de DNS

Puede configurar Route 53 para registrar información acerca de las consultas que Route 53 recibe; por ejemplo, el dominio o subdominio que se ha solicitado, la fecha y la hora de la solicitud, y el tipo de registro de DNS, como, por ejemplo, A o AAAA.

Para obtener más información, consulte [Registro de consultas de DNS públicas](#).

Se utiliza AWS CloudTrail para registrar las acciones programáticas y de la consola

CloudTrail proporciona un registro de las acciones de Route 53 realizadas por un usuario, un rol o un AWS servicio. Con la información recopilada por CloudTrail, puede realizar un seguimiento de las solicitudes que se realizan, las direcciones IP de las que se originan las solicitudes, quién realizó la solicitud, cuándo se realizó y detalles adicionales. Para obtener más información, consulte [Registrar llamadas a la API de Amazon Route 53 con AWS CloudTrail](#).

Monitorizar los registros de dominios

El panel de Route 53 ofrece información detallada sobre el estado de sus registros de dominios; por ejemplo, el estado de las transferencias de dominios y los dominios que se aproximan a la fecha de vencimiento.

Para obtener más información, consulte [Monitorizar los registros de dominios](#).

Uso de los controles de estado de Route 53 y Amazon CloudWatch para monitorear sus recursos

Puede supervisar sus recursos mediante la creación de controles de estado de Route 53, que se utilizan CloudWatch para recopilar y procesar datos sin procesar para convertirlos en métricas legibles y prácticamente en tiempo real.

Para obtener más información, consulte [Supervisión de sus recursos con los controles de estado de Amazon Route 53 y Amazon CloudWatch](#).

Uso de Amazon CloudWatch para monitorear los puntos finales de VPC Resolver de Route 53

Se puede utilizar CloudWatch para supervisar la cantidad de consultas de DNS que reenvían los puntos finales del Resolver.

Para obtener más información, consulte [Supervisión de los puntos finales de resolución de VPC de Route 53 con Amazon CloudWatch](#).

Usando AWS Trusted Advisor

Trusted Advisor se basa en las mejores prácticas aprendidas al atender a AWS los clientes. Trusted Advisor inspecciona su AWS entorno y, a continuación, hace recomendaciones cuando existen oportunidades para ahorrar dinero, mejorar la disponibilidad y el rendimiento del sistema o ayudar a cerrar las brechas de seguridad. Todos AWS los clientes tienen acceso a cinco Trusted Advisor controles. Los clientes con un plan de asistencia empresarial o empresarial pueden ver todos los Trusted Advisor cheques.

Para obtener más información, consulte [Trusted Advisor](#).

Validación de la conformidad en Amazon Route 53

Los auditores externos evalúan la seguridad y el cumplimiento de Amazon Route 53 como parte de varios programas de AWS cumplimiento. Estos incluyen SOC, PCI, FedRAMP, HIPAA y otros.

Para obtener una lista de AWS los servicios incluidos en el ámbito de los programas de conformidad específicos, consulte [AWS los servicios incluidos en el ámbito de aplicación por programa de conformidad](#). Para obtener información general, consulte [Programas de conformidad de AWS](#).

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulta [Descarga de informes en AWS Artifact](#).

Su responsabilidad de conformidad al utilizar Route 53 se determina en función de la confidencialidad de los datos, los objetivos de conformidad de su empresa, así como de la legislación y los reglamentos aplicables. Si su uso de Route 53 está sujeto al cumplimiento de estándares como HIPAA, PCI o FedRAMP, proporciona recursos para ayudarlo a: AWS

- Guías de [inicio rápido sobre seguridad y cumplimiento: estas guías](#) de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en la seguridad y el cumplimiento. AWS
- [Documento técnico sobre arquitectura para seguridad y conformidad de HIPAA](#) : en este documento técnico, se describe cómo las empresas pueden utilizar AWS para crear aplicaciones conformes con HIPAA.
- [AWS Recursos de conformidad](#): esta colección de libros de trabajo y guías puede aplicarse a su sector y ubicación.
- [AWS Config](#)— Este AWS servicio evalúa en qué medida las configuraciones de sus recursos cumplen con las prácticas internas, las directrices del sector y las normativas.
- [AWS Security Hub CSPM](#)— Este AWS servicio proporciona una visión integral del estado de su seguridad AWS que le ayuda a comprobar el cumplimiento de los estándares y las mejores prácticas del sector de la seguridad.

Resiliencia en Amazon Route 53

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. AWS Las regiones proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre zonas de disponibilidad sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Route 53 divide su funcionalidad en un plano de control y un plano de datos. El servicio Route 53, como la mayoría de servicios de AWS incluye un plano de control que permite realizar operaciones de gestión como la creación, actualización y eliminación de recursos, y un plano de datos que proporciona la funcionalidad principal del servicio. Para más información sobre los planos de control y de datos en Route 53, consulte [Conceptos de plano de datos y control](#).

Route 53 es principalmente un servicio global, pero las siguientes funciones son compatibles con las regiones: AWS

- Si usa Route 53 VPC Resolver para configurar configuraciones híbridas, crea puntos de conexión en AWS las regiones que elija y especifica las direcciones IP en varias zonas de disponibilidad. Para los puntos de enlace de salida, cree reglas en la misma región en la que haya creado el

puntos de conexión. Para obtener más información, consulte [¿Qué es el solucionador de VPC Route 53?](#).

- Puede configurar las comprobaciones de estado de Route 53 para comprobar el estado de los recursos que cree en regiones específicas, como las EC2 instancias de Amazon y los balanceadores de carga ELB.
- Al crear una comprobación de estado que monitorea un punto de conexión, si lo desea, puede especificar las regiones en las que quiere que Route 53 realice las comprobaciones de estado.

Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte Infraestructura [AWS global](#).

Seguridad de la infraestructura en Amazon Route 53

Como servicio gestionado, Amazon Route 53 está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte [Seguridad AWS en la nube](#). Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte [Protección de infraestructuras en un marco](#) de buena AWS arquitectura basado en el pilar de la seguridad.

Las llamadas a la API AWS publicadas se utilizan para acceder a Route 53 a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Envío de resultados desde Resolver DNS Firewall a Security Hub (CSPM)

[AWS Security Hub CSPM](#) le proporciona una visión completa del estado de su seguridad AWS y le ayuda a comparar su entorno con los estándares y las mejores prácticas del sector de la seguridad. Security Hub CSPM recopila datos de seguridad de todos Cuentas de AWS los productos de socios externos compatibles y los ayuda a analizar las tendencias de seguridad e identificar los problemas de seguridad más prioritarios. Servicios de AWS

Al integrar Resolver DNS Firewall con el Security Hub CSPM, puede enviar los resultados del DNS Firewall al Security Hub CSPM. Luego, Security Hub CSPM incluye esos hallazgos en su análisis de su postura de seguridad.

Contenido

- [Cómo funcionan los hallazgos en Security Hub \(CSPM\)](#)
 - [Tipos de resultados que envía DNS Firewall](#)
 - [Reintentarlo cuando el CSPM de Security Hub no está disponible](#)
 - [Actualización de resultados existentes en el CSPM de Security Hub](#)
- [Resultado típico de DNS Firewall](#)
- [Habilitación y configuración de la integración](#)
- [Detener la entrega de los hallazgos a Security Hub \(CSPM\)](#)

Cómo funcionan los hallazgos en Security Hub (CSPM)

En el CSPM de Security Hub, un resultado es un registro observable de una comprobación de seguridad o de una detección relacionada con la seguridad. Algunos hallazgos provienen de problemas detectados por otros socios Servicios de AWS o por terceros. Security Hub CSPM también tiene sus propios controles de seguridad que utiliza para detectar problemas de seguridad y generar hallazgos.

El CSPM de Security Hub proporciona herramientas para administrar resultados procedentes de todos estos orígenes. Puede ver y filtrar listas de resultados y ver los detalles de un resultado. Para obtener más información, consulte [Revisar los detalles de búsqueda y el historial de búsquedas en Security Hub CSPM](#) en la Guía del AWS Security Hub usuario. También puede actualizar los

resultados automáticamente o enviarlos a una acción personalizada. Para obtener más información, consulte [Modificación automática de los hallazgos del CSPM de Security Hub y adopción de medidas](#) al respecto en la Guía del AWS Security Hub usuario.

Todos los resultados del CSPM de Security Hub utilizan un formato JSON estándar denominado AWS Security Finding Format (ASFF). El ASFF incluye detalles sobre el origen del problema de seguridad, los recursos afectados y el estado actual del resultado. Para obtener más información, consulte [AWS Security Finding Format \(ASFF\)](#) en la Guía del usuario de AWS Security Hub .

El DNS Firewall es uno de los Servicios de AWS que envía los resultados al Security Hub CSPM.

Tipos de resultados que envía DNS Firewall

DNS Firewall tiene las siguientes integraciones:

- Listas de dominios gestionadas: datos de seguridad relacionados con consultas bloqueadas o sobre las que se ha alertado sobre los dominios asociados a las listas de dominios AWS gestionadas.
- Listas de dominios personalizadas: resultados de seguridad relacionados con consultas bloqueadas o con alertas para dominios asociados a la lista de dominios del cliente.
- DNS Firewall Advanced: resultados de seguridad relacionados con consultas bloqueadas o con alertas emitidas por DNS Firewall Advanced.

Security Hub CSPM ingiere los resultados del firewall de DNS en el [formato de búsqueda de AWS seguridad](#) (ASFF). En ASFF, el campo Types proporciona el tipo de resultado. Los resultados de DNS Firewall pueden tener los siguientes valores para Types.

- TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation

Reintentarlo cuando el CSPM de Security Hub no está disponible

Si el CSPM de Security Hub no está disponible, DNS Firewall vuelve a intentar enviar los resultados hasta que los reciba.

Actualización de resultados existentes en el CSPM de Security Hub

DNS Firewall actualizará los resultados existentes si se vuelve a observar el mismo resultado.

Resultado típico de DNS Firewall

Security Hub CSPM ingiere los hallazgos del firewall de DNS en el [formato de búsqueda de AWS seguridad \(ASFF\)](#).

Este es un ejemplo de un resultado típico de DNS Firewall en ASFF.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "00000000-0000-0000-0000-example1",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/amazon/route-53-resolver-dns-firewall-aws-list",
  "ProductName": "Route 53 Resolver DNS Firewall - AWS List",
  "CompanyName": "Amazon",
  "Region": "us-east-1",
  "GeneratorId": "arn:aws:route53resolver:us-east-1:000000000000:firewall-rule-group/rslvr-frg-example1",
  "AwsAccountId": "000000000000",
  "Types": [
    "TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation"
  ],
  "FirstObservedAt": "2024-12-06T19:58:49.000Z",
  "LastObservedAt": "2024-12-06T19:58:49.000Z",
  "CreatedAt": "2024-12-06T19:58:49.000Z",
  "UpdatedAt": "2024-12-06T19:58:49.000Z",
  "Severity": {
    "Label": "HIGH",
    "Normalized": 70
  },
  "Title": "DNS Firewall ALERT generated for domain example1.com. from VPC vpc-example1",
  "Description": "DNS Firewall ALERT",
  "ProductFields": {
    "aws/route53resolver/dnsfirewall/queryName": "example1.com.",
    "aws/route53resolver/dnsfirewall/firewallRuleGroupId": "rslvr-frg-example1",
    "aws/route53resolver/dnsfirewall/queryType": "A",
    "aws/route53resolver/dnsfirewall/queryClass": "IN",
    "aws/route53resolver/dnsfirewall/firewallDomainListId": "rslvr-fdl-example1",
    "aws/route53resolver/dnsfirewall/transport": "UDP",
    "aws/route53resolver/dnsfirewall/firewallRuleAction": "ALERT",
```

```

        "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/
amazon/route-53-resolver-dns-firewall-aws-list/000000000-0000-0000-0000-example1",
        "aws/securityhub/ProductName": "Route 53 Resolver DNS Firewall - AWS
List",
        "aws/securityhub/CompanyName": "Amazon"
    },
    "Resources": [
        {
            "Type": "Other",
            "Id": "rslvr-in-example1",
            "Partition": "aws",
            "Region": "us-east-1",
            "Details": {
                "Other": {
                    "ResourceType": "ResolverEndpoint",
                    "EndpointId": "rslvr-in-example1"
                }
            }
        },
        {
            "Type": "Other",
            "Id": "rni-example1",
            "Partition": "aws",
            "Region": "us-east-1",
            "Details": {
                "Other": {
                    "NetworkInterfaceId": "rni-example1",
                    "ResourceType": "ResolverNetworkInterface"
                }
            }
        }
    ],
    "WorkflowState": "NEW",
    "Workflow": {
        "Status": "NEW"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
        "Severity": {
            "Label": "HIGH"
        },
        "Types": [
            "TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation"
        ]
    }
}

```

```
    },  
    "ProcessedAt": "2024-12-11T19:33:35.494Z"  
}
```

Habilitación y configuración de la integración

Para integrar el Firewall de DNS con el Security Hub CSPM, primero debe habilitar el Security Hub CSPM. Para obtener información sobre cómo habilitar el CSPM de Security Hub, consulte [Habilitar el CSPM de Security Hub](#) en la Guía del usuario.AWS Security Hub

Detener la entrega de los hallazgos a Security Hub (CSPM)

Para dejar de enviar las conclusiones del firewall DNS al Security Hub CSPM, puede usar la consola CSPM de Security Hub o la API CSPM de Security Hub.

Para obtener instrucciones, consulte [Disabling the flow of findings from an integration](#) en la Guía del usuario de AWS Security Hub .

Monitoreo de Amazon Route 53

La supervisión es una parte importante del mantenimiento de la confiabilidad, la disponibilidad y el rendimiento de sus AWS soluciones. Debe recopilar los datos de supervisión de todas las partes de la AWS solución para poder depurar más fácilmente una falla multipunto en caso de que se produzca. No obstante, antes de comenzar a monitorizar, debe crear un plan de monitorización que incluya respuestas a las siguientes preguntas:

- ¿Cuáles son los objetivos de la supervisión?
- ¿Qué recursos va a supervisar?
- ¿Con qué frecuencia va a supervisar estos recursos?
- ¿Qué herramientas de supervisión va a utilizar?
- ¿Quién se encargará de realizar las tareas de supervisión?
- ¿Quién debería recibir una notificación cuando surjan problemas?

Temas

- [Registro de consultas de DNS públicas](#)
- [Registro de consultas de Resolver](#)
- [Monitorizar los registros de dominios](#)
- [Supervisión de sus recursos con los controles de estado de Amazon Route 53 y Amazon CloudWatch](#)
- [Supervisión de zonas alojadas mediante Amazon CloudWatch](#)
- [Supervisión de los puntos finales de resolución de VPC de Route 53 con Amazon CloudWatch](#)
- [Supervisión de los grupos de reglas de Resolver DNS Firewall con Amazon CloudWatch](#)
- [Administrar los eventos de Resolver DNS Firewall mediante Amazon EventBridge](#)
- [Registrar llamadas a la API de Amazon Route 53 con AWS CloudTrail](#)

Registro de consultas de DNS públicas

Puede configurar Amazon Route 53 para que registre información sobre las consultas de DNS públicas que recibe Route 53; por ejemplo:

- Dominio o subdominio que se solicitó

- La fecha y la hora de la solicitud
- El tipo de registro de DNS (por ejemplo, A o AAAA)
- La ubicación periférica de Route 53 que ha respondido a la consulta de DNS
- El código de respuesta de DNS como, por ejemplo, NoError o ServFail

Una vez que configure el registro de consultas, Route 53 enviará los CloudWatch registros a Logs. Utilice las herramientas CloudWatch de registro para acceder a los registros de consultas.

Los registros de consultas contienen únicamente las consultas que los solucionadores de DNS envían a Route 53. Si un solucionador de DNS ya ha almacenado en caché la respuesta a una consulta (por ejemplo, la dirección IP de un equilibrador de carga para example.com), el solucionador continuará devolviendo la respuesta almacenada en caché sin enviar la consulta a Route 53 hasta que venza el TTL del registro correspondiente.

Dependiendo de la cantidad de las consultas de DNS se envíen para un nombre de dominio (example.com) o nombre de subdominio(www.example.com), cuyos solucionadores están utilizando sus usuarios y el TTL para el registro, los registros de consulta puede contener información sobre una única consulta de cada varios miles de consultas que se enviaron a los solucionadores de DNS. Para obtener más información sobre cómo funciona DNS, consulte [se dirige el tráfico de Internet a su sitio web o aplicación web](#).

Si no necesitas información de registro detallada, puedes usar CloudWatch las métricas de Amazon para ver el número total de consultas de DNS a las que responde Route 53 en una zona alojada. Para obtener más información, consulte [Visualización de métricas de consultas de DNS para una zona alojada pública](#).

Temas

- [Configuración de registros para consultas del DNS](#)
- [Uso de Amazon CloudWatch para acceder a los registros de consultas de DNS](#)
- [Cambio del período de retención de registros y exportación de registros a Amazon S3](#)
- [Parar el registro de consultas](#)
- [Valores que aparecen en los registros de consulta de DNS](#)
- [Ejemplo de registro de consulta](#)

Configuración de registros para consultas del DNS

Para comenzar a registrar consultas de DNS para una determinada zona alojada especificada, realice las siguientes tareas en la consola de Amazon Route 53:

- Elija el grupo de CloudWatch registros en el que desea que Route 53 publique los registros o cree un grupo de registros nuevo.

Note

El grupo de registro debe estar en la región EE. UU. Este (Norte de Virginia).

- Para terminar, seleccione Crear.

Note

Si los usuarios envían consultas de DNS a su dominio, debe empezar a ver consultas en los registros varios minutos después de crear la configuración de registro de consulta.

Para configurar el registro para consultas de DNS

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Zonas alojadas.
3. Elija la zona alojada para la que desea configurar el registro de consultas.
4. En el panel Hosted zone details, seleccione Configure query logging.
5. Elija un grupo de registro de ya existente o cree uno nuevo.
6. Si recibe una alerta acerca de los permisos (esto sucede si no ha configurado el registro de consultas con la nueva consola antes), realice una de las siguientes acciones:
 - Si ya tiene 10 políticas de recursos, no podrá crear más. Seleccione cualquiera de sus políticas de recursos y seleccione Edit (Editar). La edición otorgará permisos a Route 53 para escribir registros en los grupos de registro. Seleccione Save. La alerta desaparece y puede continuar con el paso siguiente.
 - Si nunca ha configurado el registro de consultas (o si aún no ha creado 10 políticas de recursos), debe conceder permisos a Route 53 para escribir registros en sus grupos de

CloudWatch registros. Elija Grant permissions (Conceder permisos). La alerta desaparece y puede continuar con el paso siguiente.

7. Elija Permisos (opcional) para ver una tabla que muestre si la política de recursos coincide con el grupo de CloudWatch registros y si Route 53 tiene permiso para publicar registros en él CloudWatch.
8. Seleccione Crear.

Uso de Amazon CloudWatch para acceder a los registros de consultas de DNS

Amazon Route 53 envía los registros de consultas directamente a CloudWatch Logs; nunca se puede acceder a los registros a través de Route 53. En su lugar, utiliza CloudWatch Logs para ver los registros prácticamente en tiempo real, buscar y filtrar datos y exportar los registros a Amazon S3.

Route 53 crea un flujo de CloudWatch registros para cada ubicación de borde de Route 53 que responde a las consultas de DNS de la zona alojada especificada y envía los registros de consultas al flujo de registro correspondiente. El formato del nombre de cada flujo de registro es *hosted-zone-id/edge-location-ID*, por ejemplo, *Z1D633PJN98FT9/DFW3*.

Cada ubicación de borde se identifica mediante un código de tres letras y un número asignado arbitrariamente, por ejemplo, DFW3. El código de tres letras normalmente se corresponde con el código de aeropuerto (según la Asociación de Transporte Aéreo Internacional) más cercano a la ubicación periférica. Estas abreviaturas pueden cambiar en el futuro. Para ver una lista de ubicaciones periféricas, consulte “La red global de Amazon Route 53” en la página [Características de Amazon Route 53](#).

Note

Es posible que vea algunos prefijos o sufijos que no siguen la convención anterior. Estos codifican atributos que son solo para uso interno.

Para obtener más información, consulte la documentación aplicable:

- [Guía del usuario CloudWatch de Amazon Logs](#)
- [Referencia de la API CloudWatch de Amazon Logs](#)
- [CloudWatch Sección de registros de la Referencia de AWS CLI comandos](#)

- [Valores que aparecen en los registros de consulta de DNS](#)

Cambio del período de retención de registros y exportación de registros a Amazon S3

De forma predeterminada, CloudWatch Logs almacena los registros de consultas de forma indefinida. Si lo desea, puede especificar un período de retención para que CloudWatch Logs elimine los registros anteriores al período de retención. Para obtener más información, consulta [Cambiar la retención de datos de registro en CloudWatch Logs](#) en la Guía del CloudWatch usuario de Amazon.

Si desea conservar los datos de registro pero no necesita CloudWatch herramientas de registro para ver y analizar los datos, puede exportar los registros a Amazon S3, lo que puede reducir sus costes de almacenamiento. Para obtener más información, consulte [Exportación de datos de registro a Amazon S3](#).

Para obtener más información sobre precios, consulte la página de precios aplicable:

- «Amazon CloudWatch Logs» en la página [CloudWatch de precios](#)
- [Precios de Amazon S3](#)

Note

Al configurar Route 53 para registrar consultas de DNS, no incurrirá en ningún cargo de Route 53.

Parar el registro de consultas

Si desea que Amazon Route 53 deje de enviar registros de consultas a CloudWatch Logs, lleve a cabo el siguiente procedimiento para eliminar la configuración del registro de consultas.

Para eliminar una configuración de registro de consultas

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Zonas alojadas.
3. Elija el nombre de la zona alojada cuya configuración del registro de consultas desee eliminar.

4. En el panel Hosted zone details (Detalles de zona alojada), seleccione Configure query logging (Configuración de registro de consultas).
5. Elija Eliminar para confirmar.

Valores que aparecen en los registros de consulta de DNS

Cada archivo de registros contiene una entrada de registro por cada consulta de DNS que recibe Amazon Route 53 desde solucionadores de DNS en la ubicación periférica correspondiente. Cada entrada de registro incluye los valores siguientes:

Versión de formato de registro

El número de versión de este registro de consulta. Si añadimos campos al registro o cambiamos el formato de los campos existentes, aumentaremos este valor.

Marca de tiempo de consulta

La fecha y hora en que Route 53 respondió a la solicitud, en formato ISO 8601 y la hora universal coordinada (UTC, por sus siglas en inglés); por ejemplo, 2017-03-16T19:20:25.177Z.

Para obtener información acerca del formato ISO 8601, consulte el artículo de Wikipedia [ISO 8601](#). Para obtener información sobre UTC, consulte el artículo de Wikipedia sobre [Hora universal coordinada](#).

ID de zona alojada

El ID del nombre de la zona alojada que está asociado a todas las consultas de DNS en este registro.

Nombre de consulta

El dominio o subdominio que se ha especificado en la solicitud.

Tipo de consulta

El tipo de registro DNS que se ha especificado en la solicitud o ANY. Para obtener información acerca de los tipos que admite Route 53, consulte [Tipos de registros de DNS admitidos](#).

Código de respuesta

El código de respuesta de DNS que devolvió Route 53 en respuesta a la consulta de DNS.

Protocolo de capa 4

El protocolo que se utilizó para enviar la consulta, bien TCP o UDP.

Ubicación periférica de Route 53

Ubicación periférica en la que Route 53 ha respondido a la consulta. Cada ubicación de borde se identifica mediante un código de tres letras y un número arbitrario, por ejemplo, DFW3. El código de tres letras normalmente se corresponde con el código de aeropuerto (según la Asociación de Transporte Aéreo Internacional) más cercano a la ubicación periférica. Estas abreviaturas pueden cambiar en el futuro.

Para ver una lista de ubicaciones periféricas, consulte “La red global de Amazon Route 53” en la página [Características de Amazon Route 53](#).

Dirección IP de solucionador

La dirección IP del solucionador de DNS que envió la solicitud a Route 53.

Subred del cliente EDNS

Una dirección IP parcial para el cliente desde el que se originó la solicitud, si está disponible desde el solucionador de DNS.

Para obtener más información, consulte el borrador de IETF [Client Subnet in DNS Requests](#).

Ejemplo de registro de consulta

A continuación se muestra un ejemplo de registro de consulta (la región es un marcador de posición):

```
1.0 2017-12-13T08:16:02.130Z Z123412341234 example.com A NOERROR UDP Region 192.168.1.1
-
1.0 2017-12-13T08:15:50.235Z Z123412341234 example.com AAAA NOERROR TCP Region
192.168.3.1 192.168.222.0/24
1.0 2017-12-13T08:16:03.983Z Z123412341234 example.com ANY NOERROR UDP Region
2001:db8::1234 2001:db8:abcd::/48
1.0 2017-12-13T08:15:50.342Z Z123412341234 bad.example.com A NXDOMAIN UDP Region
192.168.3.1 192.168.111.0/24
1.0 2017-12-13T08:16:05.744Z Z123412341234 txt.example.com TXT NOERROR UDP Region
192.168.1.2 -
```

Registro de consultas de Resolver

Puede registrar las siguientes consultas de DNS:

- Consultas que se originan en Amazon Virtual Private Cloud VPCs que especifique, así como las respuestas a esas consultas de DNS.
- Consultas de recursos en las instalaciones que utilizan un punto de conexión de entrada de Resolver.
- Consultas que utilizan un punto de conexión de salida de Resolver para la resolución de DNS recursiva.
- Consultas que utilizan las reglas del firewall DNS de Resolver para bloquear, permitir o supervisar las listas de dominios.

Los registros de consultas de VPC Resolver incluyen valores como los siguientes:

- La AWS región en la que se creó la VPC
- El ID de VPC desde el que se originó la consulta
- La dirección IP de la instancia desde la que se originó la consulta
- El ID de instancia del recurso desde el que se originó la consulta
- La fecha y la hora en que se efectuó la consulta por primera vez
- El nombre de DNS solicitado (como prod.example.com)
- El tipo de registro DNS (como, por ejemplo, A o AAAA)
- El código de respuesta de DNS como, por ejemplo, NoError o ServFail
- Los datos de respuesta de DNS, como la dirección IP que se devuelve en respuesta a la consulta de DNS
- Una respuesta a una acción de regla de DNS Firewall

Para obtener una lista detallada de todos los valores registrados y un ejemplo, consulte [Valores que aparecen en los registros de consultas de VPC Resolver](#).

Note

Como es habitual en los solucionadores de DNS, los solucionadores almacenan en caché las consultas de DNS durante un período de tiempo determinado por el time-to-live TTL del solucionador. El solucionador de VPC de Route 53 almacena en caché las consultas que se originan en usted VPCs y responde desde la memoria caché siempre que es posible para acelerar las respuestas. El registro de consultas de VPC Resolver solo registra consultas únicas, no consultas a las que VPC Resolver puede responder desde la memoria caché.

Por ejemplo, supongamos que una EC2 instancia de una de las en las VPCs que una configuración de registro de consultas registra consultas envía una solicitud a `accounting.example.com`. El solucionador de VPC almacena en caché la respuesta a esa consulta y la registra. Si la interfaz de red elástica de la misma instancia realiza una consulta para `accounting.example.com` en el TTL de la memoria caché del solucionador de VPC, el solucionador de VPC responde a la consulta desde la memoria caché. La segunda consulta no se registra.

Puede enviar los registros a uno de los siguientes recursos: AWS

- Grupo de CloudWatch registros de Amazon CloudWatch Logs (Logs)
- Bucket de Amazon S3 (S3)
- Flujo de entrega de Firehose

Para obtener más información, consulte [AWS recursos a los que puede enviar registros de consultas de VPC Resolver](#).

Temas

- [AWS recursos a los que puede enviar registros de consultas de VPC Resolver](#)
- [Administración de configuraciones de registro de consultas de Resolver](#)

AWS recursos a los que puede enviar registros de consultas de VPC Resolver

Note

Si espera registrar consultas para cargas de trabajo con consultas altas por segundo (QPS), debe utilizar Amazon S3 para asegurarse de que los registros de consulta no se ven limitados de forma controlada al escribirlos en su destino. Si utilizas Amazon CloudWatch, puedes aumentar el límite de solicitudes por segundo para la `PutLogEvents` operación. Para obtener más información sobre cómo aumentar tus CloudWatch límites, consulta [las cuotas de CloudWatch registros](#) en la Guía del CloudWatch usuario de Amazon.

Puede enviar los registros de consultas de VPC Resolver a los siguientes recursos: AWS

Grupo de CloudWatch registros de Amazon CloudWatch Logs (Amazon Logs)

Puede analizar registros con Logs Insights y crear métricas y alarmas.

Para obtener más información, consulta la [Guía del usuario CloudWatch de Amazon Logs](#).

Bucket de Amazon S3 (S3)

El bucket de S3 es económico para archivar registros a largo plazo. La latencia suele ser mayor.

Se admiten todas las opciones de cifrado en el lado del servidor de S3. Para obtener más información, consulte [Protección de datos mediante cifrado del lado del servidor](#) en la Guía del usuario de Amazon S3.

Si elige el cifrado con AWS KMS claves del lado del servidor (SSE-KMS), debe actualizar la política de claves de su clave administrada por el cliente para que la cuenta de entrega de registros pueda escribir en su bucket de Amazon S3. Para obtener más información sobre la política de claves necesaria para su uso con SSE-KMS, consulte el cifrado del [lado del servidor de bucket de Amazon S3 en la Guía del usuario](#) de Amazon. CloudWatch

Si el bucket de S3 está en una cuenta de su propiedad, los permisos necesarios se agregan automáticamente a su política de bucket. Si desea enviar registros a un bucket de S3 en una cuenta que no posee, el propietario del bucket de S3 debe agregar permisos para su cuenta en su política de bucket. Por ejemplo:

JSON

```
{
  "Version": "2012-10-17",
  "Id": "CrossAccountAccess",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::your_bucket_name/
AWSLogs/your_caller_account/*"
    },
    {
      "Effect": "Allow",
```

```
    "Principal": {
      "Service": "delivery.logs.amazonaws.com"
    },
    "Action": "s3:GetBucketAcl",
    "Resource": "arn:aws:s3:::your_bucket_name"
  },
  {
    "Effect": "Allow",
    "Principal": {
      "AWS": "iam_user_arn_or_account_number_for_root"
    },
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::your_bucket_name"
  }
]
```

Note

Si desea almacenar registros en un bucket de S3 central para su organización, le recomendamos que realice la configuración del registro de consultas desde una cuenta centralizada (con los permisos necesarios para escribir en un bucket central) y que use [RAM](#) para compartir la configuración entre cuentas.

Para obtener más información, consulte la [Guía del usuario de Amazon Simple Storage Service](#).

Flujo de entrega de Firehose

Puede transmitir registros en tiempo real a Amazon OpenSearch Service, Amazon Redshift u otras aplicaciones.

Para obtener más información, consulte la [Guía para desarrolladores de Amazon Data Firehose](#).

Para obtener información sobre los precios del registro de consultas de Resolver, consulta [CloudWatch los precios de Amazon](#).

CloudWatch Se aplican cargos por Vended Logs al utilizar los registros de VPC Resolver, incluso cuando los registros se publican directamente en Amazon S3. Para obtener más información, consulta [los precios de Logs en Amazon CloudWatch](#).

Administración de configuraciones de registro de consultas de Resolver

Configuración (registro de consultas de VPC Resolver)

Puede configurar el registro de consultas de VPC Resolver de dos maneras:

- **Asociación directa de VPC:** se asocia VPCs directamente a una configuración de registro de consultas.
- **Asociación de perfiles:** asocie una configuración de registro de consultas a un perfil de Route 53, que aplica el registro a todos los VPCs asociados a ese perfil. Para obtener más información, consulte [Asocie las configuraciones de registro de consultas de VPC Resolver a un perfil de Route 53](#).

Para empezar a registrar las consultas de DNS que se originan en su VPCs, realice las siguientes tareas en la consola de Amazon Route 53:

Para configurar el registro de consultas de Resolver

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. Expanda el menú de la consola de Route 53. En la esquina superior izquierda de la consola, elija el icono de las tres barras horizontales ().
3. En el menú Resolver, elija Registro de consultas.
4. En el selector de regiones, elija la AWS región en la que desee crear la configuración de registro de consultas. Debe ser la misma región en la que creó la región para la VPCs que desea registrar las consultas de DNS. Si está VPCs en varias regiones, debe crear al menos una configuración de registro de consultas para cada región.
5. Elija Configure query logging (Configuración del registro de consultas).
6. Especifique los siguientes valores:

Nombre de configuración del registro de consultas

Ingrese un nombre para la configuración del registro de consultas. El nombre aparece en la consola en la lista de configuraciones del registro de consultas. Ingrese un nombre que le ayude a encontrar esta configuración más tarde.

Destino de los registros de consulta

Elija el tipo de AWS recurso al que quiere que VPC Resolver envíe los registros de consultas. Para obtener información sobre cómo elegir entre las opciones (grupo de CloudWatch registros, depósito S3 y transmisión de entrega Firehose), consulte [AWS recursos a los que puede enviar registros de consultas de VPC Resolver](#)

Tras elegir el tipo de recurso, puede crear otro recurso de ese tipo o elegir un recurso existente creado por la AWS cuenta corriente.

Note

Solo puede elegir recursos que se hayan creado en la región de AWS que eligió en el paso 4, la región donde está creando la configuración del registro de consultas. Si decide crear un recurso nuevo, ese recurso se creará en la misma región.

VPCs para registrar consultas para

Esta configuración de registro de consultas registrará las consultas de DNS que se originen en el VPCs que elija. Marque la casilla de verificación de cada VPC de la región actual en la que desee que VPC Resolver registre las consultas y, a continuación, seleccione Elegir.

Alternativa: en lugar de VPCs asociarla directamente, puede asociar esta configuración de registro de consultas a un perfil de Route 53, que aplicará el registro a todos los VPCs asociados a ese perfil. Para obtener más información, consulte [Asocie las configuraciones de registro de consultas de VPC Resolver a un perfil de Route 53](#).

Note

La entrega de registros de VPC solo se puede habilitar una vez para un tipo de destino específico. Los registros no se pueden enviar a varios destinos del mismo tipo; por ejemplo, los registros de VPC no se pueden entregar a dos destinos de Amazon S3.

7. Elija Configure query logging (Configuración del registro de consultas).

 Note

Debe comenzar a ver consultas de DNS realizadas por los recursos de su VPC en los registros unos minutos después de crear correctamente la configuración del registro de consultas.

Valores que aparecen en los registros de consultas de VPC Resolver

Cada archivo de registros contiene una entrada de registro por cada consulta de DNS que recibe Amazon Route 53 desde solucionadores de DNS en la ubicación de borde correspondiente. Cada entrada de registro incluye los valores siguientes:

versión

El número de versión de este formato de registro de consultas. La versión actual es 1.1.

El valor de versión contiene una versión principal y una versión secundaria con el formato **major_version.minor_version**. Por ejemplo, puede tener un valor `version` de 1.7, donde 1 es la versión principal y 7 es la versión secundaria.

Route 53 incrementa la versión principal si se realiza un cambio en la estructura del registro que no es compatible con versiones anteriores. Esto incluye eliminar un campo JSON existente o cambiar la forma en que se representa el contenido de un campo (por ejemplo, un formato de fecha).

Route 53 incrementa la versión secundaria si un cambio agrega nuevos campos al archivo de registros. Esto puede ocurrir cuando hay nueva información disponible para algunas o todas las consultas de DNS existentes dentro de una VPC.

account_id

El ID de la AWS cuenta que creó la VPC.

region

La AWS región en la que creó la VPC.

vpc_id

El ID de VPC en la que se originó la consulta.

query_timestamp

La fecha y hora en que las que se envió la consulta, en formato ISO 8601 y hora universal coordinada (UTC, por sus siglas en inglés); por ejemplo, 2017-03-16T19:20:177Z.

Para obtener información acerca del formato ISO 8601, consulte el artículo de Wikipedia [ISO 8601](#). Para obtener información sobre UTC, consulte el artículo de Wikipedia sobre [Hora universal coordinada](#).

query_name

El nombre de dominio (example.com) o nombre del subdominio (www.example.com) que se especificó en la consulta.

query_type

El tipo de registro DNS que se ha especificado en la solicitud o ANY. Para obtener información acerca de los tipos que admite Route 53, consulte [Tipos de registros de DNS admitidos](#).

query_class

La clase de consulta.

rcode

El código de respuesta de DNS que VPC Resolver devolvió en respuesta a la consulta de DNS. El código de respuesta indica si la consulta era válida o no. El código de respuesta más habitual es NOERROR, para indicar que la consulta era válida. Si la respuesta no es válida, Resolver devuelve un código de respuesta que explica el motivo. Para obtener una lista de los posibles códigos de respuesta, consulte [DNS RCODEs](#) en el sitio web de la IANA.

answer_type

El tipo de registro DNS (como A, MX o CNAME) del valor que VPC Resolver devuelve en respuesta a la consulta. Para obtener información acerca de los tipos que admite Route 53, consulte [Tipos de registros de DNS admitidos](#).

rdata

El valor que VPC Resolver devolvió en respuesta a la consulta. Por ejemplo, para un registro A, se trata de una dirección IP en IPv4 formato. Para un registro CNAME, será el nombre de dominio en el registro CNAME.

answer_class

La clase de la respuesta del solucionador de VPC a la consulta.

srcaddr

La dirección IP del host que originó la consulta.

srcport

El puerto de la instancia desde la que se originó la consulta.

transport

El protocolo utilizado para enviar la consulta de DNS.

srcids

IDs del `instanceresolver_endpoint`, y del origen o por el `resolver_network_interface` que ha pasado la consulta de DNS.

instancia

El ID de la instancia desde la que se originó la consulta.

 Note

Si ve un ID de instancia en los registros de consultas de VPC Resolver de Route 53 que no está visible en su cuenta, puede deberse a que la consulta de DNS se originó en la consola AWS Lambda Amazon EKS o AWS CloudShell Fargate, que utilizó usted.

resolver_endpoint

El ID del punto de conexión del solucionador que pasa la consulta de DNS a los servidores DNS en las instalaciones.

 Note

Si tiene registros CNAME que utilizan diferentes reglas de reenvío en cadena con distintos puntos de conexión del solucionador, los registros de consultas muestran solo el ID del último punto de conexión del solucionador utilizado en la cadena. Para rastrear la ruta de resolución completa a través de varios puntos de conexión, puede correlacionar los registros en diferentes configuraciones de registro de consultas.

firewall_rule_group_id

El ID del grupo de reglas de DNS Firewall de que coincidió con el nombre de dominio de la consulta. Esto solo se rellena si DNS Firewall encontró una coincidencia para una regla con la acción configurada de alerta o bloqueo.

Para obtener más información sobre los grupos de reglas de firewall, consulte [Reglas y grupos de reglas de DNS Firewall](#).

firewall_rule_action

La acción especificada por la regla que coincidió con el nombre de dominio de la consulta. Esto solo se rellena si DNS Firewall encontró una coincidencia para una regla con la acción configurada de alerta o bloqueo.

firewall_domain_list_id

La lista de dominios utilizada por la regla que coincidió con el nombre de dominio de la consulta. Esto solo se rellena si DNS Firewall encontró una coincidencia para una regla con la acción configurada de alerta o bloqueo.

additional_properties

Información adicional sobre los eventos de entrega del registro. `is_delay`: si hay una demora en la entrega de los registros.

Ejemplo de registro de consultas de VPC Resolver de Route 53

Presentamos un ejemplo de registro de consultas del solucionador:

