



Guía para desarrolladores

AWS Backup



AWS Backup: 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 AWS Backup?	1
Descripción general de las características	1
Administración centralizada de copias de seguridad	1
Copias de seguridad basadas en políticas	1
Políticas de copia de seguridad basadas en etiquetas	2
Políticas de administración del ciclo de vida	2
Copias de seguridad entre regiones	2
Administración entre cuentas y copias de seguridad entre cuentas	3
Auditoría e informes con AWS Backup Audit Manager	3
Copias de seguridad incrementales	4
AWS Backup Administración completa	4
Monitorización de la actividad de copia de seguridad	5
Seguridad de los datos en los almacenes de copias de seguridad	5
Introducción	6
AWS Recursos y aplicaciones compatibles	6
Precios	8
AWS Backup disponibilidad de funciones	8
Características disponibles para todos los recursos compatibles	8
Disponibilidad de características por recurso	9
Disponibilidad de las funciones por Región de AWS	14
Servicios compatibles con Región de AWS	22
Cómo funciona	29
Trabajar con AWS servicios compatibles	29
Uso de datos de Amazon S3	30
Trabajando con máquinas VMware virtuales	31
Uso de Amazon DynamoDB	31
Trabajar con los sistemas de FSx archivos de Amazon	32
Trabajando con Amazon EC2	33
Uso de Amazon EFS	34
Uso de Amazon EBS	35
Uso de Amazon RDS Y Aurora	36
Uso de Aurora DSQL	36
Trabajando con AWS BackInt	37
Trabajando con AWS Storage Gateway	37

Uso de Amazon DocumentDB	38
Uso de Amazon Neptune	38
Uso de Amazon Redshift y Amazon Redshift sin servidor	38
Uso de Amazon Timestream	38
Trabajando con AWS Organizations	38
Trabajando con CloudFormation	39
Trabajando con AWS BackInt, AWS Systems Manager para SAP y SAP HANA	39
Trabajar con Amazon EKS	39
Trabajando con Amazon GuardDuty	40
¿Cómo AWS hacen los servicios copias de seguridad de sus propios recursos	40
Medición, costos y facturación	41
AWS Backup precios	8
AWS Backup facturación	41
Etiquetas de asignación de costos	42
AWS Backup Precios de Audit Manager	42
Precios de Amazon Aurora	42
Blogs, vídeos, tutoriales y otros recursos	43
Introducción	47
Requisitos previos	47
Suscripción al servicio	48
Planes de copia de seguridad	50
Creación de plan de copia de seguridad	50
Creación de planes de copia de seguridad mediante la consola de AWS Backup	51
Cree planes de respaldo mediante el AWS CLI	53
Opciones y configuración del plan de copia de seguridad	54
CloudFormation plantillas para planes de respaldo	64
Eliminar un plan de copia de seguridad	67
Actualizar un plan de copia de seguridad	68
Introducción al resumen del plan de copia de seguridad	69
Componentes del resumen	69
Vista previa de las ejecuciones de copia de seguridad programadas	70
Validación de la compatibilidad de las características	71
Acceso a los resúmenes de planes de copia de seguridad	71
Suscripción y asignación de recursos	72
Suscripción a servicios y asignación de recursos	72
Suscripción al servicio	73

Asignación del recurso	73
Asignación de recursos a través de la consola	74
Asigne recursos con AWS CLI	76
Asigne recursos con CloudFormation	84
Cuotas de asignación de recursos	87
Almacenes de copias de seguridad	88
Creación y eliminación de almacenes de copias de seguridad	88
Permisos necesarios	88
Creación de un almacén de copias de seguridad (consola)	90
Creación de un almacén de copias de seguridad (mediante programación)	91
Nombre del almacén de copias de seguridad	91
AWS KMS clave de cifrado	91
Etiquetas de almacén de copias de seguridad	92
Eliminar un almacén	92
Tener un almacén aislado lógicamente	93
Información general de los almacenes aislados lógicamente	93
Caso de uso para almacenes aislados lógicamente	94
Comparación y contraste con un almacén de copias de seguridad estándar	95
Crear un almacén aislado lógicamente	98
Visualización de los detalles del almacén aislado lógicamente	101
Crear copias de seguridad en un almacén cerrado de forma lógica	102
Compartir un almacén aislado lógicamente	105
Restauración de una copia de seguridad desde un almacén aislado lógicamente	108
Eliminar un almacén aislado lógicamente	109
Opciones de programación adicionales para almacenes aislados lógicamente	109
Descripción de los tipos de claves de cifrado para bóvedas aisladas de forma lógica	110
Solución de un problema de almacén aislado lógicamente	117
Copias de seguridad principales en almacenes aislados lógicamente	119
Aprobación de varias partes para almacenes aislados lógicamente	137
Políticas de acceso a almacenes	153
Denegación del acceso a un tipo de recurso en un almacén de copias de seguridad	154
Denegación del acceso a un almacén de copias de seguridad	154
Denegación del acceso para eliminar puntos de recuperación en un almacén de copias de seguridad	155
Bloqueo de almacenes	156
Modos de bloqueo del almacén	157

Ventajas del bloqueo de almacenes	157
Bloqueo de un almacén de copias de seguridad mediante la consola	158
Bloqueo de un almacén de copias de seguridad mediante programación	159
Revise la configuración de Vault Lock de una AWS Backup bóveda de respaldo	161
Eliminación del bloqueo del almacén durante el periodo de gracia (modo de cumplimiento)	162
Cuenta de AWS cierre con una bóveda cerrada	163
Consideraciones adicionales de seguridad	163
Creación, mantenimiento y restauración de copias de seguridad	165
Copias de seguridad bajo demanda	166
Copias de seguridad continuas y PITR	168
Consideraciones sobre las copias de seguridad continuas y la PITR	169
Servicios admitidos	171
Búsqueda de una copia de seguridad continua	175
Restauración de una copia de seguridad continua	176
Detención o eliminación de copias de seguridad continuas	176
Copiado de copias de seguridad continuas	177
Cambio del periodo de retención	177
Eliminación de la única regla de copia de seguridad continua de un plan de copia de seguridad	178
Creación de copias de seguridad por tipo de recurso	179
Creación de copias de seguridad automáticas	179
Creación de copias de seguridad bajo demanda	179
Estados de los trabajos de copia de seguridad	179
Copias de seguridad incrementales	180
Acceso a los recursos de origen	180
CloudFormation apilar copias de seguridad	182
Copias de seguridad de Amazon Aurora DSQL	188
Copia de seguridad avanzada de DynamoDB	189
Copias de seguridad de Amazon EBS	195
Copias de seguridad de Amazon RDS	196
Copias de seguridad de Amazon Redshift	199
Copias de seguridad de Amazon Redshift sin servidor	202
Amazon EKS	205
Respaldo de SAP HANA en Amazon EC2	214
Copias de seguridad de Amazon S3	225

Copias de seguridad de Amazon Timestream	238
Copias de seguridad de máquinas virtuales	241
Creación de copias de seguridad de Windows VSS	285
Copia de seguridad y copia de etiquetas	287
Reintento de los trabajos de copia	288
Copias de seguridad entre regiones	289
Copia de seguridad entre cuentas	292
Copia de etiquetas en copias de seguridad	305
Eliminaciones de las copias de seguridad	306
Eliminación de las copias de seguridad manualmente	307
Solución de problemas de eliminaciones manuales	309
Ediciones de copia de seguridad y etiquetas	309
Búsqueda de copias de seguridad	310
Descripción general de	310
Casos de uso para índices y búsquedas de copias de seguridad	311
Acceso	311
Flujo de procesos	312
Índices de copia de seguridad	313
Búsquedas	316
Resultados de la búsqueda	319
Exportación de los resultados de búsqueda a un bucket de S3	320
Consideraciones y prácticas recomendadas sobre los costos	322
Restauración a partir de una búsqueda	322
Backup por niveles	323
Descripción general de	323
Configuraciones por niveles	324
Creación de configuraciones por niveles	325
Administrar las configuraciones de estratificación	326
Cómo se aplican las configuraciones de organización por niveles de backup de S3	329
Estructura de costos y monitoreo	329
Ejemplos de configuraciones	330
Características y limitaciones compatibles	332
Resolución de problemas	332
Restauración por tipo de recurso	333
Cómo restaurar	333
Restauraciones no destructivas	334

Pruebas de restauración	334
Copia de etiquetas durante una restauración	334
Estados de los trabajos de restauración	338
Restauración de Aurora	339
Restauración de Aurora DSQL	343
CloudFormation restaurar	350
Restauración de DocumentDB	352
Restauración de DynamoDB	354
Restauración de EBS	357
EC2 restaurar	363
Restauración de EFS	368
Restauración de EKS	373
FSx restaurar	382
Restauración de Neptune	392
Restauración de RDS	394
Restauración de Redshift	396
Restauración de Redshift sin servidor	400
Restauración de SAP HANA	404
Restauración de S3	414
Restauración de Storage Gateway	421
Restauración de Timestream	423
Restauración de VM	426
Pruebas de restauración	432
Descripción general de	433
Comparar con restauraciones	433
Administración de planes	435
Creación de un plan de prueba	436
Actualizar un plan de prueba	441
Visualización de planes de prueba	442
Visualización de trabajos de prueba	443
Eliminación de un plan	444
Auditoría de pruebas	445
Cuotas y parámetros	446
Resolución de problemas	446
Metadatos inferidos	448
Restaurar la validación de las pruebas	456

Detener un trabajo de copia de seguridad	458
Visualizar copias de seguridad existentes	459
Listado de copias de seguridad por recurso protegido en la consola	459
Listado de copias de seguridad por almacén de copias de seguridad en la consola	460
Listado de copias de seguridad mediante programación	460
AWS Backup Audit Manager	461
Uso de marcos de auditoría	462
Elección de controles	463
Activación del seguimiento de recursos	466
Creación de marcos mediante la AWS Backup consola	473
Creación de marcos mediante la AWS Backup API	474
Visualización del estado de conformidad del marco	489
Búsqueda de recursos no conformes	491
Actualización de los marcos de auditoría	491
Eliminación de los marcos de auditoría	491
Uso de informes de auditoría	492
Contexto del informe de trabajo mejorado	493
Elección de la plantilla de informe	494
Creación de planes de informes	505
Creación de planes de informes mediante la AWS Backup API	508
Creación de informes bajo demanda	511
Visualización de los informes de auditoría	512
Actualización de los planes de informes	513
Eliminación de los planes de informes	513
Uso CloudFormation para implementar los recursos AWS Backup de Audit Manager	513
Activación del seguimiento de recursos	472
Implementación de controles predeterminados	519
Exención de roles de IAM de la evaluación de control	520
Creación de un plan de informes	521
Uso de AWS Backup Audit Manager con AWS Audit Manager	522
Controles y corrección	522
Los recursos de copia de seguridad están incluidos en al menos un plan de copia de seguridad	523
Frecuencia mínima y retención mínima del plan de copia de seguridad	524
Los almacenes impiden la eliminación manual de los puntos de recuperación	524
Los puntos de recuperación están cifrados	525

Se ha establecido una retención mínima para el punto de recuperación	526
Se ha programado una copia de la copia de seguridad entre regiones	526
Se ha programado una copia de la copia de seguridad entre cuentas	527
Los recursos están en un plan de respaldo con un AWS Backup Vault Lock	527
Se creó el último punto de recuperación	528
El tiempo de restauración de los recursos cumple el objetivo	529
Recursos en un almacén aislado lógicamente	529
Administre varias cuentas con AWS Organizations	531
Descripción general de la administración entre cuentas	531
Creación de una cuenta de administración en Organizations	533
Habilitación de la administración entre cuentas	533
Políticas de copia de seguridad	534
Administrador delegado	534
Requisitos previos	536
Registro de una cuenta miembro como cuenta del administrador delegado	537
Anulación del registro de una cuenta miembro	538
Delega AWS Backup políticas a través de AWS Organizations	539
Monitorización de actividades en varias Cuentas de AWS	539
Reglas de suscripción de recursos	540
Definición de políticas, sintaxis de políticas y herencia de políticas	540
AWS Backup y CloudFormation	541
En general	541
Implementación de un almacén de copias de seguridad, un plan de copia de seguridad y una asignación de recursos con CloudFormation	541
Implementación de planes de copia de seguridad con CloudFormation	542
Implementación de marcos y planes de informes de AWS Backup Audit Manager con CloudFormation	542
Uso de CloudFormation con AWS Organizations	542
Más información	542
Network	543
Puntos de conexión	543
AWS PrivateLink	543
Consideraciones sobre los puntos de conexión de Amazon VPC	543
Crear un punto final AWS Backup de VPC	544
Uso de un punto de conexión de VPC	545
Creación de una política de punto de conexión de VPC	545

Seguridad	548
Validación de conformidad	549
Protección de datos	549
Cifrado de copias de seguridad en AWS Backup	550
Cifrado de credenciales del hipervisor de máquinas virtuales	562
Identity and Access Management	564
Autenticación	565
Control de acceso	566
Roles de servicio de IAM	576
Políticas administradas	579
Cómo utilizar roles vinculados a servicios	665
Prevención de la sustitución confusa entre servicios	674
Seguridad de la infraestructura	675
Integridad	675
AWS Backup objetivo de integridad de los datos	675
AWS Backup implementación de la integridad de los datos	676
Confirmación objetiva y auditoría de la integridad de los datos en AWS Backup	676
Retenciones legales	677
Descripción general de las retenciones legales	677
Retenciones legales múltiples	677
Creación de una retención legal	678
Visualización de las retenciones legales	679
Liberación de una retención legal	682
Protección contra malware	683
Integración con Amazon GuardDuty	684
Acceso instantáneo	684
¿Cómo utilizar el escaneo de malware	685
Acceso	685
Escaneos incrementales frente a escaneos completos	686
Supervisar tus escaneos de malware	687
Comprender los resultados de los escaneos	688
Solución de problemas de escaneo	689
Medición	690
Cuotas	690
Pasos de uso de la consola y la CLI para los tipos de análisis de malware	690
Resiliencia	695

Cuotas	696
Copia de seguridad	696
Índice de copias de seguridad y cuotas de búsqueda	698
Cuotas de políticas	699
Cuotas de escaneo de malware	700
Cuotas de recursos de Amazon Timestream	701
AWS Backup Cuotas de Audit Manager	701
Cuotas del plan de pruebas de restauración	702
AWS Backup gateway cuotas	704
Cuotas de Amazon EKS	704
Cuotas de bóvedas con huecos lógicos	705
Cuotas relacionadas	705
Monitorización AWS Backup	707
Paneles de la consola	707
Descripción general de	708
Panel de trabajos	708
Motivos que ocasionan problemas	710
Datos del panel con AWS CLI	714
Monitorización de eventos mediante EventBridge	716
Eventos de Trabajo de copia de seguridad	717
Eventos del plan de copia de seguridad	722
Eventos de Backup Vault	724
Eventos de copia de trabajos	725
Eventos de puntos de recuperación	729
Eventos de configuración regional	730
Eventos de restauración de trabajos	731
Eventos de indexación del punto de recuperación	734
Eventos de Job de escaneo de malware	737
AWS Backup métricas con Amazon CloudWatch	744
CloudWatch Tablero	744
Métricas con CloudWatch	746
Registrar las llamadas a AWS Backup la API con CloudTrail	750
AWS Backup eventos en CloudTrail	752
Descripción de las entradas de los archivos de AWS Backup registro	753
Registro de eventos de administración entre cuentas	757
Opciones de notificación con AWS Backup	761

Notificaciones de usuario y AWS Backup	761
Amazon SNS y eventos AWS Backup	761
Solución de problemas AWS Backup	769
Solución de problemas generales	769
Solución de problemas de creación de recursos	770
Solución de problemas de eliminación de recursos	771
Solución de problemas de restauración de recursos	771
Solución de problemas de errores de formateo	772
AWS BackupAPI de	773
Acciones	773
AWS Backup	778
AWS Backup gateway	1267
AWS Backup	1363
Data Types	1425
AWS Backup	1428
AWS Backup gateway	1610
AWS Backup	1636
Parámetros comunes	1669
Errores comunes	1671
Historial de revisión	1674
.....	mdccli

¿Qué es AWS Backup?

AWS Backup es un servicio totalmente gestionado que facilita la centralización y la automatización de la protección de datos en todos AWS los servicios, en la nube y en las instalaciones. Con este servicio, puede configurar las políticas de respaldo y monitorear la actividad de sus AWS recursos en un solo lugar. Le permite automatizar y consolidar las tareas de respaldo que se service-by-service realizaban anteriormente y elimina la necesidad de crear scripts personalizados y procesos manuales. Con unos pocos clics en la consola de AWS Backup , puede automatizar sus políticas y programas de protección de datos.

AWS Backup no regula las copias de seguridad que realice en su AWS entorno externo AWS Backup. Por lo tanto, si desea una end-to-end solución centralizada para cumplir con los requisitos empresariales y normativos, empiece a utilizarla AWS Backup hoy mismo.

Descripción general de las características

AWS Backup ofrece muchas funciones y capacidades, entre las que se incluyen las siguientes.

Administración centralizada de copias de seguridad

AWS Backup proporciona una consola de copias de seguridad centralizada, un conjunto de copias de seguridad APIs y el AWS Command Line Interface (AWS CLI) para gestionar las copias de seguridad de todos los AWS servicios que utilizan sus aplicaciones. Con él AWS Backup, puede administrar de forma centralizada las políticas de respaldo que cumplan con sus requisitos de respaldo. A continuación, puede aplicarlas a sus AWS recursos en todos los AWS servicios, lo que le permitirá realizar copias de seguridad de los datos de sus aplicaciones de forma coherente y conforme a las normas. La consola de backup AWS Backup centralizada ofrece una vista consolidada de las copias de seguridad y los registros de actividad de las copias de seguridad, lo que facilita la auditoría de las copias de seguridad y garantiza el cumplimiento.

Copias de seguridad basadas en políticas

Con AWS Backup ella, puede crear políticas de respaldo conocidas como planes de respaldo. Utilice estos planes de respaldo para definir sus requisitos de respaldo y, a continuación, aplíquelos a los AWS recursos que desee proteger en todos los AWS servicios que utilice. Puede crear distintos planes de copias de seguridad de forma que cada uno de ellos cumpla requisitos específicos empresariales y de conformidad normativa. Esto ayuda a garantizar que se realice una copia de

seguridad de cada AWS recurso de acuerdo con sus requisitos. Los planes de copias de seguridad facilitan el cumplimiento de la estrategia de copias de seguridad en la organización y en las aplicaciones de manera escalable.

Para ver todas las opciones de configuración de los planes de copia de seguridad, consulte [Opciones y configuración del plan de copia de seguridad](#).

Políticas de copia de seguridad basadas en etiquetas

Puede utilizarlos AWS Backup para aplicar planes de respaldo a sus AWS recursos de diversas formas, incluso etiquetándolos. El etiquetado facilita la implementación de su estrategia de respaldo en todas sus aplicaciones y garantiza que todos sus AWS recursos estén respaldados y protegidos. AWS las etiquetas son una forma excelente de organizar y clasificar AWS los recursos. La integración con AWS etiquetas le permite aplicar rápidamente un plan de copia de seguridad a un grupo de AWS recursos, de forma que se realice una copia de seguridad coherente y conforme a las normas.

Para ver todas las formas en que puede asignar sus recursos a los planes de copia de seguridad, consulte [Seleccione AWS los servicios para realizar una copia de seguridad](#).

Políticas de administración del ciclo de vida

AWS Backup le permite cumplir con los requisitos de conformidad y, al mismo tiempo, minimizar los costos de almacenamiento de las copias de seguridad al almacenar las copias de seguridad en un nivel de almacenamiento en frío de bajo costo. Puede configurar políticas de ciclo de vida que trasladarán automáticamente copias de seguridad de un almacenamiento en caliente a otro en frío en función del programa que defina.

Para obtener una lista de los recursos que pueden realizar la transición a almacenamiento en frío, consulte [Disponibilidad de características por recurso](#). Para ver los pasos para activar el almacenamiento en frío en su plan de copia de seguridad, consulte [Ciclo de vida y niveles de almacenamiento](#).

Copias de seguridad entre regiones

Con él AWS Backup, puede copiar copias de seguridad a varios tipos de copias Regiones de AWS de seguridad bajo demanda o automáticamente como parte de un plan de copias de seguridad programado. Las copias de seguridad entre regiones resultan especialmente útiles si los requisitos de continuidad del negocio o de conformidad exigen que se almacenen copias de seguridad a una

distancia mínima de los datos de producción. Para obtener más información, consulte [Creación de copias de las copias de seguridad entre Regiones de AWS](#).

Administración entre cuentas y copias de seguridad entre cuentas

Puede usarlo AWS Backup para administrar sus copias de seguridad en todo el Cuentas de AWS interior de su [AWS Organizations](#) estructura. Con la administración entre cuentas, puede utilizar automáticamente políticas de copia de seguridad para aplicar planes de copia de seguridad en las Cuentas de AWS de su organización. Esto hace que el cumplimiento de normas y la protección de datos sean eficientes de forma escalable y reduce el gasto operativo. También ayuda a eliminar la duplicación manual de planes de copias de seguridad en cuentas individuales. Para obtener más información, consulte [Administración de recursos de AWS Backup en varias Cuentas de AWS](#).

También puede copiar las copias de seguridad en varios sitios diferentes Cuentas de AWS dentro de su estructura AWS Organizations de gestión. De esta forma, puede “agrupar” las copias de seguridad en una sola cuenta de repositorio y, a continuación, “distribuir” las copias de seguridad para aumentar la resiliencia. [Creación de copias de las copias de seguridad entre Cuentas de AWS](#).

Para poder utilizar las características de administración entre cuentas y copia de seguridad entre cuentas, debe tener configurada una estructura de organización existente en AWS Organizations. Una unidad organizativa (OU) es un grupo de cuentas que se pueden administrar como una sola entidad. AWS Organizations es una lista de cuentas que se pueden agrupar en unidades organizativas y administrar como una sola entidad.

Auditoría e informes con AWS Backup Audit Manager

AWS Backup Audit Manager le ayuda a simplificar la gobernanza de los datos y la gestión del cumplimiento de todas sus copias de seguridad AWS. AWS Backup Audit Manager proporciona controles integrados y personalizables que puede alinear con los requisitos de su organización. También puede usar estos controles para realizar un seguimiento automático de sus actividades y recursos de copia de seguridad.

AWS Backup Audit Manager puede ayudarle a localizar actividades y recursos específicos que aún no cumplen con los controles que ha definido. También genera informes diarios que puede utilizar para mostrar la conformidad de sus controles a lo largo del tiempo.

Para incluir su conformidad en materia de backup junto con su postura general de conformidad, puede importar automáticamente las conclusiones de AWS Backup Audit Manager a AWS Audit Manager.

Copias de seguridad incrementales

AWS Backup almacena de forma eficiente sus copias de seguridad periódicas de forma incremental. La primera copia de seguridad de un recurso de AWS hace una copia de seguridad completa de sus datos. Para cada copia de seguridad incremental sucesiva, solo se respaldan los cambios en sus AWS recursos. Las copias de seguridad incrementales le permiten beneficiarse de la protección de datos que ofrecen las copias de seguridad frecuentes y, al mismo tiempo, minimizar los costos de almacenamiento.

Para obtener una lista de los recursos que admiten copias de seguridad incrementales, consulte [Disponibilidad de características por recurso](#).

Para obtener más información, consulte [Copias de seguridad incrementales](#).

AWS Backup Administración completa

Algunos tipos de recursos admiten una AWS Backup administración completa. Los beneficios de la AWS Backup administración completa incluyen:

- **Cifrado independiente.** AWS Backup cifra automáticamente las copias de seguridad con la clave KMS de su AWS Backup almacén, en lugar de utilizar la misma clave de cifrado que el recurso fuente. Esto aumenta sus niveles de defensa. Para obtener más información, consulte [Cifrado de copias de seguridad en AWS Backup](#).
- **awsbackup** Nombres de recursos de Amazon (ARNs). Backup ARNs comienza con `arn:aws:backup` en lugar de `arn:aws:source-resource`. Esto le permite crear políticas de acceso que se apliquen específicamente a las copias de seguridad y no a los recursos de origen. Para obtener más información, consulte [Control de acceso](#).
- **Facturación de copias de seguridad centralizada y etiquetas de asignación de costos de Cost Explorer.** Los cargos AWS Backup (incluidos el almacenamiento, las transferencias de datos, las restauraciones y la eliminación anticipada) aparecen en la sección «Backup» de la Amazon Web Services factura, en lugar de aparecer en cada recurso admitido. También puede usar las etiquetas de asignación de costos de Cost Explorer para hacer un seguimiento y optimizar sus costos de copia de seguridad. Para obtener más información, consulte [Medición, costos y facturación de AWS Backup](#).

Para ver qué tipos de recursos son aptos para una AWS Backup administración completa, consulte [Disponibilidad de características por recurso](#).

Monitorización de la actividad de copia de seguridad

AWS Backup proporciona un panel que facilita la auditoría de la actividad de copia de seguridad y restauración en todos AWS los servicios. Con solo unos pocos clics en la AWS Backup consola, puede ver el estado de los trabajos de copia de seguridad recientes. También puede restaurar los trabajos en todos AWS los servicios para garantizar que sus AWS recursos estén debidamente protegidos.

AWS Backup se integra con Amazon CloudWatch y Amazon EventBridge. CloudWatch le permite realizar un seguimiento de las métricas y crear alarmas. EventBridge le permite ver y monitorear AWS Backup los eventos. Para obtener más información, consulte [Supervisión de AWS Backup eventos mediante EventBridge](#) y [Supervisión de AWS Backup métricas con CloudWatch](#).

AWS Backup se integra con AWS CloudTrail. CloudTrail le ofrece una vista consolidada de los registros de actividad de respaldo que permite auditar rápida y fácilmente la forma en que se respaldan sus recursos. AWS Backup también se integra con Amazon Simple Notification Service (Amazon SNS) y le proporciona notificaciones sobre la actividad de las copias de seguridad, como cuando una copia de seguridad se realiza correctamente o se ha iniciado una restauración. Para obtener más información, consulte [Registrar llamadas a la AWS Backup API con CloudTrail Amazon SNS y AWS Backup eventos](#).

Seguridad de los datos en los almacenes de copias de seguridad

El contenido de cada AWS Backup copia de seguridad es inmutable, lo que significa que nadie puede modificarlo. AWS Backup protege aún más sus copias de seguridad en almacenes de copias de seguridad, lo que las separa de forma segura de sus instancias de origen. Por ejemplo, su almacén conservará sus copias de seguridad de Amazon EC2 y Amazon EBS de acuerdo con la política de ciclo de vida que elija, incluso si elimina la EC2 instancia de Amazon de origen y los volúmenes de Amazon EBS.

Los almacenes de copias de seguridad ofrecen cifrado y políticas de acceso basadas en recursos que le permiten definir quién tiene acceso a las copias de seguridad. Puede definir políticas de acceso para un almacén de copias de seguridad que define quién tiene acceso a las copias de seguridad dentro de ese almacén y qué acciones se les permite realizar. Esto proporciona una forma sencilla y segura de controlar el acceso a las copias de seguridad en todos AWS los servicios. Para revisar AWS las políticas administradas por el cliente AWS Backup, consulte [Políticas administradas para AWS Backup](#).

Puedes usar AWS Backup Vault Lock para evitar que cualquier persona (incluido tú) elimine las copias de seguridad o altere su período de retención. AWS Backup Vault Lock te ayuda a reforzar un modelo write-once-read-many(WORM) y a añadir otro nivel de defensa a tu defensa en profundidad. Para empezar, consulte [Bloqueo de almacenes de AWS Backup](#).

Introducción

Para obtener más información AWS Backup, le recomendamos que comience con [Introducción a con \(\) AWS Backup](#).

AWS Recursos y aplicaciones compatibles

Los siguientes son AWS recursos y aplicaciones de terceros de los que puede hacer copias de seguridad y restaurar AWS Backup. Para obtener más información, consulte [the section called “AWS Backup disponibilidad de funciones”](#).

Servicio	Tipos de recursos admitidos
Amazon Elastic Compute Cloud (Amazon EC2)	EC2 Instancias de Amazon respaldadas por volúmenes de Amazon EBS
Amazon Simple Storage Service (Amazon S3)	Datos de Amazon S3
Amazon Elastic Block Store (Amazon EBS)	Volúmenes de Amazon EBS
Amazon DynamoDB	Tablas de Amazon DynamoDB.
Amazon Relational Database Service (Amazon RDS)	Instancias de bases de datos de Amazon RDS (incluidos todos los motores de bases de datos); clústeres de varias zonas de disponibilidad
Amazon Aurora DSQL	Clústeres de una región y de múltiples regiones
Amazon Aurora	Clústeres de Aurora
Amazon Elastic File System (Amazon EFS)	Sistemas de archivos de Amazon EFS

Servicio	Tipos de recursos admitidos
FSx para Lustre	FSx para sistemas de archivos Lustre
FSx para Windows File Server	FSx para sistemas de archivos Windows File Server
Amazon FSx para NetApp ONTAP	FSx para sistemas de archivos ONTAP
Amazon FSx para OpenZFS	FSx para sistemas de archivos OpenZFS
AWS Storage Gateway (Volume Gateway)	AWS Storage Gateway volúmenes
Amazon DocumentDB	Clústeres basados en instancias de Amazon DocumentDB
Amazon Neptune	Clústeres de Amazon Neptune
Amazon Redshift	Clústeres de Amazon Redshift
Amazon Timestream	Tablas de Amazon Timestream
VMware Cloud™ activado AWS	VMware Máquinas virtuales Cloud™ activadas AWS
VMware Cloud™ activado AWS Outposts	VMware Máquinas virtuales Cloud™ activadas AWS Outposts
CloudFormation	CloudFormation pilas
Bases de datos de SAP HANA	Bases de datos SAP HANA en EC2 instancias de Amazon
Amazon Elastic Kubernetes Service (Amazon EKS)	Clústeres de Amazon EKS y copias de seguridad de almacenamiento persistente

Precios

Con AWS Backup, usted paga por el almacenamiento de copias de seguridad, la restauración de datos, las pruebas de restauración, la transferencia de datos entre regiones y AWS Backup Audit Manager. Para obtener más información, consulte [AWS Backup Precios](#).

AWS Backup disponibilidad de funciones

AWS Backup las funciones se ofrecen según el recurso y Región de AWS. Las siguientes secciones y tablas pueden ayudarle a determinar la disponibilidad de las características.

Contenido

- [Características disponibles para todos los recursos compatibles](#)
- [Disponibilidad de características por recurso](#)
- [Disponibilidad de las funciones por Región de AWS](#)
- [Servicios compatibles con Región de AWS](#)

Características disponibles para todos los recursos compatibles

AWS Backup ofrece las siguientes funciones para sus AWS servicios compatibles, así como para las aplicaciones de terceros compatibles. No se debe dar por hecho que una característica o servicio es compatible, a menos que se mencione explícitamente.