```
{
  "srcaddr": "4.5.64.102",
  "vpc_id": "vpc-7example",
  "answers": [
    {
      "Rdata": "203.0.113.9",
      "Type": "PTR",
      "Class": "IN"
    }
  ],
  "firewall_rule_group_id": "rslvr-frg-01234567890abcdef",
  "firewall_rule_action": "BLOCK",
```

```
{
  "query_name": "15.3.4.32.in-addr.arpa.",
  "firewall_domain_list_id": "rslvr-fdl-01234567890abcdef",
  "query_class": "IN",
  "srcids": {
    "instance": "i-0d15cd0d3example"
  },
  "rcode": "NOERROR",
  "query_type": "PTR",
  "transport": "UDP",
  "version": "1.100000",
  "account_id": "111122223333",
  "srcport": "56067",
  "query_timestamp": "2021-02-04T17:51:55Z",
  "region": "us-east-1"
}
```

Compartir las configuraciones de registro de consultas de Resolver con otras cuentas AWS

Puede compartir las configuraciones de registro de consultas que creó con una AWS cuenta con otras AWS cuentas. Para compartir configuraciones, la consola de resolución de VPC de Route 53 se integra con AWS Resource Access Manager. Para obtener más información acerca de Resource Access Manager, consulte la [Guía del usuario de Resource Access Manager](#).

Tenga en cuenta lo siguiente:

Asociación VPCs con configuraciones de registro de consultas compartidas

Si otra AWS cuenta ha compartido una o más configuraciones con la suya, puede VPCs asociarla a la configuración del mismo modo que a VPCs las configuraciones que creó.

Eliminación o dejar de compartir una configuración

Si comparte una configuración con otras cuentas y, a continuación, la elimina o deja de compartirla, y si hay una o más asociadas a la configuración, Route 53 VPC Resolver deja de registrar las consultas de DNS que VPCs se originan en esas cuentas. VPCs

Número máximo de configuraciones de registro de consultas VPCs que se pueden asociar a una configuración

Cuando una cuenta crea una configuración y la comparte con una o más cuentas, se aplica el número máximo de cuentas VPCs que se pueden asociar a la configuración por cuenta. Por ejemplo, si tiene 10 000 cuentas en su organización, puede crear la configuración de registro de consultas en la cuenta central y compartirla AWS RAM a través de ella para compartirla

con las cuentas de la organización. A continuación, las cuentas de la organización asociarán la configuración a su VPCs contabilización en función de las asociaciones de VPC de la configuración del registro de consultas de su cuenta por Región de AWS límite de 100. Sin embargo, si todas VPCs están en una sola cuenta, es posible que sea necesario aumentar los límites de servicio de la cuenta.

Para conocer las cuotas actuales de VPC Resolver, consulte. [Cuotas en el solucionador de VPC Route 53](#)

Permisos

Para compartir una regla con otra AWS cuenta, debe tener permiso para usar la [PutResolverQueryLogConfigPolicy](#) acción.

Restricciones en la AWS cuenta con la que se comparte una regla

La cuenta con la que se comparte una regla no puede cambiar o eliminar la regla.

Etiquetado

Solo la cuenta que creó una regla puede añadir, eliminar o consultar etiquetas de la regla.

Para ver el estado actual de uso compartido de una regla (incluida la cuenta que compartió la regla o la cuenta con la que se comparte una regla) y para compartir reglas con otra cuenta, siga el procedimiento que se indica a continuación.

Para ver el estado de uso compartido y compartir configuraciones de registro de consultas con otra cuenta de AWS

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Query Logging (Registro de consultas).
3. En la barra de navegación, elija la región en la que creó la regla.

La columna Sharing status (Estado de uso compartido) muestra el estado actual de uso compartido de las reglas creadas por la cuenta actual o que se comparten con la cuenta actual:

- No compartida: la AWS cuenta actual creó la regla y la regla no se comparte con ninguna otra cuenta.
- Shared by me (Compartido por mí): la cuenta actual creó la regla y la compartió con una o varias cuentas.

- Shared with me (Compartido conmigo): otra cuenta creó la regla y la compartió con la cuenta actual.
4. Elija el nombre de la regla cuya información de uso compartido desea mostrar o que desea compartir con otra cuenta.

En la *rule name* página Regla:, el valor de Propietario muestra el ID de la cuenta que creó la regla. Es la cuenta actual a menos que el valor de Sharing status (Estado de uso compartido) sea Shared with me (Compartido conmigo). En ese caso, Owner (Propietario) es la cuenta que creó la regla y la compartió con la cuenta actual.

También se muestra el estado de uso compartido.

5. Seleccione Compartir configuración para abrir la AWS RAM consola
6. Para crear un recurso compartido, siga los pasos descritos en [Crear un recurso compartido en AWS RAM](#) en la Guía del usuario de AWS RAM .

 Note

No se puede actualizar la configuración de uso compartido. Si desea cambiar cualquiera de los siguientes valores, debe volver a compartir una regla con la nueva configuración y, a continuación, quitar la configuración de uso compartido anterior.

Monitorizar los registros de dominios

El panel de Amazon Route 53 ofrece información detallada sobre el estado de sus registros de dominios, incluido lo siguiente:

- Estado de los nuevos registros de dominios
- Estado de las transferencias de dominio a Route 53
- Lista de dominios que se aproximan a la fecha de vencimiento

Le recomendamos que consulte periódicamente el panel de la consola de Route 53, especialmente después de registrar un nuevo dominio o transferirlo a Route 53, para confirmar que no hay problemas pendientes de solución.

También le recomendamos que confirme que la información de contacto de sus dominios está actualizada. A medida que se aproxima la fecha de vencimiento de un dominio, enviamos un email

al contacto del registrante del dominio con información acerca de cuándo vence el dominio y cómo renovarlo.

Supervisión de sus recursos con los controles de estado de Amazon Route 53 y Amazon CloudWatch

Puede supervisar sus recursos mediante la creación de comprobaciones de estado de Amazon Route 53, que se utilizan CloudWatch para recopilar y procesar datos sin procesar en métricas legibles prácticamente en tiempo real. Estas estadísticas se registran durante un periodo de dos semanas, de forma que pueda obtener acceso a información histórica y obtener una mejor perspectiva sobre el desempeño de sus recursos. De forma predeterminada, los datos métricos de las comprobaciones de estado de Route 53 se envían automáticamente a CloudWatch intervalos de un minuto.

Para obtener más información sobre las comprobaciones de estado de Route 53, consulte [Monitorear comprobaciones de estado mediante CloudWatch](#). Para obtener más información CloudWatch, consulta [¿Qué es Amazon CloudWatch?](#) en la Guía del CloudWatch usuario de Amazon.

Métricas y dimensiones para comprobaciones de estado de Route 53

Cuando crea una comprobación de estado, Amazon Route 53 comienza a enviar métricas y dimensiones una vez por minuto a CloudWatch aproximadamente el recurso que especifique. La consola de Route 53 le permite ver la situación de las comprobaciones de estado. También puede usar los siguientes procedimientos para ver las métricas en la CloudWatch consola o visualizarlas mediante AWS Command Line Interface (AWS CLI).

Para ver las métricas mediante la CloudWatch consola

1. Abra la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, seleccione Métricas.
3. En la pestaña All Metrics, elija Route 53.
4. Elija Health Check Metrics.

Para ver las métricas mediante el AWS CLI

- En el símbolo del sistema, ejecute el siguiente comando:

```
aws cloudwatch list-metrics --namespace "AWS/Route53"
```

Temas

- [CloudWatch métricas de las comprobaciones de estado de Route 53](#)
- [Dimensiones para métricas de comprobaciones de estado de Route 53](#)

CloudWatch métricas de las comprobaciones de estado de Route 53

El espacio de nombres AWS/Route53 incluye las siguientes métricas para las comprobaciones de estado de Route 53.

ChildHealthCheckHealthyCount

Para una comprobación de estado calculada, el número de comprobaciones de estado que son buenas.

Estadísticas válidas: Average (recomendado), Minimum, Maximum

Unidades: recuento

ConnectionTime

El tiempo medio, en milisegundos, que tardan los comprobadores de estado de Route 53 en establecer una conexión TCP con el punto de conexión. Puede consultar ConnectionTime para una comprobación de estado en todas las regiones o para una región geográfica seleccionada.

Estadísticas válidas: Average (recomendado), Minimum, Maximum

Unidades: milisegundos

HealthCheckPercentageHealthy

El porcentaje de comprobadores de estado de Route 53 que consideran que el punto de conexión seleccionado está en buen estado.

Estadísticas válidas: promedio, mínimo, máximo

Unidad: porcentaje

HealthCheckStatus

El estado del punto final de la comprobación de estado que CloudWatch se está comprobando. 1 indica que está en buen estado y 0 indica que no está bien.

Estadísticas válidas: Minimum, Average y Maximum

Unidades: ninguna

SSLHandshakeHora

El tiempo medio, en milisegundos, que tardan los comprobadores de estado de Route 53 en completar el protocolo SSL. Puede consultar `SSLHandshakeTime` para una comprobación de estado en todas las regiones o para una región geográfica seleccionada.

Estadísticas válidas: Average (recomendado), Minimum, Maximum

Unidades: milisegundos

TimeToFirstByte

El tiempo medio, en milisegundos, que tardan los comprobadores de estado de Route 53 en recibir el primer byte de la respuesta a una solicitud HTTP o HTTPS. Puede consultar `TimeToFirstByte` para una comprobación de estado en todas las regiones o para una región geográfica seleccionada.

Estadísticas válidas: Average (recomendado), Minimum, Maximum

Unidades: milisegundos

Dimensiones para métricas de comprobaciones de estado de Route 53

Las métricas de Route 53 para las comprobaciones de estado utilizan el espacio de nombres `AWS/Route53` y proporcionan métricas para `HealthCheckId`. Cuando recupere métricas, debe proporcionar la dimensión `HealthCheckId`.

Además, para `ConnectionTime`, `SSLHandshakeTime` y `TimeToFirstByte`, puede especificar `Region` si lo desea. Si lo omite `Region`, CloudWatch devuelve las métricas de todas las regiones. Si las incluye `Region`, solo CloudWatch devuelve las métricas de la región especificada.

Para obtener más información, consulte [Monitorear comprobaciones de estado mediante CloudWatch](#).

Supervisión de zonas alojadas mediante Amazon CloudWatch

Puedes monitorizar tus zonas alojadas de forma pública mediante Amazon CloudWatch para recopilar y procesar datos sin procesar en métricas legibles prácticamente en tiempo real. Las métricas están disponibles poco después de que Route 53 reciba las consultas de DNS en las que se basan las métricas. CloudWatch los datos métricos de las zonas alojadas de Route 53 tienen una granularidad de un minuto.

Para obtener más información, consulte la documentación siguiente

- Para obtener información general e información sobre cómo ver las métricas en la CloudWatch consola de Amazon y cómo recuperarlas mediante AWS Command Line Interface (AWS CLI), consulta [Visualización de métricas de consultas de DNS para una zona alojada pública](#)
- Para obtener información sobre el período de retención de las métricas, consulta [GetMetricStatistics](#) la referencia de la CloudWatch API de Amazon.
- Para obtener más información CloudWatch, consulta [¿Qué es Amazon CloudWatch?](#) en la Guía del CloudWatch usuario de Amazon.
- Para obtener más información sobre CloudWatch las métricas, consulta [Uso de CloudWatch las métricas de Amazon](#) en la Guía del CloudWatch usuario de Amazon.

Temas

- [CloudWatch métricas para las zonas alojadas públicas de Route 53](#)
- [CloudWatch dimensión de las métricas de zonas alojadas públicas de Route 53](#)

CloudWatch métricas para las zonas alojadas públicas de Route 53

El espacio de nombres AWS/Route53 incluye la siguiente métrica para zonas alojadas de Route 53:

DNSQueries

Para una zona alojada, el número de consultas de DNS a las que responde Route 53 en un período de tiempo especificado.

Estadísticas válidas: suma, SampleCount

Unidades: recuento

Región: Route 53 es un servicio global. Para obtener métricas de zona alojada, debe especificar Este de EE. UU. (Norte de Virginia) para la región.

DNSSECInternalFallo

El valor es 1 si cualquier objeto en la zona alojada tiene un estado INTERNAL_FAILURE. De lo contrario, el valor es 0.

Estadísticas válidas: Sum

Unidades: recuento

Volumen: 1 cada 4 horas por zona alojada

Región: Route 53 es un servicio global. Para obtener métricas de zona alojada, debe especificar Este de EE. UU. (Norte de Virginia) para la región.

DNSSECKeySigningKeysNeedingAction

Número de claves de firma clave (KSKs) que tienen el estado ACTION_NEEDED (debido a un error del KMS).

Estadísticas válidas: suma, SampleCount

Unidades: recuento

Volumen: 1 cada 4 horas por zona alojada

Región: Route 53 es un servicio global. Para obtener métricas de zona alojada, debe especificar Este de EE. UU. (Norte de Virginia) para la región.

DNSSECKeySigningKeyMaxNeedingActionAge

Ha transcurrido el tiempo desde que la clave de firma de claves (KSK) se estableció en el estado ACTION_NEEDED.

Estadísticas válidas: Maximum

Unidades: segundos

Volumen: 1 cada 4 horas por zona alojada

Región: Route 53 es un servicio global. Para obtener métricas de zona alojada, debe especificar Este de EE. UU. (Norte de Virginia) para la región.

DNSSECKeySigningKeyAge

El tiempo transcurrido desde que se creó la clave de firma de claves (KSK) (no desde que se activó).

Estadísticas válidas: Maximum

Unidades: segundos

Volumen: 1 cada 4 horas por zona alojada

Región: Route 53 es un servicio global. Para obtener métricas de zona alojada, debe especificar Este de EE. UU. (Norte de Virginia) para la región.

CloudWatch dimensión de las métricas de zonas alojadas públicas de Route 53

Las métricas de Route 53 para las zonas alojadas utilizan el espacio de nombres AWS/Route53 y proporcionan métricas para HostedZoneId. Para obtener el número de consultas de DNS, debe especificar el ID de la zona alojada en la dimensión HostedZoneId.

Supervisión de los puntos finales de resolución de VPC de Route 53 con Amazon CloudWatch

Puede usar Amazon CloudWatch para supervisar la cantidad de consultas de DNS que reenvían los puntos de enlace de VPC Resolver de Route 53. Amazon CloudWatch recopila y procesa datos sin procesar para convertirlos en métricas legibles y prácticamente en tiempo real. Estas estadísticas se registran durante un periodo de dos semanas, de forma que pueda obtener acceso a información histórica y obtener una mejor perspectiva sobre el desempeño de sus recursos. De forma predeterminada, los datos de las métricas de los puntos finales de Resolver se envían automáticamente a CloudWatch intervalos de cinco minutos. El intervalo de cinco minutos es también el intervalo más reducido en el que se pueden enviar los datos de las métricas.

Para obtener más información sobre VPC Resolver, consulte [¿Qué es el solucionador de VPC Route 53?](#) Para obtener más información CloudWatch, consulta [¿Qué es Amazon CloudWatch?](#) en la Guía del CloudWatch usuario de Amazon.

Métricas y dimensiones del solucionador de VPC Route 53

Al configurar el Resolver de VPC para que reenvíe consultas de DNS a la red o viceversa, el Resolver de VPC comienza a enviar [métricas](#) y [dimensiones](#) una vez cada cinco minutos hasta CloudWatch aproximadamente el número de consultas que se reenvían. Puede usar los siguientes procedimientos para ver las métricas en la CloudWatch consola o consultarlas mediante AWS Command Line Interface (AWS CLI).

Para ver las métricas de VPC Resolver mediante la consola CloudWatch

1. Abra la CloudWatch consola en. <https://console.aws.amazon.com/cloudwatch/>
2. En la barra de navegación, elija la región en la que creó el punto de conexión.
3. En el panel de navegación, seleccione Métricas.
4. En la pestaña All metrics (Todas las métricas), elija Route 53 Resolver.
5. Elija By Endpoint (Por punto de conexión) para ver los recuentos de consultas de un punto de conexión especificado. A continuación, elija los puntos de conexión de los que desea ver el número de consultas.

Seleccione Todos los puntos de conexión para ver los recuentos de consultas de todos los puntos de conexión entrantes o de todos los puntos de conexión salientes creados por la cuenta actual. AWS A continuación, elija InboundQueryVolume o desee ver los recuentos OutboundQueryVolume deseados.

Para ver las métricas mediante el AWS CLI

- En el símbolo del sistema, ejecute el siguiente comando:

```
aws cloudwatch list-metrics --namespace "AWS/Route53Resolver"
```

Temas

- [CloudWatch Métricas básicas del solucionador de VPC Route 53](#)
- [CloudWatch Métricas detalladas del solucionador de VPC Route 53](#)
- [Dimensiones de las métricas del solucionador de VPC de Route 53](#)

CloudWatch Métricas básicas del solucionador de VPC Route 53

AWS/Route53Resolver el espacio de nombres incluye métricas básicas para los puntos finales de VPC Resolver de Route 53 y para las direcciones IP de forma gratuita.

Temas

- [Métricas de los puntos finales de VPC Resolver Route 53](#)
- [Métricas de las direcciones IP de los solucionadores de VPC de Route 53](#)

Métricas de los puntos finales de VPC Resolver Route 53

El espacio de AWS/Route53Resolver nombres incluye las siguientes métricas para los puntos de conexión de VPC Resolver de Route 53.

EndpointHealthyENICount

El número de interfaces de red elásticas con el estado OPERATIONAL. Esto significa que las interfaces de red de Amazon VPC para el punto de conexión (especificado por EndpointId) están configuradas correctamente y pueden pasar consultas de DNS de entrada o salida entre la red y Resolver.

Estadísticas válidas: mínimo, máximo y promedio

Unidades: recuento

EndpointUnhealthyENICount

El número de interfaces de red elásticas con el estado AUTO_RECOVERING.

Esto significa que el solucionador está intentando recuperar una o más interfaces de red de Amazon VPC asociadas al punto de conexión (especificado por EndpointId). Durante el proceso de recuperación, el punto de conexión funciona con una capacidad limitada y no puede procesar consultas de DNS hasta que esté completamente recuperado.

Estadísticas válidas: mínimo, máximo, promedio

Unidades: recuento

InboundQueryVolume

En el caso de los puntos de enlace entrantes, el número de consultas de DNS reenviadas desde la red a la suya a VPCs través del punto de conexión especificado por. EndpointId

Estadísticas válidas: Sum

Unidades: recuento

OutboundQueryVolume

En el caso de los puntos de conexión salientes, el número de consultas de DNS reenviadas desde la red VPCs a través del punto de conexión especificado por. `EndpointId`

Estadísticas válidas: Sum

Unidades: recuento

OutboundQueryAggregateVolume

En el caso de los puntos de enlace salientes, el número total de consultas de DNS reenviadas desde Amazon VPCs a la red, incluidas las siguientes:

- El número de consultas de DNS reenviadas desde su red VPCs a través del punto final especificado por. `EndpointId`
- Cuando la cuenta corriente comparte las reglas de VPCs Resolver con otras cuentas, las consultas las crean otras cuentas y las reenvían a la red a través del punto de conexión especificado por `EndpointId`.

Estadísticas válidas: Sum

Unidades: recuento

ResolverEndpointCapacityStatus

El estado de la capacidad del punto de conexión de Resolver. La métrica indica el estado de utilización de la capacidad actual, donde: 0 = OK (capacidad operativa normal), 1 = Advertencia (al menos una interfaz de red elástica supera el 50 % de utilización de la capacidad) y 2 = Crítico (al menos una interfaz de red elástica supera el 75 % de utilización de la capacidad).

El estado de la capacidad está determinado por varios factores, como el volumen de consultas, la latencia de las consultas, los protocolos DNS, el tamaño de los paquetes DNS y el estado del seguimiento de las conexiones.

Estadísticas válidas: máximo

Unidades: ninguna

Mejores prácticas para la gestión de la capacidad de los terminales de resolución de VPC

Para solucionar los problemas de capacidad, generalmente recomendamos aumentar la cantidad de interfaces de red elásticas para su punto de conexión de Resolver. Sin embargo, hay factores importantes que se deben tener en cuenta para tipos de puntos de conexión específicos:

En el caso de los puntos de conexión de entrada, el equilibrio de carga del tráfico depende del cliente. Por lo tanto, las advertencias de capacidad o las alertas críticas pueden indicar un “punto crítico” en el que se utiliza de forma desproporcionada un subconjunto de interfaces de red elásticas.

- Para identificar posibles problemas de equilibrio de carga, examine las [InboundQueryVolume](#) métricas de cada interfaz de red elástica de forma individual.

En el caso de los puntos de conexión de salida, el tráfico se equilibra automáticamente entre las interfaces de red elásticas. Los problemas de capacidad pueden deberse a problemas con el servidor de nombres de destino o a que las consultas de alta latencia sobre los tiempos de espera sobrecargan las interfaces de red de Resolver.

- En estos casos, es posible que el solo hecho de aumentar las interfaces de red elásticas no sea eficaz, por lo que recomendamos arreglar el servidor de nombres de destino.

Métricas de las direcciones IP de los solucionadores de VPC de Route 53

El espacio de nombres AWS/Route53Resolver incluye las siguientes métricas para cada dirección IP asociada a un punto de conexión de entrada o salida de Resolver. (Al especificar un punto de conexión, VPC Resolver crea una interfaz de red [elástica](#) de Amazon VPC).

InboundQueryVolume

Para cada dirección IP de los puntos de conexión entrantes, el número de consultas de DNS reenviadas desde la red a la dirección IP especificada. Cada dirección IP se identifica mediante el ID de la dirección IP. Puede obtener este valor usando la consola de Route 53. En la página del punto de conexión correspondiente, en la sección de direcciones IP, consulte la columna IP address ID (ID de dirección IP). También puede obtener el valor mediante programación.

[ListResolverEndpointIpAddresses](#)

Estadísticas válidas: Sum

Unidades: recuento

OutboundQueryAggregateVolume

Para cada dirección IP de tus puntos de conexión salientes, el número total de consultas de DNS reenviadas desde Amazon VPCs a tu red, incluidas las siguientes:

- El número de consultas de DNS reenviadas desde tu red VPCs a través de la dirección IP especificada.
- Cuando la cuenta corriente comparte las reglas de Resolver con otras cuentas, otras cuentas crean consultas desde VPCs esa cuenta y las reenvían a la red mediante la dirección IP especificada.

Cada dirección IP se identifica mediante el ID de la dirección IP. Puede obtener este valor usando la consola de Route 53. En la página del punto de conexión correspondiente, en la sección de direcciones IP, consulte la columna IP address ID (ID de dirección IP). También puede obtener el valor mediante programación utilizando [ListResolverEndpointIpAddresses](#)

Estadísticas válidas: Sum

Unidades: recuento

CloudWatch Métricas detalladas del solucionador de VPC Route 53

El solucionador de VPC Route 53 proporciona métricas de RNI mejoradas y de servidores de nombres de destino como funciones opcionales para los puntos finales. Estas métricas se envían a CloudWatch intervalos de 1 minuto.

Note

- Las métricas detalladas no están habilitadas de forma predeterminada, pero se pueden habilitar a nivel de punto final. Estas métricas se pueden habilitar mediante programación al crear o actualizar los puntos finales mediante los `RniEnhancedMetricsEnabled` indicadores y `TargetNameServerMetricsEnabled`. Para obtener más información, consulte [CreateResolverEndpoint](#) y [UpdateResolverEndpoint](#).
- Se aplican CloudWatch precios y cargos estándar por el uso de las métricas detalladas de los puntos finales de Route 53 Resolver. Para obtener más información, consulta los [CloudWatch precios de Amazon](#).

Temas

- [Métricas mejoradas de RNI](#)
- [Métricas del servidor de nombres de destino](#)

Métricas mejoradas de RNI

Route 53 Resolver publica métricas mejoradas de RNI en Amazon CloudWatch para monitorear el rendimiento y el estado de los puntos finales y las direcciones IP de Resolver. El espacio de `AWS/Route53Resolver` nombres incluye las siguientes métricas mejoradas de RNI para los puntos de conexión entrantes y salientes de Route 53 Resolver en la dimensión `R: EndpointId RniId`

P90 ResponseTime

El percentil 90 de latencia de respuesta de las consultas de DNS recibidas por la IP del Resolver (`RniId`) asociada al punto final del Resolver (`EndpointId`)

Estadísticas válidas: máximo

Unidades: microsegundos

ServFailQueries

Número de respuestas SERVFAIL a las consultas de DNS enviadas a la IP del Resolver (`RniId`) asociada al punto final del Resolver (`EndpointId`)

Estadísticas válidas: Sum

Unidades: recuento

NxDomainQueries

Número de respuestas NXDOMAIN a las consultas de DNS enviadas a la IP del Resolver (`RniId`) asociada al punto final del Resolver (`EndpointId`)

Estadísticas válidas: Sum

Unidades: recuento

RefusedQueries

Número de respuestas RECHAZADAS a las consultas de DNS enviadas a la IP del Resolver (`RniId`) asociada al punto final del Resolver (`EndpointId`)

Estadísticas válidas: Sum

Unidades: recuento

FormErrorQueries

Número de respuestas anteriores a las consultas de DNS enviadas a la IP del Resolver (RniId) asociada al punto final del Resolver () EndpointId

Estadísticas válidas: Sum

Unidades: recuento

TimeoutQueries

Número de tiempos de espera de las consultas de DNS enviadas a la IP del Resolver (RniId) asociada al punto final del Resolver () EndpointId

Estadísticas válidas: Sum

Unidades: recuento

Métricas del servidor de nombres de destino

Route 53 Resolver publica las métricas del servidor de nombres de destino en Amazon CloudWatch para supervisar el rendimiento y la disponibilidad de los servidores de nombres de destino asociados a los puntos finales de Resolver. El espacio de AWS/Route53Resolver nombres incluye las siguientes métricas detalladas para los puntos de conexión salientes de Route 53 Resolver en dimensiones: EndpointID TargetNameServerIP

P90 ResponseTime

El percentil 90 de latencia de respuesta de la IP del servidor de nombres de destino (TargetNameServerIP) para las consultas de DNS enviadas a través del punto final del Resolver () EndpointID

Estadísticas válidas: máximo

Unidades: microsegundos

RequestQueries

Número de consultas de DNS enviadas a la IP del servidor de nombres de destino (TargetNameServerIP) a través del punto final del Resolver (). EndpointID

Estadísticas válidas: Sum

Unidades: recuento

TimeoutQueries

Número de consultas de DNS enviadas a través del punto final del Resolver (EndpointID) que han agotado el tiempo de espera en la IP del servidor de nombres de destino (TargetNameServerIP).

Estadísticas válidas: Sum

Unidades: recuento

Note

En algunos casos, se pueden observar brechas en las métricas de VPC Resolver (ResolverEndpointCapacityStatus) y en las métricas mejoradas de RNI. Estas brechas pueden producirse cuando las interfaces de red se someten a procesos programados y consecutivos de mantenimiento o actualización. Una vez que devolvemos una interfaz de red al servicio, nuestro servicio tarda al menos 1 minuto en recopilar datos operativos y publicar estas métricas. Estas brechas no indican que su punto final de VPC Resolver esté sufriendo una interrupción. Si está configurando una CloudWatch alarma para estas métricas, le recomendamos lo siguiente:

- Configura la alarma en «Tratar los datos faltantes como si se ignoraran», o
- Configure un período de evaluación de más de cinco minutos para el umbral de alarma.

Estos ajustes ayudarán a reducir las falsas alarmas durante las actividades de mantenimiento normales.

Dimensiones de las métricas del solucionador de VPC de Route 53

Las métricas de VPC Resolver de Route 53 para los puntos finales entrantes y salientes utilizan el espacio de `AWS/Route53Resolver` nombres y proporcionan métricas para las siguientes dimensiones:

- `EndpointId`: Si especificas un valor para la `EndpointId` dimensión, CloudWatch devuelve el número de consultas de DNS del punto final especificado. Si no lo especifica `EndpointId`, CloudWatch devuelve el número de consultas de DNS de todos los puntos finales que creó la AWS cuenta actual.

- RniIdse admite la dimensión OutboundQueryAggregateVolume y las InboundQueryVolume métricas.
- EndpointId, RniId la dimensión es compatible con P90ResponseTime, ServFailQueries, NxDomainQueries RefusedQueries FormErrorQueries, y TimeoutQueries para la dirección IP de la resolución asociada al punto final de la resolución.
- EndpointID, TargetNameServerIP la dimensión es compatible con P90ResponseTimeRequestQueries, y TimeoutQueries para el servidor de nombres de destino asociado al punto final de la resolución.

Supervisión de los grupos de reglas de Resolver DNS Firewall con Amazon CloudWatch

Puede utilizar Amazon CloudWatch para supervisar el número de consultas de DNS que filtran los grupos de reglas de Resolver DNS Firewall. Amazon CloudWatch recopila y procesa datos sin procesar para convertirlos en métricas legibles y prácticamente en tiempo real. Estas estadísticas se registran durante un periodo de dos semanas, de forma que pueda obtener acceso a información histórica y obtener una mejor perspectiva sobre el desempeño de sus recursos. De forma predeterminada, los datos métricos de los grupos de reglas del firewall de DNS se envían automáticamente a CloudWatch intervalos de cinco minutos.

Para obtener más información sobre DNS Firewall, consulte [Uso de DNS Firewall para filtrar el tráfico de DNS saliente](#). Para obtener más información CloudWatch, consulta [¿Qué es Amazon CloudWatch?](#) en la Guía del CloudWatch usuario de Amazon.

Métricas y dimensiones del Resolver DNS Firewall

Al asociar un grupo de reglas del firewall de DNS de Resolver a una VPC para filtrar las consultas de DNS, el firewall de DNS comienza a enviar métricas y dimensiones una vez cada 5 minutos a CloudWatch aproximadamente las consultas que filtra. Para obtener información acerca de las métricas y dimensiones de DNS Firewall, consulte [CloudWatch métricas de Resolver DNS Firewall](#).

Puedes usar los siguientes procedimientos para ver las métricas en la CloudWatch consola o consultarlas con AWS Command Line Interface (AWS CLI).

Para ver las métricas del firewall de DNS mediante la CloudWatch consola

1. Abra la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>.

2. En la barra de navegación, elija la región que desea ver.
3. En el panel de navegación, seleccione Métricas.
4. En la pestaña Todas las métricas, elija Route 53 VPC Resolver.
5. Elija una métrica que le interese.

Para ver las métricas mediante el AWS CLI

- En el símbolo del sistema, ejecute el siguiente comando:

```
aws cloudwatch list-metrics --namespace "AWS/Route53Resolver"
```

Temas

- [CloudWatch métricas de Resolver DNS Firewall](#)

CloudWatch métricas de Resolver DNS Firewall

El espacio de `AWS/Route53Resolver` nombres incluye métricas para los grupos de reglas de Resolver DNS Firewall.

Temas

- [Métricas de los grupos de reglas de Resolver DNS Firewall](#)
- [Métricas para VPCs](#)
- [Métricas para el grupo de reglas de firewall y la asociación de VPC](#)
- [Métricas de una lista de dominios en un grupo de reglas de firewall](#)

Métricas de los grupos de reglas de Resolver DNS Firewall

FirewallRuleGroupQueryVolume

El número de consultas de DNS Firewall que coinciden con un grupo de reglas de firewall (especificado por `FirewallRuleGroupId`).

Dimensiones: `FirewallRuleGroupId`

Estadísticas válidas: Sum

Unidades: recuento

Métricas para VPCs

VpcFirewallQueryVolume

El número de consultas de DNS Firewall de una VPC (especificado por VpcId).

Dimensiones: VpcId

Estadísticas válidas: Sum

Unidades: recuento

Métricas para el grupo de reglas de firewall y la asociación de VPC

FirewallRuleGroupVpcQueryVolume

El número de consultas de DNS Firewall de una VPC (especificado por VpcId) que coinciden con un grupo de reglas de firewall (especificado por FirewallRuleGroupId).

Dimensiones: FirewallRuleGroupId, VpcId

Estadísticas válidas: Sum

Unidades: recuento

Métricas de una lista de dominios en un grupo de reglas de firewall

FirewallRuleQueryVolume

El número de consultas de DNS Firewall que coinciden con una lista de dominios de firewall (especificada por FirewallDomainListId) dentro de un grupo de reglas de firewall (especificado por FirewallRuleGroupId).

Dimensiones: FirewallRuleGroupId, FirewallDomainListId

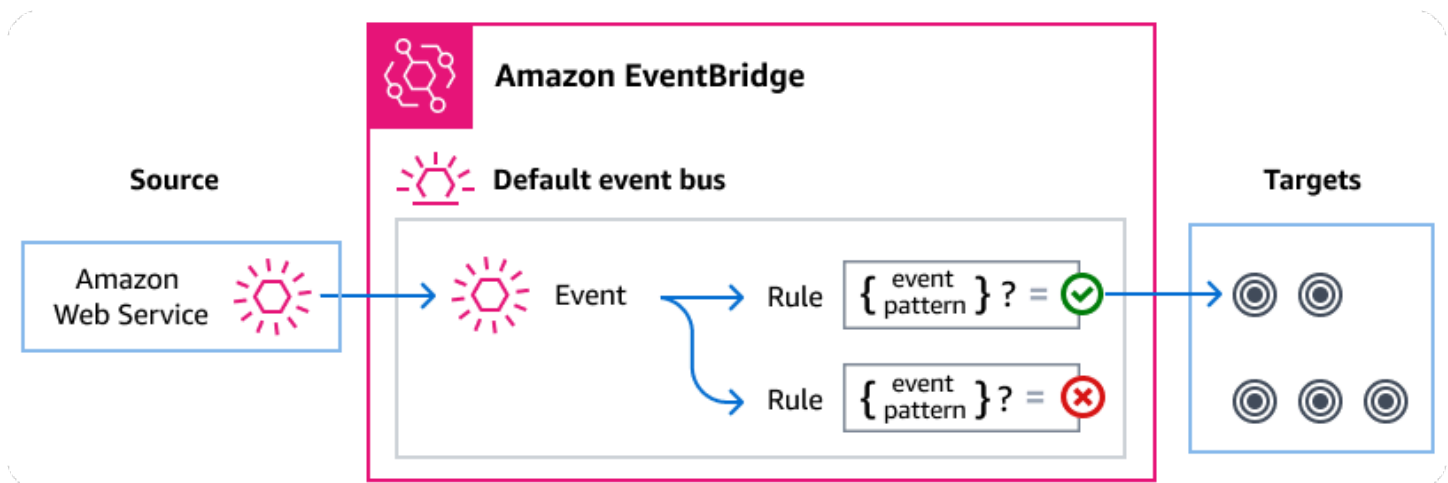
Estadísticas válidas: Sum

Unidades: recuento

Administrar los eventos de Resolver DNS Firewall mediante Amazon EventBridge

Amazon EventBridge es un servicio sin servidor que utiliza eventos para conectar los componentes de la aplicación, lo que facilita la creación de aplicaciones escalables basadas en eventos. La arquitectura basada en eventos es un estilo de creación de sistemas de software de acoplamiento flexible que funcionan juntos emitiendo eventos y respondiendo a ellos. Los eventos representan un cambio en un recurso o entorno.

Como ocurre con muchos AWS servicios, el firewall de DNS genera y envía eventos al bus de eventos EventBridge predeterminado. (El bus de eventos predeterminado se aprovisiona de manera automática en cada cuenta de AWS). Un bus de eventos es un enrutador que recibe eventos y los envía a cero o más destinos u objetivos. Las reglas que se especifican al bus de eventos evalúan los eventos a medida que llegan. Cada regla comprueba si un evento coincide con el patrón de evento de la regla. Si el evento coincide, el bus de eventos envía el evento a los destinos especificados.



Temas

- [Resolver eventos de DNS Firewall](#)
- [Enviar eventos de Resolver DNS Firewall mediante reglas EventBridge](#)
- [Amazon EventBridge permisos](#)
- [EventBridge Recursos adicionales](#)
- [Referencia detallada de los eventos de Resolver DNS Firewall](#)

Resolver eventos de DNS Firewall

El solucionador de VPC envía automáticamente los eventos del firewall de DNS al bus de EventBridge eventos predeterminado. Puede crear reglas en el bus de eventos; cada regla incluye un patrón de eventos y uno o más objetivos. Los eventos que coinciden con el patrón de eventos de una regla se envían a los objetivos especificados en [función del mejor esfuerzo](#). Es posible que los eventos se entreguen fuera de servicio.

DNS Firewall genera los siguientes eventos. Para obtener más información, consulte [EventBridge](#) en la Guía del usuario de Amazon EventBridge .

Tipo de detalle del evento	Description (Descripción)
Bloqueo de DNS Firewall	Cualquier acción de bloqueo realizada en un dominio.
Alerta de DNS Firewall	Cualquier acción de alerta realizada en un dominio.

Enviar eventos de Resolver DNS Firewall mediante reglas EventBridge

Para que el bus de eventos EventBridge predeterminado envíe los eventos del firewall de DNS a un destino, debe crear una regla que contenga un patrón de eventos que coincida con los datos de los eventos del firewall de DNS que desee.

El proceso para crear una regla consta de los siguientes pasos generales:

1. La creación de un patrón de eventos para la regla que especifica:
 - El solucionador de VPC es la fuente de los eventos que evalúa la regla.
 - (Opcional): cualquier otro dato del evento con el que se pueda comparar.

Para obtener más información, consulte [???](#)

2. (Opcional): Crear un transformador de entrada que personalice los datos del evento antes de EventBridge pasar la información al destino de la regla.

Para obtener más información, consulte [Transformación de entrada](#) en la Guía del usuario de EventBridge .

3. Especifica los objetivos a los que quieres EventBridge entregar los eventos que coincidan con el patrón de eventos.

Los objetivos pueden ser otros AWS servicios, aplicaciones software-as-a-service (SaaS), destinos de API u otros puntos finales personalizados. Para más información, consulte [Destinos](#) en la Guía del usuario de EventBridge .

Para obtener instrucciones detalladas sobre cómo crear reglas de bus de eventos, consulte [Creación de reglas que reaccionan a eventos](#) en la Guía del usuario de EventBridge .

Crear patrones de eventos para los eventos de Resolver DNS Firewall

Cuando el firewall de DNS envía un evento al bus de eventos predeterminado, EventBridge utiliza el patrón de eventos definido para cada regla para determinar si el evento debe enviarse a los objetivos de la regla. Un patrón de eventos coincide con los datos de los eventos de DNS Firewall deseados. Cada patrón de eventos es un objeto JSON que contiene:

- Un atributo `source` que identifica el servicio que envía el evento. En el caso de los eventos de DNS Firewall, la fuente es `aws.route53resolver`.
- (Opcional): un atributo `detail-type` que contiene una matriz de los tipos de eventos que deben coincidir.
- (Opcional): un atributo `detail` que contiene cualquier otro dato de evento con el que coincidir.

Por ejemplo, el siguiente patrón de eventos coincide con los eventos de alerta y bloqueo de DNS Firewall:

```
{
  "source": ["aws.route53resolver"],
  "detail-type": ["DNS Firewall Block", "DNS Firewall Alert"]
}
```

Mientras que el siguiente patrón de eventos coincide con una acción de BLOQUEO:

```
{
  "source": ["aws.route53resolver"],
  "detail-type": ["DNS Firewall Block"]
}
```

DNS Firewall envía el mismo evento para el mismo dominio solo una vez en un período de 6 horas. Por ejemplo:

1. La instancia i-123 envió una consulta de DNS a `exampledomain.com` en el momento T1. DNS Firewall envía una alerta o un evento de bloqueo, ya que es la primera vez que ocurre.
2. La instancia i-123 envió un `DNSQuery` `exampledomain.com` en el momento T1+30 minutos. DNS Firewall no envía una alerta ni bloquea un evento, ya que este evento se ha repetido dentro de las últimas 6 horas.
3. La instancia i-123 envió una consulta de DNS a `exampledomain.com` en el momento T1+7 horas. En este caso, DNS Firewall envía una alerta o bloquea el evento, ya que ha ocurrido luego del periodo de 6 horas.

Para obtener más información sobre la escritura de los patrones de eventos, consulte [Patrones de eventos](#) en la Guía del usuario de EventBridge .

Probando patrones de eventos para eventos de DNS Firewall en EventBridge

Puede usar el EventBridge Sandbox para definir y probar rápidamente un patrón de eventos, sin tener que completar el proceso más amplio de crear o editar una regla. Con el Sandbox, puede definir un patrón de eventos y usar un evento de muestra para confirmar que el patrón coincide con los eventos deseados. EventBridge le da la opción de crear una nueva regla utilizando ese patrón de eventos, directamente desde el entorno limitado.

Para obtener más información, consulte [Probar un patrón de eventos mediante el EventBridge entorno aislado](#) en la Guía del EventBridge usuario.

Creación de una EventBridge regla y un objetivo para el firewall de DNS

El siguiente procedimiento muestra cómo crear una regla que permita EventBridge enviar eventos para todas las acciones de alerta y bloqueo del Firewall de DNS, y cómo añadir una AWS Lambda función como destino de la regla.

1. Se utiliza AWS CLI para crear una EventBridge regla:

```
aws events put-rule \  
--event-pattern "{\"source\":  
[\"aws.route53resolver\"],\"detail-type\":  
[\"DNS Firewall Block\", \"DNS Firewall Alert\"]}" \  
--name dns-firewall-rule
```

2. Asocie una función de Lambda como destino para dicha regla:

```
AWS events put-targets --rule dns-firewall-rule --targets  
Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:<your_function>
```

3. Para añadir los permisos necesarios para invocar el destino, ejecute el siguiente comando de AWS CLI Lambda:

```
AWS lambda add-permission --function-name <your_function> --statement-  
id 1 --action 'lambda:InvokeFunction' --principal events.amazonaws.com
```

Amazon EventBridge permisos

DNS Firewall no requiere permisos adicionales para entregar eventos a Amazon EventBridge.

Los objetivos que especifique pueden necesitar permisos o configuraciones específicos. Para obtener más información sobre el uso de servicios específicos para los destinos, consulte [Destinos de Amazon EventBridge](#) en la Guía del usuario de Amazon EventBridge .

EventBridge Recursos adicionales

Consulte los siguientes temas de la [Guía del Amazon EventBridge usuario](#) para obtener más información sobre EventBridge cómo procesar y administrar eventos.

- Para obtener información detallada sobre cómo funcionan los buses de eventos, consulte [bus de eventos de Amazon EventBridge](#).
- Para obtener información sobre la estructura de los eventos, consulte [Eventos](#).
- Para obtener información sobre cómo crear patrones de eventos EventBridge para usarlos al comparar eventos con reglas, consulte [Patrones de eventos](#).
- Para obtener información sobre la creación de reglas para especificar qué eventos procesa EventBridge , consulte [Reglas](#).
- Para obtener información sobre cómo especificar a qué servicios u otros destinos se EventBridge envían los eventos coincidentes, consulte [Targets](#).

Referencia detallada de los eventos de Resolver DNS Firewall

Todos los eventos de los AWS servicios tienen un conjunto común de campos que contienen metadatos sobre el evento, como el AWS servicio que lo origina, la hora en que se generó el

evento, la cuenta y la región en las que tuvo lugar el evento, etc. Para ver las definiciones de estos campos generales, consulte [Referencia de estructura de eventos](#) en la Guía del usuario de Amazon EventBridge .

Además, cada evento tiene un campo `detail` que contiene datos específicos de ese evento en particular. La siguiente referencia define los campos de detalle para los distintos eventos de DNS Firewall.

Cuando se utilice EventBridge para seleccionar y administrar eventos del firewall de DNS, es útil tener en cuenta lo siguiente:

- El campo `source` para todos los eventos de DNS Firewall está establecido en `aws.route53resolver`.
- El campo `detail-type` especifica el tipo de evento.

Por ejemplo, `DNS Firewall Block` o `DNS Firewall Alert`.

- El campo `detail` contiene los datos específicos de ese evento en particular.

Para obtener más información sobre cómo construir patrones de eventos que permitan que las reglas coincidan con los eventos de DNS Firewall, consulte [Patrones de eventos](#) en la Guía del usuario de Amazon EventBridge .

Para obtener más información sobre los eventos y cómo EventBridge los procesa, consulte [Amazon EventBridge los eventos](#) en la Guía del Amazon EventBridge usuario.

Temas

- [Detalles de un evento de alerta de DNS Firewall](#)
- [Detalles de un evento de bloqueo de DNS Firewall](#)

Detalles de un evento de alerta de DNS Firewall

A continuación, se muestran los campos de detalle de los detalles del evento de estado de alerta.

Los campos `source` y `detail-type` se incluyen porque contienen valores específicos para los eventos de Route 53.

```
{...,  
  "detail-type": "DNS Firewall Alert",
```

```
"source": "aws.route53resolver",
...,
"detail": {
  "account-id": "string",
  "last-observed-at": "string",
  "query-name": "string",
  "query-type": "string",
  "query-class": "string",
  "transport": "string",
  "firewall-rule-action": "string",
  "firewall-rule-group-id": "string",
  "firewall-domain-list-id": "string",
  "firewall-protection": "string",
  "resources": [{
    "resource-type": "string",
    "instance-details": {
      "id": "string",
    }
  },
  {
    "resource-type": "string",
    "resolver-endpoint-details": {
      "id": "string"
    }
  }
]
```

detail-type

Identifica el tipo de evento.

Para este evento, este valor es `DNS Firewall Alert`.

source

Identifica el servicio que generó el evento. Para los eventos del DNS Firewall, este valor es `aws.route53resolver`.

detail

Un objeto JSON que contiene información sobre el evento. El servicio que genera el evento determina el contenido de este campo.

Para este evento, estos datos incluyen lo siguiente:

account-id

El ID de la persona Cuenta de AWS que creó la VPC.

last-observed-at

La marca de tiempo del momento en que se realizó la Alert/Block consulta en la VPC.

query-name

El nombre de dominio (example.com) o nombre del subdominio (www.example.com) que se especificó en la consulta.

query-type

El tipo de registro DNS que se ha especificado en la solicitud o CUALQUIERA. Para obtener información acerca de los tipos que admite Route 53, consulte [Tipos de registros de DNS admitidos](#).

query-class

La clase de consulta.

transport

El protocolo utilizado para enviar la consulta de DNS.

firewall-rule-action

La acción especificada por la regla que coincidió con el nombre de dominio de la consulta. ALERT o BLOCK.

firewall-rule-group-id

El ID del grupo de reglas de DNS Firewall de que coincidió con el nombre de dominio de la consulta. Para obtener más información sobre los grupos de reglas de firewall, consulte [Reglas y grupos de reglas de DNS Firewall](#) de DNS Firewall.

firewall-domain-list-id

La lista de dominios utilizada por la regla que coincidió con el nombre de dominio de la consulta.

firewall-protection

La protección avanzada del firewall de DNS: DGA, DICTIONARY_DGA o DNS_TUNNELING. Para obtener más información sobre DNS Firewall, consulte [Resolver DNS Firewall Advanced](#).

resource

Contiene los tipos de recursos y más detalles sobre ellos.

resource-type

Especifica el tipo de recurso, como un punto de conexión de Resolver o una instancia de VPC.

resource-type-detail

Detalles adicionales sobre el recurso.

Example Evento de alerta de DNS Firewall

El siguiente es un evento de alerta de ejemplo.

```
{
  "version": "1.0",
  "id": "8e5622f9-d81c-4d81-612a-9319e7ee2506",
  "detail-type": "DNS Firewall Alert",
  "source": "aws.route53resolver",
  "account": "123456789012",
  "time": "2023-05-30T21:52:17Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "account-id": "123456789012",
    "last-observed-at": "2023-05-30T20:15:15.900Z",
    "query-name": "15.3.4.32.in-addr.arpa.",
    "query-type": "A",
    "query-class": "IN",
    "transport": "UDP",
    "firewall-rule-action": "ALERT",
    "firewall-rule-group-id": "rslvr-frg-01234567890abcdef",
    "firewall-domain-list-id": "rslvr-fdl-01234567890abcdef",
    "firewall-protection": "DGA",
    "resources": [{
      "resource-type": "instance",
      "instance-details": {
        "id": "i-05746eb48123455e0",
      }
    }],
    {
      "resource-type": "resolver-endpoint",
```

```

    "resolver-endpoint-details": {
      "id": "i-05746eb48123455e0"
    }
  ],
  "src-addr": "4.5.64.102",
  "src-port": "56067",
  "vpc-id": "vpc-7example"
}

```

Detalles de un evento de bloqueo de DNS Firewall

A continuación se *event name* muestran los campos de detalles de.

Los campos `source` y `detail-type` se incluyen porque contienen valores específicos para los eventos de Route 53.

```

{...,
  "detail-type": "DNS Firewall Block",
  "source": "aws.route53resolver",
  ...,
  "detail": {
    "account-id": "string",
    "last-observed-at": "string",
    "query-name": "string",
    "query-type": "string",
    "query-class": "string",
    "transport": "string",
    "firewall-rule-action": "string",
    "firewall-rule-group-id": "string",
    "firewall-domain-list-id": "string",
    "firewall-protection": "string",
    "resources": [{
      "resource-type": "string",
      "instance-details": {
        "id": "string",
      }
    }],
  },
  {
    "resource-type": "string",
    "resolver-endpoint-details": {
      "id": "string"
    }
  }
}

```

```
    }  
  }  
]
```

detail-type

Identifica el tipo de evento.

Para este evento, este valor es `DNS Firewall Alert`.

source

Identifica el servicio que generó el evento. Para los eventos del DNS Firewall, este valor es `aws.route53resolver`.

detail

Un objeto JSON que contiene información sobre el evento. El servicio que genera el evento determina el contenido de este campo.

Para este evento, estos datos incluyen lo siguiente:

account-id

El ID de la persona Cuenta de AWS que creó la VPC.

last-observed-at

La marca de tiempo del momento en que se realizó la Alert/Block consulta en la VPC.

query-name

El nombre de dominio (example.com) o nombre del subdominio (www.example.com) que se especificó en la consulta.

query-type

El tipo de registro DNS que se ha especificado en la solicitud o CUALQUIERA. Para obtener información acerca de los tipos que admite Route 53, consulte [Tipos de registros de DNS admitidos](#).

query-class

La clase de consulta.

transport

El protocolo utilizado para enviar la consulta de DNS.

firewall-rule-action

La acción especificada por la regla que coincidió con el nombre de dominio de la consulta.
ALERT o BLOCK.

firewall-rule-group-id

El ID del grupo de reglas de DNS Firewall de que coincidió con el nombre de dominio de la consulta. Para obtener más información sobre los grupos de reglas de firewall, consulte [Reglas y grupos de reglas de DNS Firewall](#) de DNS Firewall.

firewall-domain-list-id

La lista de dominios utilizada por la regla que coincidió con el nombre de dominio de la consulta.

firewall-protection

La protección avanzada del firewall de DNS: DGA, DICTIONARY_DGA o DNS_TUNNELING.
Para obtener más información sobre DNS Firewall, consulte [Resolver DNS Firewall Advanced](#).

resource

Contiene los tipos de recursos y más detalles sobre ellos.

resource-type

Especifica el tipo de recurso, como un punto de conexión de Resolver o una instancia de VPC.

resource-type-detail

Detalles adicionales sobre el recurso.

Example Evento de ejemplo de

El siguiente es un evento de bloqueo de ejemplo.

```
{
  "version": "1.0",
  "id": "8e5622f9-d81c-4d81-612a-9319e7ee2506",
  "detail-type": "DNS Firewall Block",
  "source": "aws.route53resolver",
  "account": "123456789012",
```

```
"time": "2023-05-30T21:52:17Z",
"region": "us-west-2",
"resources": [],
"detail": {
  "account-id": "123456789012",
  "last-observed-at": "2023-05-30T20:15:15.900Z",
  "query-name": "15.3.4.32.in-addr.arpa.",
  "query-type": "A",
  "query-class": "IN",
  "transport": "UDP",
  "firewall-rule-action": "BLOCK",
  "firewall-rule-group-id": "rslvr-frg-01234567890abcdef",
  "firewall-domain-list-id": "rslvr-fdl-01234567890abcdef",
  "firewall-protection": "DNS_TUNNELING",
  "resources": [{
    "resource-type": "instance",
    "instance-details": {
      "id": "i-05746eb48123455e0"
    }
  },
  {
    "resource-type": "resolver-endpoint",
    "resolver-endpoint-details": {
      "id": "i-05746eb48123455e0",
    }
  }
],
"src-addr": "4.5.64.102",
"src-port": "56067",
"vpc-id": "vpc-7example"
}
```

Registrar llamadas a la API de Amazon Route 53 con AWS CloudTrail

Route 53 está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Route 53. CloudTrail captura todas las llamadas a la API de Route 53 como eventos, incluidas las llamadas desde la consola de Route 53 y las llamadas en código a Route 53 APIs. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Route 53. Si no configura

una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a Route 53, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Temas

- [La información de Route 53 está en CloudTrail](#)
- [Visualización de eventos de Route 53 en el historial de eventos](#)
- [Descripción de las entradas de archivos de registro de Route 53](#)

La información de Route 53 está en CloudTrail

CloudTrail está habilitada en su AWS cuenta al crear la cuenta. Cuando se produce una actividad en Route 53, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los eventos recientes en su AWS cuenta. Para obtener más información, consulta Cómo [ver eventos con el historial de CloudTrail eventos](#).

Para tener un registro continuo de los eventos de su AWS cuenta, incluidos los eventos de la Ruta 53, cree un sendero. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De manera predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de . La ruta registra los eventos de todas las regiones de la AWS partición y entrega los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para obtener más información, consulte lo siguiente:

- [Introducción a la creación de registros de seguimiento](#)
- [CloudTrail servicios e integraciones compatibles](#)
- [Configuración de las notificaciones de Amazon SNS para CloudTrail](#)
- [Recibir archivos de CloudTrail registro de varias regiones](#) y [recibir archivos de CloudTrail registro de varias cuentas](#)

Todas las acciones de Route 53 se registran CloudTrail y se documentan en la [referencia de la API de Amazon Route 53](#). Por ejemplo, las llamadas a las `CreateHostedZone` `RegisterDomain` acciones y las llamadas generan entradas en los archivos de CloudTrail registro. `CreateHealthCheck`

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales raíz o del usuario de IAM.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el [elemento `userIdentity` de CloudTrail](#).

Visualización de eventos de Route 53 en el historial de eventos

CloudTrail le permite ver los eventos recientes en el historial de eventos. Para ver los eventos de solicitudes de API de Route 53, debe elegir EE. UU. Este (Norte de Virginia) en el selector de regiones de la parte superior de la consola. Para obtener más información, consulte [Visualización de eventos con el historial de CloudTrail eventos](#) en la Guía del AWS CloudTrail usuario.

Descripción de las entradas de archivos de registro de Route 53

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

El elemento `eventName` identifica la acción que se ha producido. (En CloudTrail los registros, la primera letra está en minúscula para las acciones de registro de dominios, aunque en los nombres de las acciones esté en mayúscula. Por ejemplo, `UpdateDomainContact` aparece como `updateDomainContact` en los registros). CloudTrail admite todas las acciones de la API de Route 53. El siguiente ejemplo muestra una entrada de CloudTrail registro que muestra las siguientes acciones:

- Enumere las zonas alojadas que están asociadas a una AWS cuenta
- Crear una comprobación de estado
- Crear dos registros
- Eliminar una zona alojada

- Actualizar la información de un dominio registrado
- Cree un punto final saliente de Route 53 VPC Resolver

```
{
  "Records": [
    {
      "apiVersion": "2013-04-01",
      "awsRegion": "us-east-1",
      "eventID": "1cdbea14-e162-43bb-8853-f9f86d4739ca",
      "eventName": "ListHostedZones",
      "eventSource": "route53.amazonaws.com",
      "eventTime": "2015-01-16T00:41:48Z",
      "eventType": "AwsApiCall",
      "eventVersion": "1.02",
      "recipientAccountId": "444455556666",
      "requestID": "741e0df7-9d18-11e4-b752-f9c6311f3510",
      "requestParameters": null,
      "responseElements": null,
      "sourceIPAddress": "192.0.2.92",
      "userAgent": "Apache-HttpClient/4.3 (java 1.5)",
      "userIdentity": {
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "accountId": "111122223333",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "type": "IAMUser",
        "userName": "smithj"
      }
    },
    {
      "apiVersion": "2013-04-01",
      "awsRegion": "us-east-1",
      "eventID": "45ec906a-1325-4f61-b133-3ef1012b0cbc",
      "eventName": "CreateHealthCheck",
      "eventSource": "route53.amazonaws.com",
      "eventTime": "2018-01-16T00:41:57Z",
      "eventType": "AwsApiCall",
      "eventVersion": "1.02",
      "recipientAccountId": "444455556666",
      "requestID": "79915168-9d18-11e4-b752-f9c6311f3510",
      "requestParameters": {
        "callerReference": "2014-05-06 64832",
```

```

        "healthCheckConfig": {
            "ipAddress": "192.0.2.249",
            "port": 80,
            "type": "TCP"
        }
    },
    "responseElements": {
        "healthCheck": {
            "callerReference": "2014-05-06 64847",
            "healthCheckConfig": {
                "failureThreshold": 3,
                "ipAddress": "192.0.2.249",
                "port": 80,
                "requestInterval": 30,
                "type": "TCP"
            },
            "healthCheckVersion": 1,
            "id": "b3c9cbc6-cd18-43bc-93f8-9e557example"
        },
        "location": "https://route53.amazonaws.com/2013-04-01/healthcheck/
b3c9cbc6-cd18-43bc-93f8-9e557example"
    },
    "sourceIpAddress": "192.0.2.92",
    "userAgent": "Apache-HttpClient/4.3 (java 1.5)",
    "userIdentity": {
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "accountId": "111122223333",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "type": "IAMUser",
        "userName": "smithj"
    }
},
{
    "additionalEventData": {
        "Note": "Do not use to reconstruct hosted zone"
    },
    "apiVersion": "2013-04-01",
    "awsRegion": "us-east-1",
    "eventID": "883b14d9-2f84-4005-8bc5-c7bf0cebc116",
    "eventName": "ChangeResourceRecordSets",
    "eventSource": "route53.amazonaws.com",
    "eventTime": "2018-01-16T00:41:43Z",
    "eventType": "AwsApiCall",

```

```

"eventVersion": "1.02",
"recipientAccountId": "444455556666",
"requestID": "7081d4c6-9d18-11e4-b752-f9c6311f3510",
"requestParameters": {
  "changeBatch": {
    "changes": [
      {
        "action": "CREATE",
        "resourceRecordSet": {
          "name": "prod.example.com.",
          "resourceRecords": [
            {
              "value": "192.0.1.1"
            },
            {
              "value": "192.0.1.2"
            },
            {
              "value": "192.0.1.3"
            },
            {
              "value": "192.0.1.4"
            }
          ],
          "ttl": 300,
          "type": "A"
        }
      },
      {
        "action": "CREATE",
        "resourceRecordSet": {
          "name": "test.example.com.",
          "resourceRecords": [
            {
              "value": "192.0.1.1"
            },
            {
              "value": "192.0.1.2"
            },
            {
              "value": "192.0.1.3"
            },
            {
              "value": "192.0.1.4"
            }
          ]
        }
      }
    ]
  }
}

```

```

        }
      ],
      "ttl": 300,
      "type": "A"
    }
  ],
  "comment": "Adding subdomains"
},
"hostedZoneId": "Z1PA6795UKMFR9"
},
"responseElements": {
  "changeInfo": {
    "comment": "Adding subdomains",
    "id": "/change/C156SRE0X2ZB10",
    "status": "PENDING",
    "submittedAt": "Jan 16, 2018 12:41:43 AM"
  }
},
"sourceIPAddress": "192.0.2.92",
"userAgent": "Apache-HttpClient/4.3 (java 1.5)",
"userIdentity": {
  "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "accountId": "111122223333",
  "arn": "arn:aws:iam::111122223333:user/smithj",
  "principalId": "A1B2C3D4E5F6G7EXAMPLE",
  "type": "IAMUser",
  "userName": "smithj"
}
},
{
  "apiVersion": "2013-04-01",
  "awsRegion": "us-east-1",
  "eventID": "0cb87544-ebec-40a9-9812-e9dda1962cb2",
  "eventName": "DeleteHostedZone",
  "eventSource": "route53.amazonaws.com",
  "eventTime": "2018-01-16T00:41:37Z",
  "eventType": "AwsApiCall",
  "eventVersion": "1.02",
  "recipientAccountId": "444455556666",
  "requestID": "6d5d149f-9d18-11e4-b752-f9c6311f3510",
  "requestParameters": {
    "id": "Z1PA6795UKMFR9"
  }
},

```

```

    "responseElements": {
      "changeInfo": {
        "id": "/change/C1SIJYUYIKVJWP",
        "status": "PENDING",
        "submittedAt": "Jan 16, 2018 12:41:36 AM"
      }
    },
    "sourceIPAddress": "192.0.2.92",
    "userAgent": "Apache-HttpClient/4.3 (java 1.5)",
    "userIdentity": {
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "accountId": "111122223333",
      "arn": "arn:aws:iam::111122223333:user/smithj",
      "principalId": "A1B2C3D4E5F6G7EXAMPLE",
      "type": "IAMUser",
      "userName": "smithj"
    }
  },
  {
    "eventVersion": "1.05",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "A1B2C3D4E5F6G7EXAMPLE",
      "arn": "arn:aws:iam::111122223333:user/smithj",
      "accountId": "111122223333",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "userName": "smithj",
      "sessionContext": {
        "attributes": {
          "mfaAuthenticated": "false",
          "creationDate": "2018-11-01T19:43:59Z"
        }
      }
    },
    "invokedBy": "test"
  },
  "eventTime": "2018-11-01T19:49:36Z",
  "eventSource": "route53domains.amazonaws.com",
  "eventName": "updateDomainContact",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.92",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:52.0)
Gecko/20100101 Firefox/52.0",
  "requestParameters": {
    "domainName": {

```

```

        "name": "example.com"
      }
    },
    "responseElements": {
      "requestId": "034e222b-a3d5-4bec-8ff9-35877ff02187"
    },
    "additionalEventData": "Personally-identifying contact information is not
logged in the request",
    "requestId": "015b7313-bf3d-11e7-af12-cf75409087f6",
    "eventID": "f34f3338-aaf4-446f-bf0e-f72323bac94d",
    "eventType": "AwsApiCall",
    "recipientAccountId": "444455556666"
  },
  {
    "eventVersion": "1.05",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "A1B2C3D4E5F6G7EXAMPLE",
      "arn": "arn:aws:iam::111122223333:user/smithj",
      "accountId": "111122223333",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "sessionContext": {
        "attributes": {
          "mfaAuthenticated": "false",
          "creationDate": "2018-11-01T14:33:09Z"
        },
        "sessionIssuer": {
          "type": "Role",
          "principalId": "AROAIUZEZLWWZOEXAMPLE",
          "arn": "arn:aws:iam::123456789012:role/Admin",
          "accountId": "123456789012",
          "userName": "Admin"
        }
      }
    },
    "eventTime": "2018-11-01T14:37:19Z",
    "eventSource": "route53resolver.amazonaws.com",
    "eventName": "CreateResolverEndpoint",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.176",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:52.0)
Gecko/20100101 Firefox/52.0",
    "requestParameters": {
      "creatorRequestId": "123456789012",

```