- [Programación de copias de seguridad automatizada y administración de la retención](#)
- [Monitorización centralizada de las copias de seguridad](#)
- [Copias de seguridad cifradas](#)
- [Copias de seguridad incrementales](#)
- [Administración de cuentas cruzadas con AWS Organizations](#)
- [Auditorías e informes de respaldo automatizados con AWS Backup Audit Manager](#)
- [Escribe una vez y lee muchas veces \(WORM\) con Vault Lock AWS Backup](#)

Disponibilidad de características por recurso

Para utilizarlo AWS Backup con un AWS servicio compatible en una región determinada, el servicio debe estar disponible en esa región. Para determinar la disponibilidad del servicio en una región, consulte los [puntos de conexión del servicio](#) en la Referencia general de AWS.

Para obtener información sobre las regiones con las que se puede optar por participar y los recursos y características compatibles en ellas, consulte [Disponibilidad de las funciones por Región de AWS](#).

AWS Backup admite	Copia de seguridad entre regiones	Copia de seguridad entre cuentas	AWS Backup Audit Manager	Copia de seguridad incremental	Respuesta y punto-in-time restauración continua	Administración de cumplimiento	Ciclo de vida al almacenamiento en frío	Restauración a nivel de elemento¹	Prueba de restauración	Tener un almacén aislado lógico	Búsqueda de copias de seguridad	Backup por niveles	Protección contra malware
Amazon EC2	✓	✓	✓	✓					✓	✓			✓
Amazon S3	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓
Amazon EBS	✓	✓	✓	✓			✓	✓	✓	✓	✓		✓
Instancia individual de Amazon RDS	✓ ³	✓ ³	✓ ⁴	✓	✓				✓				
Clúster de Amazon	✓ ³	✓ ³	✓ ⁴	✓					✓				

AWS Backup admite	Copia de seguridad entre regiones	Copia de seguridad entre cuentas	AWS Backup Audit Manager	Copia de seguridad incremental	Respaldos y punto-in-time restauración continua	Administración compli	Ciclo de vida al almacenamiento en frío	Restauración a nivel de elemento¹	Pruebas de restauración	Tener un almacén aislado lógico te	Búsqueda de copias de seguridad	Backup por niveles	Protección contra malware
Amazon Aurora	✓ ³	✓ ³	✓	✓ ⁶	✓				✓	✓			
Amazon Aurora DSQL	✓	✓				✓	✓			✓			
Amazon FSx	✓	✓	✓	✓		✓	✓	✓	✓	✓			
FSx para Lustre	✓	✓	✓	✓					✓	✓			
FSx para Windows File Server	✓	✓	✓	✓					✓ ⁸	✓			
FSx para ONTAP			✓ ²	✓					✓				
FSx para Open	✓	✓					✓	✓					

AWS Backup admitido	Copia de seguridad entre regiones	Copia de seguridad entre cuentas	AWS Backup Audit Manager	Copia de seguridad incremental	Respaldos y punto-in-time restauración continua	Administración de cumplimiento	Ciclo de vida al almacenamiento en frío	Restauración a nivel de elemento¹	Pruebas de restauración	Tener un almacén aislado lógicamente	Búsqueda de copias de seguridad	Backup por niveles	Protección contra malware
AWS Storage Gateway	✓	✓	✓	✓						✓			
Amazon DocumentDB	✓ ³	✓ ³							✓	✓			
Amazon Neptune	✓ ³	✓ ³							✓	✓ ⁹			
Amazon Redshift sin servidor								✓					
Amazon TimeStream	✓	✓		✓		✓	✓			✓			
Windows VSS	✓	✓	✓	✓						✓			
Máquina virtual	✓	✓	✓	✓		✓	✓	✓		✓			
AWS CloudFormation	✓ ⁵		✓	✓ ⁵			✓						

AWS Backup admite	Copia de seguridad entre regiones	Copia de seguridad entre cuentas	AWS Backup Audit Manager	Copia de seguridad incremental	Respaldos y punto-in-time restauración continuos	Administración de cumplimiento	Ciclo de vida al almacenamiento en frío	Restauración a nivel de elemento ¹	Pruebas de restauración	Tener un almacén aislado lógico	Búsqueda de copias de seguridad	Backup por niveles	Protección contra malware
Amazon DynamoDB			✓						✓				
DynamoDB con características avanzadas de AWS Backup	✓	✓	✓			✓	✓		✓	✓			
Bases de datos SAP HANA en instancias de Amazon EKS	✓	✓		✓ ⁶	✓	✓	✓						
Amazon EKS	✓	✓				✓		✓					

Algunos tipos de recursos tienen capacidades de copia de seguridad continua y copia entre regiones y entre cuentas. Cuando se realiza una copia entre regiones o entre cuentas de una copia de seguridad continua, el punto de recuperación copiado (copia de seguridad) se convierte en una copia de seguridad de instantánea (periódica). El PITR (Point-in-Time Restore) no está disponible para estas copias.

- Amazon RDS y Amazon S3 admiten la copia entre cuentas y regiones a partir de las copias de seguridad incrementales. Amazon RDS también admite la copia simultánea de instantáneas entre regiones y cuentas en una sola acción.
- EC2 Las instancias de Amazon Aurora y SAP HANA en Amazon admiten copias entre cuentas y regiones a partir de copias de seguridad completas. Amazon Aurora también admite la copia simultánea de instantáneas entre regiones y cuentas en una sola acción.

¹ El “elemento” de una restauración a nivel de elemento varía en función del recurso compatible. Por ejemplo, un elemento del sistema de archivos es un archivo o directorio, mientras que un elemento de S3 es un objeto de S3. Un VMware elemento es un disco. Para obtener más información, consulte la sección [Restauración de una copia de seguridad por tipo de recurso](#) del recurso compatible.

² AWS Backup Audit Manager admite este recurso en todos los controles, excepto en la copia [multicuenta y en la copia interregional](#).

³ Amazon RDS, Aurora, DocumentDB y Neptune ahora admiten la copia de instantáneas entre regiones y cuentas en una sola acción. Las instancias de base de datos de varias zonas de disponibilidad (Multi-AZ) de RDS se pueden copiar, pero los clústeres de Multi-AZ no admiten la copia entre regiones o entre cuentas en estos momentos. Para obtener información adicional, consulte [Consideraciones de copia entre regiones con recursos específicos](#).

⁴ Consulte [Copias de seguridad en varias zonas de disponibilidad de Amazon RDS](#) para ver las regiones compatibles con Backup Audit Manager.

⁵ En las [copias de seguridad CloudFormation apiladas](#), los recursos anidados conservan las características de sus recursos de origen. Sin embargo, los recursos de la pila no conservan la funcionalidad de Point-in-Time restauración (PITR) (como Amazon S3 y Amazon RDS).

⁶ Las instantáneas son completas y se ofrece una copia de seguridad incremental mediante PITR.

⁷ Los sistemas de archivos Multi-AZ (zona de disponibilidad múltiple) de Amazon FSx for OpenZFS solo se pueden restaurar desde la FSx consola de Amazon o desde la solicitud de la API. [createFileSystemFromBackup](#)

⁸. Se admite en una prueba de restauración si el servidor de archivos FSx de Windows utiliza un directorio activo administrado AWS

⁹ No está disponible actualmente en la región de Asia-Pacífico (Yakarta).

Las ¹⁰ características de las copias de seguridad de almacenamiento persistente (por ejemplo, Amazon EBS) incluidas como parte de Amazon EKS Backups reflejarán la compatibilidad de funciones para los tipos de recursos respectivos de esta tabla.

Disponibilidad de las funciones por Región de AWS

AWS Backup está disponible en todo lo siguiente Regiones de AWS. AWS Backup las funciones están disponibles en todas estas regiones, a menos que se indique lo contrario en la siguiente tabla.

Algunas regiones requieren la suscripción a la cuenta, como se indica en la siguiente tabla. La disponibilidad de algunas características depende de si la suscripción es obligatoria o no. Para obtener más información, consulte [Administrar qué Regiones de AWS puede utilizar la cuenta](#) en la Guía de referencia de AWS Account Management .

Consideraciones sobre las regiones con suscripción:

- La copia entre cuentas no es compatible con Amazon DocumentDB en las regiones en las que se requiere suscripción.
- La copia entre regiones no es compatible con Amazon DocumentDB en las regiones en las que se requiere suscripción.
- Actualmente, la copia entre regiones de las copias de seguridad de Neptune solo se admite en las regiones de África (Ciudad del Cabo), Asia-Pacífico (Hong Kong), Asia-Pacífico (Yakarta), Israel (Tel Aviv), Medio Oriente (Baréin) y Medio Oriente (EAU).

Las copias multiregionales FSx de Lustre, FSx Windows File Server, FSx ONTAP y FSx OpenZFS no son compatibles en las regiones en las que se requiere la suscripción.

- La copia multicuenta no es compatible con Neptune y Timestream en las regiones en las que es necesario suscribirse. CloudFormation

Consideraciones y limitaciones a la hora de administrar varias cuentas en las regiones en las que se requiere suscripción:

- La administración multicuenta, en la Regiones de AWS que se requiere la suscripción, incluye el monitoreo multicuenta y el acceso a las políticas de respaldo; las cuentas de administrador delegado pueden implementar políticas pero no tienen acceso a las funciones de monitoreo.
- Se puede optar por utilizar tanto las cuentas de administración como las cuentas secundarias. AWS Organizations Si una cuenta secundaria opta por la administración entre cuentas antes de que la cuenta de administración pase a la administración entre cuentas, habrá un retraso (de hasta 24 horas) hasta que la supervisión entre cuentas muestre los estados de los trabajos en toda la organización.

AWS Backup apoya	Suscripción	Copia de la copia de seguridad entre regiones	Administración entre cuentas	Copia de la copia de seguridad entre cuentas	AWS Backup Panel de control de Audit Manager y trabajos	Pruebas de restauración	Búsqueda de copias de seguridad	Backup por niveles	Protección contra malware
Este de EE. UU. (Norte de Virginia)	No obligatorio	✓	✓	✓	✓	✓	✓	✓	✓
Este de EE. UU. (Ohio)	No se necesita	✓	✓	✓	✓	✓	✓	✓	✓
Oeste de EE. UU. (Norte)	No se necesita	✓	✓	✓	✓	✓	✓	✓	✓

AWS Backup apoya	Suscripción	Copia de la copia de seguridad entre regiones	Administración entre cuentas	Copia de la copia de seguridad entre cuentas	AWS Backup Panel de control de Audit Manager y trabajos	Pruebas de restauración	Búsqueda de copias de seguridad	Backup por niveles	Protección contra malware
de California)									
Oeste de EE. UU. (Oregón)	No se necesita	✓	✓	✓	✓	✓	✓	✓	✓
África (Ciudad del Cabo)	Obligatorio	✓	✓	✓	✓	✓	✓	✓	✓
Asia-Pacífico (Hong Kong)	Obligatorio	✓	✓	✓	✓	✓	✓	✓	✓
Asia-Pacífico (Hyderabad)	Obligatorio	✓	✓	✓	✓	✓	✓	✓	✓

AWS Backup apoya	Suscripción	Copia de la copia de seguridad entre regiones	Administración entre cuentas	Copia de la copia de seguridad entre cuentas	AWS Backup Panel de control de Audit Manager y trabajos	Pruebas de restauración	Búsqueda de copias de seguridad	Backup por niveles	Protección contra malware
Asia-Pacífico (Yakarta)	Obligatorio	✓	✓	✓	✓	✓	✓	✓	✓
Asia-Pacífico (Malasia)	Obligatorio	✓	✓	✓			✓	✓	✓
Asia-Pacífico (Melbourne)	Obligatorio	✓	✓	✓	✓	✓	✓	✓	✓
Asia-Pacífico (Bombay)	No obligatorio	✓	✓	✓	✓	✓	✓	✓	✓
Asia-Pacífico (Nueva Zelanda)	Obligatorio	✓		✓				✓	

AWS Backup apoya	Suscripción	Copia de la copia de seguridad entre regiones	Administración entre cuentas	Copia de la copia de seguridad entre cuentas	AWS Backup Panel de control de Audit Manager y trabajos	Pruebas de restauración	Búsqueda de copias de seguridad	Backup por niveles	Protección contra malware
Asia-Pacífico (Osaka)	No se necesita	✓	✓	✓	✓	✓	✓	✓	✓
Asia-Pacífico (Seúl)	No se necesita	✓	✓	✓	✓	✓	✓	✓	✓
Asia-Pacífico (Singapur)	No se necesita	✓	✓	✓	✓	✓	✓	✓	✓
Asia-Pacífico (Sídney)	No obligatorio	✓	✓	✓	✓	✓	✓	✓	✓
Asia-Pacífico (Taipéi)	Obligatorio	✓		✓				✓	✓

AWS Backup apoya	Suscripción	Copia de la copia de seguridad entre regiones	Administración entre cuentas	Copia de la copia de seguridad entre cuentas	AWS Backup Panel de control de Audit Manager y trabajos	Pruebas de restauración	Búsqueda de copias de seguridad	Backup por niveles	Protección contra malware
Asia-Pacífico (Tailandia)	Obligatorio	✓		✓			✓	✓	✓
Asia-Pacífico (Tokio)	No se necesita	✓	✓	✓	✓	✓	✓	✓	✓
Canadá (centro)	No obligatorio	✓	✓	✓	✓	✓	✓	✓	✓
Oeste de Canadá (Calgary)	Obligatorio	✓	✓	✓			✓	✓	✓
China (Pekín)	AWS en China	✓ ²						✓	
China (Ningxia)	AWS en China	✓ ²						✓	

AWS Backup apoya	Suscripción	Copia de la copia de seguridad entre regiones	Administración entre cuentas	Copia de la copia de seguridad entre cuentas	AWS Backup Panel de control de Audit Manager y trabajos	Pruebas de restauración	Búsqueda de copias de seguridad	Backup por niveles	Protección contra malware
Europa (Fráncfort)	No se necesita	✓	✓	✓	✓	✓	✓	✓	✓
Europa (Irlanda)	No se necesita	✓	✓	✓	✓	✓	✓	✓	✓
Europa (Londres)	No se necesita	✓	✓	✓	✓	✓	✓	✓	✓
Europa (Milán)	Obligatorio	✓	✓	✓	✓	✓	✓	✓	✓
Europa (París)	No obligatorio	✓	✓	✓	✓	✓	✓	✓	✓
Europa (España)	Obligatorio	✓	✓	✓	✓	✓	✓	✓	✓
Europa (Estocolmo)	No obligatorio	✓	✓	✓	✓	✓	✓	✓	✓
Europa (Zúrich)	Obligatorio	✓	✓	✓	✓	✓	✓	✓	✓

AWS Backup apoya	Suscripción	Copia de la copia de seguridad entre regiones	Administración entre cuentas	Copia de la copia de seguridad entre cuentas	AWS Backup Panel de control de Audit Manager y trabajos	Pruebas de restauración	Búsqueda de copias de seguridad	Backup por niveles	Protección contra malware
Israel (Tel Aviv)	Obligatorio	✓	✓	✓			✓	✓	✓
México (centro)	Obligatorio	✓		✓			✓	✓	✓
Middle East (Bahrain)	Obligatorio	✓	✓	✓	✓	✓	✓	✓	✓
Medio Oriente (EAU)	Obligatorio	✓	✓	✓	✓	✓	✓	✓	✓
América del Sur (São Paulo)	No obligatorio	✓	✓	✓	✓	✓	✓	✓	✓
AWS GovCloud (Este de EE. UU.)	AWS GovCloud (US)	✓	✓	✓ ⁴	✓ ³		✓	✓	✓

AWS Backup apoya	Suscripción	Copia de la copia de seguridad entre regiones	Administración entre cuentas	Copia de la copia de seguridad entre cuentas	AWS Backup Panel de control de Audit Manager y trabajos	Pruebas de restauración	Búsqueda de copias de seguridad	Backup por niveles	Protección contra malware
AWS GovCloud (Estados Unidos-Oeste)	AWS GovCloud (US)	✓	✓	✓ ⁴	✓ ³		✓	✓	✓

¹ La copia entre regiones y cuentas para una bóveda con huecos lógicos no está disponible actualmente en las regiones Canadá Oeste (Calgary), China (Pekín), China (Ningxia), (EE. UU. este) o (EE. UU. Oeste). AWS GovCloud AWS GovCloud

² China (Pekín) y China (Ningxia) admiten copias entre regiones de una de estas dos regiones a la otra. No se admite la copia entre regiones desde estas regiones a otras regiones o a estas regiones. No se admite la copia entre cuentas para estas regiones.

El panel de ³ empleos y los informes organizativos de AWS Backup Audit Manager no están disponibles en AWS GovCloud (EE. UU. Este) ni AWS GovCloud (EE. UU. Oeste). La agregación del panel de empleos solo está disponible en las regiones que admiten la administración multicuenta y AWS Backup Audit Manager.

⁴ AWS GovCloud (EE. UU. Este) y AWS GovCloud (EE. UU. Oeste) admiten la copia transregional de una de estas dos regiones a la otra. No se admite la copia entre regiones desde estas regiones a otras regiones ni desde otras regiones a estas regiones.

Servicios compatibles con Región de AWS

AWS Backup está disponible para estos tipos de recursos en todas las regiones en las que opera el recurso de la lista AWS Backup y en las que opera:

- Aurora
- AWS CloudFormation
- Amazon DocumentDB
- DynamoDB
- DynamoDB con funciones avanzadas AWS Backup
- Amazon EBS
- Amazon EC2
- Amazon EFS
- Amazon Redshift
- Amazon RDS

AWS Backup La compatibilidad con Amazon Neptune está disponible en la mayoría de las regiones comerciales en las que se admite Neptune. Las copias de seguridad y las restauraciones no están disponibles actualmente en la región de Europa (España).

AWS Backup La compatibilidad con Amazon DocumentDB no está disponible en África (Ciudad del Cabo), Asia Pacífico (Hong Kong), Israel (Tel Aviv) o AWS GovCloud (EE. UU. Este).

En la siguiente tabla se indica la AWS Backup compatibilidad con otros AWS servicios por región:

Usuarios y regiones	Aurora SQL	Amazon FSx	SAP HANA en instancias EC2	Amazon S3	Storage Gateway	Amazon Timestream	VMware Backup Gateway	Amazon EKS
Este de EE. UU. (Norte de Virginia)	✓	✓	✓	✓	✓	✓	✓	✓
Este de EE. UU. (Ohio)	✓	✓	✓	✓	✓	✓	✓	✓

Usuarios y regiones	Aurora SQL	Amazon FSx	SAP HANA en instancias EC2	Amazon S3	Storage Gateway	Amazon Timestream	VMware Backup Gateway	Amazon EKS
Oeste de EE. UU. (Norte de California)		✓	✓	✓	✓		✓	✓
Oeste de EE. UU. (Oregón)	✓	✓	✓	✓	✓	✓	✓	✓
África (Ciudad del Cabo)		✓	✓	✓	✓		✓	✓
Asia-Pacífico (Hong Kong)		✓	✓	✓	✓		✓	✓
Asia-Pacífico (Hyderabad)		✓		✓	✓			✓
Asia-Pacífico (Yakarta)		✓		✓	✓			✓

Usuarios y regiones	Aurora SQL	Amazon FSx	SAP HANA en instancias EC2	Amazon S3	Storage Gateway	Amazon Timestream	VMware Backup Gateway	Amazon EKS
Asia-Pacífico (Malasia)				✓				✓
Asia-Pacífico (Melbourne)		Windows; Lustre; ONTAP		✓	✓			✓
Asia-Pacífico (Mumbai)		✓	✓	✓	✓	✓	✓	✓
Asia-Pacífico (Nueva Zelanda)				✓				✓
Asia-Pacífico (Osaka)	✓	✓	✓	✓	✓		✓	✓
Asia-Pacífico (Seúl)	✓	✓	✓	✓	✓		✓	✓
Asia-Pacífico (Singapur)		✓	✓	✓	✓		✓	✓

Usuarios y regiones	Aurora SQL	Amazon FSx	SAP HANA en instancias EC2	Amazon S3	Storage Gateway	Amazon Timestream	VMware Backup Gateway	Amazon EKS
Asia-Pacífico (Sídney)		✓	✓	✓	✓	✓	✓	✓
Asia-Pacífico (Taipéi)				✓				✓
Asia-Pacífico (Tailandia)				✓				✓
Asia-Pacífico (Tokio)	✓	✓	✓	✓	✓	✓	✓	✓
Canadá (centro)		✓	✓	✓	✓		✓	✓
Oeste de Canadá (Calgary)				✓				✓
China (Pekín)		Windows; Lustre		✓ ¹	✓			
China (Ningxia)		Windows; Lustre		✓ ¹	✓			

Usuarios y regiones	Aurora SQL	Amazon FSx	SAP HANA en instancias EC2	Amazon S3	Storage Gateway	Amazon Timestream	VMware Backup Gateway	Amazon EKS
Europa (Fráncfort)	✓	✓	✓	✓	✓	✓	✓	✓
Europa (Irlanda)	✓	✓	✓	✓	✓	✓	✓	✓
Europa (Londres)	✓	✓	✓	✓	✓		✓	✓
Europa (Milán)		✓	✓	✓	✓		✓	✓
Europa (París)	✓	✓	✓	✓	✓		✓	✓
Europa (España)		✓		✓	✓			✓
Europa (Estocolmo)		✓	✓	✓	✓		✓	✓
Europa (Zúrich)		✓		✓	✓			✓
Israel (Tel Aviv)		✓		✓	✓			✓
México (centro)				✓				✓

Usuarios y regiones	Aurora SQL	Amazon FSx	SAP HANA en instancias EC2	Amazon S3	Storage Gateway	Amazon Timestream	VMware Backup Gateway	Amazon EKS
Middle East (Bahrain)		✓	✓	✓	✓		✓	✓
Medio Oriente (EAU)		✓		✓	✓			✓
América del Sur (São Paulo)		✓	✓	✓	✓		✓	✓
AWS GovCloud (EE. UU.- Oeste)		Windows; Lustre; ONTAP		✓	✓	✓	✓	✓
AWS GovCloud (EE. UU.- Este)		Windows; Lustre; ONTAP		✓	✓		✓	✓

Una marca en Amazon FSx indica que FSx Windows File Server, FSx Lustre, FSx ONTAP y FSx OpenZFS son compatibles en esa región AWS Backup; de lo contrario, aparecerán en la lista las configuraciones compatibles.

¹ No se admite la copia entre cuentas.

AWS Backup: Cómo funciona

AWS Backup es un servicio de respaldo totalmente administrado que facilita la centralización y la automatización del respaldo de los datos en todos los AWS servicios. Con él AWS Backup, puede crear políticas de respaldo denominadas planes de respaldo. Puede utilizar estos planes para definir los requisitos de copia de seguridad, como la frecuencia con la que se va a realizar la copia de seguridad de los datos y el tiempo durante el que se van a conservar esas copias de seguridad.

AWS Backup le permite aplicar planes de respaldo a sus AWS recursos simplemente etiquetándolos. AWS Backup a continuación, realiza automáticamente una copia de seguridad de sus AWS recursos de acuerdo con el plan de copia de seguridad que haya definido.

En las siguientes secciones se describe cómo AWS Backup funciona, los detalles de su implementación y las consideraciones de seguridad.

Temas

- [¿Cómo AWS Backup funciona con AWS los servicios compatibles](#)
- [Medición, costos y facturación de AWS Backup](#)
- [AWS Backup blogs, vídeos, tutoriales y otros recursos](#)

¿Cómo AWS Backup funciona con AWS los servicios compatibles

Algunos AWS servicios AWS Backup compatibles ofrecen sus propias funciones de copia de seguridad independientes. Esas características están disponibles independientemente de si utiliza AWS Backup. Sin embargo, las copias de seguridad que crean otros AWS servicios no están disponibles para el gobierno central. AWS Backup

AWS Backup Para configurar la gestión centralizada de la protección de datos de todos los servicios compatibles, debe optar por gestionar ese servicio AWS Backup, crear una copia de seguridad a pedido o programar copias de seguridad mediante un plan de copias de seguridad y almacenar las copias de seguridad en bóvedas de copias de seguridad.

Consulte [Asignación de recursos](#) para obtener información sobre cómo elegir los servicios (tipos de recurso) de los que desea hacer una copia de seguridad.

Temas

- [Uso de datos de Amazon S3](#)
- [Trabajando con máquinas VMware virtuales](#)
- [Uso de Amazon DynamoDB](#)
- [Trabajar con los sistemas de FSx archivos de Amazon](#)
- [Trabajando con Amazon EC2](#)
- [Uso de Amazon EFS](#)
- [Uso de Amazon EBS](#)
- [Uso de Amazon RDS Y Aurora](#)
- [Uso de Aurora DSQL](#)
- [Trabajando con AWS BackInt](#)
- [Trabajando con AWS Storage Gateway](#)
- [Uso de Amazon DocumentDB](#)
- [Uso de Amazon Neptune](#)
- [Uso de Amazon Redshift y Amazon Redshift sin servidor](#)
- [Uso de Amazon Timestream](#)
- [Trabajando con AWS Organizations](#)
- [Trabajando con CloudFormation](#)
- [Trabajando con AWS BackInt, AWS Systems Manager para SAP y SAP HANA](#)
- [Trabajar con Amazon EKS](#)
- [Trabajando con Amazon GuardDuty](#)
- [¿Cómo AWS hacen los servicios copias de seguridad de sus propios recursos](#)

Uso de datos de Amazon S3

AWS Backup ofrece copias de seguridad y restauración totalmente gestionadas para las copias de seguridad de Amazon S3. Para obtener más información, consulte [Copias de seguridad de Amazon S3](#).

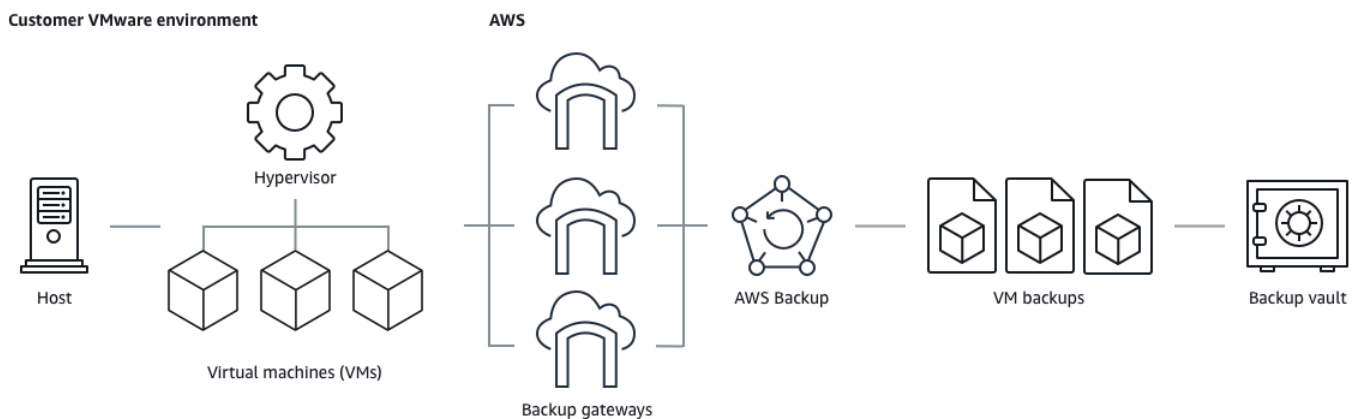
- Cómo hacer copias de seguridad de los recursos: [Introducción a con \(\) AWS Backup](#)
- Cómo restaurar los datos de Amazon S3 mediante AWS Backup: [Restaure los datos de S3 mediante AWS Backup](#)

Para obtener información detallada acerca de S3, consulte la [Documentación de Amazon S3](#).

Trabajando con máquinas VMware virtuales

AWS Backup admite la protección de datos centralizada y automatizada para las máquinas VMware virtuales locales (VMs) y también VMs en la VMware nube™ (VMC). AWS Puede realizar copias de seguridad desde sus máquinas virtuales locales y de VMC hasta. AWS Backup A continuación, puede realizar la restauración desde AWS Backup una ubicación local o desde VMC.

Backup Gateway es un AWS Backup software descargable que puede implementar en su VMware infraestructura para conectarse VMware VMs a ella AWS Backup. La puerta de enlace se conecta a su servidor de administración de máquinas virtuales para VMs detectarlos, cifrarlos y transferirlos de manera eficiente. AWS Backup El siguiente diagrama ilustra cómo Backup Gateway se conecta a su VMs:



- Cómo hacer copias de seguridad de los recursos: [Copias de seguridad de máquinas virtuales](#)
- Cómo restaurar los recursos de la máquina virtual: [Restaurar una máquina virtual mediante AWS Backup](#)

Uso de Amazon DynamoDB

AWS Backup admite la creación de copias de seguridad y la restauración de tablas de Amazon DynamoDB. DynamoDB es un servicio de bases de datos NoSQL completamente administrado que proporciona un rendimiento rápido y predecible, así como una perfecta escalabilidad.

Desde su lanzamiento, siempre AWS Backup ha sido compatible con DynamoDB. A partir de noviembre de 2021, AWS Backup también se introdujeron funciones avanzadas para las copias

de seguridad de DynamoDB. Estas funciones avanzadas incluyen copiar las copias de seguridad entre cuentas Regiones de AWS y cuentas, organizar las copias de seguridad en niveles para almacenarlas en frío y utilizar etiquetas para gestionar los permisos y los costes.

AWS Backup Los nuevos clientes que se incorporen después de noviembre de 2021 tendrán las funciones avanzadas de copia de seguridad de DynamoDB habilitadas de forma predeterminada.

Recomendamos a todos los AWS Backup clientes actuales que habiliten las funciones avanzadas de DynamoDB. No hay diferencia en los precios del almacenamiento de copias de seguridad en caliente después de habilitar las características avanzadas, y puede ahorrar dinero al organizar las copias de seguridad en niveles en el almacenamiento en frío y optimizar sus costos mediante el uso de etiquetas de asignación de costos.

Para obtener una lista completa de las características avanzadas y cómo habilitarlas, consulte [Copia de seguridad avanzada de DynamoDB](#).

- Cómo hacer copias de seguridad de los recursos: [Introducción a con \(\) AWS Backup](#)
- Cómo restaurar los recursos de DynamoDB: [Restauración de una tabla de Amazon DynamoDB](#)

Para obtener información detallada acerca de DynamoDB, consulte [¿Qué es Amazon DynamoDB?](#) en la Guía para desarrolladores de Amazon DynamoDB.

Trabajar con los sistemas de FSx archivos de Amazon

AWS Backup admite la creación de copias de seguridad y la restauración de los sistemas de FSx archivos de Amazon. Amazon FSx proporciona sistemas de archivos de terceros totalmente gestionados con la compatibilidad nativa y los conjuntos de funciones para las cargas de trabajo. AWS Backup utiliza la función de copia de seguridad integrada de Amazon FSx. Por lo tanto, las copias de seguridad tomadas desde la AWS Backup consola tienen el mismo nivel de consistencia y rendimiento del sistema de archivos, y las mismas opciones de restauración que las copias de seguridad que se realizan a través de la FSx consola de Amazon.

Si se utilizan AWS Backup para gestionar estas copias de seguridad, se obtienen funciones adicionales, como opciones de retención ilimitadas y la posibilidad de crear copias de seguridad programadas con una frecuencia de hasta una hora. Además, AWS Backup conserva las copias de seguridad incluso después de eliminar el sistema de archivos de origen. Esto protege contra la eliminación accidental o malintencionada.