```

        "name": "OutboundEndpointDemo",
        "securityGroupIds": [
            "sg-05618b249example"
        ],
        "direction": "OUTBOUND",
        "ipAddresses": [
            {
                "subnetId": "subnet-01cb0c4676example"
            },
            {
                "subnetId": "subnet-0534819b32example"
            }
        ],
        "tags": [],
    },
    "responseElements": {
        "resolverEndpoint": {
            "id": "rslvr-out-1f4031f1f5example",
            "creatorRequestId": "123456789012",
            "arn": "arn:aws:route53resolver:us-west-2:123456789012:resolver-
endpoint/rslvr-out-1f4031f1f5example",
            "name": "OutboundEndpointDemo",
            "securityGroupIds": [
                "sg-05618b249example"
            ],
            "direction": "OUTBOUND",
            "ipAddressCount": 2,
            "hostVPCId": "vpc-0de29124example",
            "status": "CREATING",
            "statusMessage": "[Trace id: 1-5bd1d51e-f2f3032eb75649f71example]
Creating the Resolver Endpoint",
            "creationTime": "2018-11-01T14:37:19.045Z",
            "modificationTime": "2018-11-01T14:37:19.045Z"
        },
    },
    "requestID": "3f066d98-773f-4628-9cba-4ba6eexample",
    "eventID": "cb05b4f9-9411-4507-813b-33cb0example",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
]
}

```

Solución de problemas de Amazon Route 53

Esta página abarca los siguientes temas de solución de problemas para Amazon Route 53:

1. Falta de disponibilidad del dominio:

- Conozca los motivos más comunes por los que el dominio podría no estar disponible en Internet, como la falta de confirmación del correo electrónico del registrante, los problemas con la transferencia del servicio DNS, la configuración incorrecta del servidor de nombres o la eliminación de zonas alojadas.

2. Suspensión del dominio:

- Obtenga información sobre las causas de la suspensión de un dominio (estado ClientHold) y cómo anular la suspensión del dominio, incluidos los dominios caducados, los cambios de correo electrónico de los registrantes no verificados y los problemas de procesamiento de pagos.

3. Error en la operación de dominio:

- Resuelva los errores en las operaciones de dominio, incluidos los problemas de registro, transferencia, renovación y actualización de contactos, causados por información de contacto no válida.

4. Transferencia de dominio fallida:

- Descubra los motivos más comunes de una transferencia de dominio fallida a Route 53, como la falta de autorización de la transferencia, los códigos de autorización no válidos o los problemas con los nombres de dominio internacionalizados.

5. La configuración de DNS no surte efecto:

- Solucione situaciones en las que los cambios en la configuración de DNS aún no se hayan aplicado, como el almacenamiento en caché del solucionador de DNS, las actualizaciones incorrectas del servidor de nombres y las múltiples zonas alojadas con el mismo nombre.

6. "Error "Server not found":

- Busque soluciones para los errores de "Server not found" en el navegador, como registros faltantes, valores de registro incorrectos o recursos no disponibles.

7. Enrutamiento del tráfico a buckets de S:

- Resuelva los problemas al intentar dirigir el tráfico a un bucket de Amazon S3 configurado para el alojamiento de un sitio web.

8. Problemas de facturación:

- Conozca los escenarios de facturación más comunes, como que se facture dos veces por la misma zona alojada, que se facturen varias facturas por dominios y que surjan problemas con el registro de dominios cuando la Cuenta de AWS está cerrada o se ha cerrado en forma definitiva.

Temas

- [Mi dominio no está disponible en Internet](#)
- [Mi dominio está suspendido \(el estado es ClientHold\)](#)
- [Se produjo un error en mi operación de dominio](#)
- [No se pudo transferir mi dominio a Amazon Route 53](#)
- [He cambiado la configuración de DNS, pero no ha tenido efecto](#)
- [Mi navegador muestra un error “Server not found”](#)
- [No puedo dirigir el tráfico a un bucket de Amazon S3 configurado para hospedar sitios web](#)
- [Me han facturado dos veces por la misma zona alojada](#)
- [Me cobraron varias facturas por mi dominio](#)
- [Mi cuenta de AWS está cerrada o se ha cerrado de forma definitiva y mi dominio está registrado con Route 53.](#)

Mi dominio no está disponible en Internet

A continuación, se muestran las razones más habituales por las que su dominio no está disponible en Internet.

Temas

- [Ha registrado un nuevo dominio, pero no hizo clic en el enlace del correo electrónico de confirmación](#)
- [Ha transferido el registro de dominio a Amazon Route 53, pero no ha transferido el servicio DNS](#)
- [Ha transferido el registro de dominio y ha especificado los servidores de nombres incorrectos en la configuración del dominio](#)
- [Ha transferido el servicio DNS en primer lugar, pero no ha esperado el tiempo suficiente antes de transferir el registro de dominio](#)
- [Ha eliminado la zona alojada que Route 53 utiliza para dirigir el tráfico de Internet del dominio.](#)

- [Su dominio se ha suspendido](#)

Ha registrado un nuevo dominio, pero no hizo clic en el enlace del correo electrónico de confirmación

Al registrar un nuevo dominio, ICANN requiere que confirmemos que es válida la dirección de correo electrónico de contacto del titular. Para confirmarlo, enviamos un correo electrónico que contiene un enlace. (Si no responde al primer correo electrónico, volvemos a enviarlo hasta dos veces más). Tiene entre 3 y 15 días para hacer clic en el enlace, según sea el dominio de nivel superior. Transcurrido ese tiempo, el enlace deja de funcionar.

Si no hace clic en el enlace del correo electrónico en el tiempo asignado, ICANN nos pide que suspendamos el dominio. Para obtener información acerca de cómo volver a enviar el correo electrónico de confirmación al titular, consulte [Reenvío de los emails de autorización y confirmación](#).

Ha transferido el registro de dominio a Amazon Route 53, pero no ha transferido el servicio DNS

Si el registrador anterior ofrecía el servicio DNS gratis con el registro de dominio, es posible que haya dejado de darle servicio DNS cuando transfirió el registro de dominio a Route 53. Efectúe el siguiente procedimiento para verificar si este es el problema y, en tal caso, para resolverlo.

Restauración del servicio DNS en caso de que su registrador anterior lo hubiera cancelado después de transferir el registro de dominio a Route 53

1. Póngase en contacto con su registrador anterior y confirme si ha cancelado el servicio DNS para su dominio. En caso afirmativo, estas son las tres formas más rápidas de restaurar el servicio DNS para el dominio, en el orden más recomendable:
 - Si el registrador anterior ofrece servicio DNS de pago, pídale que restaure el servicio DNS utilizando los registros de DNS y los servidores de nombres anteriores de su dominio.
 - Si el registrador anterior no proporciona servicio DNS de pago sin registrar el dominio, pregunte si puede devolver el registro de dominio y pídale que restaure el servicio DNS usando los registros de DNS y servidores de nombres anteriores para su dominio.
 - Si puede devolver un registro de dominio al registrador anterior, pero este ya no tiene sus registros de DNS, pregunte si puede devolverle el registro de dominio y obtener el mismo conjunto de servidores de nombres que se habían asignado anteriormente al dominio. Si

esto fuera posible, deberá crear de nuevo sus antiguos registros de DNS personalmente. Sin embargo, en cuanto lo haga, su dominio volverá a estar disponible.

Si el registrador anterior no puede ayudarlo con ninguna de estas opciones, continúe en el paso 2.

 Important

Si no puede restaurar el servicio DNS mediante los servidores de nombres que indicó al transferir su dominio a Route 53, pueden transcurrir dos días hasta que su dominio vuelva a estar disponible en Internet (tras completar los pasos restantes de este procedimiento). Por lo general, los solucionadores de DNS almacenan en caché, durante un período de 24 a 48 horas, los nombres de los servidores de nombres de un dominio. Se tarda ese tiempo hasta que todos los ellos obtengan los nombres de los nuevos servidores de nombres.

2. Elija un nuevo servicio DNS; por ejemplo, Route 53.
3. Con el método proporcionado por el nuevo servicio DNS, cree una zona alojada y registros:
 - a. Cree una zona alojada que tenga el mismo nombre que su dominio, como example.com.
 - b. Utilice el archivo de zona que ha obtenido del registrador anterior para crear registros.

Si ha elegido Route 53 como nuevo servicio DNS, puede importar el archivo de zona para crear registros. Para obtener más información, consulte [Creación de registros mediante la importación de un archivo de zona](#).

4. Obtenga los servidores de nombres para la zona alojada nueva. Si eligió Route 53 como servicio DNS, consulte [Obtener los servidores de nombres para una zona alojada pública](#).
5. Cambie los servidores de nombres de su dominio por los servidores de nombres que obtuvo en el paso 4. Para obtener más información, consulte [Adición o modificación de servidores de nombres y registros de conexión de un dominio](#).

Ha transferido el registro de dominio y ha especificado los servidores de nombres incorrectos en la configuración del dominio

Al transferir el registro de dominio a Amazon Route 53, uno de los ajustes que indica para ese dominio es el conjunto de servidores de nombres que responderá a las consultas de DNS. Estos servidores de nombres proceden de la zona alojada que tiene el mismo nombre que el dominio. La zona alojada contiene información acerca de cómo desea dirigir el tráfico para el dominio, como la dirección IP de un servidor web de `www.example.com`.

Es posible que, de manera accidental, haya especificado los servidores de nombres de la zona alojada incorrecta, algo totalmente comprensible si tiene más de una zona con el mismo nombre que el dominio. Para confirmar que el dominio está utilizando los servidores de nombres de la zona alojada correcta y, si es necesario, actualizar los servidores de nombres para el dominio, siga los procedimientos citados a continuación.

Important

Si especificó registros de servidor de nombres incorrectos al transferir el dominio a Route 53, pueden transcurrir dos días hasta que el servicio DNS quede totalmente restaurado (tras corregir los servidores de nombres para el dominio). Esto se debe a que los solucionadores de DNS en Internet suelen solicitar los servidores de nombres solo una vez cada dos días y almacenar en caché la respuesta.

Para obtener los servidores de nombres para su zona alojada nueva

1. Si utiliza otro servicio DNS para el dominio, utilice el método proporcionado por ese servicio DNS para obtener los servidores de nombres de la zona alojada. A continuación, pase directamente al siguiente procedimiento.

Si utiliza Route 53 como servicio DNS para el dominio, inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.

2. En el panel de navegación, elija Hosted Zones.
3. En la página Hosted Zones, seleccione el botón de opción (no el nombre) de la zona alojada.

 Important

Si tiene más de una zona alojada con el mismo nombre, asegúrese de que está obteniendo los servidores de nombres de la zona alojada correcta.

4. Anote los nombres de los cuatro servidores que aparecen en el panel de la derecha, en Name Servers (Servidores de nombres).

Para confirmar que el dominio está utilizando los servidores de nombres correctos

1. Si utiliza otro servicio DNS para el dominio, inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.

Si utiliza Route 53, vaya al siguiente paso.

2. En el panel de navegación, elija Registered Domains.
3. Elija el nombre del dominio cuya configuración desea editar.
4. Elija Add o Edit Name Servers.
5. Compare la lista de servidores de nombres que obtuvo en el procedimiento anterior con los servidores de nombres que figuran en el cuadro de diálogo Edit Name Servers for domain name.
6. Si los servidores de nombres que se enumeran aquí no coinciden con los servidores de nombres que obtuvo en el procedimiento anterior, cámbielos aquí y, a continuación, elija Update.

Ha transferido el servicio DNS en primer lugar, pero no ha esperado el tiempo suficiente antes de transferir el registro de dominio

Al transferir el servicio DNS a Amazon Route 53 o a otro servicio DNS, actualizó la configuración de su dominio con el registrador de dominio a fin de utilizar los servidores de nombres para el nuevo servicio DNS.

Los solucionadores de DNS que responden a las solicitudes de su dominio suelen almacenar en caché los nombres de los servidores de nombres durante un período de 24 a 48 horas. Si cambia el servicio DNS para un dominio y sustituye los servidores de nombres de un servicio DNS por los servidores de nombres de otro servicio DNS, puede tardar hasta 48 horas antes de que los solucionadores de DNS puedan empezar a utilizar los nuevos servidores de nombres y, por lo tanto, el nuevo servicio DNS.

A continuación, se describe cómo el hecho de transferir su servicio DNS y transferir después su dominio demasiado pronto puede hacer que el dominio no esté disponible en Internet:

1. Ha transferido el servicio DNS para su dominio.
2. Ha transferido su dominio a Route 53 antes de que los solucionadores de DNS comenzaran a utilizar los servidores de nombres para su nuevo servicio DNS.
3. Su registrador anterior canceló el servicio DNS para su dominio en cuanto el dominio fue transferido a Route 53.
4. Los solucionadores de DNS siguen dirigiendo consultas a su servicio DNS anterior, pero ya no hay registros que indiquen cómo dirigir el tráfico.

Cuando expire el almacenamiento en caché para los servidores de nombres del anterior servicio DNS, el DNS comenzará a utilizar su nuevo servicio DNS. Lamentablemente, no hay forma de acelerar este proceso.

Ha eliminado la zona alojada que Route 53 utiliza para dirigir el tráfico de Internet del dominio.

Si Route 53 es el servicio DNS para su dominio y usted elimina la zona alojada que se utiliza para dirigir el tráfico de Internet del dominio, el dominio dejará de estar disponible en Internet. Esto se aplica independientemente de si el dominio está registrado o no en Route 53.

Important

Restaurar el servicio de Internet para el dominio puede tardar hasta 48 horas.

Restauración del servicio de Internet si elimina una zona alojada que Route 53 utiliza para dirigir el tráfico de Internet de un dominio

1. Cree otra zona alojada que tenga el mismo nombre que el dominio. Para obtener más información, consulte [Crear una zona alojada pública](#).
2. Vuelva a crear los registros que había en la zona alojada que eliminó. Para obtener más información, consulte [Uso de registros](#).
3. Obtenga los nombres de los servidores de nombres que Route 53 ha asignado a la nueva zona alojada. Para obtener más información, consulte [Obtener los servidores de nombres para una zona alojada pública](#).

4. Actualice el registro de dominio para que utilice los servidores de nombres obtenidos en el paso 3:
 - Si el dominio está registrado en Route 53, consulte [Adición o modificación de servidores de nombres y registros de conexión de un dominio](#).
 - Si el dominio está registrado en otro registrador de dominios, utilice el método proporcionado por el registrador para actualizar el registro del dominio de modo que utilice los nuevos servidores de nombres.
5. Espere a que transcurra el TTL de los servidores de nombres para los solucionadores recursivos que han almacenado en caché los nombres de los servidores de dominio de la zona alojada eliminada. Una vez transcurrido el TTL, cuando un navegador o aplicación envíe una consulta de DNS para el dominio o uno de sus subdominios, un solucionador recursivo reenviará la consulta a los servidores de nombres de Route 53 de la nueva zona alojada. Para obtener más información, consulte [Cómo dirige Amazon Route 53 el tráfico de su dominio](#).

El TTL de los servidores de nombres puede durar hasta 48 horas, según cuál sea el TLD del dominio.

Su dominio se ha suspendido

Su dominio podría no estar disponible en Internet porque hayamos tenido que suspenderlo. Para obtener más información, consulte [Mi dominio está suspendido \(el estado es ClientHold\)](#).

Mi dominio está suspendido (el estado es ClientHold)

Si Amazon Route 53 suspende su dominio, este deja de estar disponible en Internet. Para determinar si un dominio se ha suspendido, puede seguir uno de estos procedimientos:

- En la página Registered domains (Dominios registrados) de la consola de Route 53, busque el nombre de dominio en la tabla Alerts (Alertas) en la parte inferior. Si el valor de la columna Status es clientHold, significa que el dominio se ha suspendido.
- Envíe una consulta WHOIS para el dominio. Si el valor de la columna Domain Status es clientHold, significa que el dominio se ha suspendido. El comando WHOIS está disponible en muchos sistemas operativos y también como aplicación web en muchos sitios web.

Además, cuando suspendemos un dominio, solemos enviar un correo electrónico a la dirección del titular del dominio. Sin embargo, si el dominio se hubiera suspendido por una sentencia judicial, el tribunal no nos permite notificarlo al titular.

Para que el dominio vuelva a estar disponible en Internet, debe conseguir que deje de estar suspendido. A continuación, se citan los motivos por los que un dominio puede suspenderse y cómo invertir esta situación.

Note

Si necesita ayuda para anular la suspensión de su dominio, puede ponerse en contacto con AWS Support de forma gratuita. Para obtener más información, consulte [Ponerse en contacto con AWS Support sobre problemas de registro de dominios](#).

Temas

- [Ha registrado un nuevo dominio, pero no hizo clic en el enlace del correo electrónico de confirmación](#)
- [Ha deshabilitado la renovación automática del dominio y este ha expirado](#)
- [Ha cambiado la dirección de correo electrónico del contacto del registrante, pero no ha verificado que la nueva dirección de correo electrónico sea válida](#)
- [No se pudo procesar el pago de la renovación de dominio automática y el dominio ha expirado](#)
- [Hemos suspendido el dominio debido a una vulneración de la Política de uso aceptable de AWS](#)
- [Hemos suspendido el dominio debido a una orden judicial](#)

Ha registrado un nuevo dominio, pero no hizo clic en el enlace del correo electrónico de confirmación

Al registrar un dominio en AWS por primera vez, ICANN requiere que obtengamos la confirmación de que la dirección de correo electrónico del titular es válida. Para confirmarlo, enviamos un correo electrónico que contiene un enlace. Tiene entre 3 y 15 días para hacer clic en el enlace, según sea el dominio de nivel superior. Transcurrido ese tiempo, el enlace deja de funcionar.

 Note

Si ya ha registrado uno o varios dominios con Amazon Route 53 utilizando la misma dirección del titular, no enviamos ningún correo electrónico de confirmación.

Si no hace clic en el enlace del correo electrónico en el tiempo asignado, ICANN nos pide que suspendamos el dominio. Para obtener información acerca de cómo volver a enviar el correo electrónico de confirmación al titular, consulte [Reenvío de los emails de autorización y confirmación](#). Una vez confirmada la validez de la dirección de correo electrónico, cancelamos automáticamente la suspensión del dominio.

Ha deshabilitado la renovación automática del dominio y este ha expirado

Cuando está habilitada la renovación automática para un dominio (valor predeterminado para un dominio nuevo o transferido), el registro se renovará automáticamente poco antes de la fecha de vencimiento. Si deshabilita dicha renovación automática, enviamos tres mensajes a la dirección de correo electrónico del titular para recordarle que el registro de dominio está a punto de expirar. Empezamos a enviar estos mensajes 45 días antes de que el dominio expire.

Si deshabilita la renovación automática para el dominio y no amplía manualmente el período de registro, lo normal es que suspendamos el dominio en su fecha de vencimiento. Tenga en cuenta que los registros de algunos dominios eliminan el dominio incluso antes de la fecha de vencimiento.

Para obtener más información acerca de cómo renovar un dominio expirado, consulte [Renovar el registro de un dominio](#).

Ha cambiado la dirección de correo electrónico del contacto del registrante, pero no ha verificado que la nueva dirección de correo electrónico sea válida

Si cambia la dirección de correo electrónico del contacto del registrante por una dirección que no haya verificado previamente, ICANN requiere que obtengamos confirmación de que la dirección de correo electrónico del contacto del registrante es válida. Para confirmarlo, enviamos un correo electrónico que contiene un enlace. Tiene entre 3 y 15 días para hacer clic en el enlace, según sea el dominio de nivel superior. Transcurrido ese tiempo, el enlace deja de funcionar.

Si no hace clic en el enlace del correo electrónico en el tiempo permitido por el registro de TLD, ICANN requiere que suspendamos el dominio. Para obtener información acerca de cómo volver a

enviar el correo electrónico de confirmación al titular, consulte [Reenvío de los emails de autorización y confirmación](#). Una vez confirmada la validez de la dirección de correo electrónico, cancelamos automáticamente la suspensión del dominio.

No se pudo procesar el pago de la renovación de dominio automática y el dominio ha expirado

Si está habilitada la renovación automática para un dominio, pero no hemos podido procesar el pago (por ejemplo, porque su tarjeta de crédito haya expirado), enviamos varios mensajes de correo electrónico a la dirección del titular del dominio. Si no recibimos el pago, lo normal es que suspendamos el dominio en la fecha de vencimiento. Tenga en cuenta que los registros de algunos dominios eliminan el dominio incluso antes de la fecha de vencimiento.

Para obtener más información acerca de cómo renovar un dominio expirado, consulte [Renovar el registro de un dominio](#).

Hemos suspendido el dominio debido a una vulneración de la Política de uso aceptable de AWS

Si suspendemos un dominio por una vulneración de la [Política de uso aceptable de AWS](#), enviamos una notificación por correo electrónico al titular del dominio. (Si la cuenta de AWS ya está suspendida por fraude, no enviamos ningún correo electrónico de notificación).

Para impugnar una suspensión, envíe un correo electrónico a trustandsafety@support.aws.com.

Hemos suspendido el dominio debido a una orden judicial

Si un dominio se suspende como resultado de una orden judicial, no podemos cancelar esta suspensión hasta que se haya levantado la orden judicial. Para impugnar la validez de una orden judicial, envíe un correo electrónico a trustandsafety@support.aws.com y adjunte los documentos correspondientes.

Se produjo un error en mi operación de dominio

Estos son algunos consejos para solucionar problemas en caso de que se produzca un error en la operación de su dominio. Las operaciones pueden ser el registro, la transferencia, la renovación o la actualización de contactos.

Se produjo un error en la operación de dominio debido a que la información de contacto no era válida

Si se produce un error en una operación de dominio debido a que la información de contacto no es válida, los datos de contacto que proporcionó no cumplen con los requisitos de validación del registro.

Para resolver este problema, verifique que todos los datos de contacto tengan el formato correcto:

- Nombre: asegúrese de que el nombre contenga solo caracteres válidos y que tenga el formato correcto.
- Dirección: confirme que el formato de la dirección coincida con los estándares postales del país.
- Número de teléfono: utilice el formato internacional correcto para el país.
- Campos de identificación: en el caso de los dominios que requieren números de identificación, asegúrese de que el formato sea el correcto para el país especificado.

Después de corregir la información de contacto, vuelva a intentar ejecutar la operación de dominio. Para conocer los requisitos específicos de los distintos dominios de nivel superior, consulte [Dominios que puede registrar con Amazon Route 53](#).

No se pudo transferir mi dominio a Amazon Route 53

Si la transferencia de dominio ya ha fallado o ha sido rechazada, use esta sección para diagnosticar y resolver el error.

Note

Para evitar problemas durante las transferencias activas, consulte [Prevención de problemas comunes con las transferencias a Route 53](#).

Temas

- [No hizo clic en el enlace del correo electrónico de autorización](#)
- [El código de autorización que ha recibido del registrador actual no es válido](#)
- [Error “Parameters in request are not valid” \(Los parámetros de la solicitud no son válidos\) al intentar transferir un dominio .es a Amazon Route 53](#)

- [¿El nombre de dominio internacionalizado que va a transferir a Amazon Route 53 aparece en punycode?](#)
- [Mensajes de error de transferencia comunes](#)

No hizo clic en el enlace del correo electrónico de autorización

Al transferir un registro de dominio a Amazon Route 53, ICANN, el órgano que dirige el registro de dominios, nos ha pedido la autorización del titular del dominio para hacer dicha transferencia. Para obtenerla, le enviamos un correo electrónico que contenía un enlace. Tiene entre 5 y 15 días para hacer clic en el enlace, según sea el dominio de nivel superior. Transcurrido ese tiempo, el enlace deja de funcionar.

Si no hace clic en el enlace del correo electrónico en el tiempo asignado, ICANN nos pide que cancelemos la transferencia. Para obtener información acerca de cómo volver a enviar el correo electrónico de autorización al titular, consulte [Reenvío de los emails de autorización y confirmación](#).

El código de autorización que ha recibido del registrador actual no es válido

Si solicita la transferencia de un dominio a Amazon Route 53 y no recibe el correo electrónico de autorización, consulte la [página de estado en la consola de Route 53](#). Si la página de estado muestra que no es válido el código de autorización de la transferencia recibido de su registrador, siga estos pasos:

1. Póngase en contacto con el registrador actual del dominio y solicite un nuevo código de autorización. Confirme lo siguiente:
 - Durante cuánto tiempo permanecerá activo el nuevo código de autorización. Debe solicitar una transferencia de dominio antes de que el código expire.
 - El nuevo código de autorización es diferente del código no válido. De lo contrario, pida al registrador actual que actualice el código de autorización.
2. Envíe otra solicitud para transferir el dominio. Para obtener más información, consulte [Paso 5: Solicitar la transferencia](#) en el tema [Transferencia del registro de un dominio a Amazon Route 53](#).

Error “Parameters in request are not valid” (Los parámetros de la solicitud no son válidos) al intentar transferir un dominio .es a Amazon Route 53

Amazon Route 53 devuelve un error “Parameters in request are not valid” (Los parámetros de la solicitud no son válidos) cuando intenta transferir un dominio .es a Route 53 y el tipo de contacto del titular es Company (Empresa). Para completar la transferencia, cambie el tipo de contacto del titular a Person (Persona) y vuelva a enviarlo.

¿El nombre de dominio internacionalizado que va a transferir a Amazon Route 53 aparece en punycode?

Cuando registra un nuevo nombre de dominio o crea zonas alojadas y registros, puede especificar letras distintas de a-z (por ejemplo, la ç francesa), caracteres de otros alfabetos (por ejemplo, cirílico o árabe) y caracteres en chino, japonés o coreano. Amazon Route 53 almacena estos nombres de dominio internacionalizados (IDN) en Punycode, que representa los caracteres Unicode como cadenas ASCII.

Si obtiene un error al transferir un IDN a Route 53, use punycode para representarlo y vuelva a intentarlo. Para obtener más información, consulte [Formato de nombres de dominio internacionalizados](#).

Mensajes de error de transferencia comunes

Cuando se produce un error en la transferencia de un dominio, normalmente recibe un mensaje de error en la consola de Route 53 o por correo electrónico. A continuación, se indican los mensajes de error más comunes y se explica cómo resolverlos:

«Transfer was rejected by the registry»

Este error se produce cuando el registro del dominio bloquea la transferencia por una de varias razones. Las causas más comunes son:

- El dominio no cumple con la norma de 60 días de la ICANN. La ICANN exige que las transferencias se bloqueen en un plazo de 60 días a partir del registro inicial o del cambio de contacto del titular.
- El dominio tiene el bloqueo de transferencia activado en su registrador actual.

- El dominio está en un estado que impide las transferencias, como `clientTransferProhibited`, `serverTransferProhibited`, `pendingDelete`, `pendingTransfer` o `redemptionPeriod`.

Para resolver este problema, verifique lo siguiente con su registrador actual:

- Compruebe que el dominio tenga más de 60 días desde la fecha de registro. Si cambió recientemente la información de contacto del titular, es posible que deba esperar 60 días a partir del cambio. Algunos registradores le permiten eximirlo de esta restricción, así que pregúntele a su registrador actual si esta opción está disponible.
- Desbloquee el dominio. Para ello, desactive cualquier bloqueo de transferencia o bloqueo de dominio.
- Compruebe que el estado de su dominio permita las transferencias. Para verificar el estado del dominio, puede hacer una búsqueda en WHOIS o comunicarse con su registrador actual.

«Invalid authorization code» o «Auth code is incorrect»

Este error significa que el código de autorización (también denominado código EPP o código de transferencia) que ha introducido no es válido. Esto puede ocurrir si el código ha caducado, se ha introducido de forma incorrecta o no lo ha obtenido del registrador actual.

Para resolver este problema, siga estos pasos:

- Póngase en contacto con el registrador actual y solicite un nuevo código de autorización. Asegúrese de preguntar durante cuánto tiempo permanecerá activo el código para poder completar la transferencia antes de que caduque.
- Cuando reciba el código nuevo, compruebe que sea diferente del código anterior. Si es el mismo, pídale al registrador que actualice o regenere el código de autorización.
- Compruebe que esté introduciendo el código exactamente como se lo proporcionaron, incluidas las letras mayúsculas o minúsculas, los números y los caracteres especiales.

«Transfer authorization email not received» o «Authorization timeout»

Este error se produce cuando no hace clic en el enlace de autorización que figura en el correo electrónico de confirmación de la transferencia dentro del plazo requerido (normalmente 5 días). La ICANN exige este paso de autorización para todas las transferencias de dominio.

Si no recibió el correo electrónico de autorización o no cumplió con la fecha límite, compruebe lo siguiente:

- Consulte su carpeta de correo no deseado. Los proveedores de correo electrónico a veces filtran los correos electrónicos de autorización de las transferencias.
- Compruebe que su buzón no esté lleno y que no tenga limitaciones de almacenamiento que puedan impedir la entrega del correo electrónico.
- Compruebe si su proveedor de correo electrónico tiene políticas que filtren el correo entrante de remitentes desconocidos.
- Confirme que puede acceder a la cuenta de correo electrónico del titular y que la dirección de correo electrónico sigue activa.

Si es necesario, actualice su información de contacto con su registrador actual antes de solicitar otra transferencia. Para obtener información sobre cómo reenviar el correo electrónico de autorización, consulte [Reenvío de los emails de autorización y confirmación](#).

«Domain is locked» o «Transfer prohibited»

Este error indica que su dominio tiene activado un bloqueo que impide las transferencias. La mayoría de los registradores activan bloqueos de dominio de forma predeterminada como medida de seguridad para evitar transferencias no autorizadas.

Para resolver este problema, inicie sesión en su cuenta con su registrador actual y desactive la configuración de bloqueo de dominios o de transferencias. Los pasos exactos varían según el registrador, pero normalmente encontrará estos ajustes en la configuración de administración o seguridad de su dominio. Si necesita ayuda para encontrar esta configuración, póngase en contacto con su registrador actual para que lo asista.

«Contact information verification required»

Este error se produce cuando cambió recientemente la información de contacto de su dominio. Para evitar transferencias fraudulentas, las normas de la ICANN exigen un período de espera de 60 días después de los cambios en la información de contacto antes de poder transferir un dominio.

Tiene dos opciones para resolver este problema:

- Esperar 60 días a partir de la fecha del cambio en la información de contacto para intentar hacer la transferencia de nuevo.

- Ponerse en contacto con su registrador actual para verificar su información de contacto actual. Algunos registradores tal vez le permitan desactivar la restricción de 60 días si puede verificar su identidad.

Note

Si recibe un mensaje de error que no aparece aquí, póngase en contacto con AWS Support e incluya el texto exacto del error. Nuestro equipo de asistencia puede ayudarlo a diagnosticar y resolver los problemas de transferencia específicos de su situación.

He cambiado la configuración de DNS, pero no ha tenido efecto

Si ha cambiado la configuración de DNS, a continuación le indicamos algunos motivos por los que esos cambios no han tenido efecto.

Temas

- [Ha transferido el servicio DNS a Amazon Route 53 en las últimas 48 horas, por lo que el DNS sigue utilizando su servicio DNS anterior](#)
- [Recientemente ha transferido el servicio DNS a Amazon Route 53, pero no ha actualizado los servidores de nombres con el registrador de dominio](#)
- [Los solucionadores de DNS siguen usando la configuración anterior para el registro](#)
- [Tiene más de una zona alojada con el mismo nombre y actualizó la que no está asociada al dominio](#)

Ha transferido el servicio DNS a Amazon Route 53 en las últimas 48 horas, por lo que el DNS sigue utilizando su servicio DNS anterior

Cuando transfirió el servicio DNS a Amazon Route 53, utilizó el método proporcionado por el registrador para que su dominio sustituyera los servidores de nombres del servicio DNS anterior por los cuatro servidores de nombres de Route 53.

 Note

Si no está seguro de haber hecho esto, consulte [Recientemente ha transferido el servicio DNS a Amazon Route 53, pero no ha actualizado los servidores de nombres con el registrador de dominio](#).

Los registradores de dominios suelen utilizar un tiempo de vida (TTL) de 24 a 48 horas para servidores de nombres. Esto significa que cuando un solucionador de DNS obtiene los servidores de nombres de su dominio, utiliza dicha información durante un máximo de 48 horas antes de enviar otra solicitud para los servidores de nombres actuales del dominio. Si transfirió el servicio DNS a Route 53 en las últimas 48 horas y, a continuación, cambió la configuración de DNS, algunos solucionadores de DNS siguen usando su anterior servicio DNS para dirigir el tráfico para el dominio.

Recientemente ha transferido el servicio DNS a Amazon Route 53, pero no ha actualizado los servidores de nombres con el registrador de dominio

El registrador de su dominio tiene una gran variedad de información sobre el dominio, incluidos los servidores de nombres de servicio DNS para el dominio. El registrador de dominio suele ser también su servicio DNS, por lo que los servidores de nombres asociados a su dominio pertenecen al registrador. Estos servidores de nombres le indican a DNS dónde obtener información sobre el modo en que desea dirigir el tráfico de su dominio, por ejemplo, a la dirección IP de un servidor web para su dominio.

Al transferir el servicio DNS a Amazon Route 53, debe utilizar el método que ha proporcionado el registrador de dominio para cambiar los servidores de nombres asociados a su dominio. Lo normal es sustituir los servidores de nombres que ha proporcionado el registrador por los cuatro servicios de nombre de Route 53 asociados a la zona alojada que creó para el dominio.

Si ha creado una zona alojada y registros nuevos para su dominio y ha especificado una configuración diferente de la utilizada para el servicio DNS anterior, y si el DNS sigue dirigiendo el tráfico a los antiguos recursos, es posible que no haya actualizado los servidores de nombres con el registrador de dominio. Para determinar si el registrador está usando los servidores de nombres para su zona alojada de Route 53 y, si es necesario, actualizar los servidores de nombres para el dominio, siga este procedimiento:

Para obtener los servidores de nombres de su zona alojada y actualizar la configuración del servidor de nombres con el registrador de dominio

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En el panel de navegación, elija Hosted Zones.
3. En la página Hosted Zones (Zonas alojadas), elija el nombre de la zona alojada (no el botón de radio) para dicha zona.

 Important

Si tiene más de una zona alojada con el mismo nombre, asegúrese de que está obteniendo los servidores de nombres de la zona alojada correcta.

4. En la lista Record name (Nombre del registro), anote los cuatro servidores que aparecen en Name Servers (Servidores de nombres).
5. Con el método proporcionado por el registrador para el dominio, muestre la lista de servidores de nombres en el dominio.
6. Si los servidores de nombres del dominio coinciden con los servidores de nombres obtenidos en el paso 4, la configuración del dominio es correcta.

Si los servidores de nombres del dominio no coinciden con los servidores de nombres obtenidos en el paso 4, actualice el dominio para usar los servidores de nombres de Route 53.

7.

 Important

Al cambiar los servidores de nombres del dominio por los servidores de nombres de su zona alojada de Route 53, pueden transcurrir dos días hasta que se apliquen los cambios y Route 53 se convierta en su servicio DNS. Esto se debe a que los solucionadores de DNS en Internet suelen solicitar los servidores de nombres solo una vez cada dos días y almacenar en caché la respuesta.

Los solucionadores de DNS siguen usando la configuración anterior para el registro

Si ha cambiado la configuración en un registro, pero el tráfico se sigue dirigiendo al recurso anterior, como un servidor web para su sitio web, una posible causa es que DNS todavía tenga la configuración anterior almacenada en caché. Cada registro tiene un valor de TTL (tiempo de vida) que especifica cuánto tiempo, en segundos, desea que los solucionadores de DNS almacenen en caché la información en el registro, como la dirección IP de un servidor web. Hasta que transcurra el tiempo especificado por el TTL, los solucionadores de DNS seguirán devolviendo el valor antiguo en respuesta a las consultas de DNS. Si desea conocer el TTL de un registro, efectúe el siguiente procedimiento.

Note

Para registros de alias, el TTL se determina por el recurso de AWS al que dirige el tráfico el registro. Para obtener más información, consulte [Elección entre registros de alias y sin alias](#).

Para ver el TTL de un registro

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
2. En la página Hosted Zones, elija el nombre de la zona alojada que incluye el registro.
3. En la lista de registros, busque el registro cuyo valor de TTL necesita y compruebe el valor de la columna TTL.

Note

Cambiar el TTL ahora no hará que el cambio se produzca antes. Los solucionadores de DNS ya tienen el valor almacenado en caché y no obtendrán la nueva configuración hasta que transcurra el tiempo especificado en el ajuste anterior.

Tiene más de una zona alojada con el mismo nombre y actualizó la que no está asociada al dominio

Puede crear más de una zona alojada que tenga el mismo nombre, ya sea con la misma cuenta o con varias cuentas. Para especificar la zona alojada que utiliza Route 53 a fin de dirigir el tráfico de Internet para su dominio, obtiene los cuatro servidores de nombres de Route 53 para esa zona alojada y actualiza el registro del dominio con el fin de utilizar esos servidores de nombres.

Si agrega, cambia o elimina registros en una zona alojada pero el registro de dominio utiliza los servidores de nombres de otra zona alojada, las respuestas de Route 53 a las consultas de DNS no reflejarán los cambios. Para determinar si el registro de dominio utiliza los servidores de nombres de la zona alojada en la que actualizó los registros, realice las siguientes tareas:

1. Determine qué servidores de nombres están asociados al registro de su dominio. Consulte [Adición o modificación de servidores de nombres o registros de conexión](#).
2. Compare los servidores de nombres que obtuvo en el paso 1 con los servidores de nombres que Route 53 asignó a la zona alojada en la que actualizó los registros. Consulte [Obtener los servidores de nombres para una zona alojada pública](#).

Si los servidores de nombres para el registro de dominio no coinciden con los servidores de nombres de la zona alojada en la que actualizó los registros, tiene dos opciones:

Cambiar registros en la zona alojada que está asociada actualmente al dominio (recomendado)

Tome nota de los cambios realizados en la zona alojada que no está asociada actualmente con el registro de su dominio. A continuación, vaya a la zona alojada que está asociada con el registro del dominio y realice los mismos cambios. Este es el método preferido porque los cambios surten efecto casi de inmediato. Para obtener más información, consulte [Editar registros](#).

Actualizar el registro del dominio para utilizar distintos servidores de nombres

Cambie el registro de dominio para utilizar los servidores de nombres de la zona alojada que actualizó.

Important

Si cambia los servidores de nombres asociados con el registro de su dominio, el dominio no estará disponible en Internet durante un máximo de 2 días. Esto se debe a que los solucionadores DNS suelen almacenar en caché los nombres de los servidores de

nombres durante 2 días. Para obtener información general sobre el funcionamiento de DNS, incluida información sobre el almacenamiento en caché del solucionador, consulte [Cómo dirige Amazon Route 53 el tráfico de su dominio](#).

Al cambiar los servidores de nombres asociados con el registro de dominio, básicamente está cambiando el servicio DNS para el dominio. Tiene dos opciones, en función de si el dominio está actualmente en uso:

- Si el dominio está en uso, consulte [Establecer Route 53 como el servicio DNS para un dominio que se está utilizando](#).
- Si el dominio está inactivo actualmente, realice las siguientes tareas:
 1. Obtenga los servidores de nombres de la zona alojada que desea utilizar para dirigir el tráfico a su dominio. Consulte [Obtener los servidores de nombres para una zona alojada pública](#).
 2. En la zona alojada para la que obtuvo servidores de nombres en el paso 1, confirme que el registro NS está utilizando los mismos cuatro servidores de nombres. Si no es así, actualice el registro NS. Consulte [Editar registros](#).
 3. Actualice el registro de dominio para que utilice los servidores de nombres obtenidos en el paso 1. Consulte [Adición o modificación de servidores de nombres o registros de conexión](#).

Mi navegador muestra un error “Server not found”

Si su navegador muestra un error “Server not found” cuando trata de explorar un dominio (example.com) o un subdominio (www.example.com), estas son algunas de las explicaciones habituales.

Temas

- [No creó ningún registro para el nombre de dominio o subdominio](#)
- [Ha creado un registro, pero ha especificado el valor erróneo](#)
- [El recurso al que está dirigiendo el tráfico no está disponible](#)

No creó ningún registro para el nombre de dominio o subdominio

Si no crea ningún registro para el dominio o subdominio, el DNS no sabe adónde dirigir el tráfico cuando alguien introduce ese nombre en un navegador. Para obtener más información, consulte [Uso de registros](#).

Ha creado un registro, pero ha especificado el valor erróneo

Al crear un registro, es fácil especificar un valor erróneo, como la dirección IP de un servidor web o el nombre de dominio que CloudFront ha asignado a la distribución web. Si el registro existe, pero sigue apareciendo un error “Server not found”, le recomendamos que confirme que el valor es correcto.

El recurso al que está dirigiendo el tráfico no está disponible

Si un registro especifica un recurso, como un servidor web, que no está disponible, un navegador devolverá un error “Server not found”. Conviene que compruebe el estado del recurso al que está dirigiendo el tráfico.

No puedo dirigir el tráfico a un bucket de Amazon S3 configurado para hospedar sitios web

Al configurar un bucket de Amazon S3 para alojar sitios web, debe asignarle el mismo nombre que al registro que desea utilizar para dirigir el tráfico hacia el bucket. Por ejemplo, si desea dirigir el tráfico de example.com a un bucket de S3 configurado para hospedar sitios web, el nombre del bucket debe ser example.com.

Si desea dirigir el tráfico a un bucket de S3 configurado para alojar sitios web, pero el nombre del bucket no aparece en la lista Alias Target (Objetivo de alias) de la consola de Amazon Route 53, o bien está intentando crear un registro de alias mediante programación y recibe un error “InvalidInput” (Entrada no válida) de la API de Route 53, uno de los AWS SDK, la AWS CLI o AWS Tools for Windows PowerShell, verifique lo siguiente:

- El nombre del bucket coincide exactamente con el nombre del registro, como example.com o www.example.com.
- El bucket S3 está configurado correctamente para hospedar sitios web. Para obtener más información, consulte [Alojamiento de un sitio web estático en Amazon S3](#) en la Guía del usuario de Amazon Simple Storage Service.

Me han facturado dos veces por la misma zona alojada

No le facturaremos si elimina una zona alojada en un plazo de 12 horas después de crearla.

Después de 12 horas, cobramos inmediatamente la tarifa mensual estándar de una zona alojada. La tarifa mensual por una zona alojada no se prorratea. (La misma tarifa se aplica a la zona alojada que se crea automáticamente al registrar un dominio).

Si crea una zona alojada el último día del mes (por ejemplo, 31 de enero), el cargo de enero puede aparecer en la factura de febrero, junto con el cargo de febrero. Tenga en cuenta que Amazon Route 53 utiliza la hora universal coordinada (UTC, por sus siglas en inglés) como zona horaria para determinar cuándo se ha creado una zona alojada.

Me cobraron varias facturas por mi dominio

Cuando se inscribe a una suscripción, paga una cuota de registro, una cuota de transferencia o una cuota de renovación con un costo inicial, se genera una factura única. Esta factura permanece en la consola de facturación, incluso si la transacción de pago no se realiza correctamente. La partida de facturación relacionada se muestra como [x] Cantidad en la subsección Registrar-Global de la pestaña Detalles de la factura por servicio de la consola de facturación.

Para consultar las facturas eximidas, complete los pasos que se describen a continuación:

Cómo consultar las facturas eximidas en la consola de facturación

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Administración de facturación y costos de AWS en <https://console.aws.amazon.com/costmanagement/>.
2. En el panel de navegación, seleccione Facturas.
3. Seleccione Facturas para ver los detalles de las facturas eximidas.

Para ver los pagos y los reembolsos realizados correctamente en la consola de facturación, complete los pasos siguientes:

Cómo confirmar los pagos o reembolsos que se procesaron de manera correcta

1. En el panel de navegación, elija Pagos.
2. Seleccione la pestaña Transacciones para ver la tabla de Transacciones de todas las transacciones completadas con AWS.

Mi cuenta de AWS está cerrada o se ha cerrado de forma definitiva y mi dominio está registrado con Route 53.

Si cierra su cuenta de AWS o si su cuenta está cerrada o se ha cerrado de forma definitiva, los dominios pasarán por un proceso de eliminación:

1. Le notificaremos a diario que su cuenta está cerrada y que su dominio se suspenderá en los próximos 5 días.
2. Una vez que se suspenda el dominio, ocurrirá lo siguiente:
 - Si su registrador es Amazon Registrar, le notificaremos que eliminaremos el dominio en 30 días. Para obtener más información, consulte [Búsqueda del registrador y otra información del dominio](#).
 - Si su registrador es Gandi, le notificaremos que cederemos su dominio a Gandi cuando su cuenta se cierre de manera definitiva.
3. Tras esperar 30 días, eliminaremos todos los dominios registrados en Amazon Registrar en la cuenta y le enviaremos una actualización.
4. Cuando su cuenta se cierre definitivamente, transferiremos a Gandi todos los dominios registrados con Gandi en la cuenta.

Si vuelve a abrir su cuenta durante el período en que se puedan recuperar los dominios, anularemos la suspensión de los dominios o le informaremos que se han eliminado; no obstante, es posible que se puedan restaurar. Para obtener más información, consulte [Dominios que puede registrar con Amazon Route 53](#).

Note

Una vez transcurridos 90 días desde que cerró su cuenta, ya no podrá volver a abrirla. Para obtener más información, consulte [Cierre de una cuenta](#) en la Guía de administración de cuentas de AWS.

Para obtener más información, consulte [Ponerse en contacto con AWS Support sobre problemas de registro de dominios](#).

Rangos de direcciones IP de servidores de Amazon Route 53

Amazon Web Services (AWS) publica sus rangos de direcciones IP actuales en formato JSON. Si sus firewalls o grupos de seguridad restringen el tráfico entrante en función de las direcciones IP de origen, confirme que su configuración permita el tráfico procedente de los intervalos de direcciones IP correspondientes.

Para ver los intervalos de direcciones IP actuales para Route 53, descargue [ip-ranges.json](#) y busque en el archivo los siguientes valores:

- "service": "ROUTE53"
- "service": "ROUTE53_HEALTHCHECKS"
- "service": "ROUTE53_HEALTHCHECKS_PUBLISHING"

Para obtener más información acerca de las direcciones IP de los recursos de AWS, consulte [Rangos de direcciones IP de AWS](#) en la Referencia general de Amazon Web Services.

Rangos de direcciones IP de los servidores de nombres de Route 53

"service": "ROUTE53": los servidores de nombres de Route 53 utilizan estos rangos de direcciones IP. Agregue estos intervalos en una lista de direcciones IP permitidas si utiliza Route 53 como servicio DNS en uno o varios dominios, y desea poder utilizar los comandos `dig` o `nslookup` para consultar servidores de nombres de Route 53.

Note

Las direcciones IP del servidor de nombres de Route 53 son estáticas.

Rangos de direcciones IP de las comprobaciones de estado de Route 53

"service": "ROUTE53_HEALTHCHECKS": los comprobadores de estado de Route 53 utilizan estos rangos de direcciones IP. Agregue estos intervalos a la lista de intervalos de direcciones IP permitidos si utiliza comprobaciones de estado de Route 53 para comprobar el estado de los recursos de la red.

Note

Rara vez cambiamos los rangos de direcciones IP de los comprobadores de estado. Controle el archivo [ip-ranges.json](#) para ver si hay actualizaciones de estos rangos.

Para obtener más información sobre las direcciones IP de las comprobaciones de estado, consulte [Configuración de las reglas de enrutador y de firewall para las comprobaciones de estado de Amazon Route 53](#).

Referencias de listas de prefijos

Una lista de prefijos es un conjunto de una o más entradas de bloque CIDR que puede utilizar para configurar grupos de seguridad. Su enrutador y firewall deben permitir reglas para la instancia de Amazon EC2 que permitan el tráfico entrante desde las direcciones IP que utilizan los comprobadores de estado de Route 53. Una referencia a una lista de prefijos lo ayuda a simplificar la administración de los bloques CIDR en sus reglas. Si utiliza frecuentemente los mismos bloques de CIDR en varias reglas, puede administrarlos en una única lista de prefijos, en lugar de hacer referencia repetidamente a los mismos bloques de CIDR en cada regla. Si necesita quitar un bloque CIDR, puede eliminar su entrada de la lista de prefijos, en lugar de eliminar el CIDR de todas las reglas de enrutamiento afectadas. Para obtener más información sobre las listas de prefijos en general, consulte [Agrupar bloques CIDR mediante listas de prefijos administradas](#) en la Guía del usuario de Amazon VPC.

Las listas de prefijos administradas por AWS son conjuntos de rangos de direcciones IP para servicios de AWS. AWS se encarga de crear estas listas y hacerles mantenimiento, y pueden ser utilizadas por cualquier persona que tenga una cuenta de AWS. No puede crear, modificar, compartir ni eliminar una lista de prefijos administrada por AWS.

Para obtener más información sobre las listas de prefijos administradas por AWS, consulte [Trabajar con listas de prefijos administradas por AWS](#) en la Guía del usuario de Amazon VPC.

Rangos de direcciones IP internas de las comprobaciones de estado de Route 53

"service": "ROUTE53_HEALTHCHECKS_PUBLISHING": Route 53 utiliza estos rangos de direcciones IP solo internamente. No es necesario agregar estos intervalos a la lista de intervalos permitidos.

Etiquetado de recursos de Amazon Route 53

Una etiqueta es una etiqueta que se asigna a un AWS recurso. Cada etiqueta consta de una clave y un valor, ambos definidos por el usuario. Por ejemplo, la clave puede ser “dominio” y el valor puede ser “example.com”. Puede usar etiquetas para distintos fines; un uso habitual consiste en clasificar y monitorear los costes de Amazon Route 53. Al aplicar etiquetas a las zonas alojadas, los dominios y las comprobaciones de estado de Route 53, AWS genera un informe de asignación de costos en forma de archivo de valores separados por comas (CSV) con el uso y los costos agregados por las etiquetas. Puede aplicar etiquetas que representen categorías de negocio (p. ej., centros de costos, nombres de aplicación o propietarios) para estructurar los costos entre diferentes servicios. Para obtener más información sobre el uso de etiquetas para la asignación de costes, consulte [Uso de etiquetas de asignación de costes](#) en la [Guía del usuario de AWS Billing](#).

Para facilitar su uso y obtener los mejores resultados, utilice el editor de etiquetas en el Consola de administración de AWS, que proporciona una forma centralizada y unificada de crear y administrar sus etiquetas. Para obtener más información, consulte [Uso de Tag Editor](#) en la [Introducción a la Consola de administración de AWS](#). También puede utilizar la consola de Route 53 para aplicar etiquetas a algunos recursos:

- Comprobaciones de estado: para obtener más información, consulte [Denominar y etiquetar comprobaciones de estado](#).
- Puntos finales entrantes de Route 53 VPC Resolver: para obtener más información, consulte [Valores que se especifican al crear o editar puntos de conexión de entrada](#).
- Puntos de enlace de salida de Resolver: para obtener más información, consulte [Valores que se especifican al crear o editar puntos de conexión de salida](#).
- Reglas de Resolver: para obtener más información, consulte [Valores que se especifican al crear o editar reglas](#).
- Zonas alojadas: para obtener más información, consulte [Uso de zonas alojadas](#).

Note

Los cargos por los puntos finales de Resolver se asignan por interfaz de red de VPC Resolver. Como actualmente no es posible etiquetar las interfaces de red de VPC Resolver, la asignación de costes basada en etiquetas no se admite actualmente en los puntos finales

de Resolver. Para obtener información sobre los precios de VPC Resolver, consulte los precios de [Amazon Route 53](#).

También puede aplicar etiquetas a recursos a través de la API de Route 53. Para obtener más información, consulte las acciones relacionadas con las etiquetas en el tema [Acciones de la API de Route 53 por función](#) de la Referencia de la API de Amazon Route 53.

Tutoriales

Esta sección abarca los siguientes tutoriales:

Uso de Route 53 como el servicio DNS de subdominios

Aprenda a utilizar Route 53 como el servicio DNS para un subdominio nuevo o uno existente y, mientras tanto, utilizar otro servicio DNS para el dominio principal.

Transición al enrutamiento basado en latencia

Aprenda cómo migrar de manera gradual del enrutamiento estándar al enrutamiento basado en la latencia en Route 53 y dirigir a los usuarios al punto de conexión de AWS con la mínima latencia disponible.

Combine los registros ponderados y de latencia para lograr una transición fluida y de bajo riesgo con control total y capacidad de restauración.

Adición de otra región al enrutamiento basado en latencia

Amplíe su configuración de enrutamiento basado en latencia al agregar una nueva región AWS y trasladar de forma gradual el tráfico a la nueva región.

Enrutamiento del tráfico a varias instancias de Amazon EC2 en una región

Uso de una combinación de registros ponderados y de latencia para dirigir el tráfico a varias instancias de Amazon EC2 dentro de una Región de AWS específica.

Administración de más de 100 registros ponderados

Aprenda a dirigir el tráfico a más de 100 puntos de conexión mediante la creación de un árbol de registros de alias ponderados.

Ponderación de respuestas de múltiples registros con tolerancia a errores

Aprenda a ponderar las respuestas de DNS que contienen varios registros, lo que proporciona tolerancia a errores y equilibra la carga en varios puntos de conexión.

Estos tutoriales cubren varios casos de uso y escenarios, lo que ayuda a aprovechar de manera efectiva las políticas de enrutamiento, los registros ponderados y el enrutamiento basado en la latencia de Route 53 para optimizar la administración del DNS y el enrutamiento del tráfico.

Temas

- [Uso de Amazon Route 53 como el servicio DNS de subdominios sin migrar el dominio principal](#)
- [Transición al direccionamiento basado en la latencia en Amazon Route 53](#)
- [Incorporación de otra región a su direccionamiento basado en la latencia en Amazon Route 53](#)
- [Uso de registros ponderados y de latencia en Amazon Route 53 para dirigir el tráfico a varias instancias de Amazon EC2 en una región](#)
- [Administración de más de 100 registros ponderados en Amazon Route 53](#)
- [Ponderación de respuestas de múltiples registros con tolerancia a errores en Amazon Route 53](#)

Uso de Amazon Route 53 como el servicio DNS de subdominios sin migrar el dominio principal

Amazon Route 53 proporciona flexibilidad para administrar el DNS de los subdominios, lo que le permite aprovechar sus características sin necesidad de migrar el dominio principal en su totalidad.

Puede crear un subdominio nuevo o migrar uno existente a Route 53 y, al mismo tiempo, mantener el dominio principal alojado en otro proveedor de servicios de DNS.

Creación de un subdominio nuevo con Route 53:

1. Creación de una zona alojada para el subdominio nuevo.
2. Agregue los registros DNS que desee (p. ej., A, CNAME, MX) para el subdominio a la zona alojada.
3. Obtenga los servidores de nombres de Route 53 asignados a la zona alojada.
4. Actualice la configuración de DNS del dominio principal al agregar registros NS (servidor de nombres) para el subdominio y apuntar a los servidores de nombres de Route 53.

Migración de un subdominio existente a Route 53:

1. Creación de una zona alojada para el subdominio.
2. Obtenga la configuración de DNS actual para el subdominio de su proveedor de servicios de DNS vigente.
3. Agregue los registros DNS pertinentes a la zona alojada.
4. Obtenga los servidores de nombres de Route 53 asignados a la zona alojada.

5. Actualice la configuración de DNS del dominio principal al agregar registros NS para el subdominio y apuntar a los servidores de nombres de Route 53.

Si sigue estos pasos, puede aprovechar las características avanzadas de Route 53, como las comprobaciones de estado, las políticas de enrutamiento y la administración del flujo de tráfico, para los subdominios y, al mismo tiempo, mantener la configuración de DNS del dominio principal con su proveedor actual.

Temas

- [Creación de un subdominio que usa Amazon Route 53 como el servicio DNS sin migrar el dominio principal](#)
- [Migración de un servicio DNS de un subdominio a Amazon Route 53 sin migrar el dominio principal](#)

Creación de un subdominio que usa Amazon Route 53 como el servicio DNS sin migrar el dominio principal

Puede crear un subdominio que usa Amazon Route 53 como servicio DNS sin migrar el dominio principal desde otro servicio DNS.

El proceso consta de los siguientes pasos básicos:

1. [Determinar](#) si debe utilizar este procedimiento.
2. [Crear una zona alojada de Route 53 para el subdominio](#).
3. [Agregar registros](#) para el nuevo subdominio a la zona alojada de Route 53.
4. Solo API: [Confirmar que los cambios se han propagado](#) a todos los servidores DNS de Route 53.

Note

En la actualidad, el único modo de verificar que los cambios se han propagado es utilizar la acción [GetChange API](#). Por lo general, los cambios se propagan a todos los servidores de nombres de Route 53 en un plazo de 60 segundos.

5. [Actualice el servicio DNS para el dominio principal añadiendo registros de servidores de nombres al subdominio](#).

Decisión de qué procedimientos va a utilizar para crear un subdominio

Los procedimientos de este tema explican cómo realizar una operación poco frecuente. Si ya utiliza Route 53 como servicio DNS del dominio y solo desea dirigir el tráfico de un subdominio (como, por ejemplo, `www.example.com`) a sus recursos (por ejemplo, un servidor web que se ejecuta en una instancia de EC2), consulte [Direccionamiento del tráfico de subdominios](#).

Utilice este procedimiento solo si está utilizando otro servicio DNS para un dominio, como `example.com`, y desea comenzar a utilizar Route 53 como servicio DNS para un nuevo subdominio de ese dominio, como `www.example.com`.

Creación de una zona alojada para el nuevo subdominio

Cuando desee utilizar Amazon Route 53 como servicio DNS para un nuevo subdominio sin migrar el dominio principal, comience con la creación de una zona alojada para el subdominio. Route 53 almacena información acerca de su subdominio en la zona alojada.

Para obtener información sobre cómo crear una zona alojada mediante la consola de Route 53, consulte [Crear una zona alojada pública](#).

Creación de registros

Puede crear registros mediante la consola de Amazon Route 53 o la API de Route 53. Los registros que cree en Route 53 se convertirán en los registros que el DNS utilizará después de delegar la responsabilidad del subdominio a Route 53 como se explica más adelante en [Actualización del servicio DNS con los registros de servidor de nombres para el subdominio](#).

Important

No cree registros de servidor de nombres (NS) o de inicio de autoridad (SOA) adicionales en la zona alojada de Route 53, ni elimine los registros SOA y NS existentes.

Para crear registros mediante la consola de Route 53, consulte [Uso de registros](#). Para crear registros mediante la API de Route 53, use `ChangeResourceRecordSets`. Para obtener más información, consulte [ChangeResourceRecordSets](#) en la [Referencia de la API de Amazon Route 53](#).

Comprobación del estado de sus cambios (solo para API)

La creación de una nueva zona alojada y el cambio de registros tardan un tiempo en propagarse a los servidores DNS de Route 53. Si ha utilizado [ChangeResourceRecordSets](#) para crear sus

registros, puede utilizar la acción `GetChange` a fin de determinar si los cambios se han propagado. (`ChangeResourceRecordSets` devuelve un valor para `ChangeId`, que puede incluir en una solicitud `GetChange` posterior. Si creó los registros mediante la consola, `ChangeId` no estará disponible). Para obtener más información, consulte [GET GetChange](#) en la Referencia de la API de Amazon Route 53.

 Note

Por lo general, los cambios se propagan a todos los servidores de nombres de Route 53 en un plazo de 60 segundos.

Actualización del servicio DNS con los registros de servidor de nombres para el subdominio

Después de haber propagado los cambios en los registros de Amazon Route 53 (consulte [Comprobación del estado de sus cambios \(solo para API\)](#)), actualice el servicio DNS para el dominio principal agregando registros NS para el subdominio. Esto se denomina delegación de la responsabilidad del subdominio en Route 53. Por ejemplo, si el dominio principal `example.com` está alojado con otro servicio DNS y ha creado el subdominio `test.example.com` en Route 53, debe actualizar el servicio DNS de `example.com` con los nuevos registros NS de `test.example.com`.

Realice el siguiente procedimiento.

1. Con el método proporcionado por el servicio DNS, realice un backup del archivo de zona para el dominio principal.
2. En la consola de Route 53, obtenga los servidores de nombres de la zona alojada de Route 53:
 - a. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
 - b. En el panel de navegación, haga clic en Hosted zones (Zonas alojadas).
 - c. En la página Hosted zones (Zonas alojadas), elija el botón de radio (no el nombre) de la zona alojada y luego View details (Ver detalles).
 - d. En la página de detalles de la zona alojada, elija Hosted zone details (Detalles de la zona alojada).
 - e. Anote los nombres de los cuatro servidores que aparecen en Name servers (Servidores de nombres).

También puede utilizar la acción `GetHostedZone`. Para obtener más información, consulte [GetHostedZone](#) en la Referencia de la API de Amazon Route 53.

3. Con el método proporcionado por el servicio DNS del dominio principal, añada registros NS para el subdominio al archivo de zona del dominio principal. En estos registros NS, especifique los cuatro servidores de nombres de Route 53 que están asociados con la zona alojada que ha creado en el paso 1.

Important

No añada un registro de inicio de autoridad (SOA) al archivo de zona para el dominio principal. Dado que el subdominio utilizará Route 53, el servicio DNS del dominio principal no es la autoridad para el subdominio.

Si su servicio de DNS ha añadido automáticamente un registro SOA para el subdominio, elimine dicho registro. Sin embargo, no elimine el registro SOA del dominio principal.

Migración de un servicio DNS de un subdominio a Amazon Route 53 sin migrar el dominio principal

Puede migrar un subdominio para que utilice Amazon Route 53 como servicio DNS sin migrar el dominio principal desde otro servicio DNS.

El proceso consta de los siguientes pasos básicos:

1. [Determinar](#) si debe utilizar este procedimiento.
2. [Crear una zona alojada de Route 53 para el subdominio](#).
3. [Solicite la configuración de DNS al proveedor de servicios DNS actual para el dominio principal](#).
4. [Agregue registros](#) para el subdominio a su zona alojada de Route 53.
5. Solo API: [Confirmar que los cambios se han propagado](#) a todos los servidores DNS de Route 53.

 Note

En la actualidad, el único modo de verificar que los cambios se han propagado es utilizar la acción [GetChange API](#). Por lo general, los cambios se propagan a todos los servidores de nombres de Route 53 en un plazo de 60 segundos.

6. [Actualice la configuración de DNS con el proveedor de servicios DNS para el servidor principal agregando registros de servidores de nombres al subdominio.](#)

Decisión de qué procedimientos va a utilizar para crear un subdominio

Los procedimientos de este tema explican cómo realizar una operación poco frecuente. Si ya utiliza Route 53 como servicio DNS del dominio y solo desea dirigir el tráfico de un subdominio (como, por ejemplo, `www.example.com`) a sus recursos (por ejemplo, un servidor web que se ejecuta en una instancia de EC2), consulte [Direccionamiento del tráfico de subdominios](#).

Utilice este procedimiento solo si está utilizando otro servicio DNS para un dominio, como `example.com`, y desea comenzar a utilizar Route 53 como servicio DNS para un subdominio existente de ese dominio, como `www.example.com`.

Creación de una zona alojada para el subdominio

Si desea migrar un subdominio desde otro servicio DNS a Amazon Route 53 pero no desea migrar el dominio principal, comience creando una zona alojada para el subdominio. Route 53 almacena información acerca de su subdominio en la zona alojada.

Para obtener información sobre cómo crear una zona alojada mediante la consola de Route 53, consulte [Crear una zona alojada pública](#).

Solicitar configuración de DNS actual a su proveedor de servicios DNS

Para simplificar el proceso de migración de un subdominio existente a Route 53, solicite la configuración de DNS actual del dominio al proveedor de servicios DNS que administra el dominio actualmente. Puede utilizar esta información como base a fin de configurar Route 53 como servicio DNS para el subdominio.

Lo que tiene que pedir y el formato del material que se le entregue dependen de la empresa que esté utilizando actualmente como su proveedor del servicio DNS. Idealmente, le proporcionarán

un archivo de zona, que contiene información sobre todos los registros de su configuración actual. (Los registros le indican a DNS cómo desea que se dirija el tráfico de sus dominios y subdominios. Por ejemplo, cuando alguien escribe su nombre de dominio en un navegador web, ¿desea que el tráfico se dirija a un servidor web de su centro de datos, a una instancia de Amazon EC2, a una distribución de CloudFront o a cualquier otra ubicación?) Si puede obtener un archivo de zona de su proveedor de servicio DNS actual, puede editarlo para quitar los registros que no desea migrar a Amazon Route 53. A continuación, puede importar el resto de registros a su zona alojada de Route 53, lo que simplifica significativamente el proceso. Pregunte al equipo de atención al cliente de su proveedor del servicio DNS actual cómo obtener un archivo de zona o una lista de registros.

Creación de registros

Utilizando como punto de partida los registros que ha obtenido de su proveedor de servicios DNS actual, cree los registros correspondientes en la zona alojada de Amazon Route 53 que creó para el subdominio. Los registros que cree en Route 53 se convertirán en los registros que el DNS utilizará después de delegar la responsabilidad del subdominio a Route 53 como se explica más adelante en [Actualización del servicio DNS con los registros de servidor de nombres para el subdominio](#).

Important

No cree registros de servidor de nombres (NS) o de inicio de autoridad (SOA) adicionales en la zona alojada de Route 53, ni elimine los registros SOA y NS existentes.

Para crear registros mediante la consola de Route 53, consulte [Uso de registros](#). Para crear registros mediante la API de Route 53, use `ChangeResourceRecordSets`. Para obtener más información, consulte [ChangeResourceRecordSets](#) en la [Referencia de la API de Amazon Route 53](#).

Comprobación del estado de sus cambios (solo para API)

La creación de una nueva zona alojada y el cambio de registros tardan un tiempo en propagarse a los servidores DNS de Route 53. Si ha utilizado [ChangeResourceRecordSets](#) para crear sus registros, puede utilizar la acción `GetChange` a fin de determinar si los cambios se han propagado. (`ChangeResourceRecordSets` devuelve un valor para `ChangeId`, que puede incluir en una solicitud `GetChange` posterior. Si creó los registros mediante la consola, `ChangeId` no estará disponible). Para obtener más información, consulte [GET GetChange](#) en la Referencia de la API de Amazon Route 53.

 Note

Por lo general, los cambios se propagan a todos los servidores de nombres de Route 53 en un plazo de 60 segundos.

Actualización del servicio DNS con los registros de servidor de nombres para el subdominio

Después de haber propagado los cambios en los registros de Amazon Route 53 (consulte [Comprobación del estado de sus cambios \(solo para API\)](#)), actualice el servicio DNS para el dominio principal agregando registros NS para el subdominio. Esto se denomina delegación de la responsabilidad del subdominio en Route 53. Por ejemplo, suponga que el dominio principal example.com está alojado en otro servicio DNS y está migrando el subdominio test.example.com a Route 53. Debe crear una zona alojada para test.example.com y actualizar el servicio DNS para example.com con los registros NS que Route 53 asignó a la zona alojada nueva para test.example.com.

Realice el siguiente procedimiento.

1. Con el método proporcionado por el servicio DNS, realice un backup del archivo de zona para el dominio principal.
2. Si el proveedor de servicios DNS anterior del dominio tiene un método para cambiar la configuración TTL de sus servidores de nombres, le recomendamos que cambie la configuración a 900 segundos. Esto limita el tiempo durante el que las solicitudes cliente intentarán resolver los nombres de dominio con servidores de nombres obsoletos. Si el TTL actual es de 172 800 segundos (dos días), que constituye un valor predeterminado común, aún deberá esperar dos días para que los solucionadores y los clientes dejen de almacenar en caché los registros de DNS con el TTL anterior. Cuando transcurra el tiempo de TTL especificado, podrá eliminar sin problemas los registros almacenados en el proveedor anterior y realizar cambios únicamente en Route 53.
3. En la consola de Route 53, obtenga los servidores de nombres de la zona alojada de Route 53:
 - a. Inicie sesión en la Consola de administración de AWS y abra la consola de Route 53 en <https://console.aws.amazon.com/route53/>.
 - b. En el panel de navegación, haga clic en Hosted zones (Zonas alojadas).