Úselo AWS Backup para proteger los sistemas de FSx archivos de Amazon si desea configurar políticas de respaldo y monitorear las tareas de respaldo desde una consola de respaldo central que también amplía el soporte para otros AWS servicios.

- Cómo hacer copias de seguridad de los recursos: [Introducción a con \(\) AWS Backup](#)
- Cómo restaurar los FSx recursos de Amazon: [Restaura un sistema FSx de archivos](#)

Para obtener información detallada sobre los sistemas de FSx archivos de Amazon, consulta la [FSx documentación de Amazon](#).

Trabajando con Amazon EC2

AWS Backup admite EC2 instancias de Amazon.

- Cómo hacer copias de seguridad de los recursos: [Introducción a con \(\) AWS Backup](#)
- Cómo restaurar los EC2 recursos de Amazon: [Restaurar una EC2 instancia de Amazon](#)

Puede programar o realizar trabajos de backup bajo demanda que incluyan EC2 instancias completas, incluidos sus volúmenes de Amazon EBS. Por lo tanto, puedes restaurar una EC2 instancia de Amazon completa desde un único punto de recuperación, incluidos el volumen raíz, los volúmenes de datos y algunos ajustes de configuración de la instancia, como el tipo de instancia y el key pair.

También puede hacer copias de seguridad y restaurar las aplicaciones de Microsoft Windows habilitadas para VSS. Puede programar copias de seguridad coherentes con las aplicación, definir políticas de ciclo de vida y realizar restauraciones coherentes como parte de una copia de seguridad bajo demanda o de un plan de copia de seguridad programada. Para obtener más información, consulte [Creación de copias de seguridad de Windows VSS](#).

AWS Backup no reinicia EC2 las instancias en ningún momento.

Imágenes e instantáneas

Al hacer una copia de seguridad de una EC2 instancia de Amazon, AWS Backup toma una instantánea del volumen de almacenamiento raíz de Amazon EBS, las configuraciones de lanzamiento y todos los volúmenes de EBS asociados. AWS Backup almacena determinados parámetros de configuración de la EC2 instancia, como el tipo de instancia, los grupos de seguridad, Amazon VPC, la configuración de supervisión y las etiquetas. Los datos de copia de seguridad se

almacenan como una Imagen de máquina de Amazon (AMI) respaldada por un volumen de Amazon EBS.

Si la instancia se lanzó desde una AMI desde AWS Marketplace, la instancia tiene un código de producto. Una AMI creada a partir de una instancia también tiene un código de producto. Con Amazon EC2, no puedes copiar una AMI con un código de producto a otra cuenta. Por lo tanto, AWS Backup también tiene esta restricción.

Si elimina una imagen de máquina de Amazon (AMI) o una instantánea de Amazon EBS gestionada por AWS Backup mediante AWS Backup y tiene configurada la EC2 papelera de reciclaje de Amazon, la imagen o la instantánea podrían incurrir en cargos según la política de EC2 papelera de reciclaje de Amazon. Las instantáneas e imágenes de la papelera de EC2 reciclaje de Amazon ya no están gestionadas ni serán gestionadas por AWS Backup las políticas si las restauras desde la papelera de reciclaje. AWS Backup

AWS Backup Las instantáneas de Amazon EBS gestionadas y las instantáneas asociadas a una EC2 AMI de AWS Backup Amazon gestionada que tengan aplicado el bloqueo de instantáneas de Amazon EBS no se pueden eliminar como parte del ciclo de vida del punto de recuperación si la duración del bloqueo de instantáneas supera el ciclo de vida de la copia de seguridad. Por el contrario, estos puntos de recuperación tendrán el estado de EXPIRED. Estos puntos de recuperación se pueden [eliminar manualmente](#) si decide eliminar primero el bloqueo de instantáneas de Amazon EBS.

AWS Backup puede cifrar las instantáneas de EBS asociadas a una copia de seguridad de Amazon. EC2 Esto es similar a cómo cifra las instantáneas de EBS. AWS Backup utiliza el mismo cifrado aplicado a los volúmenes de EBS subyacentes al crear una instantánea de la Amazon EC2 AMI, y los parámetros de configuración de la instancia original se conservan en los metadatos de restauración.

Una instantánea obtiene su cifrado del volumen, y el mismo cifrado se aplica a las instantáneas correspondientes. Las instantáneas que EBS realiza de una AMI copiada siempre se cifran. Si especifica una clave de KMS durante la copia, se aplicará la clave especificada. Si no utiliza una clave de KMS, se aplicará una clave de KMS predeterminada.

Para obtener más información, consulte [EC2 las instancias de Amazon](#) en la Guía del EC2 usuario de Amazon y el [cifrado de Amazon EBS](#) en la Guía del usuario de Amazon EBS.

Uso de Amazon EFS

AWS Backup es compatible con Amazon Elastic File System (Amazon EFS).

- Cómo hacer copias de seguridad de los recursos: [Introducción a con \(\) AWS Backup](#)
- Cómo restaurar los recursos de Amazon EFS: [Restauración de un sistema de archivos de Amazon EFS](#)

El almacén de copias de seguridad automáticas de Amazon EFS `aws/efs/automatic-backup-vault` está reservado únicamente para esas copias de seguridad automáticas.

Este almacén no debe utilizarse para crear copias entre cuentas ni como destino de las copias de seguridad creadas por otros planes de copia de seguridad no automatizados. Si lo usa como destino para otros planes de copia de seguridad, recibirá un mensaje de error indicando que no tiene suficientes privilegios.

Para obtener información detallada acerca de los sistemas de archivos de Amazon EFS, consulte [What is Amazon Elastic File System?](#) en la Guía del usuario de Amazon Elastic File System.

Uso de Amazon EBS

AWS Backup admite volúmenes de Amazon Elastic Block Store (Amazon EBS).

AWS Backup Las instantáneas de Amazon EBS gestionadas y las instantáneas asociadas a una EC2 AMI de AWS Backup Amazon gestionada que tengan aplicado el bloqueo de instantáneas de Amazon EBS no se pueden eliminar como parte del ciclo de vida del punto de recuperación si la duración del bloqueo de instantáneas supera el ciclo de vida de la copia de seguridad. Por el contrario, estos puntos de recuperación tendrán el estado de EXPIRED. Estos puntos de recuperación se pueden [eliminar manualmente](#) si decide eliminar primero el bloqueo de instantáneas de Amazon EBS.

- Cómo hacer copias de seguridad de los recursos: [Introducción a con \(\) AWS Backup](#)
- Cómo restaurar los volúmenes de Amazon EBS: [Restauración de un volumen de Amazon EBS](#)

También puede obtener más información en el siguiente tutorial: [Amazon EBS Backup and Restore Using AWS Backup](#).

Para obtener más información, consulte [Amazon EBS volumes](#) en la Guía del usuario de Amazon EBS.

Uso de Amazon RDS Y Aurora

AWS Backup es compatible con los motores de bases de datos de Amazon RDS y los clústeres Aurora.

- Cómo hacer copias de seguridad de los recursos: [Introducción a con \(\) AWS Backup](#)
- [Copias de seguridad de Amazon Relational Database Service](#)
- Cómo restaurar los recursos de Amazon RDS: [Restauración de una base de datos de RDS](#)
- Cómo restaurar los clústeres de Aurora: [Restauración de un clúster de Amazon Aurora](#)

También puede obtener información consultando la siguiente guía práctica: [Copias de seguridad y restauración de Amazon RDS AWS Backup](#)

Para obtener más información acerca de Amazon RDS, consulte [¿Qué es Amazon Relational Database Service?](#) en la Guía del usuario de Amazon RDS.

Para obtener información detallada acerca de Aurora, consulte [¿Qué es Amazon Aurora?](#) en la Guía del usuario de Amazon Aurora.

Si inicia un trabajo de copia de seguridad desde la consola de Amazon RDS, esto puede entrar en conflicto con un trabajo de copia de seguridad de un clúster de Aurora y provocar el error El trabajo de copia de seguridad venció antes de completarse. Si ocurre esto, configure un intervalo de copia de seguridad más largo en AWS Backup.

AWS no cobra por las instantáneas de Aurora almacenadas en un almacén de copias de seguridad siempre que Aurora tenga habilitadas las copias de seguridad automatizadas y el período de retención de las copias de seguridad automatizadas de Aurora sea superior al período de retención de las instantáneas de Aurora. Si se elimina la base de datos de las instantáneas, se cobrará a todas las instantáneas que se encuentren en el almacén de copias de seguridad (las eliminaciones pueden producirse accidentalmente o durante la implementación). blue/green

Las instantáneas de gran tamaño y las copias de seguridad frecuentes de una base de datos eliminada podrían conllevar gastos de almacenamiento significativos. Visite la [calculadora de AWS Backup](#) para estimar los posibles cargos de AWS Backup .

Uso de Aurora DSQL

AWS Backup admite clústeres Aurora DSQL para operaciones centralizadas de backup y restauración. Aurora DSQL es una base de datos SQL distribuida y sin servidor que proporciona

transacciones ACID con una sólida coherencia y aislamiento de instantáneas en múltiples Regiones de AWS.

Aurora DSQL admite configuraciones de clústeres de una sola región y multirregionales. Los clústeres multirregionales incluyen regiones de clústeres vinculadas que gestionan las operaciones de lectura y escritura, pero también regiones testigo que participan de forma consensuada sin atender el tráfico de los clientes.

- Cómo hacer copias de seguridad de los recursos: [Introducción a con \(\) AWS Backup](#)
- Cómo restaurar los clústeres de Aurora DSQL: [Restauración de Amazon Aurora DSQL](#)

Para obtener información detallada acerca de Aurora DSQL, consulte [¿Qué es Aurora DSQL?](#) en la Guía del usuario de Aurora DSQL.

Al realizar copias de seguridad de clústeres Aurora DSQL multirregionales, AWS Backup coordina las operaciones de copia de seguridad en todas las regiones de clústeres vinculadas y, al mismo tiempo, aprovecha las regiones testigo para garantizar la coherencia de las transacciones. Esto garantiza que la copia de seguridad capture un estado uniforme en todo el sistema de bases de datos distribuidas.

Trabajando con AWS BackInt

AWS Backup funciona con AWS Backint para respaldar y restaurar bases de datos de SAP HANA en EC2 instancias de Amazon.

- Instrucciones para hacer copias de seguridad y restaurar los recursos de SAP HANA: [copia de seguridad y restauración de SAP HANA Amazon EC2 Instances](#)
- Configurar AWS Backint Agent [AWS : Backint Agent para SAP HANA](#)

Trabajando con AWS Storage Gateway

AWS Backup es compatible con Storage Gateway Volume Gateway. También puede restaurar las instantáneas de Amazon EBS como volúmenes de Storage Gateway.

- Cómo hacer copias de seguridad de los recursos: [Introducción a con \(\) AWS Backup](#)
- Cómo restaurar los recursos de Storage Gateway: [Restauración de un volumen de Storage Gateway](#).

Uso de Amazon DocumentDB

AWS Backup admite clústeres de Amazon DocumentDB.

- Cómo hacer copias de seguridad de los recursos: [Introducción a con \(\) AWS Backup](#)
- Cómo restaurar los recursos de Amazon DocumentDB: [Restauración de un clúster de DocumentDB](#)

Uso de Amazon Neptune

AWS Backup es compatible con los clústeres de Amazon Neptune.

- Cómo hacer copias de seguridad de los recursos: [Introducción a con \(\) AWS Backup](#)
- Cómo restaurar los clústeres de Amazon Neptune: [Restauración de un clúster de Neptune](#).

Uso de Amazon Redshift y Amazon Redshift sin servidor

AWS Backup admite los clústeres aprovisionados de Amazon Redshift y los espacios de nombres de Redshift Serverless.

- Cómo [realizar copias de seguridad de clústeres aprovisionados de Amazon Redshift](#).
- Cómo [realizar copias de seguridad de almacenes de datos de Redshift sin servidor](#).
- Cómo [restaurar Amazon Redshift](#).
- Cómo [restaurar Redshift sin servidor](#).

Uso de Amazon Timestream

AWS Backup es compatible con las tablas Amazon Timestream.

- Cómo hacer [copias de seguridad de las tablas de Timestream](#).
- Cómo [restaurar las tablas de Timestream](#).

Trabajando con AWS Organizations

AWS Backup funciona con AWS Organizations para simplificar el monitoreo y la administración entre cuentas.

- [Cree una cuenta de administración en Organizations.](#)
- Active la [administración entre cuentas.](#)
- Diseñe [cuentas de administrador delegado y delegue políticas.](#)

Trabajando con CloudFormation

AWS Backup CloudFormation plantillas de soporte y pilas de aplicaciones

- [CloudFormation apile copias de seguridad](#)

Trabajando con AWS BackInt, AWS Systems Manager para SAP y SAP HANA

AWS Backup trabaja con AWS BackInt y con SSM para SAP para dar soporte a las funciones de backup y restauración de SAP HANA.

- [Respaldo de bases de datos de SAP HANA en EC2 instancias de Amazon](#)
- [Comience con AWS Systems Manager SAP](#)
- [AWS Backint Agent para SAP HANA](#)

Trabajar con Amazon EKS

AWS Backup admite copias de seguridad de los clústeres de Amazon EKS, incluido el estado del clúster de Kubernetes y el almacenamiento persistente adjunto al clúster de EKS mediante una declaración de volumen persistente (volúmenes de EBS, sistemas de archivos EFS y buckets de S3).

Una copia de seguridad de Amazon EKS creará un punto de recuperación compuesto, en el que habrá un punto de recuperación secundario para cada recurso del que se haga una copia de seguridad.

- Cómo hacer copias de seguridad de los recursos: [Introducción a con \(\) AWS Backup](#)
- Cómo hacer copias de seguridad de los clústeres de Amazon EKS: [Copias de seguridad de Amazon EKS](#)
- Cómo restaurar los clústeres de Amazon EKS: [Restaurar un clúster de Amazon EKS](#)

Para obtener información detallada sobre Amazon EKS, consulte [¿Qué es Amazon EKS?](#) en la Guía del usuario de Amazon EKS.

Trabajando con Amazon GuardDuty

AWS Backup se integra con Amazon GuardDuty para proporcionar un escaneo automatizado de malware de sus puntos de recuperación. Esta integración le ayuda a detectar posibles programas maliciosos en sus copias de seguridad EC2, las de EBS y las de S3.

- Escaneo automatizado: configure planes de respaldo para escanear automáticamente los puntos de recuperación a medida que se crean
- Escaneo bajo demanda: inicie manualmente los escaneos de puntos de recuperación específicos mediante la StartScanJob API
- Escaneo incremental: escanee solo los datos modificados desde el último escaneo para reducir los costos
- Resultados del escaneo: vea el estado y los resultados del escaneo en la AWS Backup consola y APIs

Para habilitar el análisis de malware, debe configurar las funciones de IAM que le GuardDuty permitan leer los puntos de recuperación e AWS Backup iniciar los escaneos. Para obtener más información, consulte [the section called “Políticas administradas”](#).

¿Cómo AWS hacen los servicios copias de seguridad de sus propios recursos

Puede consultar la documentación técnica del proceso de copia de seguridad y restauración de un AWS servicio específico, especialmente si, durante una restauración, necesita configurar una nueva instancia de ese AWS servicio. A continuación se muestra una lista de la documentación:

- [Servicios EC2 relacionados con Amazon](#)
- [Uso AWS Backup con Amazon EFS](#)
- [Backup y restauración para DynamoDB](#)
- [Instantáneas de Amazon EBS](#)
- [Copia de seguridad y restauración de instancias de base de datos de Amazon RDS](#)
 - [Información general de copias de seguridad y restauración de un clúster de base de datos de Aurora](#)

- [Se utiliza AWS Backup con el servidor FSx de archivos de Windows](#)
- [AWS Backup Utilizándolo con FSx for Lustre](#)
- [Haciendo copias de seguridad de sus volúmenes](#)
- [Backing Up and Restoring in Amazon DocumentDB](#)
- [Backing Up and Restoring an Amazon Neptune Cluster](#)

Medición, costos y facturación de AWS Backup

AWS Backup precios

AWS Backup Los precios actuales están disponibles en [AWS Backup los precios](#).

Important

Para evitar cargos adicionales, configure su política de retención con una duración de almacenamiento en caliente de al menos una semana.

Por ejemplo, supongamos que realiza copias de seguridad diarias y las retiene durante un día. Además, suponga que sus recursos protegidos son tan grandes que se tarda todo el día en completar la copia de seguridad. AWS Backup implementa el período de retención de un día y retira la copia de seguridad del almacenamiento en caliente cuando finaliza la tarea de copia de seguridad. Al día siguiente, AWS Backup no puede crear una copia de seguridad incremental porque no tiene ninguna copia de seguridad en almacenamiento caliente. Dado que este periodo de retención no siguió las prácticas recomendadas, corre el riesgo y los gastos de crear una copia de seguridad completa todos los días.

Póngase en contacto con nosotros AWS Support para obtener más ayuda.

AWS Backup facturación

Cuando un tipo de recurso admite la AWS Backup administración completa, los cargos por AWS Backup actividad (incluidos el almacenamiento, las transferencias de datos, las restauraciones y la eliminación anticipada) aparecen en la sección «Backup» de la Amazon Web Services factura. Para ver una lista de los servicios que permiten una AWS Backup administración completa, consulta la sección AWS Backup Administración completa de la [Disponibilidad de características por recurso](#) tabla.

Cuando un tipo de recurso no admite la AWS Backup administración completa, algunas de sus AWS Backup actividades, como los costos de almacenamiento de las copias de seguridad, hacen que la facturación se refleje en el AWS servicio correspondiente.

Errores en los trabajos de copia

Solo se le cobrará una vez que se haya creado un punto de recuperación en el almacén de destino. No se aplica ningún cargo cuando se produce un error en un trabajo de copia y no se crea ningún punto de recuperación.

Etiquetas de asignación de costos

Puede utilizar las etiquetas de asignación de costes para realizar un seguimiento y optimizar AWS Backup los costes de forma detallada, así como ver y filtrar esas etiquetas mediante ellas AWS Cost Explorer.

Para usar etiquetas de asignación de costos, consulte [Automatizar las copias de seguridad y optimizar los costos de las copias de seguridad para Amazon EFS mediante AWS Backup](#) y [Uso de etiquetas de asignación de costos](#).

AWS Backup Precios de Audit Manager

AWS Backup Audit Manager cobra por el uso en función del número de evaluaciones de control. Una evaluación de control es la evaluación de un recurso con respecto a un control. Los cargos por la evaluación del control aparecen en su AWS Backup factura. Para ver los precios actuales de las evaluaciones de control, consulte [Precios de AWS Backup](#).

Para utilizar los controles de AWS Backup Audit Manager, debe habilitar la AWS Config grabación para realizar un seguimiento de la actividad de backup. AWS Config cargos por cada elemento de configuración registrado y estos cargos aparecen en su AWS Config factura. Para ver los precios actuales de los elementos de configuración registrados, consulte [Precios de AWS Config](#).

Precios de Amazon Aurora

Durante el periodo de retención configurado para las copias de seguridad continuas de Aurora (hasta 35 días), las instantáneas no incurrir en cargos de almacenamiento. Las instantáneas que se retienen una vez transcurrido este intervalo se cobran como copias de seguridad completas.

AWS Backup blogs, vídeos, tutoriales y otros recursos

Para obtener más información al respecto AWS Backup, consulte lo siguiente:

- [AWS Backup añade una nueva aprobación multipartita por parte de Veliswa Boya para las bóvedas con huecos vacíos lógicos](#) (junio de 2025)
- [Streamline search and item level recovery with AWS Backup](#). Con Bisman Sethi (diciembre de 2024).
- [Construir AWS Backup la ciberresiliencia con una bóveda con huecos lógicos](#). Con Sushmitha Srinivasa Murthy y Sabith Venkitachalapathy (agosto de 2024).
- [Adjunte un par de EC2 claves de Amazon a la AWS Backup restauración de una máquina VMware virtual](#). Con Olumuyiwa Koya y Kenie Ogunsemowo (agosto de 2024).
- [Optimice y automatice la supervisión y los informes de conformidad con AWS Backup Audit Manager](#). Con Sabith Venkitachalapathy, Glenn Chia y Mark Rowland (junio de 2024).
- [Respaldo coherente con las aplicaciones para aplicaciones de Windows en Amazon EC2 con AWS Backup](#) Con Bhaskar Mazumdar y Karthikeyan KM (mayo de 2024).
- [Optimización de costes AWS Backup](#) . Con Kenneth Hui (abril de 2024).
- [Designing a resilient and cost-effective backup strategy for Amazon S3](#). Con Mojgan Toth y Harish Mandhadi (marzo de 2024).
- [Automatice la entrega de los informes de AWS Backup Audit Manager por correo electrónico](#). Con Ezekiel Oyerinde, Charles Meruwoma y Sri Gudavalli. (enero de 2024)
- [Optimización de Point-in-Time la recuperación \(PITR\) para Aurora](#) con. AWS Backup Con Enrique Ramirez (enero de 2024)
- [Backup y restaure máquinas VMware virtuales locales mediante AWS Backup](#). Por Olumuyiwa Koya y Ezekiel Oyerinde (junio de 2022).
- [Se utiliza AWS Backup para proteger las bases de datos de Amazon Aurora](#). Por Chris Hendon, Brandon Rubadou y Thomas Liddle (mayo de 2022).
- [Protecting encrypted Amazon RDS instances with cross-account and cross-Region backups](#). Por Evan Peck y Sabith Venkitachalapathy (mayo de 2022).
- [Automatice y mejore su postura de seguridad mediante AWS Backup y AWS PrivateLink](#). Por Bilal Alam (abril de 2022).
- [Obtenga informes agregados diarios entre cuentas y regiones. AWS Backup](#) Por Wali Akbari y Sabith Venkitachalapathy (febrero de 2022).

- [Automatice la visibilidad de los resultados de las copias de seguridad mediante AWS Backup y AWS Security Hub CSPM](#) Por Kanishk Mahajan (enero de 2022).
- [Las 10 mejores prácticas de seguridad para proteger las copias de seguridad en AWS](#). Por Ibukun Oyewumi (enero de 2022).
- [Optimización de SAS Grid AWS con FSx for Lustre \(y optimización de la recuperación ante desastres mediante AWS Backup\)](#). Por Matt Saeger y Shea Lutton (enero de 2022).
- [Centralización de la protección de datos y el cumplimiento en Amazon Neptune AWS Backup](#) con. Por Brian O'Keefe (noviembre de 2021).
- [Manage backup and restore of Amazon DocumentDB \(with MongoDB compatibility\) with AWS Backup](#). Por Karthik Vijayraghavan (noviembre de 2021).
- [Simplifique la auditoría de sus políticas de protección de datos con AWS Backup Audit Manager](#). Por Jordan Bjorkman y Harshitha Putta (noviembre de 2021).
- [Mejore la seguridad de sus copias de seguridad con AWS Backup Vault Lock](#). Por Rolland Miller (octubre de 2021).
- [Cómo conservar las etiquetas de recursos en los trabajos de AWS Backup restauración](#). Por Ibukun Oyewumi, Amee Shah y Sabith Venkitachalapathy (septiembre de 2021).
- [Gestione el acceso a las copias de seguridad mediante políticas de control de servicios con AWS Backup](#). Por Sabith Venkitachalapathy y Ibukun Oyewumi (agosto de 2021).
- [Automatice el respaldo centralizado a escala en todos AWS los servicios utilizando AWS Backup](#). Por Ibukun Oyewumi y Sabith Venkitachalapathy (julio de 2021).
- [Blog: Cómo simplificar las copias de seguridad de Microsoft SQL Server mediante AWS Backup VSS](#). Por Siavash Irani y Sepehr Samiei (julio de 2021).
- [Automatice la validación de la recuperación de datos con AWS Backup](#). Por Mahanth Jayadeva (junio de 2021).
- [Configurar las notificaciones para supervisar los AWS Backup trabajos](#). Por Virgil Ennes (junio de 2021).
- [Automating backups and optimizing backup costs for Amazon EFS using AWS Backup](#). Por Prachi Gupta y Rohit Verma (junio de 2021).
- [Administre los costos de respaldo de Amazon EFS: AWS Backup soporte para etiquetas de asignación de costos](#). Por Aditya Maruvada (mayo de 2021).
- [Cree y comparta copias de seguridad cifradas entre cuentas y regiones utilizando AWS Backup](#). Por Prachi Gupta (mayo de 2021).

- [AWS Backup ahora cuenta con la aprobación de FedRAMP High para sus necesidades de cumplimiento y protección de datos](#). Por Andy Grimes (mayo de 2021).
- [ZS Associates mejora la eficiencia del respaldo](#) con. AWS Backup Por Mitesh Naik, Hiranand Mulchandani y Sushant Jadhav (mayo de 2021).
- [Tutorial: Uso AWS Backup de Amazon EBS Backup and Restore](#). Por Fathima Kamal (abril de 2021).
- [Tutorial de vídeo: Managing Cross-Region Copies of Backups](#). Con David DeLuca (abril de 2021).
- [Elimine varios puntos AWS Backup de recuperación con AWS Herramientas para PowerShell](#). Por Sherif Talaat (abril de 2021).
- [Copias de seguridad entre regiones y cuentas para uso de Amazon FSx](#). AWS Backup Por Adam Hunter y Fathima Kamal (abril de 2021).
- [Amazon CloudWatch Events and Metrics para AWS Backup](#). Por Rolland Miller (marzo de 2021).
- [Tutorial: Backup y restauración de Amazon Relational Database Service \(RDS\) mediante. AWS Backup](#) Por Fathima Kamal (marzo de 2021).
- [Point-in-time recuperación y copia de seguridad continua para Amazon RDS con AWS Backup](#). Por Kelly Griffin (marzo de 2021).
- [Automatice AWS Backup con AWS Service Catalog](#) con John Husemoller (enero de 2021).
- [Secure data recovery with cross-account backup and Cross-Region copy using AWS Backup](#). Por Cher Simon (enero de 2021).
- [AWS Resumen de re:Invent: Protección de datos y cumplimiento](#). AWS Backup Por Nancy Wang (diciembre de 2020).
- [AWS Backup proporciona una protección de datos centralizada en todos](#) sus recursos. AWS Por Nancy Wang (noviembre de 2020).
- [Tech Talk: Data protection at scale with AWS Backup](#). Por Kareem Behairy (septiembre de 2020).
- [Administración centralizada de varias cuentas con el uso de copias entre regiones](#). AWS Backup Por Cher Simon (septiembre de 2020).
- [Tutorial en vídeo: Gestione las copias de seguridad a escala mientras lo utiliza. AWS OrganizationsAWS Backup](#) Por Ildar Sharafeev (julio de 2020).
- [Gestione las copias de seguridad a escala según su AWS Organizations uso AWS Backup](#). Por Nancy Wang, Avi Drabkin, Ganesh Sundaresan y Vikas Shah (junio de 2020).
- [Recupere archivos y carpetas de Amazon EFS con AWS Backup](#). Por Abrar Hussain y Gurudath Pai (mayo de 2020).

- [Scheduling automated backups using Amazon EFS and AWS Backup](#). Por Rob Barnes (diciembre de 2019).
- [re:Invent Recording: AWS re:Invent 2019: Profundiza en ft. AWS Backup Rackspace](#). Por Nancy Wang y Jason Pavao (diciembre de 2019).
- [Proteja sus datos con AWS Backup](#). Por Anthony Fiore (julio de 2019).
- [Vídeo de marketing: Introducing AWS Backup](#). Enero de 2019.
- [Vídeo: Introduction to AWS Backup](#). Con AWS formación y certificación.

Introducción a con () AWS Backup

En este tutorial se muestran los pasos genéricos para utilizar las funciones y características de AWS Backup. Al igual que con cualquier parte de esta documentación técnica, debe seguir las instrucciones con la consola de administración de AWS abierta en la otra ventana.

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Un Cuenta de AWS. Para obtener más información, consulte [Creación de una cuenta de AWS](#).
- Al menos un recurso compatible con AWS Backup. Consulte la lista de [Recursos de AWS y aplicaciones de terceros compatibles](#).

Cuando haya nuevos servicios de AWS disponibles, habilite AWS Backup para que utilice dichos servicios.

- Si tiene pensado incluir varios tipos de recurso, como volúmenes de Amazon EBS y buckets de Amazon S3, en el mismo plan de copia de seguridad, confirme que esos recursos estén en la misma Región de AWS.

Para configurar los servicios de AWS que se utilizan con AWS Backup

1. Inicie sesión en la Consola de administración de AWS y abra la consola AWS Backup en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, seleccione Configuración.
3. En la página Activación del servicio, elija Configurar recursos.
4. En la página Configurar recursos, utilice los conmutadores para habilitar o deshabilitar los servicios que se utilizan con AWS Backup. Cuando los servicios estén configurados, elija Confirmar. Asegúrese de que el servicio de AWS al que se suscribe esté disponible en su Región de AWS.

Para obtener información adicional, consulte . La consola de AWS Backup permite a un usuario asignar un tipo de recurso a un plan de copia de seguridad; esto se incluirá incluso si la suscripción no está habilitada para ese servicio en particular.

Para completar este tutorial, puede utilizar el usuario raíz de su Cuenta de AWS para iniciar sesión en la Consola de administración de AWS. Sin embargo, AWS Identity and Access Management (IAM) recomienda que no utilice el usuario raíz de la Cuenta de AWS. En su lugar, cree un administrador en su cuenta y utilice esas credenciales para administrar los recursos de su cuenta.

La consola de AWS Backup ofrece diferentes opciones para hacer una copia de seguridad de los recursos. Puede crear una copia de seguridad bajo demanda, programar y configurar la forma en que desea que se realice la copia de seguridad del recurso o configurar los recursos para que se realicen copias de seguridad automáticamente cuando se cree el recurso.

Suscripción al servicio

La consola de AWS Backup ofrece dos formas para incluir los tipos de recursos en un plan de copia de seguridad: asignar explícitamente el tipo de recurso en un plan de copia de seguridad o incluir todos los recursos. Consulte los puntos siguientes para entender cómo funcionan estas selecciones con las suscripciones a servicios.

- Si las asignaciones de recursos se basan únicamente en etiquetas, se aplica la configuración de suscripción al servicio.
- Si un tipo de recurso se asigna explícitamente a un plan de copia de seguridad, se incluirá en la copia de seguridad incluso si la suscripción no está habilitada para ese servicio en particular. Esto no se aplica a Aurora, Neptune ni Amazon DocumentDB. Para incluir estos servicios, la suscripción debe estar habilitada.
- Si en una asignación de recursos se especifican tanto el tipo de recurso como las etiquetas, los tipos de recursos especificados se filtrarán primero y, a continuación, las etiquetas filtrarán esos recursos.

La configuración de suscripción al servicio no se tiene en cuenta para la mayoría de los tipos de recursos. Sin embargo, Aurora, Neptune y Amazon DocumentDB requieren la suscripción del servicio.

- En el caso de Amazon FSx para NetApp ONTAP, cuando utilice la selección de recursos basada en etiquetas, aplique etiquetas a volúmenes individuales en lugar de a todo el sistema de archivos.