- c. En la página Hosted zones (Zonas alojadas), elija el botón de radio (no el nombre) de la zona alojada y luego View details (Ver detalles).
- d. En la página de detalles de la zona alojada, elija Hosted zone details (Detalles de la zona alojada).
- e. Anote los nombres de los cuatro servidores que aparecen en Name servers (Servidores de nombres).

También puede utilizar la acción `GetHostedZone`. Para obtener más información, consulte [GetHostedZone](#) en la Referencia de la API de Amazon Route 53.

4. Con el método proporcionado por el servicio DNS del dominio principal, añada registros NS para el subdominio al archivo de zona del dominio principal. Asigne a los registros NS el mismo nombre que el subdominio. Para los valores en los registros NS, especifique los cuatro servidores de nombres de Route 53 que están asociados a la zona alojada creada en el paso 2. Tenga en cuenta que los diferentes servicios DNS utilizan distintas terminologías. Es posible que necesite ponerse en contacto con el soporte de su servicio DNS para obtener información sobre cómo realizar este paso.

 Important

No añada un registro de inicio de autoridad (SOA) al archivo de zona para el dominio principal. Dado que el subdominio utilizará Route 53, el servicio DNS del dominio principal no es la autoridad para el subdominio.

Si su servicio de DNS ha añadido automáticamente un registro SOA para el subdominio, elimine dicho registro. Sin embargo, no elimine el registro SOA del dominio principal.

En función de la configuración de TTL de los servidores de nombres del dominio principal, la propagación de los cambios a los servicios de resolución de nombres DNS puede tardar 48 horas o más. Durante este período, los solucionadores de DNS aún pueden responder a las solicitudes con los servidores de nombres para el servicio DNS del dominio principal. Además, es posible que los equipos cliente sigan teniendo almacenados en su caché los servidores de nombres anteriores del subdominio.

5. Cuando caduque el TTL del registrador del dominio (consulte el paso 2), elimine los siguientes registros del archivo de zona para el dominio principal:
 - Los registros que agregó a Route 53, como se describe en [Creación de registros](#).

- Los registros NS del servicio DNS. Cuando haya terminado de eliminar registros NS, los únicos que quedarán en el archivo de zona serán los que creó en el paso 4.

Transición al direccionamiento basado en la latencia en Amazon Route 53

Con el direccionamiento basado en la latencia, Amazon Route 53 puede dirigir a los usuarios al punto de conexión de AWS con la mínima latencia disponible. Por ejemplo, puede asociar un nombre DNS como `www.example.com` a un balanceador de carga clásico, de aplicación o de red de ELB, o a instancias de Amazon EC2 o direcciones IP elásticas alojadas en las regiones EE. UU. Este (Ohio) y Europa (Irlanda). Los servidores DNS de Route 53 deciden, en función de las condiciones de la red de las dos últimas semanas, qué instancias (y de qué regiones) deben atender a cada usuario. Un usuario de Londres probablemente será dirigido a la instancia de Europa (Irlanda), un usuario de Chicago probablemente lo será a la instancia de EE. UU. Este (Ohio), y así sucesivamente. Route 53 admite el direccionamiento basado en la latencia para los registros A, AAAA, TXT y CNAME, así como alias para registros A y AAAA.

Note

Los datos sobre la latencia entre los usuarios y sus recursos se basan totalmente en el tráfico entre los usuarios y los centros de datos de AWS. Si no utiliza recursos en una región de AWS, la latencia real entre sus usuarios y sus recursos puede variar considerablemente con respecto a los datos de latencia de AWS. Esto es así aunque sus recursos se encuentren en la misma ciudad que una región de AWS.

Para lograr una transición suave y de bajo riesgo, puede combinar registros ponderados y de latencia. De este modo, podrá migrar gradualmente del direccionamiento estándar al direccionamiento basado en latencia, con un control total y la capacidad de restauración en cada fase. Pongamos un ejemplo en el que `www.example.com` esté alojado en una instancia de Amazon EC2 en la región EE. UU. Este (Ohio). La instancia tiene la dirección IP elástica : `W.W.W.W`. Suponga que desea continuar dirigiendo el tráfico a la región EE. UU. Este (Ohio) cuando corresponda y, al mismo tiempo, comenzar a dirigir a los usuarios a otras instancias de Amazon EC2 de la región EE. UU. Oeste (Norte de California) (IP elástica `X.X.X.X`) y de la región Europa (Irlanda) (IP elástica `Y.Y.Y.Y`). La zona alojada de Route 53 para `example.com` ya dispone de un registro para

`www.example.com`, cuyo valor de Type (Tipo) es A y cuyo valor de Value (Value) (una dirección IP) es `W.W.W.W`.

Al terminar el ejemplo siguiente, tendrá dos registros de alias ponderados:

- Convertirá su registro existente de `www.example.com` en un registro de alias ponderado que sigue dirigiendo la mayoría de su tráfico a la instancia de Amazon EC2 existente en la región EE. UU. Este (Ohio).
- Creará otro registro de alias ponderado que redirija inicialmente solo una pequeña parte de su tráfico a los registros de latencia, que a su vez redirigen el tráfico a las tres regiones.

Al actualizar las ponderaciones de esos registros de alias ponderados, puede pasar gradualmente de dirigir el tráfico solo a la región EE. UU. Este (Ohio) a dirigirlo a las tres regiones en las que tiene instancias de Amazon EC2.

Para migrar al direccionamiento basado en latencia

1. Realice una copia del registro de `www.example.com`, pero utilice un nuevo nombre de dominio, por ejemplo, `copy-www.example.com`. Asigne al nuevo registro los mismos valores de Type (Tipo) (A) y Value (Valor) (`W.W.W.W`) que el registro de `www.example.com`.
2. Actualice el registro A existente de `www.example.com` para convertirlo en un registro de alias ponderado:
 - Para Value/Route traffic to (Valor/ruta de destino del tráfico), elija Alias to another record in this hosted zone (Alias a otro registro en esta zona alojada) y especifique `copy-www.example.com`.
 - Para Weight (Peso), especifique 100.

Cuando termine la actualización, Route 53 seguirá utilizando este registro para dirigir todo el tráfico al recurso que tiene una dirección IP de `W.W.W.W`.

3. Cree un registro de latencia para cada una de sus instancias de Amazon EC2; por ejemplo:
 - EE. UU. Este (Ohio), dirección IP elástica `W.W.W.W`
 - EE. UU. Oeste (Norte de California), dirección IP elástica `X.X.X.X`
 - Europa (Irlanda), dirección IP elástica `Y.Y.Y.Y`

Asigne a todos los registros de latencia el mismo nombre de dominio, por ejemplo, `www-lbr.example.com`, y el mismo tipo, A.

Cuando termine de crear los registros de latencia, Route 53 seguirá dirigiendo el tráfico mediante el registro que actualizó en el paso 2.

Puede utilizar `www-lbr.example.com` para probar la validación, por ejemplo, para garantizar que cada puntos de conexión pueda aceptar solicitudes.

4. Ahora agreguemos el registro de latencia `www-lbr.example.com` al registro ponderado `www.example.com` y comencemos a dirigir parte del tráfico a las instancias de Amazon EC2 correspondientes. Esto significa que la instancia de Amazon EC2 de la región EE. UU. Este (Ohio) recibirá tráfico de ambos registros ponderados.

Cree otro registro de alias ponderado para `www.example.com`:

- Para Value/Route traffic to (Valor/ruta de destino del tráfico), elija Alias to another record in this hosted zone (Alias a otro registro en esta zona alojada) y especifique `www-lbr.example.com`.
- Para Weight (Peso), especifique 1.

Cuando termine y los cambios se sincronicen con los servidores de Route 53, este servicio comenzará a dirigir una pequeña fracción de su tráfico (1/101) a las instancias de Amazon EC2 para las que ha creado registros de latencia en el paso 3.

5. A medida que refuerce su confianza en que los puntos de enlace tienen la escala correcta para el tráfico entrante, ajuste los pesos. Por ejemplo, si desea que un 10% de sus solicitudes dependan del direccionamiento basado en latencia, cambie los pesos a 90 y 10, respectivamente.

Para obtener más información acerca de la creación de registros de latencia, consulte [Creación de registros con la consola de Amazon Route 53](#).

Incorporación de otra región a su direccionamiento basado en la latencia en Amazon Route 53

Si está utilizando el direccionamiento basado en latencia y desea agregar una instancia a una nueva región, puede desplazar gradualmente el tráfico a la nueva región de la misma manera que cambió poco a poco el tráfico al direccionamiento basado en latencia en [Transición al direccionamiento basado en la latencia en Amazon Route 53](#).

Por ejemplo, suponga que está utilizando el direccionamiento basado en la latencia para dirigir el tráfico de `www.example.com`, y desea agregar una instancia de Amazon EC2 en Asia-Pacífico (Tokio) a sus instancias en EE. UU. Este (Ohio), EE. UU. Oeste (Norte de California) y Europa (Irlanda). El ejemplo siguiente explica una forma de agregar una instancia a otra región.

En este ejemplo, la zona alojada de Amazon Route 53 de `example.com` ya tiene un registro de alias ponderado para `www.example.com` que está dirigiendo el tráfico a los registros basados en latencia de `www-lbr.example.com`:

- EE. UU. Este (Ohio), dirección IP elástica `W.W.W.W`
- EE. UU. Oeste (Norte de California), dirección IP elástica `X.X.X.X`
- Europa (Irlanda), dirección IP elástica `Y.Y.Y.Y`

El registro de alias ponderado tiene un peso de 100. Después de migrar al direccionamiento basado en latencia, suponga que hubiera eliminado el otro registro ponderado que utilizó para la transición.

Incorporación de otra región a su direccionamiento basado en la latencia en Route 53

1. Cree cuatro nuevos registros basados en latencia que incluyan las tres regiones originales y la región nueva a la que desea empezar a redirigir el tráfico.
 - EE. UU. Este (Ohio), dirección IP elástica `W.W.W.W`
 - EE. UU. Oeste (Norte de California), dirección IP elástica `X.X.X.X`
 - Europa (Irlanda), dirección IP elástica `Y.Y.Y.Y`
 - Asia-Pacífico (Tokio), dirección IP elástica `Z.Z.Z.Z`

Asigne a todos los registros de latencia el mismo nuevo nombre de dominio, por ejemplo, `www-lbr-2012-04-30.example.com` y el mismo tipo, A.

Cuando termine de crear los registros de latencia, Route 53 seguirá dirigiendo el tráfico mediante el registro de alias ponderado (`www.example.com`) y los registros de latencia (`www-lbr.example.com`) originales.

Puede utilizar los registros de `www-lbr-2012-04-30.example.com` para probar la validación, por ejemplo, para garantizar que cada puntos de conexión pueda aceptar solicitudes.

2. Cree un registro de alias ponderado para los nuevos registros de latencia:

- Para el nombre de dominio, especifique el nombre del registro de alias ponderado existente, `www.example.com`.
- Para Value/Route traffic to (Valor/ruta de destino del tráfico), elija Alias to another record in this hosted zone (Alias a otro registro en esta zona alojada) y especifique `www-lbr-2012-04-30.example.com`.
- Para Weight (Peso), especifique 1.

Cuando termine, Route 53 comenzará a dirigir una pequeña fracción de su tráfico (1/101) a las instancias de Amazon EC2 para las que ha creado los registros de latencia de `www-lbr-2012-04-30.example.com` en el paso 1. El resto del tráfico seguirá dirigiéndose hacia los registros de latencia de `www-lbr.example.com`, que no incluyen la instancia de Amazon EC2 de la región Asia-Pacífico (Tokio).

3. A medida que refuerce su confianza en que los puntos de enlace tienen la escala correcta para el tráfico entrante, ajuste los pesos. Por ejemplo, si desea que un 10% de las solicitudes se redirijan a los registros de latencia que incluyen la región de Tokio, cambie el peso de `www-lbr.example.com` (de 100 a 90) y el de `www-lbr-2012-04-30.example.com` (de 1 a 10).

Para obtener más información acerca de la creación de registros, consulte [Creación de registros con la consola de Amazon Route 53](#).

Uso de registros ponderados y de latencia en Amazon Route 53 para dirigir el tráfico a varias instancias de Amazon EC2 en una región

Si su aplicación se ejecuta en instancias de Amazon EC2 de dos o más regiones de Amazon EC2, y si tiene más de una instancia de Amazon EC2 en una o varias regiones, puede utilizar el

direccionamiento basado en la latencia para dirigir el tráfico a la región adecuada y, a continuación, utilizar registros ponderados para dirigir el tráfico a las instancias dentro de la región según la ponderación que especifique.

Por ejemplo, suponga que tiene tres instancias de Amazon EC2 con direcciones IP elásticas en la región EE. UU. Este (Ohio) y desea distribuir las solicitudes entre las tres IP de manera uniforme para los usuarios correspondientes a esta región. Una instancia de Amazon EC2 es suficiente en las demás regiones, aunque puede aplicar la misma técnica a muchas regiones a la vez.

Para utilizar registros ponderados y de latencia en Amazon Route 53 para dirigir el tráfico a varias instancias de Amazon EC2 en una región

1. Cree un grupo de registros ponderados para las instancias de Amazon EC2 en la región. Tenga en cuenta lo siguiente:
 - Asigne a cada registro ponderado el mismo valor para Record name (Nombre del registro) (por ejemplo, `us-east.example.com`) y Record type (Tipo de registro).
 - Para Value/Route traffic to (Valor/ruta de destino del tráfico), elija IP address or another value depending on the record type (Dirección IP u otro valor en función del tipo de registro).
 - Si desea equiparar el peso de las instancias de Amazon EC2, especifique el mismo valor para Weight (Peso).
 - Especifique un valor único para Set ID (ID de conjunto) en cada registro.

Para obtener más información acerca de los valores de registro ponderados, consulte .

[Direccionamiento ponderado](#)

2. Si tiene varias instancias de Amazon EC2 en otras regiones, repita el paso 1 en ellas. Especifique un valor diferente para Name en cada región.
3. Para cada región en la que tenga varias instancias de Amazon EC2 (por ejemplo, EE. UU. Este (Ohio)), cree un registro de alias de latencia. En Valor/ruta de destino del tráfico, seleccione Alias a otro registro en esta zona alojada y especifique el valor de Nombre del registro (por ejemplo, `us-east.example.com`) que asignó a los registros ponderados de esa región.
4. Para cada región en la que tenga una instancia de Amazon EC2, cree un registro de latencia. En Record name (Nombre del registro), indique el mismo valor que usó para los registros de alias de latencia que creó en el paso 3. Para Value/Route traffic to (Valor/ruta de destino del tráfico), elija IP address or another value depending on the record type (Dirección IP u otro valor

en función del tipo de registro) y especifique la dirección IP elástica de la instancia de Amazon EC2 de esa región.

Para obtener más información acerca de cómo agregar registros de alias a instancias de Amazon EC2, consulte [Enrutamiento del tráfico a una EC2 instancia de Amazon](#)

Para obtener más información acerca de la creación de registros, consulte [Creación de registros con la consola de Amazon Route 53](#).

Administración de más de 100 registros ponderados en Amazon Route 53

Amazon Route 53 permite configurar registros ponderados. Para un nombre y tipo concretos (por ejemplo, `www.example.com`, tipo A), puede configurar hasta 100 respuestas alternativas, cada una con su propio peso. Al responder a las consultas de `www.example.com`, los servidores DNS de Route 53 seleccionan una respuesta aleatoria ponderada para devolver a los solucionadores de DNS. El valor de un registro ponderado que tenga un peso de 2 se devuelve, de media, el doble de veces que el valor de un registro ponderado con un peso de 1.

Si necesita redirigir el tráfico a más de 100 puntos de enlace, una forma de conseguirlo es utilizar un árbol que incluya registros ponderados y registros de alias. Por ejemplo, el primer “nivel” del árbol puede tener hasta 100 registros de alias ponderados, cada uno de los cuales puede, a su vez, apuntar a un máximo de 100 registros ponderados. Route 53 permite hasta tres niveles de recursividad, lo que le permite administrar hasta 1 000 000 de puntos de enlace ponderados únicos.

Un árbol sencillo de dos niveles puede tener este aspecto:

Registros de alias ponderados

- `www.example.com` alias para `www-a.example.com` con un peso de 1
- `www.example.com` alias para `www-b.example.com` con un peso de 1

Registros ponderados

- `www-a.example.com`, tipo A, valor 192.0.2.1, peso 1
- `www-a.example.com`, tipo A, valor 192.0.2.2, peso 1

- `www-b.example.com`, tipo A, valor 192.0.2.3, peso 1
- `www-b.example.com`, tipo A, valor 192.0.2.4, peso 1

Para obtener más información acerca de la creación de registros, consulte [Uso de registros](#).

Ponderación de respuestas de múltiples registros con tolerancia a errores en Amazon Route 53

Note

Los registros que utilicen la política de direccionamiento con respuesta de varios valores se comportan prácticamente igual que la configuración documentada en este tutorial. La principal diferencia es que la configuración del tutorial le permite especificar ponderaciones, que pueden ser útiles cuando sus puntos de enlace tienen diferentes capacidades. Para obtener más información, consulte [Direccionamiento de respuesta con varios valores](#).

Un registro ponderado de Amazon Route 53 solo se puede asociar a un registro, es decir, una combinación de un nombre (por ejemplo, `example.com`) y un tipo de registro (por ejemplo, A). Sin embargo, a menudo es conveniente ponderar respuestas de DNS que contengan varios registros.

Por ejemplo, puede que tenga ocho instancias de Amazon EC2 o puntos de enlace de IP elásticas para un servicio. Si los clientes de dicho servicio admiten los reintentos de conexión (igual que todos los navegadores habituales), al proporcionar varias direcciones IP en las respuestas de DNS estará ofreciendo a los clientes puntos de enlace alternativos en caso de que se produzca un error en un puntos de conexión concreto. Puede incluso ofrecer protección ante situaciones en las que se produzca algún error en una zona de disponibilidad, siempre y cuando configure respuestas para que contengan una combinación de IP hospedadas en dos o más zonas de disponibilidad.

Las respuestas de varios registros también son útiles cuando un gran número de clientes (por ejemplo, aplicaciones web para dispositivos móviles) comparten un pequeño conjunto de memorias caché de DNS. En este caso, las respuestas de varios registros permiten a los clientes redirigir las solicitudes a varios puntos de enlace aunque reciban una respuesta de DNS común de la caché compartida.

Estos tipos de respuestas para varios registros ponderados pueden obtenerse mediante una combinación de registros y registros de alias ponderados. Puede agrupar ocho puntos de enlace en dos conjuntos de registros distintos que contienen cuatro direcciones IP cada uno:

`endpoint-a.example.com`, tipo A, con los valores siguientes:

- 192.0.2.1
- 192.0.2.2
- 192.0.2.128
- 192.0.2.129

`endpoint-b.example.com`, tipo A, con los valores siguientes:

- 192.0.2.3
- 192.0.2.4
- 192.0.2.130
- 192.0.2.131

Podrá crear después un registro de alias ponderado que apunte a cada grupo:

- Alias `www.example.com` para `endpoint-a.example.com`, tipo A, peso 1
- Alias `www.example.com` para `endpoint-b.example.com`, tipo A, peso 1

Para obtener más información acerca de la creación de registros, consulte [Uso de registros](#).

Prácticas recomendadas de Amazon Route 53

Esta sección proporciona las prácticas recomendadas para varios componentes de Amazon Route 53, entre ellos:

1. Prácticas recomendadas de DNS:

- Comprenda el equilibrio entre los valores del periodo de vida (TTL) y la capacidad de respuesta frente a la fiabilidad.
- Utilice registros de alias en lugar de registros CNAME siempre que sea posible para mejorar el rendimiento y ahorrar costos.
- Configure políticas de enrutamiento predeterminadas para garantizar que todos los clientes reciban una respuesta.
- Aproveche el enrutamiento basado en la latencia para minimizar la latencia de las aplicaciones y el geolocation/geoproximity enrutamiento para lograr estabilidad y previsibilidad.
- Verifique la propagación de los cambios mediante la API GetChange para flujos de trabajo automatizados.
- Delege subdominios de la zona principal para un enrutamiento consistente.
- Evite las respuestas únicas de gran tamaño mediante el enrutamiento de respuesta con varios valores.

2. Prácticas recomendadas de Resolver:

- Prevenga los bucles de enrutamiento al evitar asociar la misma VPC tanto a una regla de Resolver como al punto de conexión de entrada.
- Implemente reglas de grupos de seguridad para reducir la sobrecarga de seguimiento de las conexiones y maximizar el rendimiento de las consultas.
- Configure los puntos de conexión de entrada con direcciones IP en varias zonas de disponibilidad para la redundancia.
- Esté al tanto de los posibles ataques de desplazamiento por zonas de DNS y póngase en contacto con AWS Support si sus puntos finales sufren una limitación.

3. Prácticas recomendadas de comprobación de estado:

- Siga las recomendaciones para optimizar las comprobaciones de estado de Amazon Route 53 y garantizar una supervisión fiable de los recursos.

Si sigue estas prácticas recomendadas, puede optimizar el rendimiento, la fiabilidad y la seguridad de su infraestructura de DNS, lo que garantiza un enrutamiento eficiente y efectivo del tráfico a las aplicaciones y los servicios

Temas

- [Prácticas recomendadas de Amazon Route 53 DNS](#)
- [Mejores prácticas para VPC Resolver](#)
- [Prácticas recomendadas de las comprobaciones de estado de Amazon Route 53](#)

Prácticas recomendadas de Amazon Route 53 DNS

Siga estas prácticas recomendadas para obtener los mejores resultados al utilizar el servicio DNS de Amazon Route 53.

Utilice las funciones del plano de datos para la conmutación por error de DNS y la recuperación de aplicaciones

Los planos de datos de Route 53, incluidas las comprobaciones de estado y el control de enrutamiento del Control de recuperación de aplicaciones de Amazon Route 53 (ARC), se distribuyen a nivel mundial y están diseñados para ofrecer una disponibilidad y funcionalidad del 100 %, incluso durante eventos graves. Se integran entre sí y no dependen de la funcionalidad del plano de control. Si bien los planos de control de estos servicios, incluidas sus consolas, suelen ser muy fiables, están diseñados de forma más centralizada y priorizan la durabilidad y la consistencia en lugar de la alta disponibilidad. Para escenarios como la conmutación por error durante la recuperación ante desastres, se recomienda que utilice características como las comprobaciones de estado de Route 53 y el control de enrutamiento de ARC que dependen de la funcionalidad del plano de datos para actualizar el DNS. Para obtener más información, consulte [Conceptos de plano de datos y control](#) y [Blog: Creating Disaster Recovery Mechanisms Using Amazon Route 53 \(Creación de mecanismos de recuperación de desastres mediante Amazon Route 53\)](#).

Elección de valores TTL para registros DNS

El TTL de DNS es el valor numérico (en segundos) que utilizan los solucionadores de DNS para decidir durante cuánto tiempo se puede almacenar en caché un registro sin realizar otra consulta a Route 53. Todos los registros de DNS deben tener un TTL especificado para ellos. El intervalo recomendado para los valores de TTL es de 60 a 172,800 segundos.

La elección de un TTL implica un compromiso entre latencia y fiabilidad y la capacidad de respuesta a los cambios. Con un registro más corto TTLs, los solucionadores de DNS detectan las actualizaciones del registro más rápido, ya que deben realizar consultas con más frecuencia. Esto aumenta el volumen de consultas (y el costo). A medida que se alarga el TTL, los solucionadores de DNS responden a las consultas de la caché con más frecuencia, lo que suele ser más rápido, económico y, en algunas situaciones, más fiable porque evita consultas en Internet. No hay un valor ideal, pero vale la pena considerar qué es más importante para usted, si la capacidad de respuesta o la fiabilidad.

Entre los aspectos a tener en cuenta al configurar los valores de TTL se cuentan:

- Establece un registro de DNS TTLs durante el tiempo que puedas permitirte esperar a que se produzca un cambio. Esto es especialmente cierto en las delegaciones (conjuntos de registros NS) u otros registros que rara vez cambian, por ejemplo, registros MX. Para estos registros, TTLs se recomienda que sean más largos. Una opción común es un valor de entre una hora (3600 s) o un día (86,400 s).
- En el caso de los registros que deben modificarse como parte de un mecanismo de conmutación por error rápida (especialmente los registros cuyo estado ha sido comprobado), lo más adecuado es reducir el TTLs valor. Configurar un TTL de 60 o 120 segundos es una opción común para esta situación.
- Si desea realizar cambios en las entradas de DNS críticas, le recomendamos que las TTLs acorte temporalmente. A continuación, puede realizar los cambios, observar y revertir rápidamente de ser necesario. Una vez finalizados los cambios y funcionando como se esperaba, puede aumentar el TTL.

Para obtener más información, consulte [TTL \(segundos\)](#).

Registros CNAME

Los registros CNAME en DNS son una forma de indicar un nombre de dominio a otro. Si un solucionador de DNS resuelve el dominio-1.ejemplo.com y encuentra un CNAME que indica al domain-2.example.com, el solucionador de DNS debe proceder a solucionar el domain-2.example.com antes de poder responder. Estos registros son útiles en muchas situaciones, por ejemplo, para garantizar la consistencia cuando un sitio web tiene más de un nombre de dominio.

Sin embargo, los solucionadores de DNS deben realizar más consultas para responder CNAMEs, lo que aumenta la latencia y los costes. Siempre que sea posible, una alternativa más rápida y económica es utilizar un registro de alias de Route 53. Los registros de alias permiten a Route

53 responder con una respuesta directa para AWS los recursos (por ejemplo, un balanceador de carga) y para otros dominios dentro de la misma zona hospedada.

Para obtener más información, consulte [Enrutar el tráfico de Internet a sus AWS recursos](#).

Enrutamiento de DNS avanzado

- Al utilizar la geolocalización, la geoproximidad o el enrutamiento basado en la latencia, establezca siempre un valor predeterminado, a menos que desee que algunos clientes reciban un mensaje de tipo sin respuesta.
- Para minimizar la latencia de las aplicaciones, utilice el enrutamiento basado en la latencia. Este tipo de datos de enrutamiento puede cambiar con frecuencia.
- Para proporcionar estabilidad y previsibilidad en el enrutamiento, utilice el enrutamiento por geolocalización o por geoproximidad.

Para obtener más información, consulte [Enrutado de geolocalización](#), [Enrutamiento por geoproximidad](#) y [Enrutado basado en latencia](#).

Propagación de cambios de DNS

Al crear o actualizar un registro o una zona alojada mediante la consola o la API de Route 53, el cambio tarda un tiempo en reflejarse en Internet. Esto se llama propagación de cambios. Si bien la propagación generalmente es inferior a un minuto a nivel mundial, en ocasiones hay retrasos, por ejemplo, debido a problemas de sincronización con una ubicación o, en raras ocasiones, a problemas dentro del plano de control central. Si está creando flujos de trabajo de aprovisionamiento automatizados y es importante esperar a que se complete la propagación de los cambios antes de continuar con el siguiente paso del flujo de trabajo, utilice la [GetChangeAPI](#) para comprobar que los cambios de DNS se han aplicado (Status =INSYNC).

Delegación de DNS

Al delegar varios niveles de subdominios en DNS, es importante delegar siempre desde la zona principal. Por ejemplo, si va a delegar `www.dept.example.com`, debería hacerlo desde la zona `dept.example.com`, y no desde la zona `example.com`. Las delegaciones de una zona de abuelos a una de niños pueden no funcionar en absoluto o hacerlo de forma inconsistente. Para obtener más información, consulte [Direccionamiento del tráfico de subdominios](#).

Tamaño de la respuesta de DNS

Evite crear respuestas individuales de gran tamaño. Por encima de 512 bytes, muchos solucionadores de DNS deben volver a intentarlo a través de TCP en lugar de UDP, lo que puede reducir la fiabilidad y generar respuestas más lentas. Recomendamos utilizar enrutamiento

de respuestas de varios valores que elijan 8 direcciones IP aleatorias y en buen estado para mantener las respuestas dentro del límite de 512 bytes.

Para obtener más información, consulte [Direccionamiento de respuesta con varios valores](#) y [Servidor de prueba de tamaño de respuesta DNS](#).

Mejores prácticas para VPC Resolver

En esta sección se proporcionan las prácticas recomendadas para optimizar la resolución de VPC de Amazon Route 53 y se tratan los siguientes temas:

1. Cómo evitar las configuraciones en bucle con los puntos de conexión de Resolver

- Evite los bucles de enrutamiento al garantizar que la misma VPC no esté asociada tanto a una regla de Resolver como a su punto de conexión de entrada.
- Úselo AWS RAM para compartir VPCs entre cuentas y, al mismo tiempo, mantener las configuraciones de enrutamiento adecuadas.

Para obtener más información, consulte [Evitar las configuraciones en bucle con los puntos de enlace de Resolver](#)

2. Escalado de los puntos de conexión de Resolver:

- Implemente reglas de grupos de seguridad que permitan el tráfico en función del estado de la conexión para reducir la sobrecarga de seguimiento de las conexiones.
- Siga las reglas de los grupos de seguridad recomendadas para los puntos de conexión de Resolver, tanto de entrada como de salida, a fin de maximizar el rendimiento de las consultas.
- Supervise las combinaciones únicas de direcciones IP y puertos que generan tráfico de DNS para evitar limitaciones de capacidad.

Para obtener más información, consulte [Escalado de los puntos de enlace de Resolver](#)

3. Alta disponibilidad para puntos de conexión de Resolver:

- Cree puntos de conexión de entrada con las direcciones IP al menos en dos zonas de disponibilidad para la redundancia.
- Aprovisionamiento de interfaces de red adicionales para garantizar la disponibilidad durante el mantenimiento o los picos de tráfico

Para obtener más información, consulte [Alta disponibilidad para puntos de enlace de Resolver](#)

4. Prevención de los ataques de desplazamiento por zonas DNS:

- Esté atento a los posibles ataques de desplazamiento de zonas DNS, en los que los atacantes intentan recuperar todo el contenido de las zonas DNS firmadas por DNSSEC.
- Si sus puntos finales sufren una ralentización debido a la sospecha de que están caminando por zonas, póngase en contacto con AWS Support para obtener ayuda.

Para obtener más información, consulte [Consulta exhaustiva de nombres de zona DNS](#)

Si sigue estas prácticas recomendadas, puede optimizar el rendimiento, la escalabilidad y la seguridad de sus implementaciones de VPC Resolver, garantizando una resolución de DNS fiable y eficiente para sus aplicaciones y recursos.

Evitar las configuraciones en bucle con los puntos de enlace de Resolver

No asocie la misma VPC a una regla de Resolver y a su punto de conexión de entrada (tanto si se trata de un destino directo del punto de conexión como si se realiza a través de un servidor DNS en las instalaciones). Cuando el punto de conexión de salida de una regla de Resolver apunta a un punto de conexión de entrada que comparte una VPC con la regla, puede provocar un bucle en el que la consulta se pasa continuamente entre los puntos de conexión de entrada y salida.

La regla de reenvío puede seguir asociándose a otras VPCs que se compartan con otras cuentas mediante (). AWS Resource Access Manager AWS RAM Las zonas alojadas privadas asociadas al centro, o una VPC central, seguirán resolviendo desde las consultas hasta los puntos de enlace de entrada, porque las reglas de resolución de reenvío no cambian esta resolución.

Escalado de los puntos de enlace de Resolver

Los grupos de seguridad de los puntos de enlace de Resolver utilizan el seguimiento de las conexiones para recopilar información sobre el tráfico hacia y desde los puntos de enlace. Cada interfaz de punto final tiene un número máximo de conexiones de las que se puede realizar un seguimiento, pero un gran volumen de consultas de DNS puede superar las conexiones y causar limitación controlada y pérdida de consultas. El seguimiento de conexiones AWS es el comportamiento predeterminado para supervisar el estado del tráfico que fluye a través de los grupos de seguridad (SGs). Si utiliza el seguimiento de SGs conexiones para reducir el rendimiento del tráfico, puede implementar conexiones sin seguimiento para reducir la sobrecarga y mejorar el rendimiento. Para obtener más información, consulte [Conexiones sin seguimiento](#).

Si el seguimiento de conexiones se aplica mediante reglas restrictivas del grupo de seguridad o las consultas se enrutan a través del Equilibrador de carga de red (consulte [Conexiones con](#)

[seguimiento automático](#)), el número máximo total de consultas por segundo por dirección IP para un punto de conexión puede ser tan bajo como 1500.

Recomendaciones de reglas del grupo de seguridad de entrada y salida para el punto de conexión de entrada de Resolver

Reglas de entrada

Tipo de protocolo	Número de puerto	IP de origen
TCP	53	0.0.0.0/0
UDP	53	0.0.0.0/0

Reglas de salida

Tipo de protocolo	Número de puerto	IP de destino
TCP	Todos	0.0.0.0/0
UDP	Todos	0.0.0.0/0

Recomendaciones de reglas de grupos de seguridad de entrada y salida para el punto de conexión de salida de Resolver

Reglas de entrada

Tipo de protocolo	Número de puerto	IP de origen
TCP	Todos	0.0.0.0/0
UDP	Todos	0.0.0.0/0

Reglas de salida

Tipo de protocolo	Número de puerto	IP de destino
TCP	53	0.0.0.0/0
UDP	53	0.0.0.0/0

 Note

Requisitos de puerto del grupo de seguridad:

- Los puntos de conexión de entrada requieren reglas de entrada que permitan que el TCP y el UDP del puerto 53 reciban consultas de DNS de su red. Las reglas de salida pueden permitir todos los puertos, ya que es posible que el punto de conexión deba responder a las consultas de diferentes puertos de origen.
- Los puntos de conexión de salida requieren reglas de salida que permitan que el TCP y UDP accedan a los puertos que utiliza para las consultas de DNS en su red. En el ejemplo anterior se muestra el puerto 53 porque es el puerto DNS más común, pero es posible que su red utilice puertos diferentes. Las reglas de entrada pueden permitir que todos los puertos admitan las respuestas de sus servidores DNS.

Puntos de enlace de entrada de Resolver

Para los clientes que utilizan un punto de conexión de entrada de Resolver, la capacidad de la interfaz de red elástica se verá afectada si tiene más de 40 000 combinaciones únicas de direcciones IP y puertos que generan el tráfico DNS.

Alta disponibilidad para puntos de enlace de Resolver

Al crear los puntos finales de entrada de VPC Resolver, Route 53 requiere que cree al menos dos direcciones IP a las que los resolutores de DNS de su red reenviarán las consultas. También debe especificar las direcciones IP en dos zonas de disponibilidad como mínimo para la redundancia.

Si necesita más de un punto de conexión para la interfaz de red elástica para garantizar la disponibilidad en todo momento, le recomendamos que cree al menos una interfaz de red más de la que necesita para asegurarse de disponer de capacidad adicional para gestionar posibles sobretensiones de tráfico. La interfaz de red adicional también garantiza la disponibilidad durante las operaciones de servicio, como mantenimiento o actualizaciones.

Para obtener más información, consulte este artículo detallado del blog: [Cómo lograr una alta disponibilidad de DNS con los puntos finales](#) de Resolver y. [Valores que se especifican al crear o editar puntos de conexión de entrada](#)

Consulta exhaustiva de nombres de zona DNS

Los ataques de consulta exhaustiva de nombres de zona DNS intentan obtener todo el contenido de las zonas DNS firmadas por DNSSEC. Si el equipo de resolución de VPC detecta un patrón de tráfico que coincide con los que se generan cuando se recorren zonas de DNS en su punto final, el equipo de servicio reducirá el tráfico en su punto final. Como consecuencia, puede observar un alto porcentaje de las consulta de DNS que agotan su tiempo de espera.

Si observa una reducción de la capacidad en sus terminales y cree que se ha reducido el límite de carga por error, vaya a `home#` para `https://console.aws.amazon.com/support/` crear un caso de soporte.

Prácticas recomendadas de las comprobaciones de estado de Amazon Route 53

Una configuración eficaz de la comprobación de estado es esencial para mantener una infraestructura resistente y de alta disponibilidad. Estas son algunas prácticas recomendadas para tener en cuenta al configurar y administrar las comprobaciones de estado de Amazon Route 53:

1. Uso de direcciones IP elásticas para los puntos de conexión de comprobación de estado:
 - Utilice direcciones IP elásticas para los puntos de conexión de comprobación de estado a fin de garantizar una supervisión uniforme.
 - Si ya no utilizas una EC2 instancia de Amazon, recuerda eliminar todos los controles de estado asociados para evitar posibles riesgos de seguridad o comprometer los datos.

Para obtener más información, consulte [Valores que especifica al crear o actualizar comprobaciones de estado](#).

2. Configuración de los intervalos de comprobación de estado adecuados:
 - Establezca intervalos de comprobación de estado en función de los requisitos de la aplicación y de la importancia de los recursos supervisados.
 - Los intervalos más cortos permiten detectar las fallas con mayor rapidez, pero pueden aumentar los costos de Route 53 y aumentar la carga de recursos.
 - Los intervalos más largos reducen los costos y la carga de recursos, pero pueden retrasar la detección de fallas.

Para obtener más información, consulte [Configuración avanzada \(solo "Monitor an endpoint" \(Monitorización de un punto de conexión\)\)](#).

3. Implementación de notificaciones de alarma:

- Configura Amazon CloudWatchalarms para recibir notificaciones cuando los controles de estado fallen o se recuperen.
- Establezca los umbrales de alarma adecuados en función de los requisitos de la aplicación y del comportamiento esperado de los recursos.
- Integre las notificaciones en los procesos de supervisión y de respuesta a incidentes.

Para obtener más información, consulte [Monitorear comprobaciones de estado mediante CloudWatch](#).

4. Utilización de las regiones de comprobación de estado de forma estratégica:

- Elija las regiones de comprobación de estado en función de la distribución geográfica de los usuarios y recursos.
- Considere la posibilidad de utilizar varias regiones de comprobación de estado para los recursos esenciales a efectos de mejorar la fiabilidad y reducir el impacto de las interrupciones regionales.

5. Supervisión de las métricas y los registros de comprobación de estado:

- Revisa periódicamente los registros y las CloudWatch métricas de los chequeos de estado de Route 53 para identificar posibles problemas o cuellos de botella en el rendimiento
- Analice los motivos de los errores en la comprobación de estado y tome las medidas adecuadas para resolver los problemas subyacentes.

6. Implementación de estrategias de conmutación por error y conmutación por recuperación:

- Aproveche las políticas de enrutamiento de conmutación por error de Route 53 para enrutar de manera automática el tráfico a recursos en buen estado en caso de que se produzcan fallas.
- Planifique y pruebe los procesos de conmutación por error y conmutación por recuperación para garantizar una transición fluida durante las interrupciones y la recuperación.

Para obtener más información, consulte [Configuración de la recuperación ante errores a nivel de DNS](#).

7. Revisión y actualización periódica de las comprobaciones de estado:

- Actualice los puntos de conexión, los intervalos y los umbrales de alarma de las comprobaciones de estado según sea necesario para mantener una supervisión y un rendimiento óptimos.

Si sigue estas prácticas recomendadas, puede aprovechar eficazmente las comprobaciones de estado de Amazon Route 53 para supervisar el estado y la disponibilidad de nuestros recursos, lo que garantiza una infraestructura fiable y de alto rendimiento para las aplicaciones y los servicios.

Cuotas

Las solicitudes API y las entidades de Amazon Route 53 están sujetas a las siguientes cuotas (anteriormente denominadas “límites”).

Temas

- [Uso de Service Quotas para ver y administrar cuotas](#)
- [Cuotas de entidades](#)
- [Valores máximos de las solicitudes API](#)

Uso de Service Quotas para ver y administrar cuotas

Puede utilizar el servicio Service Quotas para ver las cuotas y solicitar aumentos de las cuotas de muchos servicios de AWS . Para obtener más información, consulte la [Guía del usuario de Service Quotas](#). (Actualmente, puede usar Service Quotas para ver y administrar los dominios y las cuotas de VPC Resolver de Route 53 y Route 53).

Note

Con el fin de ver las cuotas y solicitar cuotas superiores para Route 53, debe cambiar la región a EE. UU. Este (Norte de Virginia). Para ver las cuotas y solicitar cuotas más altas para VPC Resolver, cambie a la región correspondiente.

Cuotas de entidades

Las entidades de Amazon Route 53 están sujetas a las siguientes cuotas.

Para obtener información acerca de cómo obtener las cuotas actuales (anteriormente denominadas “límites”), consulte las siguientes acciones de Route 53:

- [GetAccountLimit](#)— Obtiene las cuotas de los controles de estado, las zonas alojadas, los conjuntos de delegación reutilizables, las políticas de flujo de tráfico y los registros de políticas de flujo de tráfico
- [GetHostedZoneLimit](#)— Obtiene las cuotas de registros de una zona alojada y de Amazon VPCs que puede asociar a una zona alojada privada

- [GetReusableDelegationSetLimit](#)— Obtiene la cuota del número de zonas alojadas que puede asociar a un conjunto de delegación reutilizable

Temas

- [Cuotas de dominios](#)
- [Cuotas en zonas alojadas](#)
- [Cuotas de registros](#)
- [Cuotas en el solucionador de VPC Route 53](#)
- [Cuotas de comprobaciones de estado](#)
- [Cuotas de configuraciones de registro de consulta](#)
- [Cuotas de políticas de flujo de tráfico y de registros de políticas](#)
- [Cuotas sobre conjuntos de delegación reutilizables](#)
- [Cuotas en perfiles de Route 53](#)

Cuotas de dominios

Entidad	Cuota
Dominios	20* por cuenta AWS Solicitar una ampliación de la cuota.

* El límite es de 20 para nuevos clientes a partir de marzo de 2021.

Si tiene una cuenta existente y el límite predeterminado ahora es 50, este se quedará en 50.

Cuotas en zonas alojadas

Entidad	Cuota
Zonas alojadas	Cuota inicial de 500 por AWS cuenta, pero puedes solicitar una cuota mayor según sea necesario.

Entidad	Cuota
	Solicitar una ampliación de la cuota.
Zonas hospedadas que pueden utilizar el mismo conjunto de delegación reutilizable	100 Solicitar una ampliación de la cuota.
Amazon VPCs que puedes asociar a una zona alojada privada por zona alojada	300 Si desea más de 300 asociaciones, le recomendamos que utilice los perfiles de Route 53. Para obtener más información, consulte ¿Qué son los perfiles de Amazon Route 53? .
Zonas hospedadas privadas que puede asociar a una VPC	Sin cuota *
Autorizaciones que puede crear para poder asociar las VPCs que creó una cuenta con una zona alojada creada por otra cuenta	1 000
Número de claves de firma de clave (KSK) que puede crear por zona alojada	2

* Puede asociar una VPC a cualquiera o a todas las zonas alojadas privadas que controla a través de sus AWS cuentas. Por ejemplo, supongamos que tiene tres AWS cuentas y las tres tienen la cuota predeterminada de 500 zonas alojadas. Si crea 500 zonas hospedadas privadas para las tres cuentas, puede asociar una VPC con las 1500 zonas hospedadas privadas.

Cuotas de registros

Entidad	Cuota
Registros	10 000 por zona alojada Solicitar una ampliación de la cuota. Para una cuota superior a 10 000 registros en una zona alojada se aplica un cargo adicional. Para obtener más información, consulte los precios de Amazon Route 53 .
Registros en un conjunto de registros	400 por conjunto de registros
Registros de geolocalización, latencia, respuesta multivalente, ponderada y basada en IP	100 registros que tengan el mismo nombre y tipo
Registros de geoproximidad	30 registros que tengan el mismo nombre y tipo
Colecciones CIDR	5 por Cuenta de AWS. Solicitar una ampliación de la cuota.
Bloques CIDR	1000 por colección CIDR. Solicitar una ampliación de la cuota.

Cuotas en el solucionador de VPC Route 53

Esta sección incluye todas las cuotas de VPC Resolver de Route 53

Cuotas en el solucionador de VPC Route 53

Utilice el siguiente procedimiento para aumentar las cuotas del Solucionador de VPC Route 53.

Aumento de las cuotas de Resolver

1. Abra la consola de Service Quotas en <https://console.aws.amazon.com/servicequotas/home/services/route53resolver/quotas>.
2. Vaya a la región en la que desea aumentar el límite.
3. Seleccione el nombre de la cuota de resolución de VPC de Route 53 que desee aumentar.
4. Seleccione Request quota increase (Solicitar aumento de cuota), ingrese el valor de cuota y, a continuación, seleccione Request (Solicitar).

Cuotas en los puntos finales de VPC Resolver de Route 53

Entidad	Cuota
Puntos finales por región AWS	4 por cuenta AWS Solicitar una ampliación de la cuota.
Direcciones IP por punto de conexión	6 Solicitar una ampliación de la cuota.
Direcciones IP por regla	6
Reglas por AWS región	1000 por AWS cuenta Solicitar una ampliación de la cuota.
Asociaciones entre reglas y VPCs por AWS región	2000 por AWS cuenta Solicitar una ampliación de la cuota.
Consultas UDP por segundo por dirección IP en un punto de conexión	10 000*

* Cada dirección IP de un punto de conexión puede procesar hasta 10 000 consultas de DNS UDP por segundo (QPS). El número de QPS de DNS varía según el tipo de consulta, el tamaño de la respuesta, el estado de los servidores de nombres de destino, los tiempos de respuesta de la consulta, la latencia de ida y vuelta y el protocolo en uso. Por ejemplo, las consultas a un servidor de nombres de destino que tarde en responder pueden reducir significativamente la capacidad de la interfaz de red. Además, para garantizar una alta disponibilidad, Route 53 Resolver genera consultas de salida redundantes para cada solicitud DNS que recibe. Como resultado, el QPS de cada interfaz de red saliente no coincidirá con el QPS enviado al Resolver de VPC de Route 53. Utilice CloudWatch métricas para medir el número de consultas que se envían a cada interfaz de red. Para obtener más información, consulte [Métricas de las direcciones IP de los solucionadores de VPC de Route 53](#). Si la velocidad máxima de consulta supera el 50 % de la capacidad de cualquier interfaz de red del punto de conexión, puede agregar más interfaces de red para aumentar su capacidad.

Las conexiones realizadas a través de aplicaciones como Network Load Balancer y AWS Lambda (para obtener una lista completa, consulte [Conexiones con seguimiento automático](#)) se rastrean automáticamente, incluso si la configuración del grupo de seguridad no requiere ningún otro seguimiento.

Si el seguimiento de la conexión se aplica mediante reglas de grupo de seguridad restrictivas o las consultas se enrutan a través de Equilibrador de carga de red, el número máximo total de consultas por segundo por dirección IP para un punto de conexión entrante puede ser tan bajo como 1500.

Cuotas en los registros de consultas de VPC Resolver de Route 53

Entidad	Cuota
Configuraciones de registro de consultas por región AWS	20 Solicitar una ampliación de la cuota.
Asociaciones de VPC de configuración del registro de consultas por región de AWS	100 * Solicitar una ampliación de la cuota.
Consulte las asociaciones de VPC de configuración del registro por cuenta	100

Entidad	Cuota
y AWS región (incluidas las configuraciones de consulta largas compartidas mediante la RAM) para la cuenta con la que se compartió la configuración.	Solicitar una ampliación de la cuota.

* Se trata de un límite regional que se aplica de forma acumulativa en todas las configuraciones de registro de consultas de VPC Resolver dentro de una sola región. La creación de configuraciones de registro de consultas adicionales en la misma región no proporciona capacidad adicional de asociación de VPC.

Cuotas en el firewall DNS de Resolver

Entidad	Cuota
Número de grupos de reglas asociados a una VPC para una sola cuenta por región de AWS	5
Número de dominios de DNS Firewall en un único archivo de Amazon S3 para una sola cuenta por AWS región	250.000 Solicitar una ampliación de la cuota.
Número de grupos de reglas de firewall de DNS para una sola cuenta por AWS región	1 000 Solicitar una ampliación de la cuota.
Número de reglas dentro de un grupo de reglas para una sola cuenta por AWS región	100 Solicitar una ampliación de la cuota.
Número de listas de dominios para una sola cuenta por AWS región	1 000

Entidad	Cuota
	Solicitar una ampliación de la cuota.
El número máximo de dominios que puede especificar en todas las listas de dominios para una cuenta única por región de AWS .	100 000 Solicitar una ampliación de la cuota.

Cuotas de Resolver on Outpost

Entidad	Cuota
Límite de instancias de Resolver on Outpost	6 (se requiere un mínimo de 4)

Tipos de instancias de Resolver en Outpost y número de consultas de DNS por segundo que puede admitir cada tipo de instancia:

Tipo de instancia	Consultas por segundo
c5.large	Hasta 7000
c5.xlarge	Hasta 12 000
c5.2xlarge	Hasta 24 000
c5.4xlarge	Hasta 56 000
c5d.large	Hasta 7000
c5d.xlarge	Hasta 12 000

Tipo de instancia	Consultas por segundo
c5d.2xlarge	Hasta 24 000
c5d.4xlarge	Hasta 56 000
m5.large	Hasta 7000
m5.xlarge	Hasta 12 000
m5.2xlarge	Hasta 24 000
m5.4xlarge	Hasta 56 000
m5d.large	Hasta 7000
m5d.xlarge	Hasta 12 000
m5d.2xlarge	Hasta 24 000
m5d.4xlarge	Hasta 56 000
r5.large	Hasta 7000
r5.xlarge	Hasta 12 000
r5.2xlarge	Hasta 24 000
r5.4xlarge	Hasta 56 000
r5d.large	Hasta 7000

Tipo de instancia	Consultas por segundo
r5d.xlarge	Hasta 12 000
r5d.2xlarge	Hasta 24 000
r5d.4xlarge	Hasta 56 000

Tipos de instancias de punto de conexión de Resolver en Outpost y número de consultas de DNS por segundo que puede admitir cada tipo de instancia:

Tipo de instancia	Consultas por segundo
c5.large	Hasta 5000
c5.xlarge	Hasta 10 000
c5.2xlarge	Hasta 18 000
c5.4xlarge	Hasta 30 000
c5d.large	Hasta 5000
c5d.xlarge	Hasta 10 000
c5d.2xlarge	Hasta 18 000
c5d.4xlarge	Hasta 30 000
m5.large	Hasta 5000
m5.xlarge	Hasta 10 000

Tipo de instancia	Consultas por segundo
m5.2xlarge	Hasta 18 000
m5.4xlarge	Hasta 30 000
m5d.large	Hasta 5000
m5d.xlarge	Hasta 10 000
m5d.2xlarge	Hasta 18 000
m5d.4xlarge	Hasta 30 000
r5.large	Hasta 5000
r5.xlarge	Hasta 10 000
r5.2xlarge	Hasta 18 000
r5.4xlarge	Hasta 30 000
r5d.large	Hasta 5000
r5d.xlarge	Hasta 10 000
r5d.2xlarge	Hasta 18 000
r5d.4xlarge	Hasta 30 000

Cuotas de comprobaciones de estado

Entidad	Cuota
Comprobaciones de estado	200 controles de estado activos por AWS cuenta Solicitar una ampliación de la cuota.
Comprobaciones de estado secundarias que puede monitorear una comprobación de estado calculada	255
Longitud total máxima de los encabezados de la respuesta a una solicitud de comprobación de estado	16 384 bytes (16 K)

Cuotas de configuraciones de registro de consulta

Entidad	Cuota
Consultar configuraciones de log	1 por zona alojada

Cuotas de políticas de flujo de tráfico y de registros de políticas

Entidad	Cuota
Políticas de tráfico	50 por AWS cuenta
Para obtener más información acerca del flujo de tráfico de Route 53,	Solicitar una ampliación de la cuota.

Entidad	Cuota
consulte Uso de flujo de tráfico para dirigir el tráfico DNS .	
Versiones de la política de tráfico	1000 por política de tráfico
Registros de políticas de tráfico (denominados «instancias de políticas» en la API de Route 53 AWS SDKs AWS Command Line Interface, y AWS Tools for Windows PowerShell)	5 por AWS cuenta Solicitar una ampliación de la cuota.

Cuotas sobre conjuntos de delegación reutilizables

Entidad	Cuota
Conjuntos de delegación reutilizables	100 por AWS cuenta Solicitar una ampliación de la cuota.

Cuotas en perfiles de Route 53

Entidad	Cuota
Número de perfiles de Route 53 por Cuenta de AWS región	5 Solicitar una ampliación de la cuota.
Número de VPCs ellos que se puede asociar a un perfil	1 000 Solicitar una ampliación de la cuota.

Entidad	Cuota
Número de grupos de reglas de DNS Firewall por perfil	5
Número de reglas de solucionador por perfil	1 000 Solicitar una ampliación de la cuota.
Número de zonas alojadas privadas por perfil	1 000 Solicitar una ampliación de la cuota.
Número de configuraciones de registro de consultas de VPC Resolver por perfil	2

Valores máximos de las solicitudes API

Las solicitudes de la API de Amazon Route 53 están sujetas a los siguientes valores máximos.

Temas

- [Número de elementos y caracteres en las solicitudes ChangeResourceRecordSets](#)
- [Frecuencia de las solicitudes de la API de Amazon Route 53](#)
- [Frecuencia de las solicitudes de la API de resolución de VPC de Route 53](#)

Número de elementos y caracteres en las solicitudes ChangeResourceRecordSets

Elementos ResourceRecord

Una solicitud no puede contener más de 1 000 elementos ResourceRecord (incluidos los registros de alias). Cuando el valor del elemento Action es UPSERT, cada elemento ResourceRecord se cuenta dos veces.

Número máximo de caracteres

La suma de la cantidad de caracteres (incluidos los espacios) en todos los elementos `Value` de una solicitud no puede superar los 32 000 caracteres. Cuando el valor del elemento `Action` es `UPSERT`, cada carácter `Value` se cuenta dos veces.

Frecuencia de las solicitudes de la API de Amazon Route 53

Todas las solicitudes de la API de Amazon Route 53

Para [Amazon Route 53](#), APIs cinco solicitudes por segundo por AWS cuenta. Si envía más de cinco solicitudes por segundo, Amazon Route 53 devuelve un error HTTP 400 (`Bad request`). El encabezado de respuesta incluye también un elemento `Code` con un valor de `Throttling` y un elemento `Message` con un valor de `Rate exceeded`.

Note

Si la aplicación supera este límite, recomendamos que implemente el retardo exponencial para los reintentos. Para obtener más información, consulte [Reintentos de error y retroceso exponencial en AWS](#) en la Referencia general de Amazon Web Services.

Solicitudes **ChangeResourceRecordSets**

Si Route 53 no puede procesar una solicitud antes de que llegue la siguiente, rechazará las siguientes solicitudes de la misma zona alojada y devolverá un error HTTP 400 (`Bad request`). El encabezado de respuesta incluye también un elemento `Code` con un valor de `PriorRequestNotComplete` y un elemento `Message` con un valor de `The request was rejected because Route 53 was still processing a prior request`.

Solicitudes **CreateHealthCheck**

Puede enviar una `CreateHealthCheck` solicitud cada 2 segundos cada una Cuenta de AWS.

Frecuencia de las solicitudes de la API de resolución de VPC de Route 53

Todas las solicitudes

Cinco solicitudes por segundo por AWS cuenta y región. Si envías más de cinco solicitudes por segundo en una región, VPC Resolver devuelve un error HTTP 400 (Bad request). El encabezado de respuesta incluye también un elemento Code con un valor de `Throttling` y un elemento Message con un valor de `Rate exceeded`.

Note

Si la aplicación supera este límite, recomendamos que implemente el retardo exponencial para los reintentos. Para obtener más información, consulte [Reintentos de error y retroceso exponencial en AWS](#) en la Referencia general de Amazon Web Services.

Información relacionada

Los recursos relacionados siguientes pueden serle de ayuda cuando trabaje con este servicio.

Temas

- [AWSRecursos de](#)
- [Herramientas y bibliotecas de terceros](#)
- [Interfaces gráficas de usuario](#)

AWSRecursos de

Varias guías útiles, foros y otros recursos están disponibles en Amazon Web Services.

- [Referencia de la API de Amazon Route 53](#): una guía de referencia que incluye la ubicación de esquema, descripciones completas de las acciones, parámetros y tipos de datos de la API, así como una lista de errores que el servicio devuelve.
- [Tipo AWS::Route53::RecordSet](#) en la AWS CloudFormationGuía del usuario de: una propiedad para usar Amazon Route 53 con CloudFormation a fin de crear nombres DNS personalizados para las pilas de CloudFormation.
- [Foros de discusión](#): un foro de la comunidad en el que los desarrolladores pueden debatir aspectos técnicos relacionados con Route 53.
- [Centro de asistencia de AWS](#): este sitio reúne información sobre casos de soporte recientes y resultados de AWS Trusted Advisor, y comprobaciones de estado. Además, proporciona enlaces a foros de discusión, preguntas técnicas frecuentes, panel de estado del servicio e información sobre los planes de soporte de AWS.
- [Información sobre AWS Premium Support](#): página web principal con información sobre AWS Premium Support, un canal de soporte individualizado y de respuesta rápida que lo ayudará a crear y ejecutar aplicaciones en los servicios de infraestructura de AWS.
- [Contacte con nosotros](#): enlaces para hacernos llegar sus preguntas sobre facturación o su cuenta. Para preguntas técnicas, utilice los foros de debate o los enlaces de soporte previamente proporcionados.
- [Información de producto de Route 53](#): página web principal para obtener información sobre Route 53, incluidos precios, características, etc.

- [Clases y talleres](#): enlaces a cursos basados en roles y especializados, además de laboratorios autoguiados para ayudarlo a desarrollar sus conocimientos sobre AWS y obtener experiencia práctica.
- [Centro para desarrolladores de AWS](#): explore los tutoriales, descargue herramientas y obtenga información sobre los eventos para desarrolladores de AWS.
- [Herramientas para desarrolladores de AWS](#): enlaces a herramientas para desarrolladores, SDK, conjuntos de herramientas de IDE y herramientas de línea de comandos para desarrollar y administrar aplicaciones de AWS.
- [Centro de recursos de introducción](#): aprenda a configurar su Cuenta de AWS, únase a la comunidad de AWS y lance su primera aplicación.
- [Tutoriales prácticos](#): comience con tutoriales paso a paso antes de lanzar su primera aplicación en AWS.
- [Documentos técnicos de AWS](#): enlaces a una lista completa de documentos técnicos de AWS que tratan una gran variedad de temas técnicos, como arquitecturas, seguridad y economía de la nube, escritos por arquitectos de soluciones de AWS o expertos técnicos.
- [Centro de AWS Support](#): el punto para crear y administrar los casos de AWS Support. También incluye enlaces a otros recursos útiles como foros, preguntas técnicas frecuentes, estado de los servicios y de AWS Trusted Advisor.
- [Soporte](#): la página web principal para obtener información acerca de Soporte, un canal de soporte individualizado y de respuesta rápida que le ayudará a crear y ejecutar aplicaciones en la nube.
- [Contacta con nosotros](#) – Un punto central de contacto para las consultas relacionadas con la facturación AWS, cuentas, eventos, abuso y demás problemas.
- [AWS Términos del sitio de](#) : información detallada sobre nuestros derechos de autor y marca comercial, su cuenta, licencia y acceso al sitio, entre otros temas.

Herramientas y bibliotecas de terceros

Además de los recursos de AWS, puede encontrar varias herramientas y bibliotecas de terceros que funcionan con Amazon Route 53.

- [AmazonRoute53AppsScript](#) (a través de webos-goodies)

Administración de hojas de cálculo de Google de Amazon Route 53.

- [Componentes de AWS para .NET](#) (a través de SprightlySoft)

Componente SprightlySoft .NET para Amazon Web Services con soporte para operaciones REST y Route 53.

- [Descarga de la API Boto](#) (a través de github)

Interfaz Python de Boto a Amazon Web Services.

- [cli53](#) (a través de github)

Interfaz de la línea de comandos de Route 53.

- [API Dasein Cloud](#)

API basada en Java.

- [R53.py](#) (a través de github)

Mantiene una versión canónica de configuraciones de DNS en control de código fuente y calcula el conjunto mínimo de cambios que son necesarios para cambiar una configuración.

- [route53d](#)

Front-end de DNS para la API de Route 53 (habilita la transferencia de zona progresiva (IXFR)).

- [Route53Manager](#) (a través de github)

Interfaz basada en web.

- [Ruby Fog](#) (a través de github)

Biblioteca de servicios en la nube en Ruby.

- [WebService::Amazon::Route53](#) (a través de CPAN)

Interfaz de Perl a la API de Amazon Route 53.

Interfaces gráficas de usuario

Las siguientes herramientas de terceros proporcionan interfaces gráficas de usuario (GUI) para trabajar con Amazon Route 53:

- [R53 Fox](#)
- [Ylastic](#)

Historial de documentos

En las siguientes entradas se describen los cambios importantes en cada versión de la documentación de Route 53. Para recibir notificaciones sobre los cambios en esta documentación, puede suscribirse a una fuente RSS.

Temas

- [Versiones de 2025](#)
- [Lanzamientos de 2024](#)
- [Lanzamientos de 2023](#)
- [Versiones de 2022](#)
- [Versiones de 2021](#)
- [Versiones de 2020](#)
- [Versiones de 2018](#)
- [Versiones de 2017](#)
- [Versiones de 2016](#)
- [Versiones de 2015](#)
- [Versiones de 2014](#)
- [Versiones de 2013](#)
- [Versión de 2012](#)
- [Versiones de 2011](#)
- [Versión de 2010](#)

Versiones de 2025

15 de diciembre de 2025

Se agregaron CloudWatch métricas detalladas para los puntos finales de Route 53 Resolver. Las nuevas métricas proporcionan capacidades de supervisión mejoradas a nivel de la interfaz de red del Resolver y del servidor de nombres de destino, incluida la latencia de respuesta del P90 en las consultas de DNS, el seguimiento de los estados de respuesta de SERVFAIL, NXDOMAIN, REFUSED y FORMERR, y la supervisión de la disponibilidad de los servidores de nombres de

destino para los puntos finales de Resolver salientes. Para obtener más información, consulte [CloudWatch Métricas detalladas del solucionador de VPC Route 53](#).

26 de junio de 2025

Se agregó ResolverEndpointCapacityStatus al espacio de nombres AWS/Route53Resolver. Para obtener más información, consulte [Métricas de los puntos finales de VPC Resolver Route 53](#).

25 de junio de 2025

Amazon Route 53 ahora admite registros de alias para los puntos de conexión del dominio del servicio de VPC Lattice. Para obtener más información, consulte [Enrutamiento del tráfico al punto de conexión del dominio del servicio de Amazon VPC Lattice](#).

24 de junio de 2025

Ahora puede usar la delegación entrante y saliente con VPC Resolver. Para obtener más información, consulte [Cómo los solucionadores de DNS de su red reenvían las consultas de DNS a los puntos finales del Resolver](#).

1 de junio de 2025

Se agregaron permisos para `cloudwatch:GetMetricData`, `tag:GetResources`, `es:ListDomainNames`, `es:DescribeDomains`, `cloudfront:GetDistributionTenantByDomain`, `cloudfront:GetConnectionGroup` y `lightsail:GetContainerServices`. Estos permisos le permiten obtener hasta 500 métricas de chequeos de CloudWatch estado, hasta 100 nombres de chequeos de estado, obtener la configuración de dominio para los dominios de Amazon OpenSearch Service especificados y enumerar los nombres de todos los dominios de Amazon OpenSearch Service propiedad del usuario actual en la región activa, obtener las distribuciones CloudFront multiusuario y obtener los servicios de contenedores de Lightsail. Para obtener más información, consulte [AWS política gestionada: AmazonRoute 53 FullAccess](#).

28 de abril de 2025

Ahora puede asociar los puntos de conexión de VPC de la interfaz a los perfiles de Route 53. Para obtener más información, consulte [Asociación de puntos de conexión de VPC de interfaz a un perfil de Route 53](#).

28 de abril de 2025

Ahora puede añadir un registro de alias a un arrendatario de distribución. CloudFront Para obtener más información, consulte [Enrutar el tráfico a una CloudFront distribución de Amazon mediante tu nombre de dominio](#).

27 de febrero de 2025

Se actualizó la guía de Route 53 con la nueva experiencia de consola con Flujo de tráfico. Para obtener más información, consulte [Crear y administrar políticas de tráfico](#) y [Creación y administración de registros de política](#).

14 de enero de 2025

Amazon Route 53 ahora admite registros de alias para los puntos de enlace de dominio personalizados del OpenSearch Servicio. Para obtener más información, consulte [Enrutamiento del tráfico al punto final OpenSearch del dominio de Amazon Service](#).

13 de enero de 2025

Se agregaron los resultados del Resolver DNS Firewall al Security Hub CSPM. Para obtener más información, consulte [Envío de resultados desde Resolver DNS Firewall a Security Hub \(CSPM\)](#).

Lanzamientos de 2024

15 de noviembre de 2024

Se agregó Resolver DNS Firewall Advanced, un nuevo conjunto de funciones de Resolver DNS Firewall que le permite identificar y bloquear el tráfico de DNS asociado a amenazas de DNS avanzadas, como la tunelización de DNS, el algoritmo de generación de dominios (DGA) y las amenazas basadas en el DGA de diccionario. Para obtener más información, consulte [Resolver DNS Firewall Advanced](#).

29 de octubre de 2024

Se agregó compatibilidad con los registros DNS de tipo HTTPS, SSHFP, SVCB y TLSA. Para obtener más información, consulte [Tipos de registros de DNS admitidos](#).

3 de octubre de 2024

Se ha agregado compatibilidad con la indicación del nombre de servicio (SNI) en los puntos de conexión de salida de Resolver para DoH. Para obtener más información, consulte [Valores que se especifican al crear o editar reglas](#).

3 de septiembre de 2024

Ahora puede utilizar una condición `route53:VPCs` política para conceder un acceso detallado a la gestión de las asociaciones de zonas alojadas a. VPCs Para obtener más información, consulte [Uso de condiciones de las políticas de IAM para control de acceso preciso](#).

27 de agosto de 2024

`AmazonRoute53ProfilesFullAccess` agregó permisos para `GetProfilePolicy` y `PutProfilePolicy`. Estas son acciones de IAM solo de permiso. Si a un director de IAM no se le conceden estos permisos, se producirá un error al intentar compartir el perfil mediante el servicio. AWS RAM Para obtener más información, consulte [AWS política administrada: 53 AmazonRoute ProfilesFullAccess](#).

27 de agosto de 2024

`AmazonRoute53ProfilesReadOnlyAccess` agregó el permiso para `GetProfilePolicy`. Esta es una acción de IAM que solo requiere permisos. Si a una entidad principal de IAM no se le ha concedido este permiso, se producirá un error al intentar acceder a la política del perfil mediante el AWS RAM servicio. Para obtener más información, consulte [AWS política gestionada: 53 AmazonRoute ProfilesReadOnlyAccess](#).

5 de agosto de 2024

Se ha agregado un ID de instrucción (Sid) para identificar de forma exclusiva la política `AmazonRoute53ResolverFullAccess` administrada. Para obtener más información, consulte [AWS política gestionada: AmazonRoute 53 ResolverFullAccess](#).

5 de agosto de 2024

Se ha agregado un ID de instrucción (Sid) para identificar de forma exclusiva la política `AmazonRoute53ResolverReadOnlyAccess` administrada. Para obtener más información, consulte [AWS política gestionada: AmazonRoute 53 ResolverReadOnlyAccess](#).

18 de julio de 2024

Se ha actualizado la guía de Route 53 completa con la experiencia de la nueva consola para comprobaciones de estado. Para obtener más información, consulte [Creación, actualización y eliminación de comprobaciones de estado](#).

30 de abril de 2024

Ahora puede decidir si una regla de DNS Firewall inspeccionará (opción predeterminada) o confiará en la cadena de redireccionamiento de DNS. Para obtener más información, consulte

[Componentes y ajustes del firewall DNS de Resolver](#) y [Configuración de las reglas en DNS Firewall](#).

22 de abril de 2024

Ahora puede usar los perfiles de Route 53 para compartir configuraciones específicas de DNS con muchos usuarios VPCs y con AWS cuentas. Para obtener más información, consulte [¿Qué son los perfiles de Amazon Route 53?](#).

22 de abril de 2024

Se han agregado las políticas administradas `AmazonRoute53ProfilesReadOnlyAccess` y `AmazonRoute53ProfilesFullAccess` para conceder acceso completo y de solo lectura a los perfiles de Amazon Route 53. Para obtener más información, consulte [AWS políticas gestionadas para Amazon Route 53](#).

5 de febrero de 2024

Ahora puedes usar Amazon EventBridge para recibir alertas en tiempo real con DNS Firewall. Para obtener más información, consulte [Administrar los eventos de Resolver DNS Firewall mediante Amazon EventBridge](#).

9 de enero de 2024

Ahora puede usar el tipo de consulta de DNS como un valor opcional para la regla de DNS Firewall a fin de diferenciar la respuesta de la regla para un tipo de consulta de DNS específico. Para obtener más información, consulte [Componentes y ajustes del firewall DNS de Resolver](#) y [Configuración de las reglas en DNS Firewall](#).

9 de enero de 2024

Ahora puede usar el registro de creación rápida o el asistente de creación de registros para crear registros de enrutamiento de geoproximidad. Para obtener más información, consulte [Enrutamiento por geoproximidad](#), [Valores específicos de registros de geoproximidad](#) y [Valores específicos de registros de alias de geoproximidad](#).

Lanzamientos de 2023

20 de diciembre de 2023

Ahora puedes usar DNS a través de HTTPS con los puntos finales de Resolver. Para obtener más información, consulte [Elección de protocolos para los puntos de conexión](#).

20 de julio de 2023

Amazon Route 53 en Outposts ya está disponible en AWS Outposts estanterías. Incluye un solucionador de VPC que almacena en caché todas las consultas de DNS que se originan en. AWS Outposts También puede configurar la conectividad híbrida entre un Outpost y un Resolver de DNS en las instalaciones mediante la implementación de puntos de conexión entrantes y salientes. Para obtener más información, consulte [¿Qué es Amazon Route 53 on Outposts?](#).

19 de julio de 2023

Ahora puede usar zonas locales con enrutamiento de geoproximidad (solo flujo de tráfico) después de habilitarlas. Para obtener más información, consulte [Enrutamiento por geoproximidad](#) y [Formato de documento de política de tráfico](#).

22 de marzo de 2023

Se actualizó toda la guía de Route 53 con la nueva experiencia de consola para dominios. También puede utilizar la nueva experiencia de consola para transferir un dominio de uno Cuenta de AWS a otro. Cuenta de AWS Para obtener más información, consulte [Registrar un nuevo dominio](#) y [Transferencia de dominios](#).

10 de marzo de 2023

Ahora puede conectarse a sus recursos mediante IPv4 puntos de conexión de doble pila o con Route 53 VPC Resolver. IPv6 Para obtener más información, consulte [Valores que se especifican al crear o editar puntos de conexión de entrada](#) y [Valores que se especifican al crear o editar puntos de conexión de salida](#).

Versiones de 2022

21 de septiembre de 2022

Ahora puede utilizar las condiciones de la política para dar a los usuarios un acceso detallado a la actualización de los conjuntos de registros de recursos en Amazon Route 53. Para obtener más información, consulte [Uso de condiciones de las políticas de IAM para control de acceso preciso](#).

30 de agosto de 2022

Amazon Route 53 ahora admite registros de alias para AWS App Runner los servicios que se creen después del 1 de agosto de 2022. Para obtener más información, consulte [Enrutar el tráfico a un AWS App Runner servicio](#).

1 de junio de 2022

La opción de enrutamiento basada en IP ya está disponible en Amazon Route 53. Para obtener más información, consulte [Direccionamiento basado en IP](#).

16 de marzo de 2022

Las opciones de geolocalización y de enrutamiento basado en la latencia ahora son compatibles con las zonas alojadas privadas en Amazon Route 53. Para obtener más información, consulte [Consideraciones sobre el uso de una zona alojada privada](#).

25 de enero de 2022

El proceso de cambio de propiedad de .com.au y .net.au se TLDs ha simplificado para incluir la respuesta a dos correos electrónicos (tanto de los registrantes antiguos como de los nuevos) y no incluye la cumplimentación de formularios. Para obtener más información, consulte [.com.au \(Australia\)](#) y [.net.au \(Australia\)](#).

Versiones de 2021

26 de octubre de 2021

Se ha agregado compatibilidad para desactivar reglas DNS inversas predeterminadas con Amazon Route 53. Ahora puede desactivar la creación de estas reglas y en su lugar, reenviar consultas de espacios de nombres DNS inversos a servidores externos si lo desee. Para obtener más información, consulte [Reglas de reenvío para consultas de DNS inversas en VPC Resolver](#).

1 de septiembre de 2021

Se ha añadido un nuevo tema de introducción que te explica cómo crear CloudFront distribuciones de Amazon para un sitio web estático. Para obtener más información, consulte [Usa una CloudFront distribución de Amazon para ofrecer un sitio web estático](#).

14 de julio de 2021

Se ha empezado a rastrear las políticas AWS gestionadas de Amazon Route 53. Para obtener más información, consulte [AWS políticas gestionadas para Amazon Route 53](#).

31 de marzo de 2021

Se agregó el firewall Resolver DNS. Con el firewall de DNS, puede proteger las solicitudes de DNS salientes de su VPCs. Para obtener más información, consulte [Uso de DNS Firewall para filtrar el tráfico de DNS saliente](#).

Versiones de 2020

17 de diciembre de 2020