Las opciones de suscripción se aplican a la cuenta y específicas Región de AWS. Cuando una cuenta utiliza AWS Backup (crea un almacén de copias de seguridad o un plan de copias de seguridad) en una región, la cuenta se suscribe automáticamente a todos los tipos de recursos admitidos por AWS Backup en la región en ese momento. Los servicios compatibles que se

agreguen a esa región en una fecha posterior no se incluirán automáticamente en un plan de copia de seguridad. Puede optar por utilizar esos tipos de recursos una vez que se admitan.

Dado que AWS Backup admite cada vez más servicios de AWS y aplicaciones de terceros, es posible que tenga que volver a este paso para optar por los nuevos recursos compatibles.

AWS Backup no regula ni administra las copias de seguridad realizadas en entornos de AWS distintos de AWS Backup.

Para optar por utilizar AWS Backup para proteger todos los tipos de recursos compatibles

1. Inicie sesión en la Consola de administración de AWS y abra la consola AWS Backup en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación izquierdo, elija Configuración.
3. En Activación del servicio, elija Configurar recursos.
4. Active todos los recursos compatibles con AWS Backup moviendo todos los conmutadores hacia la derecha.
5. Elija Confirmar.

Planes de copia de seguridad

En AWS Backup, un plan de respaldo es una expresión de política que define cuándo y cómo desea realizar copias de seguridad de sus AWS recursos, como las tablas de Amazon DynamoDB o los sistemas de archivos Amazon Elastic File System (Amazon EFS). Puede asignar recursos a los planes de respaldo y realizar copias de seguridad y conservar AWS Backup automáticamente las copias de seguridad de esos recursos de acuerdo con el plan de respaldo. Puede crear varios planes de copia de seguridad si tiene cargas de trabajo con requisitos de copia de seguridad diferentes. De forma predeterminada, AWS Backup optimiza los intervalos de copia de seguridad. Puede personalizar el intervalo de copia de seguridad en la consola o mediante programación.

AWS Backup almacena de forma eficiente las copias de seguridad periódicas de forma incremental. La primera copia de seguridad de un recurso de AWS hace una copia de seguridad completa de sus datos. Para cada copia de seguridad incremental sucesiva, solo se respaldan los cambios en sus AWS recursos. Las copias de seguridad incrementales le permiten beneficiarse de la protección de datos que ofrecen las copias de seguridad frecuentes y, al mismo tiempo, minimizar los costos de almacenamiento.

AWS Backup también administra sin problemas el ciclo de vida de su plan de respaldo en función de su configuración de retención, lo que le permite realizar restauraciones cuando sea necesario.

En las siguientes secciones se proporcionan los aspectos básicos de la gestión de su estrategia de copia de seguridad AWS Backup.

Temas

- [Creación de plan de copia de seguridad](#)
- [Introducción al resumen del plan de copia de seguridad](#)
- [Seleccione AWS los servicios para realizar una copia de seguridad](#)

Creación de plan de copia de seguridad

Puede crear un plan de respaldo mediante la AWS Backup consola, la API, la CLI, el SDK o una AWS CloudFormation plantilla.

Temas

- [Creación de planes de copia de seguridad mediante la consola de AWS Backup](#)
- [Cree planes de respaldo mediante el AWS CLI](#)

- [Opciones y configuración del plan de copia de seguridad](#)
- [CloudFormation plantillas para planes de respaldo](#)
- [Eliminar un plan de copia de seguridad](#)
- [Actualizar un plan de copia de seguridad](#)

Creación de planes de copia de seguridad mediante la consola de AWS Backup

Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>. En el panel de control, elija Administrar planes de Backup. O, en el panel de navegación, elija Planes de copia de seguridad y, a continuación, elija Crear plan de copia de seguridad.

Opciones de inicio

Tienes tres opciones para el nuevo plan de copia de seguridad:

- Crear un plan de copia de seguridad basado en uno existente
- Crear un plan nuevo
- [Cree un plan de respaldo mediante AWS CLI](#)

En este procedimiento, creamos un plan nuevo. Cada parte de la configuración tiene un enlace a una sección ampliada situada más adelante en la página, a la que puede desplazarse para obtener más detalles.

1. Introduzca el nombre del plan en [Nombre del plan de copia de seguridad](#). No puede cambiar el nombre de un plan después de crearlo.

Si intenta crear un plan de copia de seguridad idéntico a uno existente, recibirá un error `AlreadyExistsException`.

2. Si lo desea, puede agregar etiquetas a su plan de copia de seguridad.
3. Configuración de reglas de copia de seguridad: en la sección de configuración de reglas de copia de seguridad, establezca la programación, la ventana y el ciclo de vida de la copia de seguridad.
4. Programación:
 - a. Introduzca el nombre de la regla de copia de seguridad en el campo de texto.

- b. En el menú del almacén de copia de seguridad, elija Predeterminado o elija Crear nuevo almacén de copia de seguridad para crear un almacén.
 - c. En el menú de frecuencia de copia de seguridad, elija la frecuencia con la que desea que este plan cree una copia de seguridad.
5. Intervalo de copia de seguridad:
- a. Hora de inicio se establece de manera predeterminada a la 0:30 a. m., en la zona horaria local del sistema.
 - b. Comenzar en un plazo de se establece de manera predeterminada en 8 horas. Puede cambiarlo para especificar un intervalo de tiempo para que se inicie la copia de seguridad.
 - c. Completar en se establece de manera predeterminada en 7 días. Asegúrese de que haya tiempo suficiente para que se complete la copia de seguridad, incluso si el trabajo comienza al final del periodo de inicio.
6. [RespalDOS y point-in-time recuperación continuos \(PITR\)](#): Puede seleccionar Activar copias de seguridad continuas para point-in-time la recuperación (PITR). Para verificar qué recursos son compatibles con este tipo de copia de seguridad, consulte la matriz de [Disponibilidad de características por recurso](#).
7. Ciclo de vida
- a. Almacenamiento en frío: seleccione esta casilla para permitir que los tipos de recursos que cumplen los requisitos pasen al almacenamiento en frío de acuerdo con el calendario que especifique en el periodo de retención total. Para utilizar el almacenamiento en frío debe tener un periodo de retención total de 90 días o más.
 - b. El almacenamiento en frío para Amazon EBS es [Archivo de instantáneas de Amazon EBS](#). Las instantáneas que pasen al nivel de almacenamiento de archivo se mostrarán en la consola como nivel frío. Si está habilitado el almacenamiento en frío y la frecuencia de copia de seguridad es mensual o menor, puede hacer que el plan de copia de seguridad cambie a instantáneas de EBS.
 - c. El periodo de retención total es el número de días que se almacenan los recursos en AWS Backup. Es el número total de días de almacenamiento templado más almacenamiento en frío.
8. (Opcional) Puede optar por crear un índice de copias de seguridad con cada copia de seguridad periódica de un tipo de recurso compatible (para las copias de seguridad continuas se crean índices diarios). Solo los puntos de recuperación (copias de seguridad) con un índice asociado se pueden incluir en una [búsqueda de copias de seguridad](#).

Por ejemplo, cada vez que su plan de copia de seguridad cree una copia de seguridad de S3, también puede crear un índice de copia de seguridad para esa copia de seguridad. Esto permitirá que esa copia de seguridad en particular se incluya en una búsqueda futura.

Marque las casillas de verificación junto a los tipos de recurso para los que desea crear índices.

9. (Opcional) Habilite el análisis de malware para analizar automáticamente las copias de seguridad una vez creadas. Al configurar la protección contra malware, especifique los tipos de recursos que se van a analizar (Amazon EC2, Amazon EBS, Amazon S3 o todos los recursos compatibles) y los tipos de análisis (completos o incrementales). El análisis de malware se aplica únicamente a los tipos de recursos seleccionados. Por ejemplo, si su plan de copias de seguridad incluye los EC2 recursos de Amazon S3 y Amazon, pero habilita el escaneo de malware solo para Amazon EC2, el servicio escaneará solo sus EC2 copias de seguridad. Para cada regla de copia de seguridad, puede configurar el tipo de escaneo que desea utilizar. La programación de la regla de copia de seguridad determinará la frecuencia con la que se realiza el tipo de escaneo.

 Important

Antes de activar la protección contra el malware, asegúrese de que su función de copia de seguridad y de escáner tengan los permisos necesarios. Para obtener más información, consulta [la documentación sobre permisos](#).

10. (Opcional) Utilice Copiar en el destino para crear una copia entre regiones de los recursos que cumplen los requisitos si desea almacenar una copia de seguridad en otra Región de AWS.
11. (Opcional) Etiquetas agregadas a puntos de recuperación.
12. Cuando todas las secciones estén configuradas según sus especificaciones, elija Guardar regla de copia de seguridad.

Cree planes de respaldo mediante el AWS CLI

También puede definir su plan de copia de seguridad en un documento JSON y proporcionarlo mediante la consola de AWS Backup o la AWS CLI. El siguiente documento JSON contiene un ejemplo de plan de copia de seguridad que crea una copia de seguridad diaria a la 1:00, hora del Pacífico (la hora local se ajusta a las condiciones del horario diurno, estándar o de verano, si corresponde). Elimina automáticamente una copia de seguridad tras un año.

```
{
  "BackupPlan": {
    "BackupPlanName": "test-plan",
    "Rules": [
      {
        "RuleName": "test-rule",
        "TargetBackupVaultName": "test-vault",
        "ScheduleExpression": "cron(0 1 ? * * *)",
        "ScheduleExpressionTimezone": "America/Los_Angeles",
        "StartWindowMinutes": integer, // Value is in minutes
        "CompletionWindowMinutes": integer, // Value is in minutes
        "IndexActions": [
          {
            "ResourceTypes": [ "string" ]
          }
        ],
        "Lifecycle": {
          "DeleteAfterDays": integer, // Value is in days
        }
      }
    ]
  }
}
```

Puede almacenar el documento JSON con el nombre que elija. El siguiente comando de la CLI muestra [create-backup-plan](#) con un JSON denominado `test-backup-plan.json`:

```
aws backup create-backup-plan --cli-input-json file://PATH-TO-FILE/test-backup-
plan.json
```

Tenga en cuenta que, si bien algunos sistemas numeran los días de la semana del 0 al 6, nosotros los numeramos del 1 al 7. Para obtener más información, consulte [Expresiones cron y de frecuencia](#). Para obtener más información sobre las zonas horarias, consulta la referencia de [TimeZone](#) la API de Amazon Location Service.

Opciones y configuración del plan de copia de seguridad

Al definir un plan de respaldo en la AWS Backup consola, se configuran las siguientes opciones:

Nombre del plan de copia de seguridad

Debe proporcionar un nombre para el plan de copia de seguridad. Los nombres están limitados a 50 caracteres, incluidos caracteres alfanuméricos, guiones, guiones bajos y puntos.

Reglas de copia de seguridad

Los planes de copias de seguridad se componen de una o más reglas de copia de seguridad. Para agregar reglas de copia de seguridad a un plan de copia de seguridad o para editar las reglas existentes en un plan de copia de seguridad:

1. En la AWS Backup consola, en el panel de navegación izquierdo, selecciona Planes de Backup.
2. En Nombre del plan de copia de seguridad, seleccione un plan de copia de seguridad.
3. En la sección Reglas de copia de seguridad:
 - Para agregar una regla de copia de seguridad, elija Agregar regla de copia de seguridad.
 - Para editar una regla de copia de seguridad existente, elija la regla y, a continuación, elija Editar.

Note

Si tiene un plan de respaldo con varias reglas y los plazos de ambas reglas se superponen, AWS Backup optimiza la copia de seguridad y toma una copia de seguridad para la regla con el mayor tiempo de retención. La optimización tiene en cuenta el intervalo de inicio completo, no solo el momento en que se realiza la copia de seguridad diaria.

Cada regla de copia de seguridad consta de los siguientes elementos.

Nombre de la regla de copia de seguridad

Los nombres de la regla de copia de seguridad distinguen mayúsculas de minúsculas. Deben contener de 1 a 50 caracteres alfanuméricos o guiones.

Backup frequency (Frecuencia de copia de seguridad)

La frecuencia de las copias de seguridad determina la frecuencia con la que se AWS Backup crea una copia de seguridad instantánea. En la consola, puede elegir una frecuencia de cada hora, cada

12 horas, diaria, semanal o mensual. También puede crear una expresión cron que cree copias de seguridad instantáneas con una frecuencia de una hora. Con la AWS Backup CLI, puede programar copias de seguridad de instantáneas con una frecuencia de hasta una hora.

Si selecciona semanalmente, puede especificar en qué días de la semana desea que se lleven a cabo las copias de seguridad. Si selecciona mensualmente, puede elegir un día determinado del mes.

También puede marcar la casilla **Habilitar copias de seguridad continuas** para los recursos compatibles para crear una regla de copia de seguridad continua habilitada para la point-in-time restauración (PITR). A diferencia de las copias de seguridad instantáneas, las copias de seguridad continuas permiten realizar restauraciones. point-in-time Para obtener más información sobre las copias de seguridad continuas, consulte [Point-in-Time Recuperación](#).

Intervalo de copia de seguridad

Los periodos de copia de seguridad constan de la hora de comienzo del periodo de copia de seguridad y de la duración del periodo indicada en horas. Los trabajos de copia de seguridad comienzan dentro de este periodo. La configuración predeterminada de la consola es:

- 0:30 h en la zona horaria local del sistema (0:30 h en sistemas que utilizan el formato de 24 horas)
- Inicio dentro de 8 horas
- Conclusión en 7 días

(completar el parámetro no se aplica a los FSx recursos de Amazon)

Puede personalizar la frecuencia de las copias de seguridad y la hora de inicio del periodo de copia de seguridad mediante una expresión cron. Para ver los seis campos de las expresiones AWS cron, consulta las expresiones [cron y rate en la Guía EventBridge](#) del usuario de Amazon. Dos ejemplos de expresiones AWS cron son `15 * ? * * *` (haz una copia de seguridad cada hora 15 minutos después de la hora) y `0 12 * * ? *` (haz una copia de seguridad todos los días a las 12 del mediodía UTC). Para ver una tabla de ejemplos, haga clic en el enlace anterior y desplácese hacia abajo en la página.

AWS Backup evalúa las expresiones cron entre las 00:00 y las 23:59. Si crea una regla de copia de seguridad “cada 12 horas” pero especifica una hora de inicio posterior a las 11:59, solo se ejecutará una vez al día.

Los planes de copia de seguridad pueden verse afectados por el cambio de hora estacional. Puede cambiar a UTC o crear una copia de seguridad manual el día que se adelante la hora. Para obtener más información, consulte el [horario](#) de verano en Scheduler. EventBridge

Las copias de seguridad y la point-in-time restauración continuas (PITR) hacen referencia a los cambios registrados durante un período de tiempo; por lo tanto, no se pueden programar con una expresión de hora o cron.

En general, los servicios de AWS bases de datos no pueden iniciar las copias de seguridad 1 hora antes o durante el período de mantenimiento y Amazon FSx no puede iniciar las copias de seguridad 4 horas antes o durante el período de mantenimiento o el período de respaldo automático (Amazon Aurora está exento de esta restricción de período de mantenimiento). Las copias de seguridad instantáneas programadas durante esos periodos producirán un error. Hay una excepción cuando opta por utilizar AWS Backup tanto para copias de seguridad instantáneas como continuas para un servicio compatible. AWS Backup programará los intervalos de copia de seguridad automáticamente para evitar conflictos. Consulte [Point-in-Time Recuperación](#) para obtener una lista de los servicios compatibles e instrucciones sobre cómo utilizarlos AWS Backup para realizar copias de seguridad continuas.

Reglas de copia de seguridad superpuestas

En ocasiones, un plan de copia de seguridad puede contener varias reglas superpuestas. Cuando las ventanas de inicio de diferentes reglas se superpongan, AWS Backup conserva la copia de seguridad según la regla con un período de retención más largo. Por ejemplo, considere un plan de copia de seguridad con dos reglas:

1. Copia de seguridad cada hora, con un intervalo de inicio de 1 hora y retención de 1 día.
2. Copia de seguridad cada 12 horas, con un intervalo de inicio de 8 horas y retención de 1 semana.

Al cabo de 24 horas, la segunda regla crea dos copias de seguridad (ya que es la que tiene un periodo de retención más largo). La primera regla crea ocho copias de seguridad (porque el intervalo de inicio de 8 horas de la segunda regla impedía que se ejecutaran más copias de seguridad por hora). En concreto:

Durante este intervalo de inicio	Esta regla crea una copia de seguridad
De medianoche a 8 h	12 horas

Durante este intervalo de inicio	Esta regla crea una copia de seguridad
De 8 a 9	Por hora
De 9 a 10	Por hora
De 10 a 11	Por hora
De 11 a mediodía	Por hora
De mediodía a 20 h	12 horas
De 8 a 9	Por hora
De 9 a 10	Por hora
De 10 a 11	Por hora
De 11 a medianoche	Por hora

Durante el intervalo de inicio, el estado del trabajo de copia de seguridad permanece en ese estado CREATED hasta que comience correctamente o hasta que se agote el tiempo del intervalo de inicio. Si dentro de la ventana de inicio, Time AWS Backup recibe un error que permite volver a intentar el trabajo, AWS Backup volverá a intentarlo automáticamente al menos cada 10 minutos hasta que la copia de seguridad comience correctamente (el estado del trabajo cambia a RUNNING) o hasta que el estado del trabajo cambie a EXPIRED (lo que se espera que ocurra cuando termine el tiempo de la ventana de inicio).

Ciclo de vida y niveles de almacenamiento

Las copias de seguridad se almacenan durante el número de días que especifique, lo que se conoce como ciclo de vida de la copia de seguridad. Las copias de seguridad se pueden restaurar hasta el final de su ciclo de vida.

Se establece como el período de retención total en la sección del ciclo de vida de la configuración de las reglas de respaldo en la AWS Backup consola.

Si lo usa AWS CLI, se establece mediante el parámetro [DeleteAfterDays](#). El periodo de retención de las instantáneas puede oscilar entre 1 día y 100 años (o indefinidamente si no se introduce nada), mientras que el periodo de retención de las copias de seguridad continuas puede oscilar entre 1

y 35 días. La fecha de creación de una copia de seguridad es la fecha en que se inició el trabajo de copia de seguridad, no la fecha en que se completó. Si el trabajo de copia de seguridad no se completa en la misma fecha en que se inició, utilice la fecha en la que comenzó para calcular los períodos de retención.

Las copias de seguridad se mantienen en un nivel de almacenamiento. Cada nivel conlleva un costo de almacenamiento y restauración diferente, tal como se indica en [Precios de AWS Backup](#). Todas las copias de seguridad se crean y se almacenan en almacenamiento templado. Según el tiempo que decida almacenar la copia de seguridad, es posible que desee pasarla a un nivel de menor costo denominado almacenamiento en frío. [Disponibilidad de características por recurso](#) muestra qué recursos tienen esta característica opcional.

Console

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. Cree o edite un plan de copia de seguridad.
3. En la sección de ciclo de vida de la configuración de reglas de copia de seguridad, marca la casilla Mover copias de seguridad de almacenamiento templado almacenamiento en frío.
4. (Opcional) Si Amazon EBS es uno de los recursos de los que hace copias de seguridad y la frecuencia de copia de seguridad es mensual o menor, puede pasarlas a nivel frío mediante el archivado de instantáneas de EBS.
5. Introduzca el valor (en días) que desee que sus copias de seguridad permanezcan almacenadas en caliente. AWS Backup recomienda un mínimo de 8 días.
6. Introduzca un valor (en días) para el periodo de retención total. La diferencia entre el periodo de retención total y el tiempo de almacenamiento en caliente será el número de días que las copias de seguridad permanezcan en almacenamiento en frío.

AWS CLI

1. Utilice [create-backup-plan](#) o [update-backup-plan](#).
- 2.
3. Incluya el parámetro booleano [OptInToArchiveForSupportedResources](#) para los recursos de EBS.
4. Incluya el parámetro [MoveToColdStorageAfterdays](#).

5. Utilice el parámetro `DeleteAfterDays`. Este valor debe ser 90 (días) más el valor que introduzca para `MoveToColdStorageAfterDays`.

El almacenamiento en frío está disponible actualmente para los siguientes tipos de recursos:

Tipo de recurso	Copia de seguridad incremental o completa en almacenamiento en frío
AWS CloudFormation	Incremental
DynamoDB con características avanzadas de	Completa; no hay copias de seguridad incrementales en ningún nivel
Amazon EBS (mediante Archivo de instantáneas de EBS)	Completa; las copias de seguridad incrementales se convertirán en completas después de la transición.
Amazon EFS	Incremental
Bases de datos SAP HANA que se ejecutan en EC2 instancias de Amazon	Incremental
Amazon Timestream	Incremental
VMware máquinas virtuales	Incremental

Una vez que haya activado la transición al almacenamiento en frío mediante la consola o la línea de comandos, se cumplen las siguientes condiciones para copias de seguridad en almacenamiento (o archivo) en frío:

- Las copias de seguridad transicionadas deben almacenarse en cámaras frigoríficas durante un mínimo de 90 días, además del tiempo que permanezcan almacenadas en cámara caliente. AWS Backup requiere que la retención se establezca durante 90 días más que la configuración de «transición al frío después de días». El valor de "transition to cold after days" (número de días tras los cuales migrará a almacenamiento en frío) no puede modificarse una vez que una copia de seguridad se ha migrado al almacenamiento en frío.
- Algunos servicios admiten copias de seguridad incrementales. Para las copias de seguridad incrementales, debe tener al menos una copia de seguridad completa en caliente. AWS Backup

recomienda configurar su ciclo de vida para no mover la copia de seguridad a una cámara frigorífica hasta transcurridos al menos 8 días. Si la copia de seguridad completa pasa a una cámara de almacenamiento en frío demasiado pronto (por ejemplo, si se pasa a una cámara de almacenamiento en frío después de un día), AWS Backup se creará otra copia de seguridad completa en caliente.

- En el caso de los tipos de recursos que admiten copias de seguridad incrementales, AWS Backup los datos pasan del almacenamiento en caliente al almacenamiento en frío si las copias de seguridad en caliente ya no hacen referencia a los datos en transición. Los datos de las copias de seguridad retenidas en almacenamiento en frío a los que solo hacen referencia otras copias de seguridad en frío se facturan según los precios de los niveles de almacenamiento en frío. Otras copias de seguridad continúan con los precios de los niveles de almacenamiento en caliente.

Almacén de copias de seguridad

Un almacén de copias de seguridad es un contenedor que sirve para organizar las copias de seguridad. Las copias de seguridad creadas por una regla de copia de seguridad se organizan en el almacén de copia de seguridad que especifique en la regla de copia de seguridad. Puede usar las bóvedas de respaldo para establecer la clave de cifrado AWS Key Management Service (AWS KMS) que se usa para cifrar las copias de seguridad en la bóveda de respaldo y para controlar el acceso a las copias de seguridad en la bóveda de respaldo. También puede añadir etiquetas a los almacenes de copias de seguridad para organizarlos. Si no desea utilizar el almacén predeterminado, puede crear el suyo propio. Para obtener step-by-step instrucciones sobre cómo crear un almacén de copias de seguridad, consulte [Creación y eliminación de almacenes de copias de seguridad](#)

Realizar copias entre regiones

Como parte de su plan de copia de seguridad, si lo desea, puede crear una copia de seguridad en el mismo lugar o en otro Región de AWS. Estas copias se pueden realizar en la misma cuenta o en otra. Para obtener más información sobre las copias de las copias de seguridad, consulte [Creación de copias de las copias de seguridad entre Regiones de AWS](#).

Cuando defina una réplica de una copia de seguridad, tendrá que establecer las siguientes opciones:

Región de destino

Región de destino de la copia de seguridad.

Almacén de copias de seguridad (configuración avanzada)

Almacén de copia de seguridad de destino de la copia.

(Configuración avanzada) Rol de IAM

La función de IAM que se AWS Backup utiliza al crear la copia. El rol también debe AWS Backup figurar como entidad de confianza, lo que AWS Backup permite asumirlo. Si eliges Predeterminado y el rol AWS Backup predeterminado no está presente en tu cuenta, se crea un rol para ti con los permisos correctos.

(Configuración avanzada) Ciclo de vida

Especifica cuándo se va a migrar la copia de seguridad al almacenamiento en frío y cuándo va a caducar (eliminarse). Las copias de seguridad que se transfieran al almacenamiento en frío deben almacenarse en dicho almacenamiento durante un mínimo de 90 días. Una vez que la copia ha migrado al almacenamiento en frío, no se puede modificar este valor.

Vencimiento especifica el número de días que deben transcurrir desde la creación hasta que se elimina la copia. Este valor debe ser 90 días superior al valor de Transferir al almacenamiento en frío.

Si el valor de [Lifecycle:DeleteAfterDays](#) (que se muestra como Vencimiento en la consola) no se especifica en la configuración de la copia, se mantendrá la configuración del ciclo de vida de la copia de seguridad desde la que se copie.

Etiquetas agregadas a puntos de recuperación

Las etiquetas que enumere aquí se añaden automáticamente a las copias de seguridad cuando se crean.

Etiquetas agregadas a planes de copia de seguridad

Estas etiquetas están asociadas con el propio plan de copias de seguridad para ayudarle a organizar y realizar un seguimiento de su plan de copias de seguridad.

Configuración de copia de seguridad avanzada

La configuración avanzada de las copias de seguridad le permite configurar opciones de copia de seguridad específicas de cada recurso para distintos servicios. AWS

Configuración EC2 avanzada de copias de seguridad de Amazon

Permite realizar copias de seguridad coherentes con las aplicaciones de terceros que se ejecutan en EC2 instancias de Amazon. Actualmente, AWS Backup es compatible con las copias de seguridad de Windows VSS. AWS Backup excluye tipos específicos de EC2 instancias de Amazon de las

copias de seguridad de Windows VSS. Para obtener más información, consulte [Creación de copias de seguridad de Windows VSS](#).

Configuración avanzada de copias de seguridad de Amazon S3

AWS Backup proporciona ajustes avanzados para controlar los metadatos que se incluyen en las copias de seguridad de Amazon S3. Si lo desea, puede excluir las listas de control de acceso (ACLs) y las etiquetas de objetos de sus copias de seguridad, lo que se ajusta a las prácticas recomendadas de Amazon S3 de utilizar permisos a nivel de bucket en lugar de a nivel de objeto. ACLs

Para obtener información detallada sobre la configuración de las opciones de copia de seguridad ACLs y las etiquetas de objetos de Amazon S3, consulte [Configuración avanzada de las copias de seguridad de Amazon S3](#).

Important

Al excluirlos de las copias ACLs de seguridad, los objetos que se restauren sin ellas ACLs utilizarán la configuración de propiedad predeterminada del depósito de destino. El bucket de destino deberá tener la configuración de propiedad de objetos adecuada.

Note

Cuando hay un trabajo de copia de seguridad continua en ejecución para un bucket de Amazon S3 y se inicia un trabajo de copia de seguridad de instantánea, la instantánea mantiene la misma configuración de ACL y etiquetas de objetos que la copia de seguridad continua, independientemente de la configuración especificada para el trabajo de instantánea.

Escaneo de malware

AWS Backup se integra con Amazon GuardDuty para proporcionar un escaneo automatizado de malware de sus puntos de recuperación. Cuando habilitas la detección de malware en tu plan de copias de seguridad, escanea AWS Backup automáticamente tus copias de seguridad en busca de malware y proporciona resultados de análisis para ayudarte a tomar decisiones informadas sobre la restauración de tus datos.

Para configurar el análisis de malware para tu plan de copias de seguridad:

1. Cree una función de IAM que confíe en la política AWS `AWSBackupGuardDutyRolePolicyForScans` gestionada `malware-protection.guardduty.amazonaws.com` y la adjunte.
2. Adjunte la política AWS gestionada `AWSBackupServiceRolePolicyForScans` a la función de IAM de la selección de copias de seguridad.
3. En la configuración de su plan de respaldo, añada ajustes de escaneo que especifiquen:
 - El servicio de escaneo (GuardDuty)
 - Los tipos de recursos que se van a escanear (Amazon EC2, Amazon EBS, Amazon S3)
 - El rol de IAM que debe asumir ARN GuardDuty
4. Configure las acciones de escaneo en sus reglas de respaldo para especificar:
 - El servicio de escaneo (GuardDuty)
 - El tipo de escaneo (escaneo incremental o completo)

Para obtener más información sobre las políticas administradas, consulte [the section called “AWSBackupGuardDutyRolePolicyForScans”](#) y [the section called “AWSBackupServiceRolePolicyForScans”](#).

CloudFormation plantillas para planes de respaldo

Proporcionamos dos CloudFormation plantillas de muestra para su referencia. La primera plantilla crea un plan de copia de seguridad sencillo. La segunda plantilla permite realizar copias de seguridad VSS en un plan de copia de seguridad.

Note

Si utiliza el rol de servicio predeterminado, *service-role* sustitúyalo por `AWSBackupServiceRolePolicyForBackup`.

Description: backup plan template to back up all resources daily at 5am UTC, and tag all recovery points with backup:daily.

Resources:

KMSKey:

Type: `AWS::KMS::Key`

Properties:

Description: "Encryption key for daily"

EnableKeyRotation: True

Enabled: True

KeyPolicy:

Version: "2012-10-17"

Statement:

- Effect: Allow

Principal:

"AWS": { "Fn::Sub": "arn:\${AWS::Partition}:iam:\${AWS::AccountId}:root" }

Action:

- kms:*

Resource: "*"

BackupVaultWithDailyBackups:

Type: "AWS::Backup::BackupVault"

Properties:

BackupVaultName: "BackupVaultWithDailyBackups"

EncryptionKeyArn: !GetAtt KMSKey.Arn

BackupPlanWithDailyBackups:

Type: "AWS::Backup::BackupPlan"

Properties:**BackupPlan:**

BackupPlanName: "BackupPlanWithDailyBackups"

BackupPlanRule:

- RuleName: "RuleForDailyBackups"

TargetBackupVault: !Ref BackupVaultWithDailyBackups

ScheduleExpression: "cron(0 5 ? * * *)"

DependsOn: BackupVaultWithDailyBackups

DDBTableWithDailyBackupTag:

Type: "AWS::DynamoDB::Table"

Properties:

TableName: "TestTable"

AttributeDefinitions:

- AttributeName: "Album"

AttributeType: "S"

KeySchema:

- AttributeName: "Album"

KeyType: "HASH"

ProvisionedThroughput:

ReadCapacityUnits: "5"

WriteCapacityUnits: "5"

Tags:

- Key: "backup"
Value: "daily"

BackupRole:

Type: "AWS::IAM::Role"

Properties:

AssumeRolePolicyDocument:

Version: "2012-10-17"

Statement:

- Effect: "Allow"
Principal:
Service:
 - "backup.amazonaws.com"Action:
 - "sts:AssumeRole"

ManagedPolicyArns:

- "arn:aws:iam::aws:policy/service-role/*service-role*"

TagBasedBackupSelection:

Type: "AWS::Backup::BackupSelection"

Properties:

BackupSelection:

SelectionName: "TagBasedBackupSelection"

IamRoleArn: !GetAtt BackupRole.Arn

ListOfTags:

- ConditionType: "STRINGEQUALS"
ConditionKey: "backup"
ConditionValue: "daily"

BackupPlanId: !Ref BackupPlanWithDailyBackups

DependsOn: BackupPlanWithDailyBackups

Description: backup plan template to enable Windows VSS and add backup rule to take backup of assigned resources daily at 5am UTC.