Se agregó compatibilidad con la firma de DNSSEC para Route 53 VPC Resolver. Para obtener más información, consulte [Configuración de la firma de DNSSEC en Amazon Route 53](#).

Se agregó soporte para la validación de DNSSEC para Route 53 VPC Resolver. Para obtener más información, consulte [Activar la validación de DNSSEC en Amazon Route 53](#).

23 de septiembre de 2020

Se actualizó toda la guía de Route 53 con la nueva experiencia de consola. Para obtener más información, consulte [¿Qué es Amazon Route 53?](#).

1 de septiembre de 2020

Se agregó soporte para los registros de consulta de Resolver. Para obtener más información, consulte [Registro de consultas de Resolver](#).

Versiones de 2018

20 de diciembre de 2018

Puede crear registros de alias de Route 53 que dirijan el tráfico a API Gateway APIs o a los puntos finales de la interfaz de Amazon VPC. Para obtener más información, consulte [Valor/ruta de destino del tráfico](#).

28 de noviembre de 2018

La asignación automática de nombres de Route 53 (también conocida como Service Discovery) es ahora un servicio independiente. AWS Cloud Map Para obtener más información, consulte la [Guía para desarrolladores de AWS Cloud Map](#).

19 de noviembre de 2018

Puede usar Route 53 Resolver para configurar la resolución de DNS entre la VPC y la red a través de una conexión de VPN o Direct Connect. (Resolver es el nuevo nombre del servicio de DNS recursivo que se proporciona a todos los clientes de forma predeterminada en Amazon Virtual Private Cloud (Amazon VPC)). De este modo puede reenviar consultas de DNS de los solucionadores de su red al solucionador Route 53 Resolver. Resolver también le permite

reenviar consultas de nombres de dominio seleccionados (example.com) y nombres de subdominio (api.example.com) desde una VPC a los solucionadores de su red. Para obtener más información, consulte [¿Qué es el solucionador de VPC Route 53?](#).

7 de noviembre de 2018

Al usar el flujo de tráfico de Route 53 y el direccionamiento de geoproximidad, puede utilizar un mapa interactivo para visualizar cómo se direccionará a los usuarios finales a sus puntos de conexión en todo el mundo. Para obtener más información, consulte [Visualización de un mapa que muestra el efecto de la configuración de geoproximidad](#).

18 de octubre de 2018

Puede utilizar la consola y la API de Route 53 para desactivar temporalmente una comprobación de estado de Route 53. De este modo obtiene una forma sencilla de pausar la monitorización de un punto de conexión, como un servidor web, para que pueda realizar el mantenimiento del mismo sin desencadenar alarmas o generar registros o mensajes de estado innecesarios. Para obtener más información, consulte “Desactivado” en [Valores que especifica al crear o actualizar comprobaciones de estado](#). La función está disponible para los tres tipos de controles de estado de Route 53: controles de estado que monitorean un punto final, controles de estado que monitorean otros controles de estado y controles de estado que monitorean una CloudWatch alarma.

13 de marzo de 2018

Si utiliza la asignación de nombres automática, ahora puede usar un comprobador de estado de terceros para evaluar el estado de los recursos. Esto resulta útil cuando un recurso no está disponible en Internet debido, por ejemplo, a que la instancia está en una VPC de Amazon. Para obtener más información, consulte [HealthCheckCustomConfig](#) la referencia de la API de Amazon Route 53.

9 de marzo de 2018

IAM incluye ahora políticas administradas para la asignación de nombres automática. Para obtener más información, consulte [AWS políticas gestionadas para Amazon Route 53](#).

6 de febrero de 2018

Ahora puede configurar la asignación de nombres automática para crear registros de alias que redirijan el tráfico a equilibradores de carga de ELB o para crear registros CNAME. Para obtener más información, consulte [Atributos](#) en la documentación de la [RegisterInstance](#) API en la referencia de API de Amazon Route 53.

Versiones de 2017

5 de diciembre de 2017

Ahora puede utilizar la API de nomenclatura automática de Route 53 para aprovisionar instancias para microservicios. La nomenclatura automática le permite crear registros de DNS automáticamente y, de forma opcional, comprobaciones de estado basadas en una plantilla que defina. Para obtener más información, consulta [¿Qué es AWS Cloud Map?](#) en la Guía para AWS Cloud Map desarrolladores.

16 de noviembre de 2017

Ahora puede obtener mediante programación tanto las cuotas actuales para los recursos de Route 53 como zonas alojadas y comprobaciones de estado, como el número de cada recurso que se está utilizando actualmente. Para obtener más información, consulte [GetAccountLimit](#), [GetHostedZoneLimit](#), y [GetReusableDelegationSetLimit](#) en la referencia de la API de Amazon Route 53.

3 de octubre de 2017

Route 53 ahora es un servicio compatible con HIPAA. Para obtener más información, consulte [Validación de la conformidad en Amazon Route 53](#).

29 de septiembre de 2017

Ahora puede comprobar mediante programación si un dominio puede transferirse a Route 53. Para obtener más información, consulte [CheckDomainTransferability](#) la referencia de la API de Amazon Route 53.

11 de septiembre de 2017

Ahora puede crear registros de alias de Route 53 que enruten el tráfico de Internet a los balanceadores de carga de red ELB. Para obtener más información acerca de los registros de alias, consulte [Elección entre registros de alias y sin alias](#).

7 de septiembre de 2017

Si utiliza Route 53 como servicio DNS público autorizado, ahora puede registrar las consultas de DNS que recibe Route 53. Para obtener más información, consulte [Registro de consultas de DNS públicas](#).

1 de septiembre de 2017

Si utiliza el flujo de tráfico de Route 53, ahora puede utilizar el direccionamiento de geoproximidad, que le permite dirigir el tráfico en función de la distancia física entre los usuarios y los recursos. También puede dirigir más o menos tráfico a cada recurso especificando un sesgo positivo o negativo. Para obtener más información, consulte [Enrutamiento por geoproximidad](#).

21 de agosto de 2017

Ahora puede utilizar Route 53 para crear registros de autorización de la entidad de certificación (CAA), que le permiten especificar las entidades de certificación que pueden emitir certificados para sus dominios y subdominios. Para obtener más información, consulte [Tipo de registro de CAA](#).

18 de agosto de 2017

Ahora puede transferir un gran número de dominios a Route 53 mediante la consola de Route 53. Para obtener más información, consulte [Transferencia del registro de un dominio a Amazon Route 53](#).

4 de agosto de 2017

Cuando registras un dominio, los registros de algunos dominios de nivel superior (TLDs) requieren que compruebes que has especificado una dirección de correo electrónico válida para el contacto del registrante. Ahora puede enviar el correo electrónico de verificación y obtener la confirmación de que ha verificado correctamente la dirección de correo electrónico durante el proceso de registro del dominio. Para obtener más información, consulte [Registrar un nuevo dominio](#).

21 de junio de 2017

Si desea dirigir el tráfico de forma aproximativa aleatoriamente a varios recursos, como servidores web, ahora puede crear un registro de respuesta con varios valores para cada recurso y, de manera opcional, asociar una comprobación de estado de Route 53 a cada registro. Route 53 responde a las consultas de DNS con hasta ocho registros en buen estado en respuesta a cada consulta de DNS, y da diferentes respuestas a distintos solucionadores de DNS. Para obtener más información, consulte [Direccionamiento de respuesta con varios valores](#).

10 de abril de 2017

Al utilizar la consola de Route 53 para transferir un registro de dominio a Route 53, ahora puede elegir una de las siguientes opciones para asociar los servidores de nombres al servicio DNS del dominio con el registro de dominio transferido:

- Usar los servidores de nombres de una zona alojada de Route 53 que elija
- Usar los servidores de nombres para el servicio DNS actual del dominio
- Usar servidores de nombres que especifique

Route 53 asocia automáticamente estos servidores de nombres con el registro de dominio transferido.

Versiones de 2016

21 de noviembre de 2016

Ahora puede crear comprobaciones de estado que utilicen IPv6 direcciones para comprobar el estado de los puntos finales. Para obtener más información, consulte [Creación y actualización de comprobaciones de estado](#).

15 de noviembre de 2016

Ahora puede utilizar una acción de la API de Route 53 para asociar una Amazon VPC que ha creado con una cuenta con una zona alojada privada que creó con otra cuenta. Para obtener más información, consulte [Asociar una Amazon VPC y una zona alojada privada que haya creado con cuentas diferentes AWS](#).

30 de agosto de 2016

En esta versión, Route 53 agrega las siguientes características nuevas:

- Registros NAPTR (Name Authority Pointer, señalizador de autoridad de asignación de nombres): ahora puede crear registros NAPTR, que usan las aplicaciones DDDS (Dynamic Delegation Discovery System, sistema de detección de delegación dinámica) para convertir un valor en otro o para sustituir un valor por otro. Por ejemplo, un uso común es convertir números de teléfono en SIP URIs. Para obtener más información, consulte [Tipo de registro NAPTR](#).
- Herramienta de comprobación de consultas de DNS: ahora puede simular las consultas de DNS para un registro y consultar el valor que devuelve Route 53. Para los registros de geolocalización y latencia, también puede simular las solicitudes de una dirección IP concreta de un and/or cliente de resolución de DNS para averiguar qué respuesta devolvería Route 53 a un cliente con esa and/or dirección IP de resolución. Para obtener más información, consulte [Comprobación de las respuestas de DNS de Route 53](#).

11 de agosto de 2016

Con esta versión, puede crear registros de alias que dirijan el tráfico a los equilibradores de carga de aplicaciones de ELB. El proceso es el mismo que para el de Classic Load Balancer. Para obtener más información, consulte [Valor/ruta de destino del tráfico](#).

9 de agosto de 2016

En esta versión, Route 53 agrega compatibilidad con DNSSEC para el registro de dominio. DNSSEC le permite proteger su dominio de los ataques de suplantación de DNS, también conocidos como ataques. man-in-the-middle Para obtener más información, consulte [Configurar DNSSEC para un dominio](#).

7 de julio de 2016

Ahora puede ampliar manualmente el registro de un dominio y registrar un dominio con un período de registro inicial superior al periodo de registro mínimo especificado por el registro. Para obtener más información, consulte [Ampliación del periodo de registro de un dominio](#).

6 de julio de 2016

Si es un cliente de AISPL con una dirección de contacto en India, ahora puede utilizar Route 53 para registrar dominios. Para obtener más información, consulte la sección [Administración de una cuenta en la India](#).

26 de mayo de 2016

En esta versión, Route 53 agrega las siguientes características nuevas:

- Informe de facturación de dominios: ahora puede descargar un informe que enumera todos los cargos de registro de dominio, por dominio, durante un período de tiempo especificado. El informe incluye todas las operaciones de registro de dominios por las que hay que pagar, como el registro de dominios, la transferencia de dominios a Route 53, la renovación del registro de dominios y (en algunos casos TLDs) el cambio de propietario de un dominio. Para obtener más información, consulte la siguiente documentación sobre :
 - Consola de Route 53: consulte [Descargar un informe de facturación de dominios](#)
 - API de Route 53: consulte [ViewBilling](#) la referencia de la API de Amazon Route 53.
- Nuevo TLDs: ahora puede registrar dominios que tengan lo siguiente
TLDs: .college, .consulting, .host, .name, .online, .republican, .rocks, .sucks, .trade, .website y .uk. Para obtener más información, consulte [Dominios que puede registrar con Amazon Route 53](#).

- Nuevos APIs para el registro de dominios: para las operaciones que requieren la confirmación de que la dirección de correo electrónico del contacto del registrante es válida, como el registro de un nuevo dominio, ahora puede determinar mediante programación si el contacto registrante ha hecho clic en el enlace del correo electrónico de confirmación y, de no ser así, si el enlace sigue siendo válido. También puede solicitar mediante programación que enviemos otro email de confirmación. Para obtener más información, consulte la documentación siguiente en la Referencia de la API de Amazon Route 53:
 - [GetContactReachabilityStatus](#)
 - [ResendContactReachabilityEmail](#)

5 de abril de 2016

En esta versión, Route 53 agrega las siguientes características nuevas:

- Controles de estado basados en CloudWatch métricas: ahora puede crear controles de estado basados en el estado de alarma de cualquier CloudWatch métrica. Esto es útil para comprobar el estado de los puntos de conexión a los que no se puede tener acceso mediante una comprobación de estado de Route 53 estándar, como las instancias incluidas en una Amazon Virtual Private Cloud (VPC) que solo tengan direcciones IP privadas. Para obtener más información, consulte la siguiente documentación sobre :
 - Consola de Route 53: consulte [Monitoreo de una alarma CloudWatch](#) en el tema “Valores que se especifican al crear o actualizar las comprobaciones de estado”.
 - API de Route 53: consulte [CreateHealthCheck](#) [UpdateHealthCheck](#) en la referencia de la API de Amazon Route 53.
- Ubicaciones de comprobación de estado configurables: ahora puede elegir las regiones de comprobación de estado de Route 53 que comprueban el estado de los recursos, lo que reduce la carga en el punto de conexión en las comprobaciones de estado. Esto resulta útil si sus clientes se concentran en una o varias regiones geográficas. Para obtener más información, consulte la siguiente documentación sobre :
 - Consola de Route 53: consulte [Configuración avanzada \(solo "Monitor an endpoint" \(Monitorización de un punto de conexión\)\)](#) en el tema “Valores que se especifican al crear o actualizar las comprobaciones de estado”.
 - API de Route 53: consulte el Regions elemento correspondiente [CreateHealthCheck](#) [UpdateHealthCheck](#) en la referencia de la API de Amazon Route 53.
- Conmutación por error en zonas alojadas privadas: ahora puede crear registros de conmutación por error y de alias de conmutación por error en una zona alojada privada. Al combinar esta característica con las comprobaciones de estado basadas en métricas, puede

configurar la conmutación por error de DNS incluso para puntos de conexión que solo tienen direcciones IP privadas y no están accesibles mediante las comprobaciones de estado de Route 53 estándar. Para obtener más información, consulte la siguiente documentación sobre :

- Consola de Route 53: consulte [Configuración de la conmutación por error en una zona alojada privada](#).
- API de Route 53: consulte [ChangeResourceRecordSets](#) la referencia de la API de Amazon Route 53.
- Registros de alias en zonas alojadas privadas: anteriormente, se podían crear registros de alias que dirigían las consultas de DNS únicamente a otros registros de Route 53 en la misma zona alojada. Con esta versión, también puede crear registros de alias que dirijan las consultas de DNS a entornos de Elastic Beanstalk que tienen subdominios regionalizados, balanceadores de carga ELB y buckets de Amazon S3. (Aún no puede crear registros de alias que dirijan las consultas de DNS a una distribución). CloudFront Para obtener más información, consulte la siguiente documentación sobre :
 - Consola de Route 53: consulte [Elección entre registros de alias y sin alias](#).
 - API de Route 53: consulte [ChangeResourceRecordSets](#) la referencia de la API de Amazon Route 53.

23 de febrero de 2016

Al crear o actualizar las comprobaciones de estado HTTPS, ahora puede configurar Route 53 para que envíe el nombre de host al punto de conexión durante la negociación de TLS. Esto permite que el punto final responda a la solicitud HTTPS con el SSL/TLS certificado correspondiente. Para obtener más información, consulte la descripción de SNI en el campo [Configuración avanzada \(solo "Monitor an endpoint" \(Monitorización de un punto de conexión\)\)](#) en el tema "Valores que se especifican al crear o actualizar las comprobaciones de estado". Para obtener información sobre cómo habilitar el SNI cuando utiliza la API para crear o actualizar una comprobación de estado, consulte [CreateHealthChecky](#) [UpdateHealthCheck](#) en la referencia de la API de Amazon Route 53.

27 de enero de 2016

Ahora puede registrar dominios para más de 100 dominios de nivel superior adicionales (TLDs), como .accountants, .band y .city. Para obtener una lista completa de los compatibles, consulte. TLDs [Dominios que puede registrar con Amazon Route 53](#)

19 de enero de 2016

Ahora puede crear registros de alias que dirijan el tráfico a entornos de Elastic Beanstalk. Para obtener información sobre cómo crear registros mediante la consola de Route 53, consulte [Creación de registros con la consola de Amazon Route 53](#). Para obtener información sobre el uso de la API para crear registros, consulte [ChangeResourceRecordSets](#) la referencia de la API de Amazon Route 53.

Versiones de 2015

3 de diciembre de 2015

Ahora la consola de Route 53 incluye un editor visual que permite crear rápidamente las configuraciones de direccionamiento complejas que utilizan una combinación de políticas de direccionamiento ponderadas, de latencia, conmutación por error y geolocalización de Route 53. A continuación, puede asociar la configuración con uno o varios nombres de dominio (como example.com) o nombres de subdominio (como www.example.com) en la misma zona alojada o en varias zonas alojadas. Además, puede revertir las actualizaciones si la nueva configuración no tiene el desempeño previsto. La misma funcionalidad está disponible mediante la API de Route 53 AWS SDKs AWS CLI, la y AWS Tools for Windows PowerShell. Para obtener información sobre cómo usar el editor visual, consulte [Uso de flujo de tráfico para dirigir el tráfico DNS](#). Para obtener información sobre el uso de la API para crear configuraciones de flujo de tráfico, consulte la [Referencia de la API de Amazon Route 53](#).

19 de octubre de 2015

En esta versión, Route 53 agrega las siguientes características nuevas:

- Registro de dominios para dominios.com y .net por parte de Amazon Registrar, Inc.: Amazon es ahora un registrador acreditado por la ICANN para los dominios de nivel superior .com y .net () TLDs a través de Amazon Registrar, Inc. Cuando utilice Route 53 para registrar un dominio.com o .net, Amazon Registrar será el registrador registrado y aparecerá como el «Registrador patrocinador» en los resultados de sus consultas de Whois. Para obtener información sobre el uso de Route 53 para registrar dominios, consulte [Registro y administración de dominios mediante Amazon Route 53](#).
- Protección de privacidad de los dominios .com y .net: ahora, cuando registra un dominio .com o .net con Route 53, toda la información personal, incluido el nombre y los apellidos, se oculta. El nombre y los apellidos no están ocultos para otros dominios que registre con Route 53.

Para obtener más información sobre la protección de la privacidad, consulte [Activación o desactivación de la protección de privacidad para la información de contacto para un dominio](#).

15 de septiembre de 2015

En esta versión, Route 53 agrega las siguientes características nuevas:

- Comprobaciones de estado calculadas: ahora puede crear comprobaciones de estado cuya situación se determine por la situación de estado de otras comprobaciones de estado. Para obtener más información, consulte [Creación y actualización de comprobaciones de estado](#). Además, consulte la referencia [CreateHealthCheck](#) de la API de Amazon Route 53.
- Mediciones de latencia para las comprobaciones de estado: ahora puede configurar Route 53 para medir la latencia entre los comprobadores de estado y el punto de conexión. Los datos de latencia aparecen en los CloudWatch gráficos de Amazon en la consola de Route 53. Para habilitar las medidas de latencia de las nuevas comprobaciones de estado, consulte la configuración Latency measurements (Medidas de latencia) en [Configuración avanzada \(solo "Monitor an endpoint" \(Monitorización de un punto de conexión\)\)](#) del tema [Valores que especifica al crear o actualizar comprobaciones de estado](#). (No puede habilitar las medidas de latencia de las comprobaciones de estado existentes.) Además, consulte el tema MeasureLatency de la referencia [CreateHealthCheck](#) de la API de Amazon Route 53.
- Actualizaciones del panel de controles de estado de la consola de Route 53: el panel para monitorear los controles de estado se ha mejorado de diversas maneras, incluyendo CloudWatch gráficos para monitorear la latencia entre los verificadores de estado de Route 53 y los puntos de conexión. Para obtener más información, consulte [Monitorizar el estado de la comprobación de estado y recibir notificaciones](#).

3 de marzo de 2015

En la Guía para desarrolladores de Amazon Route 53 ahora se explica cómo configurar los servidores de nombres de etiqueta blanca de zonas alojadas de Route 53. Para obtener más información, consulte [Configuración de servidores de nombres de etiqueta blanca](#).

26 de febrero de 2015

Ahora puedes usar la API de Route 53 para enumerar las zonas alojadas asociadas a una AWS cuenta en orden alfabético por nombre. También puede obtener un recuento de las zonas alojadas que están asociadas con una cuenta. Para obtener más información, consulte [ListHostedZonesByName](#) y consulte [GetHostedZoneCount](#) la referencia de la API de Amazon Route 53.

11 de febrero de 2015

En esta versión, Route 53 agrega las siguientes características nuevas:

- Estado de comprobación de estado: la página de comprobaciones de estado de la consola de Route 53 ahora incluye la columna Status (Estado) que permite ver la situación general de todas las comprobaciones de estado. Para obtener más información, consulte [Ver el estado de la verificación de salud y el motivo de los fallos de la verificación de salud](#).
- Integración con AWS CloudTrail: Route 53 ahora funciona CloudTrail para capturar información sobre todas las solicitudes que su AWS cuenta envía a la API de Route 53. La integración de Route 53 CloudTrail le permite determinar qué solicitudes se realizaron a la API de Route 53, la dirección IP de origen desde la que se realizó cada solicitud, quién la hizo, cuándo se realizó, etc. Para obtener más información, consulte [Registrar llamadas a la API de Amazon Route 53 con AWS CloudTrail](#).
- Alarmas rápidas para comprobaciones de estado: al crear una comprobación de estado mediante la consola de Route 53, ahora puede crear simultáneamente una CloudWatch alarma de Amazon para la comprobación de estado y especificar a quién notificar cuando Route 53 considere que el punto final está en mal estado durante un minuto. Para obtener más información, consulte [Creación y actualización de comprobaciones de estado](#).
- Etiquetado de zonas alojadas y dominios: ahora puede asignar etiquetas, que se utilizan habitualmente para la asignación de costes, a las zonas alojadas y los dominios de Route 53. Para obtener más información, consulte [Etiquetado de recursos de Amazon Route 53](#).

5 de febrero de 2015

Ahora puede utilizar la consola de Route 53 para actualizar la información de contacto de un dominio. Para obtener más información, consulte [Valores que especifican cuando registra o transfiere un dominio](#).

22 de enero de 2015

Ahora puede especificar nombres de dominio internacionalizados al registrar un nuevo nombre de dominio con Route 53. (Route 53 ya admitía los nombres de dominio internacionalizados para zonas alojadas y registros). Para obtener más información, consulte [Formato de nombres de dominio DNS](#).

Versiones de 2014

25 de noviembre de 2014

En esta versión, puede editar el comentario que especificó para una zona alojada cuando la creó. En la consola, haga clic en el icono de lapicero situado junto al campo Comment y escriba un nuevo valor. Para obtener más información sobre cómo cambiar el comentario mediante la API de Route 53, consulte [UpdateHostedZoneComment](#) la referencia de la API de Amazon Route 53.

5 de noviembre de 2014

En esta versión, Route 53 agrega las siguientes características nuevas:

- DNS privado VPCs creado con el servicio Amazon Virtual Private Cloud: ahora puede usar Route 53 para administrar sus nombres de dominio internos VPCs sin exponer los datos del DNS a la Internet pública. Para obtener más información, consulte [Uso de zonas alojadas privadas](#).
- Motivos de los errores de la comprobación de estado: ahora puede ver el estado actual de una comprobación de estado seleccionada, así como detalles sobre por qué la comprobación de estado ha terminado teniendo un error, según lo comunicado por cada uno de los comprobadores de estado de Route 53. El estado incluye el código de estado HTTP y los motivos de error incluyen información sobre numerosos tipos de errores, como los errores de comparación de cadenas y el tiempo de espera agotado de respuesta. Para obtener más información, consulte [Ver el estado de la verificación de salud y el motivo de los fallos de la verificación de salud](#).
- Conjuntos de delegación reutilizables: ahora puede aplicar el mismo conjunto de cuatro servidores de nombres autorizados, lo que se conoce colectivamente como un conjunto de delegación, a varias zonas alojadas que corresponden a diferentes nombres de dominio. Esto simplifica considerablemente el proceso de migración de servicio DNS a Route 53 y la administración de un gran número de zonas alojadas. El uso de conjuntos de delegación reutilizables actualmente requiere usar la API de Route 53 o un AWS SDK. Para obtener más información, consulte la [referencia de API de Amazon Route 53](#).
- Enrutamiento de geolocalización mejorado: hemos mejorado aún más la precisión del enrutamiento de geolocalización al añadir soporte para la edns-client-subnet extensión de EDNS0. Para obtener más información, consulte [Enrutado de geolocalización](#).
- Soporte de Signature v4: ahora puede firmar todas las solicitudes de la API de Route 53 con Signature versión 4. Para obtener más información, consulte [Firmar solicitudes de la API de Route 53](#) en la Referencia de la API de Amazon Route 53.

31 de julio de 2014

Con esta versión, ahora puede hacer lo siguiente:

- Registrar nuevos nombres de dominio mediante Route 53. Para obtener más información, consulte [Registro y administración de dominios mediante Amazon Route 53](#).
- Configurar Route 53 para responder a las consultas de DNS en función de la ubicación geográfica donde se originen las consultas. Para obtener más información, consulte [Enrutado de geolocalización](#).

2 de julio de 2014

Con esta versión, ahora puede hacer lo siguiente:

- Editar la mayoría de valores de las comprobaciones de estado. Para obtener más información, consulte [Creación, actualización y eliminación de comprobaciones de estado](#).
- Utilice la API de Route 53 para obtener una lista de los rangos de IP que los comprobadores de estado de Route 53 utilicen para comprobar el estado de los recursos. Puede utilizar estas direcciones IP para configurar las reglas de router y de firewall para permitir que los comprobadores de estado comprueben el estado de los recursos. Para obtener más información, consulte [GetCheckerIpRanges](#) la referencia de la API de Amazon Route 53.
- Asignar etiquetas de asignación de costos a las comprobaciones de estado, lo que también le permite asignar un nombre a dichas comprobaciones. Para obtener más información, consulte [Denominar y etiquetar comprobaciones de estado](#).
- Utilice la API de Route 53 para obtener el número de comprobaciones de estado asociadas a su AWS cuenta. Para obtener más información, consulte [GetHealthCheckCount](#) la referencia de la API de Amazon Route 53.

30 de abril de 2014

En esta versión, ahora puede crear comprobaciones de estado y utilizar un nombre de dominio en vez de una dirección IP para especificar el punto de conexión. Esto resulta útil cuando la dirección IP de un punto final no es fija o la proporcionan varias instancias IPs, como Amazon EC2 o Amazon RDS. Para obtener más información, consulte [Creación y actualización de comprobaciones de estado](#).

Además se ha trasladado información sobre el uso de la API de Route 53 que anteriormente aparecía en la Guía para desarrolladores de Amazon Route 53. Ahora toda la documentación de la API aparece en la Referencia de la API de Amazon Route 53.

18 de abril de 2014

En esta versión, Route 53 pasa un valor diferente en el encabezado Host cuando el valor Port (Puerto) de la comprobación de estado es 443 y el valor de Protocol (Protocolo) es HTTPS. Durante una comprobación de estado, Route 53 ahora pasa al punto de conexión un encabezado Host que contiene el valor del campo Nombre del host. Si ha creado la comprobación de estado mediante la acción de la API CreateHealthCheck, se trata del valor del elemento FullyQualifiedDomainName.

Para obtener más información, consulte [Creación, actualización y eliminación de comprobaciones de estado](#).

9 de abril de 2014

En esta versión, ahora puede ver el porcentaje de comprobadores de estado de Route 53 que actualmente están informando de que un punto de conexión funciona correctamente.

Además, el comportamiento de la métrica Health Check Status en Amazon CloudWatch ahora solo muestra cero (si el punto final estuvo en mal estado durante un período de tiempo determinado) o uno (si el punto final estuvo en buen estado durante ese período de tiempo). La métrica ya no muestra valores entre 0 y 1 reflejando la parte de las comprobaciones de estado de Route 53 que informan de que el punto de conexión funciona correctamente.

Para obtener más información, consulte [Monitorear comprobaciones de estado mediante CloudWatch](#).

18 de febrero de 2014

En esta versión, Route 53 agrega las siguientes características:

- Umbral de conmutación por error de comprobación de estado: ahora puede especificar en cuántas comprobaciones de estado consecutivas se debe producir un error en un punto de conexión antes de que Route 53 considere que el punto de conexión no funciona correctamente, entre 1 y 10 comprobaciones consecutivas. Un punto de conexión que no funciona correctamente debe superar el mismo número de comprobaciones para que se considere que funciona correctamente. Para obtener más información, consulte [Cómo determina Amazon Route 53 si la comprobación de estado es correcta](#).
- Intervalo de solicitud de comprobación de estado: ahora puede especificar la frecuencia con la que Route 53 envía solicitudes a un punto de conexión para determinar si funciona correctamente. Los valores válidos son 10 y 30 segundos. Para obtener más información, consulte [Cómo determina Amazon Route 53 si la comprobación de estado es correcta](#).

30 de enero de 2014

En esta versión, Route 53 agrega las siguientes características:

- Comprobaciones de estado de coincidencia de cadenas HTTP y HTTPS: Route 53 ahora admite las comprobaciones de estado que determinan el estado de un punto de conexión en función del aspecto de una cadena especificada en el cuerpo de la respuesta. Para obtener más información, consulte [Cómo determina Amazon Route 53 si la comprobación de estado es correcta](#).
- Comprobaciones de estado HTTPS: Route 53 ahora admite las comprobaciones de estado para sitios web seguros de solo SSL. Para obtener más información, consulte [Cómo determina Amazon Route 53 si la comprobación de estado es correcta](#).
- **UPSERT** para la acción **ChangeResourceRecordSets** de la API: al crear o modificar registros mediante la acción `ChangeResourceRecordSets` de la API, ahora puede utilizar la acción UPSERT para crear un registro nuevo si no hay ninguno con un determinado nombre y tipo, o para actualizar un registro existente. Para obtener más información, consulte [ChangeResourceRecordSets](#) la referencia de la API de Amazon Route 53.

7 de enero de 2014

En esta versión, Route 53 agrega soporte para las comprobaciones de estado que determinan el estado de un punto de conexión en función de si una cadena especificada aparece en el cuerpo de la respuesta. Para obtener más información, consulte [Cómo determina Amazon Route 53 si la comprobación de estado es correcta](#).

Versiones de 2013

14 de agosto de 2013

En esta versión, Route 53 permite la creación de registros mediante la importación de un archivo de zona con formato BIND. Para obtener más información, consulte [Creación de registros mediante la importación de un archivo de zona](#).

Además, CloudWatch las métricas de las comprobaciones de estado de Route 53 se han integrado en la consola de Route 53 y se han simplificado. Para obtener más información, consulte [Monitorear comprobaciones de estado mediante CloudWatch](#).

26 de junio de 2013

Con esta versión, Route 53 añade la compatibilidad con la integración de las comprobaciones de estado con CloudWatch las métricas, de forma que pueda hacer lo siguiente:

- Comprobar que una comprobación de estado está configurada correctamente.
- Revisar el estado de un punto de conexión de comprobación de estado durante un periodo de tiempo especificado.
- CloudWatch Configúrelo para enviar una alerta del Amazon Simple Notification Service (Amazon SNS) cuando todos los verificadores de estado de Route 53 consideren que el punto final especificado está en mal estado.

Para obtener más información, consulte [Monitorear comprobaciones de estado mediante CloudWatch](#).

11 de junio de 2013

Con esta versión, Route 53 añade soporte para crear registros de alias que enruten las consultas de DNS a nombres de dominio alternativos para CloudFront las distribuciones de Amazon. Puede utilizar esta característica tanto para nombres de dominio alternativo en el vértice de zona (example.com) como para nombres de dominio alternativo para subdominios (www.example.com). Para obtener más información, consulte [Enrutar el tráfico a una CloudFront distribución de Amazon mediante tu nombre de dominio](#).

30 de mayo de 2013

Con esta versión, Route 53 añade soporte para evaluar el estado de los balanceadores de carga ELB y las instancias de Amazon EC2 asociadas. Para obtener más información, consulte [Creación de comprobaciones de estado de Amazon Route 53](#).

28 de marzo de 2013

La documentación sobre las comprobaciones de estado y la conmutación por error se ha vuelto a redactar para mejorar el uso. Para obtener más información, consulte [Creación de comprobaciones de estado de Amazon Route 53](#).

11 de febrero de 2013

En esta versión, Route 53 agrega soporte para la conmutación por error y las comprobaciones de estado. Para obtener más información, consulte [Creación de comprobaciones de estado de Amazon Route 53](#).

Versión de 2012

21 de marzo de 2012

En esta versión, Route 53 permite crear registros de latencia. Para obtener más información, consulte [Enrutado basado en latencia](#).

Versiones de 2011

21 de diciembre de 2011

Con esta versión, la consola de Route 53 de Consola de administración de AWS le permite crear un registro de alias al elegir un Elastic Load Balancer de una lista en lugar de introducir manualmente el ID de la zona alojada y el nombre DNS del balanceador de carga. La nueva funcionalidad se documenta en la Guía para desarrolladores de Amazon Route 53.

16 de noviembre de 2011

Con esta versión, puede usar la consola de Route 53 Consola de administración de AWS para crear y eliminar zonas alojadas, así como para crear, cambiar y eliminar registros. La nueva funcionalidad se documenta en la Guía para desarrolladores de Amazon Route 53, según corresponda.

18 de octubre de 2011

La Guía de introducción a Amazon Route 53 se fusionó en la Guía para desarrolladores de Amazon Route 53, y la Guía para desarrolladores se ha reorganizado para facilitar su uso.

24 de mayo de 2011

Esta versión de Amazon Route 53 incorpora registros de alias, que le permiten crear alias de vértice de zona, registros ponderados, una nueva API (2011-05-05) y un acuerdo de nivel de servicios. Además, después de seis meses en versión beta, Route 53 ya tiene disponibilidad general. Para obtener más información, consulte la [Página del producto de Amazon Route 53](#) y [Elección entre registros de alias y sin alias](#) la Guía para desarrolladores de Amazon Route 53.

Versión de 2010

5 de diciembre de 2010

Esta es la primera versión de la Guía para desarrolladores de Amazon Route 53.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.