Resources:

KMSKey:

Type: AWS::KMS::Key

Properties:

Description: "Encryption key for daily"

EnableKeyRotation: True

Enabled: True

KeyPolicy:

```

Version: "2012-10-17"
Statement:
  - Effect: Allow
    Principal:
      "AWS": { "Fn::Sub": "arn:${AWS::Partition}:iam:${AWS::AccountId}:root" }
    Action:
      - kms:*
    Resource: "*"

```

```

BackupVaultWithDailyBackups:
  Type: "AWS::Backup::BackupVault"
  Properties:
    BackupVaultName: "BackupVaultWithDailyBackups"
    EncryptionKeyArn: !GetAtt KMSKey.Arn

```

```

BackupPlanWithDailyBackups:
  Type: "AWS::Backup::BackupPlan"
  Properties:
    BackupPlan:
      BackupPlanName: "BackupPlanWithDailyBackups"
      AdvancedBackupSettings:
        - ResourceType: EC2
          BackupOptions:
            WindowsVSS: enabled
    BackupPlanRule:
      - RuleName: "RuleForDailyBackups"
        TargetBackupVault: !Ref BackupVaultWithDailyBackups
        ScheduleExpression: "cron(0 5 ? * * *)"

```

```

DependsOn: BackupVaultWithDailyBackups

```

Eliminar un plan de copia de seguridad

Puede eliminar un plan de copias de seguridad solo después de haber eliminado todas las selecciones de recursos asociadas. Estas selecciones también se conocen como asignaciones de recursos. Si no se eliminaron antes de eliminar el plan de copia de seguridad, la consola mostrará el siguiente error: "Las selecciones asociadas al plan de copia de seguridad deben eliminarse antes de eliminar el plan de copia de seguridad". Use la consola o use [DeleteBackupSelection](#).

La eliminación de un plan de copias de seguridad elimina la versión actual del plan. Las versiones actual y anterior, si las hay, existen todavía, pero ya no se incluyen en la consola en Backup plans (Planes de copias de seguridad).

 Note

Cuando se elimina un plan de copia de seguridad, las copias de seguridad existentes no se eliminan. Para eliminar las copias de seguridad existentes, tiene que suprimirlas en el almacén de copias de seguridad en [Eliminación de copias de seguridad](#).

Para eliminar un plan de respaldo mediante la AWS Backup consola

1. Inicie sesión en y abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
[Consola de administración de AWS](#)
2. En el panel de navegación de la izquierda, seleccione Backup plans (Planes de copia de seguridad).
3. Elija el plan de copias de seguridad en la lista.
4. Seleccione las asignaciones de recursos que están asociadas al plan de copia de seguridad.
5. Elija Eliminar.

Actualizar un plan de copia de seguridad

Tras crear un plan de copia de seguridad, puede modificar el plan; por ejemplo, puede agregar etiquetas o puede agregar, modificar o eliminar reglas de copia de seguridad. Los cambios que realice en un plan de copias de seguridad no tienen ningún efecto sobre las copias de seguridad existentes creadas por el plan de copia de seguridad. Los cambios se aplican únicamente a las copias de seguridad que se crean en el futuro.

Por ejemplo, cuando se actualiza el período de retención en una regla de copia de seguridad, el período de retención de las copias de seguridad creadas antes de la actualización sigue siendo el mismo. Las copias de seguridad que cree dicha regla en el futuro muestran el periodo de retención actualizado.

No puede cambiar el nombre de un plan después de crearlo.

Para editar un plan de respaldo mediante la AWS Backup consola

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, seleccione Backup plans (Planes de copias de seguridad).

3. En el segundo panel, Planes de copia de seguridad, se muestran los planes de copia de seguridad existentes. Seleccione el enlace subrayado en la columna Nombre del plan de copia de seguridad para ver los detalles del plan de copia de seguridad elegido.
4. Puede editar una regla de copia de seguridad, ver las asignaciones de recursos, ver los trabajos de copia de seguridad, administrar etiquetas o cambiar la configuración de Windows VSS.
5. Para actualizar una regla de copia de seguridad, seleccione el nombre de la regla de copia de seguridad.

Seleccione Administrar etiquetas para agregar o eliminar etiquetas.

Seleccione Editar junto a Configuración avanzada de copia de seguridad para activar o desactivar Windows VSS.

6. Cambie la configuración que prefiera y, a continuación, seleccione Guardar.

Introducción al resumen del plan de copia de seguridad

La característica de resumen del plan de copia de seguridad ofrece una visión integral de la configuración del plan de copia de seguridad, que le permite asegurarse de que su estrategia de copia de seguridad cumpla sus requisitos. El resumen incluye tres componentes clave que abordan los desafíos comunes de los clientes a la hora de administrar configuraciones de respaldo complejas en varios AWS servicios.

Componentes del resumen

Cada resumen de plan de copia de seguridad incluye la siguiente información:

- Las diez próximas ejecuciones de copia de seguridad programadas: muestra cuándo se ejecutarán las reglas de copia de seguridad, incluidas las reglas fusionadas y la gestión adecuada de las zonas horarias.
- Notas sobre la compatibilidad de las funciones: información sobre qué servicios admiten la point-in-time recuperación (PITR) y el almacenamiento en capa fría, si estos servicios forman parte de la norma de su plan de respaldo.

Vista previa de las ejecuciones de copia de seguridad programadas

La vista previa de las ejecuciones programadas muestra hasta diez futuras ejecuciones de copias de seguridad en función de las reglas de su plan de copia de seguridad. Esta vista previa le ayuda a comprender cuándo se realizarán las copias de seguridad y cómo interactúan varias reglas entre sí.

Cómo se fusionan varias reglas

Si tiene varias reglas de respaldo en un plan, AWS Backup aplica una lógica de combinación para determinar el comportamiento final del respaldo:

- Intervalos de copia de seguridad superpuestos: se recomienda no tener dos reglas que se contradigan. Cuando se ejecuten dos reglas al mismo tiempo, AWS Backup selecciona una.
- Combinaciones de PITR e instantáneas: la PITR se aplica a los recursos compatibles, mientras que las instantáneas se aplican a todos los recursos de la selección.
- Varias zonas horarias: cada regla respeta su zona horaria configurada para programar la ejecución.
- Acciones de copia entre regiones: las acciones de copia se conservan y se muestran con la información de destino. Tenga en cuenta que si una regla de copia está asociada a una regla de programación en conflicto, la regla de copia solo se ejecutará si se ha ejecutado la regla de programación.

Example Ejemplo de fusión de reglas

Piense en un plan de copia de seguridad con dos reglas:

- Regla 1: instantánea diaria a las 8:00 PDT, que se conserva durante 35 días
- Regla 2: instantánea semanal a las 8:00 PDT, que se conserva durante 90 días

Si ambas reglas se ejecutan el mismo día (por ejemplo, el domingo), la vista previa muestra la regla 2 porque se guarda durante más tiempo (90 días frente a 35 días).

Tipos de ejecución

La vista previa de las ejecuciones programadas muestra diferentes tipos de ejecución en función de la configuración de la regla:

- CONTINUOUS: copias de seguridad continuas para los servicios compatibles

- **SNAPSHOTs**: copias de seguridad (periódicas) de instantáneas de todos los recursos de la selección
- **CONTINUOUS_AND_SNAPSHOTs**: Point-in-time-restore (PITR) para los tipos de recursos que lo admiten; instantánea (periódica) para todos los demás tipos de recursos.

Validación de la compatibilidad de las características

El resumen incluye recordatorios de compatibilidad para ayudarle a entender qué AWS servicios admiten funciones avanzadas de copia de seguridad. Esto evita errores de configuración y costos inesperados.

Point-in-time soporte de recuperación

Al activar las copias de seguridad continuas en una regla, el resumen le recuerda que la PITR solo se admite para:

- Bases de datos de Aurora
- Bases de datos de Amazon RDS
- bases de datos SAP HANA
- Buckets de Amazon S3

Compatibilidad con el almacenamiento en nivel frío

Al configurar transiciones de nivel frío, el resumen muestra qué servicios admiten esta característica:

- Tablas de Amazon DynamoDB
- Sistemas de archivos de Amazon Elastic File System
- Bases de datos SAP HANA
- Bases de datos de Amazon Timestream
- VMware máquinas virtuales

Acceso a los resúmenes de planes de copia de seguridad

Puede ver los resúmenes del plan de respaldo en la AWS Backup consola después de crear o actualizar un plan de respaldo. El resumen aparece en la página de detalles del plan y proporciona información inmediata sobre cómo afecta la configuración.

Cómo ver el resumen del plan de copia de seguridad

1. Abra la AWS Backup consola en. <https://console.aws.amazon.com/backup/>
2. En el panel de navegación, seleccione Backup plans (Planes de copias de seguridad).
3. Elija el plan de copia de seguridad que desea revisar.
4. El resumen del plan de copia de seguridad aparecerá en la página de detalles del plan. Amplíe el resumen para ver las ejecuciones programadas y las notas de compatibilidad.

También puede obtener la información del plan de copia de seguridad con la AWS CLI:

```
aws backup get-backup-plan --backup-plan-id 012345678
```

Seleccione AWS los servicios para realizar una copia de seguridad

Suscripción a servicios y asignación de recursos

AWS Backup funciona con muchos [AWS servicios diferentes](#). Antes de decidir qué servicios incluir en el plan de respaldo, utilice la [AWS Backup consola](#) o [AWS CLI](#) o opte por utilizarla AWS Backup para trabajar con esos servicios.

Luego, en cada plan de copia de seguridad, especifique en la [consola](#) o mediante la [CLI](#) qué tipos de recurso quiere incluir en ese plan.

Por ejemplo, puede optar por todos los servicios AWS Backup compatibles y, a continuación, incluir solo los buckets de Amazon S3 y los clústeres Aurora en un plan de respaldo.

Temas

- [AWS Backup suscripción al servicio](#)
- [Asignación de recursos del plan de copia de seguridad](#)
- [Asignación de recursos mediante la consola AWS Backup](#)
- [Asigne recursos con AWS CLI](#)
- [Asigne AWS Backup recursos mediante CloudFormation](#)
- [Cuotas de asignación de recursos del plan de copia de seguridad](#)

AWS Backup suscripción al servicio

Suscripción al servicio a través de la consola AWS Backup

Para configurar los AWS servicios que se van a utilizar con AWS Backup

1. Inicie sesión en y abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
[Consola de administración de AWS](#)
2. En el panel de navegación, seleccione Configuración.
3. En la página Activación del servicio, elija Configurar recursos.
4. En la página Configurar recursos, utilice los conmutadores para activar o desactivar los servicios con los que se utilizan. AWS Backup Cuando los servicios estén configurados, elija Confirmar. Asegúrese de que el AWS servicio por el que está optando esté disponible en su. Región de AWS

Suscripción al servicio a través de AWS CLI

Utilice el [aws backup update-region-settings](#) comando para cambiar los servicios (tipos de recursos) que utilizará su cuenta u organización AWS Backup para organizar la creación de copias de seguridad. Utilice el comando [aws backup describe-region-settings](#) para determinar a qué servicios se ha suscrito en una región específica.

Asignación de recursos del plan de copia de seguridad

A través de la [AWS Backup consola](#) o a través de ella [AWS CLI](#), la asignación de recursos de su plan de respaldo especifica qué recursos AWS Backup incluirá. AWS Backup proporciona una configuración predeterminada sencilla y controles detallados para asignar recursos.

Puede asignar recursos de las siguientes formas:

- Asignar explícitamente los tipos de recurso al plan de copia de seguridad
- Incluye todos los recursos (luego AWS Backup buscará todos los tipos de recursos compatibles)
- Utilizar etiquetas para incluir o excluir recursos

Si solo utiliza etiquetas para la asignación de recursos, se seguirá aplicando la configuración de suscripción a los servicios.

Puede refinar aún más la asignación de recursos mediante el uso de etiquetas y condiciones. Existen algunos límites en cuanto al número de ARNs condiciones y etiquetas que se pueden usar en una sola asignación de recursos.

La selección de recursos desde la CLI se basa en los nombres de los servicios y los tipos de recurso. Consulte [Asigne recursos con AWS CLI](#) para obtener información sobre la elección de recursos.

Asignación de recursos mediante la consola AWS Backup

Para ir a la página Asignación de recursos:

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. Elija Planes de copia de seguridad.
3. Elija Crear plan de copia de seguridad.
4. Seleccione cualquier plantilla en la lista desplegable Elegir plantilla y, a continuación, elija Crear plan.
5. Escriba el Nombre del plan de copia de seguridad.
6. Elija Crear plan.
7. Elija Asignar recursos.

Para comenzar la asignación de recursos, en la sección General:

1. Escriba un Nombre de asignación de recursos.
2. Elija el Rol predeterminado o Elegir un rol de IAM.

Note

Si elige un rol de IAM, verifique que tiene permiso para hacer copias de seguridad de todos los recursos que va a asignar. Si su rol encuentra un recurso para el que no tiene permiso para hacer una copia de seguridad, se producirá un error en el plan de copia de seguridad.

Para asignar sus recursos, en la sección Asignar recursos, elija una de las dos opciones que aparecen en Definir la selección de recurso:

- Incluir todos los tipos de recursos. Esta opción configura su plan de respaldo para proteger todos los recursos AWS Backup compatibles actuales y futuros asignados a su plan de respaldo. Utilice esta opción para proteger su patrimonio de datos de forma rápida y sencilla.

Si elige esta opción, como siguiente paso, puede Ajustar la selección mediante etiquetas.

- Incluir tipos de recursos específicos. Al elegir esta opción, debe Seleccionar tipos de recursos específicos mediante los siguientes pasos:

1. En el menú desplegable Seleccionar tipos de recursos, asigne uno o más tipos de recursos.

Cuando termine, le AWS Backup presenta la lista de tipos de recursos que ha seleccionado y su configuración predeterminada, que consiste en proteger todos los recursos de cada tipo de recurso seleccionado.

2. Si lo desea, si desea excluir recursos específicos de un tipo de recurso que haya seleccionado:
 1. Usa el menú desplegable Elegir recursos y anule la selección de la opción predeterminada.
 2. Seleccione los recursos específicos para asignarlos a su plan de copia de seguridad.
3. Si lo desea, puede excluir un recurso específico IDs de los tipos de recursos seleccionados. Utilice esta opción si desea excluir uno o varios recursos de entre muchos, ya que hacerlo puede resultar más rápido que seleccionar muchos recursos en el paso anterior. Debe incluir un tipo de recurso antes de poder excluir los recursos de ese tipo de recurso. Para excluir un ID de recurso, use los siguientes pasos:
 1. En Excluir un recurso específico IDs de los tipos de recursos seleccionados, elija uno o más de los tipos de recursos que incluyó mediante la opción Seleccionar tipos de recursos.
 2. Para cada tipo de recurso, use el menú Elegir recursos para seleccionar uno o más recursos para excluirlos.

Además de las opciones anteriores, puede realizar selecciones aún más detalladas mediante la característica opcional Ajustar la selección mediante etiquetas. Esta característica le permite ajustar su selección actual para incluir un subconjunto de sus recursos mediante etiquetas.

Las etiquetas son pares clave-valor que puede asignar a recursos concretos para ayudarle a identificar, organizar y filtrar los recursos. Las etiquetas distinguen entre mayúsculas y minúsculas. Para obtener más información sobre las etiquetas, consulte [Etiquetar AWS los recursos](#).

Al ajustar la selección con dos o más etiquetas, el efecto es una condición AND. Por ejemplo, si ajusta su selección con dos etiquetas, `env: prod` y `role: application`, solo asignas recursos con AMBAS etiquetas a su plan de copia de seguridad.

Para ajustar su selección mediante etiquetas:

1. En Ajustar la selección mediante etiquetas, elija una Clave de la lista.
2. Seleccione una Condición de valor de la lista.
 - El valor hace referencia a la siguiente entrada, el valor del par clave-valor.
 - La condición puede ser `Equals`, `Contains`, `Begins with` o `Ends with`, o su inversa: `Does not equal`, `Does not contain`, `Does not begin with` o `Does not end with`.
3. Elija un Valor de la lista.
4. Para ajustar aún más utilizando otra etiqueta, elija Agregar etiqueta.

Asigne recursos con AWS CLI

Filtrado por servicios o tipos de recurso

La selección de recursos se basa en los nombres de los servicios y los tipos de recurso. El método de selección de recursos determina si un recurso se incluye en la copia de seguridad. Esta inclusión depende de los nombres de los servicios, los tipos de recurso y la configuración de suscripción.

Selección por nombre de servicio

Si solo especifica un nombre de servicio en la selección de recursos, la inclusión de la copia de seguridad dependerá de la configuración de suscripción de los tipos de recursos subyacentes. Por ejemplo, `conarn:aws:ec2:*`, EC2 las instancias se incluirán en la copia de seguridad solo si la configuración opcional para el tipo de EC2 recurso está habilitada.

Selección por tipo de recurso

Si especifica la selección de recursos directamente con el tipo de recurso, se incluirá en la copia de seguridad independientemente de la configuración de suscripción para ese servicio en particular. Por ejemplo, `conarn:aws:ec2:::instance/*`, se realizará una copia de seguridad de las EC2 instancias independientemente de la configuración de suscripción.

Tipos de recursos compartidos

Si varios recursos comparten el mismo tipo de recurso, deberá habilitar la configuración de suscripción para los tipos de recurso específicos para iniciar las copias de seguridad.

Example

Los clústeres de Aurora y RDS comparten el formato de ARN: `arn:aws:rds:::cluster:*`.

Para hacer copias de seguridad de bases de datos de Aurora, deberá habilitar la configuración de suscripción de Aurora.

FSx y FSx para OpenZFS comparten el formato ARN. `arn:aws:fsx:::file-system/*` Habilite la configuración de suscripción correspondiente para hacer copias de seguridad de estos sistemas de archivos.

Uso de un JSON para definir la asignación de recursos del plan de copia de seguridad

Puede definir una asignación de recursos en un documento JSON.

Puede especificar condiciones, etiquetas o recursos para definir lo que se incluirá en su plan de copia de seguridad. Para obtener más información que le ayude a determinar qué parámetros incluir, consulte [BackupSelection](#).

En este ejemplo de asignación de recursos se asignan todas las EC2 instancias de Amazon al plan ***BACKUP-PLAN-ID*** de backup:

```
{
  "BackupPlanId": "BACKUP-PLAN-ID",
  "BackupSelection": {
    "SelectionName": "resources-list-selection",
    "IamRoleArn": "arn:aws:iam::ACCOUNT-ID:role/IAM-ROLE-ARN",
    "Resources": [
      "arn:aws:ec2:::instance/*"
    ]
  }
}
```

Suponiendo que este JSON esté almacenado como `backup-selection.json`, puede asignar estos recursos a su plan de copia de seguridad mediante el siguiente comando de la CLI:

```
aws backup create-backup-selection --cli-input-json file://PATH-TO-FILE/backup-selection.json
```

A continuación, se muestran ejemplos de asignaciones de recursos, junto con el documento JSON correspondiente. Para facilitar la lectura de esta tabla, en los ejemplos se omiten los campos "BackupPlanId", "SelectionName" y "IamRoleArn". El comodín * representa cero o más caracteres que no sean espacios en blanco.

Example Ejemplo: Selecciona todos los recursos de mi cuenta

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ]
  }
}
```

Example Ejemplo: Selecciona todos los recursos de mi cuenta, pero excluye los volúmenes de EBS

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "NotResources":[
      "arn:aws:ec2:*:*:volume/*"
    ]
  }
}
```

Example Ejemplo: Selecciona todos los recursos etiquetados con "backup":"true", pero excluye los volúmenes de EBS

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "NotResources":[
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Conditions":{
      "StringEquals":[
        {
```

```

        "ConditionKey": "aws:ResourceTag/backup",
        "ConditionValue": "true"
    }
]
}
}
}

```

Important

RDS, Aurora, Neptune y DocumentDB ARNs comienzan con. `arn:aws:rds:` Refine la selección con etiquetas y operadores condicionales si no tiene previsto incluir todos esos tipos.

Example Ejemplo: Selecciona todos los volúmenes de EBS y las instancias de base de datos de RDS etiquetados con `"backup": "true"` y `"stage": "prod"`

La aritmética booleana es similar a la de las políticas de IAM: con aquellas en `"Resources"` combinados utilizando un OR booleano y aquellas en `"Conditions"` combinadas utilizando un AND booleano.

La expresión `"arn:aws:rds:*:*:db:*"` de `"Resources"` solo selecciona instancias de base de datos de RDS porque no hay recursos de Aurora, Neptune o DocumentDB correspondientes.

```

{
  "BackupSelection": {
    "Resources": [
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:rds:*:*:db:*"
    ],
    "Conditions": {
      "StringEquals": [
        {
          "ConditionKey": "aws:ResourceTag/backup",
          "ConditionValue": "true"
        },
        {
          "ConditionKey": "aws:ResourceTag/stage",
          "ConditionValue": "prod"
        }
      ]
    }
  }
}

```



```
    ]
  }
}
}
```

Example Ejemplo: Selecciona todos los volúmenes de EBS y las instancias de RDS etiquetados con "backup":"true", pero no con "stage":"test"

```
{
  "BackupSelection":{
    "Resources":[
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:rds:*:*:db:*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ],
      "StringNotEquals":[
        {
          "ConditionKey":"aws:ResourceTag/stage",
          "ConditionValue":"test"
        }
      ]
    }
  }
}
```

Example Ejemplo: Selecciona todos los recursos etiquetados con "key1" y un valor que comience por "include", pero no con "key2" y un valor que contenga la palabra "exclude"

Puede utilizar el carácter comodín al principio, al final y al centro de una cadena. Observe el uso del carácter comodín (*) en `include*` y `*exclude*` en el ejemplo anterior. También puede utilizar el carácter comodín en el centro de una cadena, como se muestra en el ejemplo anterior, `arn:aws:rds:*:*:db:*`.

```
{
  "BackupSelection":{
    "Resources":[
```

```

    "*"
  ],
  "Conditions":{
    "StringLike":[
      {
        "ConditionKey":"aws:ResourceTag/key1",
        "ConditionValue":"include*"
      }
    ],
    "StringNotLike":[
      {
        "ConditionKey":"aws:ResourceTag/key2",
        "ConditionValue":"*exclude*"
      }
    ]
  }
}
}
}

```

Example Ejemplo: seleccione todos los recursos etiquetados con, "backup":"true" excepto los sistemas de FSx archivos y los recursos de RDS, Aurora, Neptune y DocumentDB

Los elementos incluidos NotResources se combinan utilizando el booleano OR.

```

{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "NotResources":[
      "arn:aws:fsx:*",
      "arn:aws:rds:*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ]
    }
  }
}
}

```

Example Ejemplo: Selecciona todos los recursos etiquetados con una etiqueta "backup" y cualquier valor

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "Conditions":{
      "StringLike":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"*"
        }
      ]
    }
  }
}
```

Example Ejemplo: seleccione todos los sistemas de FSx archivos, el clúster "my-aurora-cluster" Aurora y todos los recursos etiquetados con "backup":"true", excepto los recursos etiquetados con "stage":"test"

```
{
  "BackupSelection":{
    "Resources":[
      "arn:aws:fsx:*",
      "arn:aws:rds:*:*:cluster:my-aurora-cluster"
    ],
    "ListOfTags":[
      {
        "ConditionType":"StringEquals",
        "ConditionKey":"backup",
        "ConditionValue":"true"
      }
    ],
    "Conditions":{
      "StringNotEquals":[
        {
          "ConditionKey":"aws:ResourceTag/stage",
          "ConditionValue":"test"
        }
      ]
    }
  }
}
```

```

    }
  }
}
```

Example Ejemplo: Selecciona todos los recursos etiquetados con la etiqueta **"backup":"true"**, excepto los volúmenes de EBS etiquetados con **"stage":"test"**

Utilice dos comandos de la CLI para crear dos selecciones para seleccionar este grupo de recursos. La primera selección se aplica a todos los recursos, excepto a los volúmenes de EBS. La segunda selección se aplica a los volúmenes de EBS.

```

{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "NotResources":[
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ]
    }
  }
}
```

```

{
  "BackupSelection":{
    "Resources":[
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ]
    }
  },
```

```

    "StringNotEquals":[
      {
        "ConditionKey":"aws:ResourceTag/stage",
        "ConditionValue":"test"
      }
    ]
  }
}
}
}

```

Asigne AWS Backup recursos mediante CloudFormation

Esta end-to-end CloudFormation plantilla crea una asignación de recursos, un plan de respaldo y un almacén de respaldo de destino:

- Un almacén de copias de seguridad denominado *CloudFormationTestBackupVault*.
- Nombre de un plan de respaldo *CloudFormationTestBackupPlan*. Este plan contiene dos reglas de copia de seguridad, que hacen copias de seguridad todos los días a las 12 del mediodía UTC y las retienen durante 210 días.
- Una selección de recursos denominada *BackupSelectionName*.
- La asignación de recursos hace una copia de seguridad de los siguientes recursos:
 - Cualquier recurso etiquetado con el par clave-valor backupplan:dsi-sandbox-daily.
 - Cualquier recurso etiquetado con el valor prod o valores que comiencen por prod/.
- La asignación de recursos no hace una copia de seguridad de los siguientes recursos:
 - Cualquier clúster de RDS, Aurora, Neptune o DocumentDB.
 - Cualquier recurso etiquetado con el valor test o valores que comiencen por test/.

Description: "Template that creates Backup Selection and its dependencies"

Parameters:

BackupVaultName:

Type: String

Default: "CloudFormationTestBackupVault"

BackupPlanName:

Type: String

Default: "CloudFormationTestBackupPlan"

BackupSelectionName:

Type: String

Default: "CloudFormationTestBackupSelection"

```

BackupPlanTagValue:
  Type: String
  Default: "test-value-1"
RuleName1:
  Type: String
  Default: "TestRule1"
RuleName2:
  Type: String
  Default: "TestRule2"
ScheduleExpression:
  Type: String
  Default: "cron(0 12 * * ? *)"
StartWindowMinutes:
  Type: Number
  Default: 60
CompletionWindowMinutes:
  Type: Number
  Default: 120
RecoveryPointTagValue:
  Type: String
  Default: "test-recovery-point-value"
MoveToColdStorageAfterDays:
  Type: Number
  Default: 120
DeleteAfterDays:
  Type: Number
  Default: 210
Resources:
  CloudFormationTestBackupVault:
    Type: "AWS::Backup::BackupVault"
    Properties:
      BackupVaultName: !Ref BackupVaultName
  BasicBackupPlan:
    Type: "AWS::Backup::BackupPlan"
    Properties:
      BackupPlan:
        BackupPlanName: !Ref BackupPlanName
        BackupPlanRule:
          - RuleName: !Ref RuleName1
            TargetBackupVault: !Ref BackupVaultName
            ScheduleExpression: !Ref ScheduleExpression
            StartWindowMinutes: !Ref StartWindowMinutes
            CompletionWindowMinutes: !Ref CompletionWindowMinutes
            RecoveryPointTags:

```

```

        test-recovery-point-key-1: !Ref RecoveryPointTagValue
    Lifecycle:
        MoveToColdStorageAfterDays: !Ref MoveToColdStorageAfterDays
        DeleteAfterDays: !Ref DeleteAfterDays
    - RuleName: !Ref RuleName2
    TargetBackupVault: !Ref BackupVaultName
    ScheduleExpression: !Ref ScheduleExpression
    StartWindowMinutes: !Ref StartWindowMinutes
    CompletionWindowMinutes: !Ref CompletionWindowMinutes
    RecoveryPointTags:
        test-recovery-point-key-1: !Ref RecoveryPointTagValue
    Lifecycle:
        MoveToColdStorageAfterDays: !Ref MoveToColdStorageAfterDays
        DeleteAfterDays: !Ref DeleteAfterDays
    BackupPlanTags:
        test-key-1: !Ref BackupPlanTagValue
    DependsOn: CloudFormationTestBackupVault

TestRole:
    Type: "AWS::IAM::Role"
    Properties:
        AssumeRolePolicyDocument:
            Version: "2012-10-17"
            Statement:
                - Effect: "Allow"
                  Principal:
                      Service:
                          - "backup.amazonaws.com"
                  Action:
                      - "sts:AssumeRole"
        ManagedPolicyArns:
            - !Sub "arn:${AWS::Partition}:iam::aws:policy/service-
role/AWSBackupServiceRolePolicyForBackup"
    BasicBackupSelection:
        Type: 'AWS::Backup::BackupSelection'
    Properties:
        BackupPlanId: !Ref BasicBackupPlan
        BackupSelection:
            SelectionName: !Ref BackupSelectionName
            IamRoleArn: !GetAtt TestRole.Arn
        ListOfTags:
            - ConditionType: STRINGEQUALS
              ConditionKey: backupplan
              ConditionValue: dsi-sandbox-daily

```

```
NotResources:
  - 'arn:aws:rds:*:*:cluster:*'
Conditions:
  StringEquals:
    - ConditionKey: 'aws:ResourceTag/path'
      ConditionValue: prod
  StringNotEquals:
    - ConditionKey: 'aws:ResourceTag/path'
      ConditionValue: test
  StringLike:
    - ConditionKey: 'aws:ResourceTag/path'
      ConditionValue: prod/*
  StringNotLike:
    - ConditionKey: 'aws:ResourceTag/path'
      ConditionValue: test/*
```

Cuotas de asignación de recursos del plan de copia de seguridad

Las siguientes cuotas se aplican a una sola asignación de recursos:

- 500 nombres de recursos de Amazon (ARNs) sin caracteres comodín
- 30 ARNs con expresiones comodín
- 30 condiciones
- 30 etiquetas por asignación de recurso (y un número ilimitado de recursos por etiqueta)

Almacenes de copias de seguridad

En AWS Backup, una bóveda de copias de seguridad es un contenedor que almacena y organiza las copias de seguridad.

Al crear un almacén de copias de seguridad, debe especificar la clave de cifrado AWS Key Management Service (AWS KMS) que cifra algunas de las copias de seguridad almacenadas en este almacén. El cifrado de otras copias de seguridad lo administran sus AWS servicios de origen. Para obtener más información acerca del cifrado de copias de seguridad, consulte el gráfico [Cifrado para copias de seguridad en AWS](#).

En estas secciones se proporciona información general sobre cómo administrar los almacenes de copia de seguridad en AWS Backup.

Temas

- [Creación y eliminación de almacenes de copias de seguridad](#)
- [Tener un almacén aislado lógicamente](#)
- [Políticas de acceso a almacenes](#)
- [AWS Backup Vault Lock](#)

Creación y eliminación de almacenes de copias de seguridad

Debe crear al menos un almacén antes de crear un plan de copia de seguridad o iniciar un trabajo de copia de seguridad.

Cuando utiliza por primera vez la página Backup Vaults de la AWS Backup consola de una Región de AWS, la consola crea automáticamente un almacén predeterminado para la región.

Sin embargo, si utiliza AWS Backup el AWS SDK o CloudFormation el AWS CLI almacén predeterminado, no se crea un almacén predeterminado. Debe crear su propio almacén.

Permisos necesarios

Debe disponer de los siguientes permisos para crear un almacén de copias de seguridad mediante AWS Backup.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowKMSOperations",
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:DescribeKey",
        "kms:RetireGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "arn:aws:kms:us-east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    {
      "Sid": "AllowCreateBackupVault",
      "Effect": "Allow",
      "Action": [
        "backup:CreateBackupVault"
      ],
      "Resource": "arn:aws:backup:us-east-1:444455556666:backup-vault:*"
    },
    {
      "Sid": "AllowMountCapsule",
      "Effect": "Allow",
      "Action": [
        "backup-storage:MountCapsule"
      ],
      "Resource": "*"
    }
  ]
}
```

Creación de un almacén de copias de seguridad (consola)

En lugar de utilizar el almacén de copias de seguridad predeterminado que se crea automáticamente en la consola de AWS Backup, puede crear almacenes de copia de seguridad específicos para guardar y organizar grupos de copias de seguridad en el mismo almacén.

Cómo crear un almacén de copias de seguridad

1. En la AWS Backup consola, en el panel de navegación, seleccione Backup Vaults.

Note

Si el panel de navegación no está visible en el lado izquierdo, puede abrirlo seleccionando el icono de menú situado en la esquina superior izquierda de la consola. AWS Backup

2. Seleccione Create backup vault (Crear almacén de copias de seguridad).
3. Escriba un nombre para su almacén de copias de seguridad. Puede asignar un nombre a su almacén para reflejar lo que almacenará en él o para facilitar la búsqueda de las copias de seguridad que necesite. Por ejemplo, podría denominarlo **FinancialBackups**.
4. Seleccione una tecla AWS Key Management Service (AWS KMS). Puede usar una clave que ya haya creado o seleccionar la clave AWS Backup KMS predeterminada.

Note

La AWS KMS clave que se especifica aquí solo se aplica a las copias de seguridad de los servicios que admiten el cifrado AWS Backup independiente. Para ver la lista de tipos de recursos que admiten el cifrado AWS Backup independiente, consulte la sección «AWS Backup Administración total» de la [Disponibilidad de características por recurso](#) tabla.

5. Opcionalmente, añada etiquetas que le ayudarán a buscar e identificar el almacén de copias de seguridad. Por ejemplo, podría añadir una etiqueta **BackupType:Financial**.
6. Seleccione Create Backup vault (Crear almacén de copias de seguridad).
7. En el panel de navegación, elija Backup vaults (Almacenes de copias de seguridad) y verifique que se ha añadido el almacén de copias de seguridad.

 Note

Ahora puede editar una regla de uno de los planes para que las copias de seguridad creadas por esa regla se guarden en el almacén que acaba de crear.

Creación de un almacén de copias de seguridad (mediante programación)

El siguiente AWS Command Line Interface comando crea una bóveda de respaldo:

```
aws backup create-backup-vault --backup-vault-name test-vault
```

También puede especificar las siguientes configuraciones para un almacén de copias de seguridad.

Nombre del almacén de copias de seguridad

Los nombres de los almacenes de copia de seguridad distinguen entre mayúsculas y minúsculas. Deben tener de 2 a 50 caracteres alfanuméricos, guiones o guiones bajos.

AWS KMS clave de cifrado

La clave AWS KMS de cifrado protege sus copias de seguridad en esta bóveda de copias de seguridad. De forma predeterminada, AWS Backup crea una clave de KMS con el alias `aws/backup` automáticamente. Puede elegir esa clave o cualquier otra clave de su cuenta (las claves de KMS entre cuentas se pueden usar mediante la CLI).

Puede crear una nueva clave de cifrado siguiendo el procedimiento [Creating Keys](#) de la Guía para desarrolladores de AWS Key Management Service .

Después de crear una bóveda de respaldo y configurar la clave de AWS KMS cifrado, ya no podrá editar la clave de esa bóveda de respaldo.

La clave de cifrado que se especifica en un AWS Backup almacén se aplica a las copias de seguridad de determinados tipos de recursos. Para obtener más información acerca del cifrado de copias de seguridad, consulte [Cifrado de copias de seguridad en AWS Backup](#) en la sección Seguridad. Las copias de seguridad de los demás tipos de recursos se realizan con la clave que se usa para cifrar el recurso de origen.

Etiquetas de almacén de copias de seguridad

Estas etiquetas están asociadas al almacén de copias de seguridad para ayudarle a organizar y realizar un seguimiento de sus almacenes de copias de seguridad.

Eliminar un almacén

Para evitar la eliminación masiva accidental o malintencionada, solo puede eliminar un almacén de copias de seguridad en AWS Backup después de eliminar (o de que su plan de copia de seguridad complete el ciclo de vida) todos los puntos de recuperación del almacén de copias de seguridad. Para eliminar todos los puntos de recuperación manualmente, consulte [Depuración de recursos](#).

Cuando se elimina un almacén de copias de seguridad, actualice los planes de copias de seguridad para que apunten a nuevos almacenes de copias de seguridad. Un plan de copias de seguridad que apunte a un almacén de copias de seguridad eliminado provocará un error en la creación de la copia de seguridad.

No puede eliminar el almacén de copias de seguridad predeterminado o el almacén de copias de seguridad automáticas de Amazon EFS mediante Consola de administración de AWS. Puede eliminar un almacén de respaldo predeterminado utilizando el AWS CLI si está vacío. Sin embargo, si abre la AWS Backup consola y selecciona esa región, la consola vuelve a crear el almacén de copias de seguridad predeterminado. Puede eliminar las instantáneas no utilizadas en el almacén de copias de seguridad automático de Amazon EFS.

Para eliminar un almacén de copias de seguridad mediante la consola AWS Backup

1. Inicie sesión en y abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
[Consola de administración de AWS](#)
2. En el panel de navegación, elija Backup vaults (Almacenes de copia de seguridad).
3. Elija el nombre del almacén de copias de seguridad para abrir su página de detalles.
4. Elija y elimine todas las copias de seguridad que estén asociadas al almacén de copias de seguridad.
5. Elija Eliminar almacén. Cuando le pidan confirmación, escriba el nombre del almacén y elija Eliminar almacén de copias de seguridad.

Tener un almacén aislado lógicamente

Información general de los almacenes aislados lógicamente

AWS Backup ofrece un tipo de almacén secundario que puede almacenar las copias de seguridad en un contenedor con funciones de seguridad adicionales. Una bóveda hermética lógica es una bóveda especializada que proporciona una seguridad superior a la de una bóveda de copias de seguridad estándar, además de la posibilidad de compartir el acceso a la bóveda con otras cuentas, de modo que los objetivos de tiempo de recuperación (RTOs) puedan ser más rápidos y flexibles en caso de que se produzca un incidente que requiera una restauración rápida de los recursos.

Lógicamente, las bóvedas herméticas vienen equipadas con funciones de protección adicionales; cada bóveda se cifra con una [AWS clave](#) propia (predeterminada) o, opcionalmente, con una clave KMS administrada por el cliente, y cada bóveda está equipada con el modo de cumplimiento de [AWS Backup Vault Lock](#). La información sobre el tipo de clave de cifrado es visible a través de una consola para generar informes de transparencia AWS Backup APIs y conformidad.

Puede integrar sus bóvedas herméticas de forma lógica con la [aprobación de varias partes](#) (MPA) para poder recuperar las copias de seguridad que se encuentran en las bóvedas, incluso si no se puede acceder a la cuenta propietaria del almacén, lo que ayuda a mantener la continuidad empresarial. Además, puede optar por integrarse con [AWS Resource Access Manager](#)(RAM) para compartir una bóveda aislada de forma lógica con otras AWS cuentas (incluidas las cuentas de otras organizaciones), de modo que las copias de seguridad almacenadas en la bóveda se puedan restaurar desde una cuenta con la que se comparte la bóveda, si es necesario para [realizar pruebas de recuperación ante pérdidas de datos o de restauración](#). Como parte de esta seguridad adicional, un almacén cerrado de forma lógica almacena sus copias de seguridad en una cuenta propiedad del AWS Backup servicio (lo que hace que las copias de seguridad se muestren como compartidas fuera de la organización en los elementos de atributos de modificación de los AWS CloudTrail registros).

Para aumentar la resiliencia, te recomendamos crear copias entre regiones en bóvedas agrupadas de forma lógica en cuentas iguales o independientes. Sin embargo, si quiere reducir los costes de almacenamiento manteniendo una sola copia, puede utilizar las [copias de seguridad principales para almacenar de forma lógica espacios vacíos, tras incorporarlas a MPA](#). AWS

En la página de [precios de AWS Backup](#), puede consultar los precios del almacenamiento de las copias de seguridad de los servicios compatibles en un almacén aislado lógicamente.

Consulte en [Disponibilidad de características por recurso](#) los tipos de recursos que puede copiar en un almacén aislado lógicamente.

Temas

- [Caso de uso para almacenes aislados lógicamente](#)
- [Comparación y contraste con un almacén de copias de seguridad estándar](#)
- [Crear un almacén aislado lógicamente](#)
- [Visualización de los detalles del almacén aislado lógicamente](#)
- [Crear copias de seguridad en un almacén cerrado de forma lógica](#)
- [Compartir un almacén aislado lógicamente](#)
- [Restauración de una copia de seguridad desde un almacén aislado lógicamente](#)
- [Eliminar un almacén aislado lógicamente](#)
- [Opciones de programación adicionales para almacenes aislados lógicamente](#)
- [Descripción de los tipos de claves de cifrado para bóvedas aisladas de forma lógica](#)
- [Solución de un problema de almacén aislado lógicamente](#)
- [Copias de seguridad principales en almacenes aislados lógicamente](#)
- [Aprobación de varias partes para almacenes aislados lógicamente](#)

Caso de uso para almacenes aislados lógicamente

Un almacén aislado lógicamente es un almacén secundario que sirve como parte de una estrategia de protección de datos. Este almacén puede ayudar a mejorar la estrategia de retención y la recuperación de su organización cuando quiera un almacén para sus copias de seguridad que

- esté configurado automáticamente con un bloqueo de almacén en [modo de cumplimiento](#);
- De forma predeterminada, ofrece cifrado con una clave propia. AWS Si lo desea, puede proporcionar una clave gestionada por el cliente
- Contiene copias de seguridad que, mediante AWS RAM MPA, se pueden compartir y restaurar desde una cuenta diferente a la que creó la copia de seguridad

Consideraciones y limitaciones

- La copia entre regiones en un almacén aislado lógicamente o desde este no está disponible actualmente para las copias de seguridad que contienen Amazon Aurora, Amazon DocumentDB y Amazon Neptune.

- Una copia de seguridad que contenga uno o más volúmenes de Amazon EBS y que se copie en un almacén aislado lógicamente debe tener un tamaño inferior a 16 TB; no se admiten copias de seguridad para este tipo de recurso que sean de mayor tamaño.
- [EC2 Se permiten EC2](#) ofertas de Amazon AMIs. Si esta configuración está habilitada en su cuenta, añada el alias `aws-backup-vault` a su lista de permitidos.

Si no se incluye este alias, las operaciones de copia de un almacén con espacios vacíos de forma lógica a un almacén de respaldo y las operaciones de restauración de EC2 instancias desde un almacén con espacios vacíos de forma lógica fallarán y aparecerá un mensaje de error como «La AMI de origen ami-xxxxxx no se encuentra en la región».

- El ARN (nombre de recurso de Amazon) de un punto de recuperación almacenado en un almacén aislado lógicamente sustituirá al tipo de recurso subyacente por `backup`. Por ejemplo, si el ARN original comienza por `arn:aws:ec2:region::image/ami-*`, entonces el ARN del punto de recuperación en el almacén aislado lógicamente será `arn:aws:backup:region:account-id:recovery-point:*`.

Puede utilizar el comando CLI [list-recovery-points-by-backup-vault](#) para determinar el ARN.

Comparación y contraste con un almacén de copias de seguridad estándar

Un almacén de copias de seguridad es el tipo de almacén principal y estándar que se utiliza en AWS Backup. Cada copia de seguridad se almacena en un almacén de copias de seguridad cuando se crea la copia de seguridad. Puede asignar políticas basadas en recursos para administrar las copias de seguridad almacenadas en el almacén, como el ciclo de vida de las copias de seguridad almacenadas.

Un almacén aislado lógicamente es un almacén especializado con seguridad adicional y uso compartido flexible para acelerar el tiempo de recuperación (RTO). Este almacén almacena las copias de seguridad principales o copias de las copias de seguridad que se crearon inicialmente y se almacenaron en una bóveda de copias de seguridad estándar.

Los almacenes de copias de seguridad se cifran con una clave, que es un mecanismo de seguridad que limita el acceso a los usuarios previstos. Estas claves pueden gestionarse o AWS gestionarse por el cliente. Consulte [Cifrado de copias](#) para conocer el comportamiento de cifrado durante los trabajos de copia, incluida la copia en un almacén aislado lógicamente.

Además, un almacén de copias de seguridad tener más seguridad con un bloqueo de almacén; los almacenes aislados lógicamente vienen equipados con un bloqueo de almacén en modo de cumplimiento.

[Al igual que las bóvedas de respaldo, las bóvedas con huecos lógicos también admiten etiquetas restringidas para las copias de seguridad de Amazon. EC2](#)

Característica	Almacén de copias de seguridad	Tener un almacén aislado lógicamente
AWS Backup Audit Manager	Puede utilizar AWS Backup Audit Manager Controles y corrección para supervisar sus almacenes de backup.	Asegúrese de que la copia de seguridad de un recurso específico se almacene en al menos una bóveda aislada de forma lógica según un cronograma que usted determine, además de los controles disponibles para las bóvedas estándar.
Facturación	Los cargos por almacenamiento y transferencia de datos de los recursos totalmente administrados por AWS Backup figuran en "AWS Backup". Los cargos de almacenamiento y transferencia de datos de otros tipos de recursos se aplicarán en sus respectivos servicios. Por ejemplo, las copias de seguridad de Amazon EBS se mostrarán en "Amazon EBS"; las copias de seguridad de Amazon S3 se mostrarán en "AWS Backup".	Todos los cargos de facturación de estos almacenes (almacenamiento o transferencia de datos) se incluyen en "AWS Backup".

Característica	Almacén de copias de seguridad	Tener un almacén aislado lógicamente
Regiones	Disponible en todas las regiones en las que opera AWS Backup	Disponible en la mayoría de las regiones compatibles con AWS Backup. Actualmente no está disponible en Asia Pacífico (Malasia), Canadá Oeste (Calgary), México (Central), Asia Pacífico (Tailandia), Asia Pacífico (Taipéi), Asia Pacífico (Nueva Zelanda), China (Pekín), China (Ningxia), (EE. UU. Este) o (EE. UU. Oeste) AWS GovCloud . AWS GovCloud
Recursos	Puede almacenar copias de copias de seguridad para la mayoría de los tipos de recursos que admiten las copias entre cuentas.	Consulte la columna del almacén aislado lógicamente en Disponibilidad de características por recurso para ver los recursos que se pueden copiar a este almacén.
Restaurar	Las copias de seguridad se pueden restaurar por medio de la misma cuenta a la que pertenece el almacén.	Las copias de seguridad se pueden restaurar con una cuenta distinta de la que es propietaria del almacén si el almacén se comparte con esa cuenta independiente.

Característica	Almacén de copias de seguridad	Tener un almacén aislado lógicamente
Seguridad	Opcionalmente, se puede cifrar con una clave (administrada por AWS o por el cliente) Puede utilizar opcionalmente un bloqueo de almacén en modo de cumplimiento o gobernanza	Se puede cifrar con una clave propia o AWS gestionada por el cliente Siempre se bloquea con un bloqueo de almacén en modo de cumplimiento La información sobre el tipo de clave de cifrado se conserva y es visible cuando los almacenes se comparten a través AWS RAM de un MPA
Uso compartido	El acceso se puede administrar mediante políticas y AWS Organizations No es compatible con AWS RAM	Opcionalmente, se puede compartir entre cuentas mediante AWS RAM

Crear un almacén aislado lógicamente

Puede crear una bóveda aislada de forma lógica a través de la AWS Backup consola o mediante una combinación de AWS Backup comandos CLI AWS RAM .

Cada almacén aislado lógicamente viene equipado con un bloqueo de almacén en modo de cumplimiento. Consulte [AWS Backup Vault Lock](#) para determinar los valores del período de retención más adecuados para su operación

Console

Creación de un almacén aislado lógicamente desde la consola

1. [Abra la AWS Backup consola en /backup. https://console.aws.amazon.com](https://console.aws.amazon.com/backup/)

2. En el panel de navegación, seleccione Almacenes.
3. Se mostrarán ambos tipos de almacén. Seleccione Crear nuevo almacén.
4. Escriba un nombre para su almacén de copias de seguridad. Puede asignar un nombre a su almacén para reflejar lo que almacenará en él o para facilitar la búsqueda de las copias de seguridad que necesite. Por ejemplo, podría denominarlo `FinancialBackups`.
5. Seleccione el botón de opción de Almacén aislado lógicamente.
6. (Opcional) Elija una clave de cifrado. Puede seleccionar una clave KMS administrada por el cliente para tener un control adicional sobre el cifrado o usar la clave de AWS propiedad predeterminada (se recomienda).
7. Establezca el Periodo de retención mínimo.

Este valor (en días, meses o años) es el tiempo mínimo que se puede retener una copia de seguridad en este almacén. Las copias de seguridad con periodos de retención inferiores a este valor no se podrán copiar a este almacén.

El valor mínimo permitido es 7 días. Los valores de meses y años cumplen con este mínimo.

8. Establezca el Periodo de retención máximo.

Este valor (en días, meses o años) es el tiempo máximo que se puede retener una copia de seguridad en este almacén. Las copias de seguridad con periodos de retención superiores a este valor no se podrán copiar a este almacén.

9. (Opcional) Defina la clave de cifrado.

Especifique la clave que se va a utilizar con la bóveda. Puede elegir una AWS clave propia (gestionada por AWS Backup) o introducir el ARN de una clave gestionada por el cliente que, preferiblemente, pertenezca a una cuenta diferente a la que tenga acceso. AWS Backup recomienda utilizar una clave AWS propia.

10. (Opcional) Agregue etiquetas que le ayuden a buscar e identificar su almacén aislado lógicamente. Por ejemplo, podría añadir una etiqueta `BackupType:Financial`.
11. Seleccione Crear almacén.
12. Revise la configuración. Si todos los ajustes se muestran como esperaba, seleccione Crear almacén aislado lógicamente.
13. La consola le llevará a la página de detalles del nuevo almacén. Compruebe que los detalles del almacén son los esperados.

14. Seleccione Almacenes para ver los almacenes de su cuenta. Aparecerá su almacén aislado lógicamente. La clave de KMS estará disponible aproximadamente entre 1 y 3 minutos después de la creación del almacén. Actualice la página para ver la clave asociada. Una vez que la clave esté visible, el almacén estará disponible y se podrá utilizar.

AWS CLI

Crear un almacén aislado lógicamente desde CLI

Se puede utilizar AWS CLI para realizar operaciones mediante programación en bóvedas con huecos de forma lógica. Cada CLI es específica del AWS servicio en el que se origina. Los comandos relacionados con el uso compartido llevan el prefijo `aws ram`; todos los demás comandos deben llevar el prefijo `aws backup`.

Utilice el comando de CLI [create-logically-air-gapped-backup-vault](#) modificado con los parámetros siguientes:

```
aws backup create-logically-air-gapped-backup-vault
--region us-east-1 // optional
--backup-vault-name sampleName // required
--min-retention-days 7 // required Value must be an integer 7 or greater
--max-retention-days 35 // required
--encryption-key-arn arn:aws:kms:us-east-1:123456789012:key/12345678-1234-1234-1234-123456789012 // optional
--creator-request-id 123456789012-34567-8901 // optional
```

El `--encryption-key-arn` parámetro opcional le permite especificar una clave KMS administrada por el cliente para el cifrado del almacén. Si no se proporciona, el almacén utilizará una clave propia AWS.

Ejemplo de comando de CLI para crear un almacén aislado lógicamente:

```
aws backup create-logically-air-gapped-backup-vault
--region us-east-1
--backup-vault-name sampleName
--min-retention-days 7
--max-retention-days 35
--creator-request-id 123456789012-34567-8901 // optional
```

Ejemplo de comando CLI para crear una bóveda aislada de forma lógica con cifrado administrado por el cliente:

```
aws backup create-logically-air-gapped-backup-vault
--region us-east-1
--backup-vault-name sampleName
--min-retention-days 7
--max-retention-days 35
--encryption-key-arn arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012
--creator-request-id 123456789012-34567-8901 // optional
```

Consulte los [elementos de respuesta CreateLogicallyAirGappedBackupVault de la API](#) para obtener información después de la operación de creación. Si la operación se realizó correctamente, la nueva bóveda con huecos lógicos tendrá el de. VaultState CREATING

Una vez que se complete la creación y se haya asignado la clave cifrada KMS, VaultState pasará a. AVAILABLE Cuando esté disponible, se podrá utilizar el almacén. VaultState se puede recuperar llamando a [DescribeBackupVault](#) o [ListBackupVaults](#).

Visualización de los detalles del almacén aislado lógicamente

Puede ver los detalles del almacén, como el resumen, los puntos de recuperación, los recursos protegidos, el uso compartido de cuentas, la política de acceso y las etiquetas, a través de la AWS Backup consola o la AWS Backup CLI.

Console

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación izquierdo, seleccione Almacenes.
3. Debajo de las descripciones de las bóvedas hay tres listas: las bóvedas creadas por esta cuenta, las bóvedas compartidas mediante la RAM y las bóvedas a las que se puede acceder mediante la aprobación de varias partes. Seleccione la pestaña que desee para ver los almacenes.
4. En Nombre del almacén , haga clic en el nombre del almacén para abrir la página de detalles. Puede ver el resumen, los puntos de recuperación, los recursos protegidos, las cuentas compartidas, la política de acceso y los detalles de las etiquetas.

Los detalles mostrados dependen del tipo de cuenta: las cuentas que poseen un almacén pueden ver las cuentas compartidas; las cuentas que no poseen un almacén no podrán ver las cuentas compartidas. En el caso de los almacenes compartidos, el tipo de clave de

cifrado (clave KMS AWS propiedad o gestionada por el cliente) se muestra en el resumen del almacén.

AWS CLI

Visualización de detalles de un almacén aislado lógicamente mediante la CLI

El comando de CLI [describe-backup-vault](#) se puede utilizar para obtener detalles sobre un almacén. El parámetro `backup-vault-name` es obligatorio; `region` es opcional.

```
aws backup describe-backup-vault
--region us-east-1
--backup-vault-name testvaultname
```

Ejemplo de respuesta:

```
{
  "BackupVaultName": "LOG-AIR-GAP-VAULT-TEST",
  "BackupVaultArn": "arn:aws:backup:us-east-1:234567890123:backup-vault:IAD-LAGV-01",
  "VaultType": "LOGICALLY_AIR_GAPPED_BACKUP_VAULT",
  "EncryptionKeyType": "AWS_OWNED_KMS_KEY",
  "CreationDate": "2024-07-25T16:05:23.554000-07:00",
  "NumberOfRecoveryPoints": 0,
  "Locked": true,
  "MinRetentionDays": 8,
  "MaxRetentionDays": 30,
  "LockDate": "2024-07-25T16:05:23.554000-07:00"
}
```

Crear copias de seguridad en un almacén cerrado de forma lógica

Lógicamente, las bóvedas con espacios vacíos pueden ser el destino de un trabajo de copia en un plan de respaldo o un objetivo para un trabajo de copia bajo demanda. También se puede utilizar como destino principal de la copia de seguridad. Consulte [Copias de seguridad principales en bóvedas aisladas de forma lógica](#).

Cifrado compatible

Para completar un trabajo de copia correctamente desde un almacén de copias de seguridad a un almacén aislado lógicamente, es necesaria una clave de cifrado determinada por el tipo de recurso que se va a copiar.

Al crear o copiar una copia de seguridad de un [tipo de recurso totalmente gestionado, el recurso](#) de origen se puede cifrar mediante una clave gestionada por el cliente o mediante una clave gestionada. AWS

Al crear o copiar una copia de seguridad de otros tipos de recursos (los que [no estén totalmente gestionados](#)), la fuente debe cifrarse con una clave gestionada por el cliente. AWS no se admiten las claves administradas para los recursos que no están completamente administrados.

Cree o copie copias de seguridad en una bóveda aislada de forma lógica mediante un plan de copias de seguridad

Puede copiar una copia de seguridad (punto de recuperación) de una bóveda de copias de seguridad estándar a una bóveda vacía de forma lógica [creando un nuevo plan de copias](#) de seguridad o [actualizando uno existente](#) en la AWS Backup consola o mediante los comandos y. AWS CLI [create-backup-planupdate-backup-plan](#) También puede crear copias de seguridad directamente en una bóveda aislada de forma lógica utilizándola como destino principal. Consulte [Copias de seguridad principales en bóvedas con espacios vacíos de forma lógica para obtener más información](#).

Puede copiar bajo demanda una copia de seguridad de un almacén aislado lógicamente a otro (este tipo de copia de seguridad no se puede programar en un plan de copias de seguridad). Puede copiar una copia de seguridad de un almacén aislado lógicamente a un almacén de copias de seguridad estándar siempre que la copia esté cifrada con una clave administrada por el cliente.

Copia de seguridad bajo demanda a un almacén aislado lógicamente

Para crear una copia única y [bajo demanda](#) de una copia de seguridad en un almacén aislado lógicamente, puede copiarla desde un almacén de copias de seguridad estándar. Las copias entre regiones o entre cuentas están disponibles si el tipo de recurso es compatible con el tipo de copia.

Disponibilidad de copias

Se puede crear una copia de seguridad desde la cuenta a la que pertenece el almacén. Las cuentas con las que se ha compartido el almacén tienen la capacidad de ver o restaurar una copia de seguridad, pero no de crear una copia.

Solo se pueden incluir [los tipos de recursos que admitan la copia entre regiones o entre cuentas](#).

Console

1. [Abra la consola en /backup. AWS Backup https://console.aws.amazon.com](https://console.aws.amazon.com/backup)
2. En el panel de navegación izquierdo, seleccione Almacenes.
3. En la página de detalles del almacén, se muestran todos los puntos de recuperación del almacén. Coloque una marca de verificación junto al punto de recuperación que desee copiar.
4. Seleccione Acciones y Editar en el menú desplegable.
5. En la siguiente pantalla, introduzca los detalles del destino.
 - a. Especifique la región de destino.
 - b. El menú desplegable del almacén de copias de seguridad de destino muestra los almacenes de destino elegibles. Seleccione uno con el tipo `logically air-gapped vault`
6. Seleccione Copiar una vez que todos los detalles estén configurados según sus preferencias.

En la página Trabajos de la consola, puede seleccionar Trabajos de copia para ver los trabajos de copia actuales.

AWS CLI

Utilice [start-copy-job](#) para copiar una copia de seguridad existente en almacén de copias de seguridad a un almacén aislado lógicamente.

Ejemplo de entrada de la CLI:

```
aws backup start-copy-job
--region us-east-1
--recovery-point-arn arn:aws:resourcetype:region::snapshot/snap-12345678901234567
--source-backup-vault-name sourcevaultname
--destination-backup-vault-arn arn:aws:backup:us-east-1:123456789012:backup-vault:destinationvaultname
--iam-role-arn arn:aws:iam::123456789012:role/service-role/servicerole
```

Para obtener más información, consulte [Copia de una copia de seguridad](#), [Copia de seguridad entre regiones](#) y [Copia de seguridad entre cuentas](#).

Compartir un almacén aislado lógicamente

Puede usar AWS Resource Access Manager (RAM) para compartir una bóveda aislada de forma lógica con otras cuentas que designe. Al compartir depósitos, la información sobre el tipo de clave de cifrado (clave KMS propia o AWS gestionada por el cliente) se conserva y es visible para las cuentas con las que se comparte el depósito.

Un almacén se puede compartir con una cuenta de su organización o con una cuenta de otra organización. El almacén no se puede compartir con toda la organización, solo con las cuentas de la organización.

Solo las cuentas con determinados privilegios de IAM pueden compartir y administrar el uso compartido de almacenes.

Para compartir el uso AWS RAM, asegúrese de tener lo siguiente:

- Dos o más cuentas a las que puedan acceder AWS Backup
- Una cuenta propietaria de almacenes que quiera compartir tiene los permisos de RAM necesarios. El permiso `ram:CreateResourceShare` es necesario para realizar este procedimiento. La política `AWSResourceAccessManagerFullAccess` contiene todos los permisos relacionados con RAM necesarios:
 - `backup:DescribeBackupVault`
 - `backup:DescribeRecoveryPoint`
 - `backup:GetRecoveryPointRestoreMetadata`
 - `backup:ListProtectedResourcesByBackupVault`
 - `backup:ListRecoveryPointsByBackupVault`
 - `backup:ListTags`
 - `backup:StartRestoreJob`
- Al menos un almacén aislado lógicamente

Console

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación izquierdo, seleccione Almacenes.

3. Debajo de las descripciones de los almacenes hay dos listas: Almacenes propiedad de esta cuenta y Almacenes compartidos con esta cuenta. Los almacenes propiedad de la cuenta son aptos para compartirse.
4. En Nombre del almacén , seleccione el nombre del almacén aislado lógicamente para abrir la página de detalles.
5. El panel de Uso compartido de cuentas muestra con qué cuentas se comparte el almacén.
6. Para empezar a compartir con otra cuenta o editar las cuentas que ya se comparten, seleccione Administrar el uso compartido.
7. La AWS RAM consola se abre cuando se selecciona Administrar el uso compartido. Para ver los pasos para compartir un recurso mediante la AWS RAM, consulte [Crear un recurso compartido en la AWS RAM](#) en la Guía del usuario de AWS RAM.
8. La cuenta invitada a aceptar una invitación para recibir un recurso compartido tiene 12 horas para aceptarla. Consulte [Accepting and rejecting resource share invitations](#) en la Guía del usuario de AWS RAM.
9. Si ha completado y aceptado los pasos para compartir, la página de resumen del almacén aparecerá en la sección Uso compartido de cuentas = “Compartido; consulte la tabla de cuentas compartidas que aparece a continuación”.

AWS CLI

AWS RAM usa el comando `CLI create-resource-share`. El acceso a este comando solo está disponible para cuentas con suficientes permisos. Consulte [Creating a resource share in AWS RAM](#) para ver los pasos de la CLI.

Los pasos 1 a 4 se llevan a cabo con la cuenta propietaria del almacén aislado lógicamente. Los pasos 5 a 8 se llevan a cabo con la cuenta con la que se compartirá el almacén aislado lógicamente.

1. Inicie sesión en la cuenta propietaria O solicite que complete estos pasos un usuario de su organización con suficientes credenciales para acceder a la cuenta de origen.
 - Si antes se había creado un recurso compartido y desea agregarle un recurso adicional, utilice, en cambio, la CLI `associate-resource-share` con el ARN del nuevo almacén.
2. Obtenga las credenciales de un rol con permisos suficientes para compartir a través de RAM. [Introdúzcalos en la CLI.](#)

- El permiso `ram:CreateResourceShare` es necesario para realizar este procedimiento. La política [AWSResourceAccessManagerFullAccess](#) contiene todos los permisos relacionados con la RAM.

3. Utilice [create-resource-share](#).

- a. Incluya el ARN del almacén aislado lógicamente.
- b. Ejemplo de entrada:

```
aws ram create-resource-share
--name MyLogicallyAirGappedVault
--resource-arns arn:aws:backup:us-east-1:123456789012:backup-vault:test-
vault-1
--principals 123456789012
--region us-east-1
```

- c. Ejemplo de salida:

```
{
  "resourceShare":{
    "resourceShareArn":"arn:aws:ram:us-east-1:123456789012:resource-
share/12345678-abcd-09876543",
    "name":"MyLogicallyAirGappedVault",
    "owningAccountId":"123456789012",
    "allowExternalPrincipals":true,
    "status":"ACTIVE",
    "creationTime":"2021-09-14T20:42:40.266000-07:00",
    "lastUpdatedTime":"2021-09-14T20:42:40.266000-07:00"
  }
}
```

4. Copie el ARN del recurso compartido en el resultado (lo que es necesario para los pasos siguientes). Entregue el ARN al operador de la cuenta a la que invita a recibir el uso compartido.
5. Obtenga el ARN del recurso compartido.
 - a. Si no ha realizado los pasos 1 a 4, obtenga el permiso `resourceShareArn` de quien lo haya hecho.
 - b. Ejemplo: `arn:aws:ram:us-east-1:123456789012:resource-share/12345678-abcd-09876543`

6. En la CLI, asuma las credenciales de la cuenta del destinatario.
7. Obtenga una invitación para compartir recursos con [get-resource-share-invitations](#). Para obtener más información, consulte [Accepting and rejecting invitations](#) en la Guía del usuario de AWS RAM .
8. Acepte la invitación en la cuenta de destino (recuperación).
 - Use [accept-resource-share-invitation](#) (también puede [reject-resource-share-invitation](#)).

Puede usar los comandos AWS RAM CLI para ver los elementos compartidos:

- Recursos que ha compartido:

```
aws ram list-resources --resource-owner SELF --resource-type  
backup:backup-vault --region us-east-1
```

- Mostrar la entidad principal:

```
aws ram get-resource-share-associations --association-type PRINCIPAL  
--region us-east-1
```

- Recursos compartidos por otras cuentas:

```
aws ram list-resources --resource-owner OTHER-ACCOUNTS --resource-type  
backup:backup-vault --region us-east-1
```

Restauración de una copia de seguridad desde un almacén aislado lógicamente

Puede restaurar una copia de seguridad almacenada en un almacén aislado lógicamente desde la cuenta propietaria del almacén o desde cualquier cuenta con la que se comparta el almacén.

Consulte [Restauración de una copia de seguridad](#) para obtener información sobre cómo restaurar un punto de recuperación mediante la consola AWS Backup .

Una vez que se haya compartido una copia de seguridad desde un almacén aislado lógicamente con su cuenta, podrá utilizar [start-restore-job](#) para restaurarla.

Un ejemplo de entrada de la CLI puede incluir el comando y los parámetros siguientes:

```
aws backup start-restore-job
--recovery-point-arn arn:aws:backup:us-east-1:accountnumber:recovery-
point:RecoveryPointID
--metadata {"availabilityzone\":\"us-east-1d\"}
--idempotency-token TokenNumber
--resource-type ResourceType
--iam-role arn:aws:iam::number:role/service-role/servicerole
--region us-east-1
```

Eliminar un almacén aislado lógicamente

Consulte [Eliminación de un almacén](#). Los almacenes no se pueden eliminar si aún contienen copias de seguridad (puntos de recuperación). Asegúrese de que el almacén esté vacío antes de iniciar una operación de eliminación.

Al eliminar un almacén, también se elimina la clave asociada al almacén siete días después de su eliminación, de acuerdo con la política de eliminación de claves.

El siguiente comando de la CLI de ejemplo, [delete-backup-vault](#), se puede utilizar para eliminar un almacén.

```
aws backup delete-backup-vault
--region us-east-1
--backup-vault-name testvaultname
```

Opciones de programación adicionales para almacenes aislados lógicamente

El comando de la CLI [list-backup-vaults](#) se puede modificar para enumerar todos los almacenes que pertenecen a la cuenta y están presentes en ella:

```
aws backup list-backup-vaults
--region us-east-1
```

Para enumerar solo los almacenes aislados lógicamente, agregue el parámetro

```
--by-vault-type LOGICALLY_AIR_GAPPED_BACKUP_VAULT
```

Incluya el parámetro `by-shared` para filtrar la lista de almacenes devuelta para mostrar solo los almacenes aislados lógicamente compartidos. La respuesta incluirá información sobre el tipo de clave de cifrado de cada almacén compartido.

```
aws backup list-backup-vaults
--region us-east-1
--by-shared
```

Ejemplo de respuesta que muestra información sobre el tipo de clave de cifrado:

```
{
  "BackupVaultList": [
    {
      "BackupVaultName": "shared-logically air-gapped-vault",
      "BackupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-
vault:shared-logically air-gapped-vault",
      "VaultType": "LOGICALLY_AIR_GAPPED_BACKUP_VAULT",
      "EncryptionKeyType": "AWS_OWNED_KMS_KEY",
      "CreationDate": "2024-07-25T16:05:23.554000-07:00",
      "Locked": true,
      "MinRetentionDays": 7,
      "MaxRetentionDays": 30
    }
  ]
}
```

Descripción de los tipos de claves de cifrado para bóvedas aisladas de forma lógica

Lógicamente, las bóvedas con huecos vacíos admiten diferentes tipos de claves de cifrado, y esta información es visible a través de una consola. AWS Backup APIs Cuando las bóvedas se comparten a través AWS RAM de una MPA, la información del tipo de clave de cifrado se conserva y se hace visible para las cuentas con las que se comparte la bóveda. Esta transparencia le ayuda a comprender la configuración de cifrado de los almacenes y a tomar decisiones informadas sobre las operaciones de copia de seguridad y restauración.

Valores de los tipos de clave de cifrado

El `EncryptionKeyType` campo puede tener los siguientes valores:

- **AWS_OWNED_KMS_KEY**- La bóveda está cifrada con una clave AWS propia. Este es el método de cifrado predeterminado para las bóvedas aisladas de forma lógica cuando no se especifica ninguna clave gestionada por el cliente.
- **CUSTOMER_MANAGED_KMS_KEY**- El almacén se cifra con una clave KMS gestionada por el cliente que usted controla. Esta opción proporciona un control adicional sobre las claves de cifrado y las políticas de acceso.

Note

- AWS Backup recomienda utilizar las llaves AWS propias con bóvedas cerradas de forma lógica. Sin embargo, si la política de su organización exige el uso de una clave administrada por el cliente, utilice las claves de otra cuenta de una organización secundaria dedicada a la recuperación como práctica recomendada. Puede consultar el blog [Encrypt AWS Backup: bóvedas aisladas de forma lógica con claves gestionadas por el cliente para obtener más información sobre la configuración de bóvedas](#) aisladas lógicas basadas en CMK.
- Solo puede AWS seleccionar una clave de cifrado KMS durante la creación de la bóveda. Una vez creadas, todas las copias de seguridad contenidas en el almacén se cifrarán con esa clave. No puede cambiar ni migrar sus almacenes para utilizar una clave de cifrado diferente.

Política de claves para la creación de bóvedas cifradas por CMK de forma lógica

Al crear un depósito cerrado de forma lógica con una clave gestionada por el cliente, debe aplicar la política gestionada a la AWS función de su cuenta. `AWSBackupFullAccess` Esta política incluye `Allow` acciones que permiten interactuar con AWS Backup las claves de KMS AWS KMS para crear concesiones durante las operaciones de respaldo, copia y almacenamiento. Además, debe asegurarse de que su política de claves administradas por el cliente (si se utiliza) incluya los permisos específicos necesarios.

- La CMK debe compartirse con la cuenta en la que se encuentra la bóveda cerrada de forma lógica

```
{  
  "Sid": "Allow use of the key to create a logically air-gapped vault",  
  "Effect": "Allow",
```



```

    "Principal": {
      "AWS": "arn:aws:iam::[account-id]:role/TheRoleToAccessAccount"
    },
    "Action": [
      "kms:CreateGrant",
      "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "backup.*.amazonaws.com"
      }
    }
  }
}

```

Política clave de copia/restauración

Para evitar errores en las tareas, revisa tu política AWS KMS clave para asegurarte de que incluye todos los permisos necesarios y no contiene ninguna declaración de denegación que pueda bloquear las operaciones. Se aplican las siguientes condiciones:

- En todos los escenarios de copia, se CMKs debe compartir con la función de copia de origen

```

{
  "Sid": "Allow use of the key for copy",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::[source-account-id]:role/service-role/
AWSBackupDefaultServiceRole"    //[Source copy role]
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:ViaService": "backup.*.amazonaws.com"
    }
  }
}

```

```

    }
  },
  {
    "Sid": "Allow AWS Backup to create grant on the key for copy",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::[source-account-id]:role/service-role/
AWSBackupDefaultServiceRole" //[Source copy role]
    },
    "Action": [
      "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
      "Bool": {
        "kms:GrantIsForAWSResource": "true"
      },
      "StringLike": {
        "kms:ViaService": "backup.*.amazonaws.com"
      }
    }
  }
}

```

- Al copiar desde una bóveda comprimida de forma lógica cifrada mediante CMK a una bóveda de respaldo, la CMK también debe compartirse con la cuenta de destino SLR

```

{
  "Sid": "Allow use of the key for copy from a CMK encrypted logically air-gapped
vault to normal backup vault",
  "Effect": "Allow",
  "Principal": {
    "AWS": ["arn:aws:iam::[source-account-id]:role/service-role/
AWSBackupDefaultServiceRole",      //[Source copy role]
           "arn:aws:iam::[destination-account-id]:role/aws-service-role/
backup.amazonaws.com/AWSServiceRoleForBackup"], //[Destination SLR]
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ]
}

```

```

    ],
    "Resource": "*"
  },
  {
    "Sid": "Allow AWS Backup to create grant on the key for copy",
    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "arn:aws:iam::[source-account-id]:role/service-role/AWSBackupDefaultServiceRole", // [Source copy role]
        "arn:aws:iam::[destination-account-id]:role/aws-service-role/backup.amazonaws.com/AWSServiceRoleForBackup", // [Destination SLR]
      ],
    },
    "Action": [
      "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
      "Bool": {
        "kms:GrantIsForAWSResource": "true"
      }
    }
  }
}

```

- Al copiar o restaurar desde una cuenta de recuperación mediante una bóveda compartida con huecos lógicos RAM/MPA

```

{
  "Sid": "Allow use of the key for copy/restore from a recovery account",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::[recovery-account-id]:role/service-role/AWSBackupDefaultServiceRole", // [Recovery account copy/restore role]
      "arn:aws:iam::[destination-account-id]:role/aws-service-role/backup.amazonaws.com/AWSServiceRoleForBackup" // [Destination SLR]
    ],
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
}

```

```

    "Resource": "*"
  },
  {
    "Sid": "Allow AWS Backup to create grant on the key for copy",
    "Effect": "Allow",
    "Principal": {
      "AWS": ["arn:aws:iam::[recovery-account-id]:role/service-role/
AWSBackupDefaultServiceRole" // [Recovery account copy/restore role]
            "arn:aws:iam::[destination-account-id]:role/aws-service-role/
backup.amazonaws.com/AWSServiceRoleForBackup"], // [Destination SLR]
    },
    "Action": [
      "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
      "Bool": {
        "kms:GrantIsForAWSResource": "true"
      }
    }
  }
}

```

IAM Role

Al realizar operaciones de copia de bóvedas ocultas de forma lógica, los clientes pueden utilizar la política gestionada, que incluye la `AWSBackupDefaultServiceRole` política gestionada. `AWSAWSBackupServiceRolePolicyForBackup` Sin embargo, si los clientes prefieren implementar un enfoque de política de privilegios mínimos, su política de IAM debe incluir un requisito específico:

- La función de copia de la cuenta de origen debe tener permisos de acceso tanto al origen como al destino. CMKs

```

{
  "Version": "2012-10-17"
  ,
  "Statement": [
    {
      "Sid": "KMSPermissions",
      "Effect": "Allow",
      "Action": "kms:DescribeKey",

```

```

        "Resource": [
            "arn:aws:kms:*: [source-account-id]:key/*", - Source logically air-
gapped vault CMK -
            "arn:aws:kms:*: [destination-account-id]:key/*". - Destination
logically air-gapped vault CMK -
        ]
    },
    {
        "Sid": "KMSCreateGrantPermissions",
        "Effect": "Allow",
        "Action": "kms:CreateGrant",
        "Resource": [
            "arn:aws:kms:*: [source-account-id]:key/*", - Source logically air-
gapped vault CMK -
            "arn:aws:kms:*: [destination-account-id]:key/*". - Destination
logically air-gapped vault CMK -
        ]
        "Condition": {
            "Bool": {
                "kms:GrantIsForAWSResource": "true"
            }
        }
    },
]
}

```

Por lo tanto, uno de los errores más comunes de los clientes se produce durante la copia, cuando los clientes no proporcionan los permisos suficientes para sus funciones de CMKs copiado y las de copia.

Visualización de los tipos de claves de cifrado

Puede ver la información del tipo de clave de cifrado tanto en la AWS Backup consola como mediante programación mediante la AWS CLI tecla o. SDKs

Consola: al ver las bóvedas ocultas de forma lógica en la AWS Backup consola, el tipo de clave de cifrado se muestra en la página de detalles de la bóveda, en la sección de información de seguridad.

AWS CLI/API: el tipo de clave de cifrado se devuelve en respuesta a las siguientes operaciones cuando se consultan bóvedas aisladas de forma lógica:

- `list-backup-vaults`(incluso para bóvedas compartidas) `--by-shared`

- `describe-backup-vault`
- `describe-recovery-point`
- `list-recovery-points-by-backup-vault`
- `list-recovery-points-by-resource`

Consideraciones sobre el cifrado de bóvedas

Al trabajar con bóvedas aisladas de forma lógica y tipos de claves de cifrado, tenga en cuenta lo siguiente:

- Selección de la clave durante la creación: si lo desea, puede especificar una clave KMS administrada por el cliente al crear un almacén aislado de forma lógica. Si no se especifica, se utilizará una clave propia AWS.
- Visibilidad del almacén compartido: las cuentas con las que se comparte un almacén pueden ver el tipo de clave de cifrado, pero no pueden modificar la configuración de cifrado.
- Información sobre el punto de recuperación: el tipo de clave de cifrado también está disponible al ver los puntos de recuperación dentro de bóvedas aisladas de forma lógica.
- Operaciones de restauración: conocer el tipo de clave de cifrado le ayuda a planificar las operaciones de restauración y a comprender los posibles requisitos de acceso.
- Conformidad: la información sobre el tipo de clave de cifrado respalda los requisitos de auditoría y presentación de informes de conformidad, ya que proporciona transparencia sobre los métodos de cifrado utilizados para las copias de seguridad de los datos.

Solución de un problema de almacén aislado lógicamente

Si encuentra errores durante su flujo de trabajo, consulte los siguientes ejemplos de errores y soluciones sugeridas:

AccessDeniedException

Error: An error occurred (AccessDeniedException) when calling the `[command]` operation: Insufficient privileges to perform this action."

Causa posible: el parámetro `--backup-vault-account-id` no se incluyó cuando se ejecutó una de las siguientes solicitudes en un almacén compartido por la RAM:

- `describe-backup-vault`
- `describe-recovery-point`
- `get-recovery-point-restore-metadata`
- `list-protected-resources-by-backup-vault`
- `list-recovery-points-by-backup-vault`

Solución: vuelva a probar el comando que devolvió el error, pero incluya el parámetro `--backup-vault-account-id` que especifica la cuenta propietaria del almacén.

OperationNotPermittedException

Error: `OperationNotPermittedException` se devuelve tras una llamada de `CreateResourceShare`.

Causa posible: si ha intentado compartir un recurso, como un almacén aislado lógicamente, con otra organización, es posible que reciba esta excepción. Un almacén se puede compartir con una cuenta de otra organización, pero no se puede compartir con la otra organización en sí.

Solución: vuelva a probar la operación, pero especifique una cuenta como valor `principals` en lugar de una organización o unidad organizativa.

No se muestra el tipo de clave de cifrado

Problema: el tipo de clave de cifrado no está visible al ver una bóveda con huecos lógicos o sus puntos de recuperación.

Causas posibles:

- Está viendo una bóveda antigua que se creó antes de que se añadiera la compatibilidad con el tipo de clave de cifrado
- Está utilizando una versión anterior del AWS CLI o del SDK
- La respuesta de la API no incluye el campo de tipo de clave de cifrado

Solución:

- Actualice su versión AWS CLI a la última
- En el caso de los almacenes más antiguos, el tipo de clave de cifrado se rellenará automáticamente y debería aparecer en las siguientes llamadas a la API

- Compruebe que está utilizando las operaciones de API correctas que devuelven información sobre el tipo de clave de cifrado
- En el caso de las bóvedas compartidas, compruebe que la bóveda se comparte correctamente mediante AWS Resource Access Manager

«FALLÓ» VaultState con AccessDeniedException los registros CloudTrail

Error en CloudTrail: "User: <assumed role> is not authorized to perform: kms:CreateGrant on this resource because the resource does not exist in this Region, no resource-based policies allow access, or a resource-based policy explicitly denies access"

Causas posibles:

- El almacén se creó con una clave gestionada por el cliente, pero el rol asumido no tiene CreateGrant permiso sobre la política de claves necesaria para utilizar la clave en la creación del almacén

Solución:

- Conceda los permisos especificados en la [the section called “Política de claves para la creación de bóvedas cifradas por CMK de forma lógica”](#) sección y, a continuación, vuelva a intentar el flujo de trabajo de creación del almacén.

Copias de seguridad principales en almacenes aislados lógicamente

Descripción general de

La función de copia de seguridad principal de una bóveda aislada de forma lógica le ofrece la opción de especificar una bóveda aislada de forma lógica como destino de la copia de seguridad principal dentro de la misma cuenta, tanto para las tareas de copia de seguridad programadas como para las solicitadas. Esto elimina la necesidad de mantener copias separadas tanto en una bóveda de copias de seguridad estándar como en una bóveda vacía de forma lógica, lo que reduce los costes y simplifica los flujos de trabajo, a la vez que preserva las ventajas de seguridad que ofrece la archivación lógica.

En los planes de backup, en las políticas de toda la organización o en las copias de seguridad bajo demanda, puede asignar un almacén cerrado de forma lógica como objetivo principal. Antes, para

realizar una copia de seguridad en un almacén cerrado de forma lógica, primero había que crear una copia de seguridad en un almacén de copias de seguridad y, a continuación, copiarla en un almacén cerrado de forma lógica. Con esta función, según el tipo de recurso, AWS Backup puede crear copias de seguridad directamente en su bóveda vacía de forma lógica o gestionar automáticamente las copias de seguridad temporales que se copian en su bóveda vacía de forma lógica y, a continuación, se eliminan.

El comportamiento depende de dos factores:

- Si el tipo de recurso es compatible con una bóveda con huecos lógicos.
- [Si el tipo de recurso admite una administración completa. AWS Backup](#)

Warning

Si adopta esta capacidad, le recomendamos que integre sus bóvedas herméticas de forma lógica con la [aprobación multipartita](#) (MPA). Esto permite recuperar las copias de seguridad del almacén incluso si no se puede acceder a la cuenta propietaria del almacén.

No hay nuevos precios para esta función. Solo se le cobrará por las copias de seguridad almacenadas en bóvedas ocultas de forma lógica y por las instantáneas temporales (durante su período de retención en el sistema) de los recursos aplicables, según las tarifas vigentes. Para obtener más información, consulte los [AWS Backup precios](#).

Temas

- [Funcionamiento](#)
- [Consideraciones sobre costos](#)
- [Configure la copia de seguridad principal de la bóveda aislada de forma lógica](#)
- [Supervise de forma lógica la copia de seguridad principal de la bóveda aislada](#)
- [Incorporación y migración](#)
- [Resolución de problemas](#)

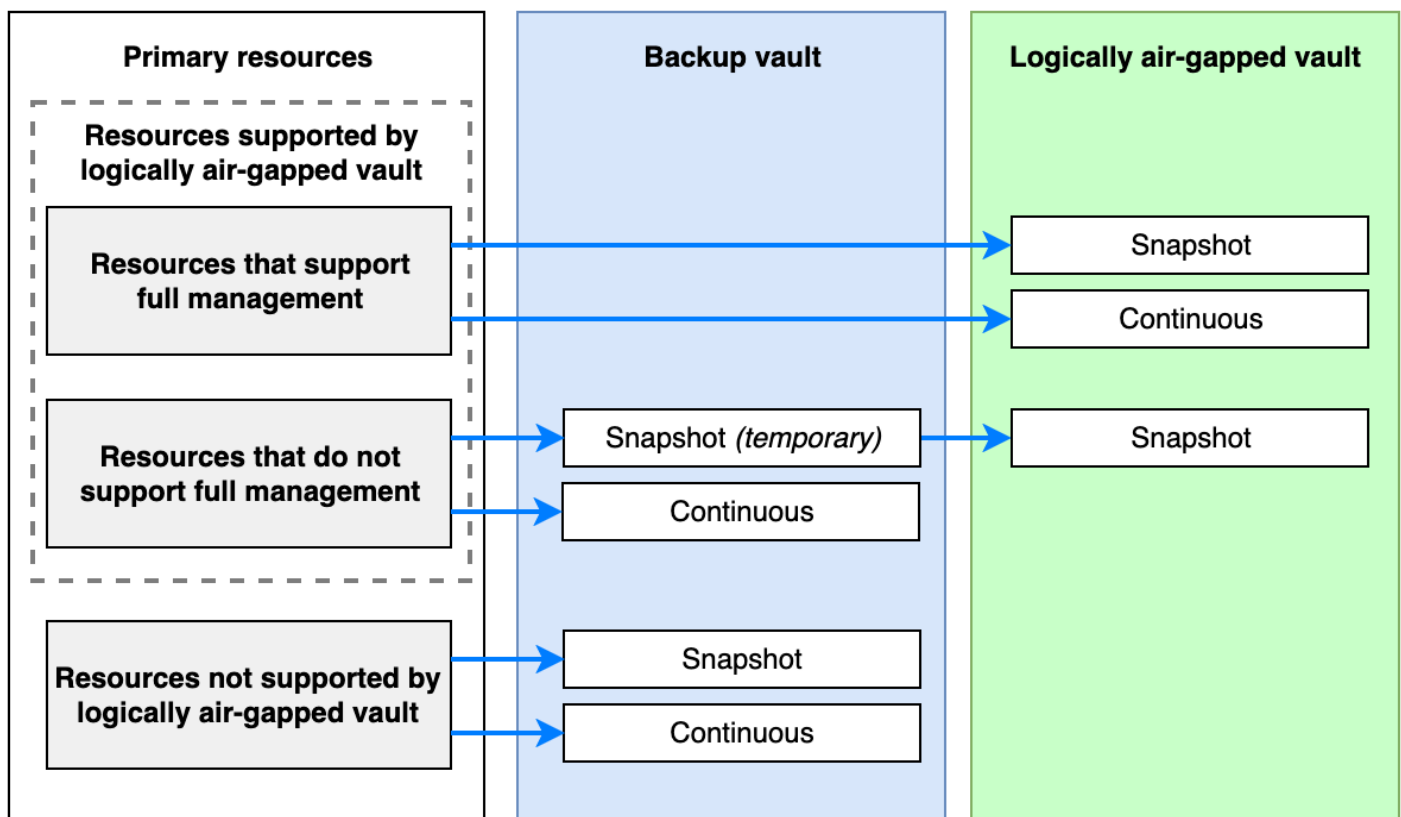
Funcionamiento

Puede incorporar esta función actualizando su plan de copia de seguridad existente o creando uno nuevo y añadiendo un ARN de almacén (nombre de

campo:TargetLogicallyAirGappedBackupVaultArn) con huecos lógicos como destino principal de la copia de seguridad. Puede realizar esta operación a través de la AWS Backup consola o mediante comandos AWS Backup CLI.

```
"TargetLogicallyAirGappedBackupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-vault:AirGappedVault",
```

Al especificar un almacén de copias de seguridad y un almacén con espacios vacíos de forma lógica como destinos para sus tareas de copia de seguridad, AWS Backup determina el flujo de trabajo adecuado en función del tipo de recurso y la configuración de cifrado.



Recursos compatibles para la copia de seguridad principal en bóvedas aisladas de forma lógica

[Para ver la lista completa de recursos compatibles con las bóvedas aisladas de forma lógica, consulta la disponibilidad de las funciones. AWS Backup](#) Todos los recursos que admiten bóvedas aisladas de forma lógica siguen el principio de mantener solo una copia de la copia de seguridad, en lugar de almacenar dos copias separadas, cuando se utiliza esta función.

 Warning

Es posible que los recursos que actualmente no se admiten para esta función tengan habilitada su compatibilidad en el futuro. Cuando eso ocurra, el recurso que acabas de admitir empezará a hacer copias de seguridad automáticamente en una bóveda con huecos lógicos mediante el flujo de trabajo que se muestra arriba.

Consideraciones y limitaciones:

- Solo en la misma cuenta y región: para poder utilizar esta función, tu bóveda hermética y lógica debe estar en la misma AWS cuenta y región que tus recursos. No puede crear copias de seguridad directamente entre cuentas o regiones. Recomendamos hacer las copias de seguridad en una bóveda cerrada lógicamente en la misma región para permitir una recuperación más rápida sin necesidad de una copia. Si necesita una copia de sus datos en una segunda región para la recuperación ante desastres (DR), le recomendamos replicar sus recursos principales entre regiones para una rápida conmutación por error o realizar copias puntuales de recuperación entre regiones en una bóveda de respaldo bloqueada.
- Restricciones relacionadas con el uso de claves AWS administradas: los recursos que no admiten una AWS Backup administración completa y que están cifrados con claves AWS administradas (por ejemplo `aws/ebs`, `aws/rds`) no se pueden copiar en bóvedas aisladas de forma lógica. Estos recursos deben estar cifrados con una clave KMS administrada por el cliente o no estar cifrados. Los recursos que respaldan AWS Backup la administración completa no tienen esta restricción.
- Frecuencia de respaldo y copias simultáneas: en el caso de los recursos que no admiten la AWS Backup administración completa, asegúrese de que la frecuencia de respaldo permita suficiente tiempo para que se completen las copias. Si las copias de seguridad se programan con más frecuencia de la que pueden finalizar las copias, los trabajos de copia se pondrán en cola y, eventualmente, podrían fallar. Para obtener información sobre los límites de copias simultáneas, [consulte](#) las cuotas.
- Compatibilidad con el ciclo de vida: el período de retención especificado en su plan de copias de seguridad debe ser compatible con los períodos de retención mínimo y máximo configurados para su almacén limitado de forma lógica.
- Bóvedas de respaldo bloqueadas: si la bóveda de respaldo de destino tiene activado el bloqueo de bóveda, los puntos de recuperación temporales no se pueden eliminar manualmente y se conservarán hasta que se complete la copia o venza el período de retención.

- Restaure las pruebas, la indexación y el escaneo: las pruebas de restauración, la indexación de los puntos de recuperación y el escaneo de malware ignorarán los puntos de recuperación temporales durante un ciclo de vida. `DELETE_AFTER_COPY` La indexación de puntos de recuperación no admite puntos de recuperación en bóvedas aisladas de forma lógica. El análisis de malware no permite realizar escaneos programados de los puntos de recuperación copiados, lo que incluye las copias automáticas realizadas como parte de las copias de seguridad principales en una bóveda aislada de forma lógica.

Recursos que respaldan la administración completa AWS Backup

Algunos tipos de recursos, como Amazon EFS, Amazon S3, Amazon DynamoDB [AWS Backup con funciones avanzadas](#), etc., que admiten una administración AWS Backup completa, pueden realizar copias de seguridad directamente en su almacén aislado de forma lógica. No se crea ningún punto de recuperación en el almacén de copias de seguridad ni se requiere ninguna operación de copia. Todas las acciones de copia programadas en su plan de copia de seguridad utilizan como fuente el punto de recuperación de su bóveda, lógicamente estancada.

Los recursos que admiten la copia de seguridad continua, como Amazon S3, también pueden realizar copias de seguridad continuas directamente en un almacén aislado de forma lógica.

Para obtener una lista de los tipos de recursos que permiten la AWS Backup administración completa y los almacenes aislados de forma lógica, consulte [Disponibilidad de funciones por recurso](#) en las columnas denominadas «Administración total» y «Depósito aislado de forma lógica».

El AWS Backup recurso no admite la administración completa

Recursos como Amazon EBS/EC2, Amazon Aurora y Amazon FSx no pueden realizar copias de seguridad directamente en bóvedas aisladas de forma lógica. Para estos tipos de recursos, AWS Backup crea un punto de recuperación temporal en la bóveda de copias de seguridad y, a continuación, lo copia automáticamente en la bóveda aislada de forma lógica.

El punto de recuperación temporal tiene una configuración de ciclo de vida especial llamada. `DELETE_AFTER_COPY` Una vez que la copia de la bóveda con huecos lógicos se complete correctamente, AWS Backup se eliminará automáticamente el punto de recuperación temporal. Todas las demás acciones de copia programadas de su plan de copia de seguridad comienzan en paralelo con la copia que se envía a su bóveda aislada de forma lógica y no afectan a su experiencia de copia actual.

Si se produce un error en la copia guardada en la bóveda de respaldo, el punto de recuperación temporal se conserva en la bóveda de copia de seguridad según el período de retención que haya especificado. Esto garantiza que siempre tendrá un punto de recuperación utilizable una vez finalizado un trabajo de copia de seguridad. Si el punto de recuperación se copia posteriormente de forma manual en una bóveda con huecos lógicos, se limpia automáticamente de acuerdo con la regla. `DELETE_AFTER_COPY`

 Warning

Los recursos cifrados con claves AWS administradas (por ejemplo `aws/ebs`) no se pueden copiar a bóvedas con espacios vacíos de forma lógica. Estos recursos deben estar cifrados con una clave administrada por el AWS Key Management Service cliente o no estar cifrados. Los recursos que respaldan AWS Backup la administración completa no tienen esta limitación.

Ciclo de vida de eliminación tras copia

Los puntos de recuperación temporales tienen un nuevo atributo de ciclo de vida denominado `DeleteAfterEvent` con un valor de `DELETE_AFTER_COPY`. Este atributo indica que el punto de recuperación se eliminará automáticamente una vez que se hayan completado todos los trabajos de copia o después del período de retención que especificó, lo que ocurra primero.

Un punto de recuperación temporal se elimina cuando se cumplen todas las condiciones siguientes:

- Todos los trabajos de copia automáticos y programados han finalizado.
- Se ha completado un trabajo de copia en la bóveda de destino, lógicamente cerrada, con un período de retención igual o superior al del punto de recuperación de origen.

Si necesita evitar la eliminación manual del punto de recuperación temporal mientras se están realizando las copias, considere la posibilidad de utilizar un almacén de copias de seguridad bloqueado como almacén de copias de seguridad de destino.

El respaldo continuo de Resource no admite la AWS Backup administración completa

En el caso de recursos como Amazon Aurora, si habilita la copia de seguridad continua, AWS Backup crea un punto de recuperación continua en su bóveda de copias de seguridad y toma una instantánea temporal que se copia en su bóveda aislada de forma lógica. La instantánea

temporal siempre se elimina una vez finalizada la copia, independientemente de si la copia se realiza correctamente o no, ya que se conserva un punto de recuperación continua en el almacén de copias de seguridad.

Si no desea crear un punto de recuperación continua para Amazon Aurora en su bóveda de copias de seguridad, pero sí desea un punto de recuperación continua para Amazon S3 en su bóveda aislada de forma lógica, puede deshabilitar la configuración de backup continuo (`EnableContinuousBackup`) en el plan actual y habilitar S3 continuo desde un plan diferente.

Puede obtener más información sobre el almacenamiento de copias de seguridad de Aurora en [Descripción del uso del almacenamiento de copias de seguridad de Amazon Aurora](#).

Recursos no compatibles

Si un tipo de recurso no es compatible con bóvedas aisladas de forma lógica, o si un recurso que no está totalmente gestionado está cifrado con una clave AWS administrada, AWS Backup crea la copia de seguridad únicamente en su almacén de copias de seguridad. No se intenta realizar ninguna copia de su bóveda aislada de forma lógica. El trabajo de copia de seguridad se completa correctamente con un mensaje en el que se indica por qué la copia de seguridad no ha llegado a su bóveda, que es lógica.

Consideraciones sobre costos

- Esta función no implica nuevos cargos. Solo pagas por el almacenamiento en tus bóvedas.
- En el caso de los recursos que permiten una AWS Backup gestión completa, mantener las copias de seguridad únicamente en un almacén cerrado de forma lógica puede suponer un importante ahorro de costes en comparación con el mantenimiento de dos copias de seguridad tanto en un almacén de copias de seguridad como en un almacén cerrado de forma lógica.
- En el caso de los recursos que no permiten una AWS Backup administración completa, se le cobrará tanto por el punto de recuperación temporal de su almacén de copias de seguridad como por los puntos de recuperación de su almacén, lógicamente cerrado.
 - Aún puede lograr importantes ahorros de costos si conserva una sola copia de respaldo, pero estos ahorros pueden variar en función de la frecuencia de los respaldos y la tasa de cambio.
 - Las frecuencias de respaldo más bajas generalmente generan mayores ahorros, ya que los puntos de recuperación temporales ocupan el almacenamiento durante un porcentaje más corto del período de facturación.
 - Algunos recursos tienen una duración mínima de facturación, lo que aumenta los costes de los puntos de recuperación temporales.

- Deshabilite la recuperación de etiquetas o ACLs metadatos en la configuración de respaldo si no utiliza estas funciones de S3. Esto reduce las llamadas a la API y los cargos asociados a las comprobaciones de metadatos durante las operaciones de copia.

Configure la copia de seguridad principal de la bóveda aislada de forma lógica

Puede configurar la copia de seguridad principal del almacén de forma lógica mediante la AWS Backup consola, las políticas de copia de seguridad o las políticas de copia de seguridad. AWS CLI
AWS CloudFormation AWS Organizations

Configurar un plan de Backup

Console

Para configurar la copia de seguridad principal de una bóveda aislada de forma lógica para un plan de copia de seguridad

1. [Abra la AWS Backup consola en /backup. https://console.aws.amazon.com](https://console.aws.amazon.com/backup)
2. En el panel de navegación, elija Planes de respaldo y, a continuación, elija Crear plan de respaldo o seleccione un plan de respaldo existente para editarlo.
3. En la sección Configuración de la regla de respaldo, especifique la configuración de la regla de respaldo.
4. Para Backup Vault, elija la bóveda de copias de seguridad donde se almacenarán los puntos de recuperación temporales (para los recursos que no se administren en su totalidad) o donde se almacenarán las copias de seguridad si no se pueden colocar en su bóveda lógicamente aislada.
5. En el caso de una bóveda con huecos lógicos (opcional), elija la bóveda con huecos lógicos en la que desee que se almacenen las copias de seguridad.

Note

La bóveda con huecos lógicos debe estar en la misma cuenta y región que la bóveda de copias de seguridad.

6. Configure el resto de los ajustes de las reglas de copia de seguridad, incluidas las opciones de ciclo de vida y copia.
7. Selecciona Crear plan o Guardar cambios.

AWS CLI

Use el comando CLI [create-backup-plan](#) para crear un plan nuevo o [update-backup-plan](#) para actualizar un plan existente e incluya el `TargetLogicallyAirGappedBackupVaultArn` parámetro en la regla de respaldo.

Ejemplo de comando CLI para crear un plan de respaldo mediante un documento JSON:

```
aws backup create-backup-plan --cli-input-json file://PATH-TO-FILE/test-backup-plan.json
```

Ejemplo de comando CLI para crear un plan de respaldo directamente en CLI:

```
aws backup create-backup-plan --backup-plan '{
  "BackupPlanName": "MyPlan",
  "Rules": [
    {
      "RuleName": "MyRule",
      "TargetBackupVaultName": "MyBackupVault",
      "TargetLogicallyAirGappedBackupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-vault:MyLagVault",
      "ScheduleExpression": "cron(0 1 ? * * *)",
      "ScheduleExpressionTimezone": "America/Los_Angeles",
      "StartWindowMinutes": 60,
      "CompletionWindowMinutes": 120,
      "Lifecycle": {
        "DeleteAfterDays": 35
      }
    }
  ]
}'
```

Configure el respaldo bajo demanda

Console

Para configurar una copia de seguridad principal de un almacén aislado de forma lógica para una copia de seguridad bajo demanda

1. [Abra la AWS Backup consola en /backup. https://console.aws.amazon.com](https://console.aws.amazon.com/backup)
2. En el panel de navegación, elija Protected resources (Recursos protegidos).

3. En la página Recursos protegidos, seleccione Crear copia de seguridad bajo demanda.
4. Seleccione el tipo de recurso y el ARN del recurso de los que desea hacer una copia de seguridad.
5. En Backup Vault, seleccione el Backup Vault.
6. En el caso de la bóveda con huecos lógicos (opcional), elija la bóveda con huecos lógicos en la que desee almacenar la copia de seguridad.
7. Configure los ajustes restantes y seleccione Crear copia de seguridad bajo demanda.

AWS CLI

Utilice el `start-backup-job` comando con el nuevo `--logically-air-gapped-backup-vault-arn` parámetro:

```
aws backup start-backup-job \  
  --backup-vault-name MyBackupVault \  
  --logically-air-gapped-backup-vault-arn arn:aws:backup:us-east-1:123456789012:backup-vault:MyLagVault \  
  --resource-arn arn:aws:ec2:us-east-1:123456789012:volume/vol-abcd1234 \  
  --iam-role-arn arn:aws:iam::123456789012:role/service-role/AWSBackupDefaultServiceRole \  
  --lifecycle DeleteAfterDays=35
```

Supervise de forma lógica la copia de seguridad principal de la bóveda aislada

Puede supervisar el estado de sus copias de seguridad y trabajos de copia mediante la AWS Backup consola o EventBridge los eventos de Amazon. AWS CLI

Supervise los trabajos de Backup

Supervise el estado de las tareas de respaldo ([DescribeBackupJob](#)) para garantizar que sus recursos permanezcan protegidos. Un trabajo de copia de seguridad fallido indica que no se creó ningún punto de recuperación.

- Compruebe la ubicación de creación del punto de recuperación: cuando un trabajo de copia de seguridad se completa correctamente, dispondrá de un punto de recuperación en la bóveda de copia de seguridad de destino o en la bóveda de destino aislada de forma lógica. Marque el `BackupVaultArn` campo para determinar dónde se creó el punto de recuperación.

- Compruebe el estado del trabajo: si un recurso no es compatible con bóvedas aisladas de forma lógica, el trabajo de copia de seguridad se completa con un signo de LOGICALLY_AIR_GAPPED_BACKUP_VAULT_NOT_SUPPORTED y un mensaje MessageCategory de estado en el que se explica por qué la copia de seguridad se creó en su almacén de copias de seguridad.
- Verificar el tipo de punto de recuperación temporal: para comprobar si un punto de recuperación es temporal, busque el `RecoveryPointLifecycle.DeleteAfterEvent` campo con un valor de `DELETE_AFTER_COPY`

Supervise los trabajos de copia

Supervise los trabajos de copia ([ListCopyJobs](#)) en su bóveda con huecos lógicos para detectar errores. Un trabajo de copia fallido significa que su punto de recuperación permanece en su bóveda de respaldo estándar sin una protección lógica de la bóveda vacía.

- Compruebe el estado del trabajo de copia: puede supervisar el estado del trabajo de copia mediante el evento existente. `Copy Job State Change EventBridge` Si lo desea, filtre por el almacén de destino (`destinationBackupVaultArn`) para centrarse en las copias del almacén agrupadas de forma lógica.
- Verifique las copias para un punto de recuperación de origen: utilice la [ListCopyJobsAPI](#) con el nuevo `BySourceRecoveryPointArn` filtro para encontrar todos los trabajos de copia asociados a un punto de recuperación específico, incluidas las copias automáticas a su almacén con espacios vacíos de forma lógica y las copias programadas para otros destinos.
- Verifique la eliminación del punto de recuperación temporal: realice un seguimiento de la finalización de la eliminación del punto de recuperación temporal. Si el estado del trabajo de copia es `RUNNING`, el punto de recuperación aún no se ha eliminado. Si la copia guardada en su almacén con huecos lógicos sí lo ha hecho `FAILED`, el punto de recuperación se conservará durante el período de retención especificado.

Note

Los registros de trabajos copiados caducan y se eliminan 30 días después de su finalización. Una vez transcurrido este período, no podrá utilizarlos `ListCopyJobs` para determinar el estado histórico de las copias.

Supervise el punto de recuperación

Supervise los puntos de EXPIRED recuperación ([ListRecoveryPointsByBackupVault](#)), lo que puede indicar que no se han AWS Backup podido eliminar (posiblemente debido a la falta de permisos). EXPIRED los puntos de recuperación pueden repercutir en los costes.

- Verifique el estado del punto de recuperación: utilice el EventBridge evento de cambio de estado del punto de recuperación existente para monitorear los vencimientos.
- Verifique la eliminación del punto de recuperación temporal: si no se DeleteAfterEvent: DELETE_AFTER_COPY ha eliminado un punto de recuperación, utilice la ListCopyJobs API para determinar el motivo, como se mencionó anteriormente.

Incorporación y migración

Si actualmente utiliza acciones de copia para copiar las copias de seguridad a un almacén con espacios vacíos de forma lógica, puede migrar a una copia de seguridad principal de un almacén con huecos lógicos para reducir los costes. También puede migrar sus copias de seguridad continuas de Amazon S3 existentes de una bóveda de copias de seguridad a una bóveda aislada de forma lógica. En esta guía se explican los requisitos previos y los pasos necesarios para migrar a la función de copia de seguridad principal de la bóveda, que tiene lagunas lógicas.

Requisitos previos y mejores prácticas

Antes de poder utilizar de forma eficaz la función de copia de seguridad principal de la bóveda, estructurada de forma lógica, hay requisitos previos y prácticas recomendadas recomendadas.

Requisitos previos

En la actualidad, un almacén cerrado de forma lógica como destino principal de las copias de seguridad solo admite las copias de seguridad de la misma AWS cuenta y región que sus recursos de copia de seguridad. AWS Como es lógico, las copias de seguridad en bóveda se almacenan de forma inherente en cuentas de servicio independientes, lo que aísla entre cuentas y organizaciones sin necesidad de realizar copias en cuentas separadas. Si necesita copias de seguridad entre regiones, siga utilizando el almacén cerrado de forma lógica como destino de las copias. Antes de migrar a esta función, asegúrese de cumplir los siguientes requisitos:

- Requisitos de región y cuenta
 - Tu bóveda, lógicamente cerrada, debe estar en la misma AWS cuenta y región que tus recursos

- Compatibilidad de recursos
 - [Compruebe que sus recursos estén respaldados por bóvedas aisladas de forma lógica en Disponibilidad de funciones por recurso.](#)
 - [Compruebe si sus recursos son compatibles con la administración completa o no. AWS Backup](#)
La experiencia de crear copias de seguridad aisladas difiere entre estos dos tipos de recursos, aunque el resultado es similar para ambos.
- Requisitos de cifrado
 - Los recursos que no admitan una AWS Backup administración completa deben estar cifrados o cifrados con claves administradas por el cliente (CMKs). AWS Los recursos cifrados con clave gestionada (AMK) no son compatibles con un almacén cerrado de forma lógica.

Prácticas recomendadas

- Comience con una migración piloto de recursos no críticos.
- Revise y ajuste las frecuencias de respaldo en función del rendimiento del trabajo de copia.
- Implemente una supervisión integral antes de la migración completa.
- Verifique periódicamente la creación de puntos de recuperación en los almacenes previstos.

Planeando tu migración

- Revise los planes y políticas de respaldo existentes.
- Identifique qué recursos respaldan AWS Backup la administración completa y cuáles no.
 - Recursos que respaldan la AWS Backup administración completa (por ejemplo, EFS, S3): pueden realizar copias de seguridad directamente en una bóveda aislada de forma lógica
 - Los recursos que no permiten una AWS Backup administración completa (por ejemplo EC2, EBS FSx): requieren una copia de seguridad temporal en una bóveda de respaldo antes de copiarlos a una bóveda aislada lógicamente
- Revise el volumen y la frecuencia de las copias de seguridad actuales y asegúrese de que la configuración se ajuste a los límites de copias simultáneas de todos los recursos que no permiten una administración completa. AWS Backup
 - Omite este paso si ya realiza copias en una bóveda aislada de forma lógica con la misma frecuencia que las copias de seguridad de las bóvedas estándar.

- Considere ajustar la frecuencia de las copias de seguridad, si es necesario, para evitar que las copias se queden en cola.
- Si las tareas de copia se ponen en cola, seguirá teniendo un punto de recuperación utilizable en su almacén de copias de seguridad estándar mientras espera que se complete la copia y se deposite en su almacén cerrado de forma lógica. Sin embargo, ese punto de recuperación no proporcionará el nivel de protección que ofrece la bóveda aislada de Logically.

Recursos que respaldan la ruta de migración de la administración completa AWS Backup

Si se trata de recursos totalmente gestionados, puede realizar copias de seguridad directamente en su bóveda aislada de forma lógica sin necesidad de realizar operaciones de copia.

Para copias de seguridad basadas en instantáneas

Este proceso se aplica a todos los escenarios de instantáneas, independientemente de si el almacén de copias de seguridad está bloqueado. Al migrar un plan de copias de seguridad existente o al utilizar una bóveda de copias de seguridad existente (principal) y una bóveda aislada de forma lógica (copia) en un nuevo plan de copias de seguridad:

1. Mantenga su almacén de respaldo existente o agréguelo como destino de respaldo ().
`TargetBackupVaultName` Esta bóveda no almacenará ninguna copia de seguridad, pero debe proporcionarse para garantizar la compatibilidad con versiones anteriores.
2. Actualice su plan de copias de seguridad para incluir la bóveda
(`TargetLogicallyAirGappedBackupVaultArn`), que se encuentra en la misma cuenta, como objetivo principal.
3. Revisa cualquier acción de copia existente a otra bóveda aislada lógicamente para determinar si sigue siendo necesaria. También puedes mover esta bóveda como objetivo principal en el paso 2 si está en la misma cuenta.

Para copias de seguridad continuas de Amazon S3

La bóveda aislada de forma lógica como destino principal de la copia de seguridad admite la copia de seguridad continua para Amazon S3. Sin embargo, solo puede mantener un punto de recuperación continuo activo por recurso en un único almacén. Si ya tiene un punto de recuperación continua de Amazon S3 activo, debe desasociarlo o eliminarlo antes de crear uno nuevo en un almacén diferente. Si añade un objetivo de almacén con lagunas lógicas (de la misma cuenta) a su

plan de backup, con un punto de recuperación continua Amazon S3 activo, se producirá un error en el trabajo de backup continuo.

Para migrar su punto de recuperación continua de Amazon S3 a su bóveda aislada de forma lógica desde una bóveda de copias de seguridad desbloqueada:

1. Actualice su plan de copias de seguridad para añadir una acción de copia a su bóveda aislada de forma lógica. Esto reducirá el costo de generar la copia de seguridad inicial en su bóveda, que tiene un vacío lógico. Omita este paso si ya está copiando en su bóveda local con espacios vacíos lógicos.
2. Compruebe que al menos una copia instantánea se haya completado correctamente en su almacén con huecos lógicos antes de continuar.
3. Desasocie el punto de recuperación continua de Amazon S3 existente. Llame a la [DisassociateRecoveryPoint](#) API para cambiar el estado del punto de recuperación de DISPONIBLE a DETENIDO. Esta acción preserva los datos de respaldo existentes y evita que se agreguen nuevos datos.
4. Actualice el plan de copia de seguridad para añadir una bóveda aislada (`TargetLogicallyAirGappedBackupVaultArn`) de forma lógica como destino de la copia de seguridad.
5. Elimine cualquier acción de copia anterior del plan.
6. La próxima vez que se ejecute el plan de respaldo, se creará un nuevo punto de recuperación continua en su bóveda aislada de forma lógica. Este punto de recuperación será gradual y se basará en la instantánea copiada del paso 1.

Para migrar su punto de recuperación continua de Amazon S3 a su bóveda aislada de forma lógica desde una bóveda de backup bloqueada:

1. Actualice su plan de copias de seguridad para añadir una acción de copia a su bóveda aislada de forma lógica. Esto reducirá el costo de generar la copia de seguridad inicial en su bóveda, que tiene un vacío lógico. Omita este paso si ya está copiando en su bóveda local con espacios vacíos lógicos.
2. Compruebe que al menos una copia instantánea se haya completado correctamente en su almacén con huecos lógicos antes de continuar. Asegúrese de que la instantánea copiada tenga un período de retención lo suficientemente largo como para permanecer disponible hasta que complete todos los pasos.
3. Añada la bóveda con huecos lógicos como objetivo principal y elimine cualquier acción de copia.

- a. Este paso es obligatorio porque las bóvedas bloqueadas no permiten la disociación de los puntos de recuperación continua.
 - b. Su punto de recuperación continua actual en la bóveda de backup bloqueada seguirá acumulando datos hasta que caduquen según su ciclo de vida.
 - c. Los nuevos trabajos de backup continuo fallarán porque solo puede existir un punto de recuperación continua activo por recurso. Como estos trabajos están fallando, no se ejecutará ninguna acción de copia.
4. Espere a que caduque el punto de recuperación continua existente. Tras la caducidad, se creará un nuevo punto de recuperación continua en la bóveda con huecos lógicos. Este punto de recuperación se incrementará en función de la instantánea copiada del paso 1, siempre que la instantánea siga existiendo en su almacén con espacios vacíos de forma lógica.
 5. Todos los datos acumulados en su almacén estándar se perderán al caducar. Solo se conservarán los datos de los que se haya hecho una copia de seguridad tras la creación del nuevo punto de recuperación en la bóveda aislada de forma lógica.

Los recursos no admiten la ruta de migración de la administración completa AWS Backup

Los recursos que no se gestionan en su totalidad requieren una operación de copia en el almacén cerrado de forma lógica. El proceso crea un punto de recuperación temporal (facturable) en el almacén de copias de seguridad estándar, que se copia automáticamente en el almacén vacío de forma lógica y, después, se elimina una vez finalizada la copia. Cuando actualices tu plan de copias de seguridad para incluir un objetivo de bóveda cerrado de forma lógica:

- Los trabajos de backup crearán un punto de recuperación en su bóveda de backup. Esto tiene un ciclo de vida determinado por el `DELETE_AFTER_COPY` evento.
- Un trabajo de copia inicia automáticamente la transferencia del punto de recuperación a su bóveda con huecos lógicos.
- Cuando la copia se haya completado correctamente, se eliminará el punto de recuperación temporal del almacén.
- Si la copia falla, el punto de recuperación temporal se conserva durante un período máximo de acuerdo con el período de retención especificado, lo que garantiza que tenga un punto de recuperación utilizable.

Resolución de problemas

El trabajo de backup o copia falla debido a un error de incompatibilidad del ciclo de vida

Error en los trabajos de copia de seguridad: Backup job failed because the lifecycle is outside the valid range for backup vault.

Error en los trabajos de copia: Copy job failed. The retention specified in the job is not within the range specified for the target Backup Vault.

Causa posible: los trabajos de Backup o de copia fallan porque el período de retención no es compatible con la configuración de retención mínima o máxima de la bóveda, lógicamente aislada.

Solución: actualice su plan de copias de seguridad para especificar un período de retención que se sitúe dentro de los períodos de retención mínimo y máximo configurados para su almacén con brechas lógicas.

Los trabajos de copia de seguridad continua fallan si «ya tiene habilitada la copia de seguridad continua»

Error: Bucket {bucket_name} already has continuous backup enabled for another vault Backup job failed.

Causa posible: los trabajos de respaldo continuo fallan porque ya existe un punto de recuperación continua para el recurso en otro almacén.

Solución: cada recurso solo puede tener un punto de recuperación continuo. Si su almacén de respaldo está desbloqueado, desasocie el punto de recuperación continua existente mediante el [disassociate-recovery-point](#) comando. Si su almacén de copias de seguridad está bloqueado, espere a que caduque el punto de recuperación continua existente según su ciclo de vida.

El trabajo de backup finaliza con el mensaje «Finalizado con problemas» (tipo de recurso no compatible)

Mensaje: Backup job completed successfully to the target backup vault. This resource type is not supported by logically air-gapped backup vault.

Causa posible: los trabajos de Backup de recursos no gestionados en su totalidad no compatibles muestran el mensaje «Se ha completado con problemas» con un mensaje que indica que el recurso no es compatible.

Solución: los tipos de recursos que no se admiten solo se realizarán copias de seguridad en el almacén de copias de seguridad. Si desea conservar estas copias de seguridad en su almacén de copias de seguridad, no es necesario realizar ninguna acción. Si prefiere no mezclar recursos no compatibles con su bóveda, que es lógica, puede:

- Elimine el recurso o el objetivo de la bóveda con lagunas lógicas de su plan de respaldo para estos recursos y continúe haciendo copias de seguridad únicamente en su bóveda de respaldo. Posteriormente, puede añadir el recurso como parte de un plan diferente.

El trabajo de backup finaliza con el mensaje «Finalizado con problemas»: clave de cifrado no compatible

Mensaje: Backup job completed successfully to the target backup vault. This resource is encrypted with an AWS managed key and cannot be copied to a logically air-gapped backup vault.

Causa posible: los trabajos de Backup de recursos no gestionados en su totalidad no compatibles muestran el mensaje «Finalizado con problemas» con un mensaje que indica que el recurso está cifrado con una clave AWS gestionada.

Solución: los recursos no gestionados en su totalidad cifrados con claves AWS gestionadas no se pueden copiar a almacenes aislados de forma lógica. Si desea conservar estas copias de seguridad en su almacén de copias de seguridad, no es necesario realizar ninguna acción. Si prefiere no mezclar recursos no compatibles con su bóveda, que es lógica, puede:

- Vuelva a cifrar sus recursos con una clave KMS administrada por el cliente, o
- Elimine el recurso o el objetivo de la bóveda con limitaciones lógicas de su plan de copias de seguridad para estos recursos y continúe realizando copias de seguridad únicamente en su almacén de copias de seguridad. Posteriormente, puede añadir el recurso como parte de un plan diferente.

Los puntos de recuperación permanecen en **EXPIRED** estado

Causa posible: los puntos de recuperación temporales pasan al EXPIRED estado pero no se eliminan.

Solución: AWS Backup puede carecer de permisos para eliminar los puntos de recuperación. Compruebe que su función de respaldo tenga los permisos de IAM necesarios. Es posible que tengas que eliminar manualmente los puntos expired de recuperación.

Los trabajos de copia están en cola o fallan debido a la alta frecuencia de las copias de seguridad

Causa posible: los trabajos de copia a bóvedas con espacios vacíos, por lógica, están en cola o fallan porque las copias de seguridad se programan con más frecuencia de la que se pueden completar las copias.

Solución: reduzca la frecuencia de las copias de seguridad o ajuste la programación de las copias de seguridad para permitir más tiempo entre las copias de seguridad. Consulte la [documentación sobre AWS Backup las cuotas](#) para obtener información sobre los límites de copias simultáneas.

Aprobación de varias partes para almacenes aislados lógicamente

Información general sobre la aprobación de varias partes en un almacén aislado lógicamente

AWS Backup le ofrece la opción de añadir la [aprobación multipartita](#), una capacidad desde, a sus bóvedas aisladas de AWS Organizations forma lógica. La aprobación de varias partes es una opción adicional para proteger las operaciones críticas mediante un proceso de aprobación distribuido.

La aprobación de varias partes está diseñada para proteger los recursos críticos y minimizar el tiempo de inactividad, por ejemplo, en caso de una interrupción provocada por agentes malintencionados o eventos de malware. Esta configuración puede ayudarle a restaurar el contenido de un almacén aislado lógicamente que podría estar comprometido.

La integración y el uso de equipos de aprobación de varias partes con almacenes aislados lógicamente de AWS Backup no generan ningún costo adicional (se aplican cargos por almacenamiento y transferencias entre regiones, tal y como se muestra en la página de [precios](#)).

Como AWS Backup cliente, puede utilizar la aprobación de varias partes para conceder la capacidad de aprobación de algunas operaciones a un grupo de personas de confianza que puedan aprobar de forma colaborativa el acceso a un depósito cerrado de forma lógica desde una cuenta de recuperación creada por separado en caso de sospecha de actividad maliciosa que pueda comprometer el uso de la cuenta principal.

En los siguientes pasos se describe el flujo recomendado para configurar una organización de AWS de recuperación, definir la aprobación de varias partes y, a continuación, utilizar dicha aprobación con sus almacenes aislados lógicamente:

1. Un administrador [crea una nueva organización a través de Organizations](#) para utilizarla en las operaciones de recuperación.

2. En la cuenta de administración de esta nueva organización, el administrador crea y configura una instancia de IAM Identity Center (IDC) (para activar una instancia de organización, consulte [Activación del IAM Identity Center](#) en la Guía del usuario del IAM Identity Center). Consulte también la secuencia de [Creación de un origen de identidad de aprobación de varias partes](#) en la Guía del usuario de aprobación de varias partes.
3. A continuación, el administrador [creará un equipo de aprobación](#), que es el grupo central de personas de confianza que serán los principales usuarios de la aprobación de varias partes.
4. El administrador suele AWS RAM [compartir un equipo de aprobación](#) con cada cuenta que posea al menos un depósito cerrado de forma lógica (probablemente tu cuenta principal). Tanto la cuenta propietaria del almacén como la organización secundaria deben tener la RAM configurada.
5. El administrador de esas cuentas [asocia un almacén aislado lógicamente con un equipo de aprobación](#).
6. Una cuenta de recuperación [solicita acceder](#) a una cuenta que tiene un almacén aislado lógicamente con un equipo de aprobación de varias partes asociado (“equipo”). El equipo asociado a la cuenta [aprueba o rechaza la solicitud](#).
7. El administrador de la cuenta propietaria del almacén aislado lógicamente puede solicitar que [se desasocie al equipo de aprobación del almacén](#). La solicitud requiere la aprobación del equipo actual.
8. Un administrador puede [actualizar la membresía del equipo de aprobación](#) según sea necesario de acuerdo con sus prácticas de seguridad o cuando las personas se unan o abandonen su organización.

Requisitos previos y prácticas recomendadas para utilizar la aprobación de varias partes con un almacén aislado lógicamente

Para poder utilizar la aprobación de varias partes en sus almacenes aislados lógicamente de forma eficaz y segura, deben cumplirse una serie de requisitos previos y seguirse las prácticas recomendadas.

Prácticas recomendadas:

- Dos (o más) AWS organizaciones a través de Organizations. Una de ellas debe ser la organización principal, en la que tiene una o más cuentas con al menos un almacén aislado lógicamente. La organización secundaria debe ser la organización de recuperación. Es en esta organización donde se administrará el equipo de aprobación de varias partes.

Requisitos previos

1. [Ha configurado la aprobación de varias partes](#) y dispone de al menos un equipo de aprobación.
2. Como mínimo, una cuenta de la organización principal debe tener un almacén aislado lógicamente (y el almacén de copias de seguridad original).
3. La cuenta de administración de la organización principal está suscrita a la aprobación de varias partes.

Tip

AWS Backup recomienda aplicar una política de control de servicios (SCP) a su organización principal y configurarla con los permisos adecuados para la organización y para cada equipo de aprobación. Consulte la sección [Términos de la aprobación de varias partes](#) para ver una política de ejemplo.

4. El equipo de aprobación de varias partes de la organización secundaria (de recuperación) se [comparte a través de AWS RAM](#) con ambas cuentas que poseen los almacenes aislados lógicamente y las cuentas de recuperación.

Consideraciones y dependencias entre regiones a la hora de utilizar la aprobación de varias partes

Si activa la aprobación de varias partes y su instancia de IAM Identity Center en regiones diferentes, la aprobación de varias partes llama al IAM Identity Center desde distintas regiones. Esto significa que la información de los usuarios y los grupos se transfiere de una región a otra. Los recursos del equipo de aprobación multipartito solo se pueden crear y almacenar en Región de AWS EE. UU. Este (Virginia del Norte).

Los demás recursos del equipo de aprobación multipartito Regiones de AWS que hagan referencia dependerán de la zona Este de EE. Región de AWS UU. (Virginia del Norte). En consecuencia, la aprobación multipartita permitirá realizar llamadas entre regiones si su instancia del Centro de Identidad (bóveda, and/or lógicamente cerrada) no se encuentra en EE. UU. Este (Virginia del Norte).

Términos, conceptos y usuarios de la aprobación de varias partes

La aprobación por parte de varias partes en una bóveda hermética es una integración de AWS Organizations las funciones (IAM) y (AWS Account Management RAM) y AWS Backup(RAM). AWS Identity and Access Management AWS RAM A través de la CLI, puede interactuar con cada servicio

para enviar los comandos correspondientes. También puede usar la consola, pero tendrá que ir a la consola del servicio correspondiente para completar tareas específicas.

La forma en que interactúes con la aprobación multipartita depende de tus funciones y responsabilidades en tus organizaciones, así como de los permisos que tengas en tus cuentas. AWS Backup

Tal como se muestra en la [Guía del usuario de la aprobación de varias partes](#), los miembros de su organización que utilicen la aprobación de varias partes serán un solicitante, un administrador o un aprobador. Se aplican permisos específicos a cada [rol de trabajo](#). De acuerdo con las prácticas recomendadas de seguridad, un usuario solo debe llevar a cabo un rol de trabajo.

Consolas, portales y sesiones

AWS Backup las cuentas con una o más bóvedas aisladas de forma lógica pueden utilizar la aprobación de varias partes.

Antes del proceso de aprobación multipartito, el administrador suele crear una organización secundaria con fines de recuperación (una organización de recuperación) si no se ha creado ninguna anteriormente. AWS Organizations

A continuación, el administrador utiliza la memoria AWS Resource Access Manager RAM para configurar el intercambio entre organizaciones entre la organización principal y la organización de recuperación.

La organización principal alberga las cuentas que poseen y utilizan un almacén aislado lógicamente en el que se almacenan los datos protegidos.

La organización de recuperación alberga al menos una cuenta de recuperación. Esta cuenta incluye un punto de acceso que puede utilizarse como “puerta trasera” esencial para acceder al almacén aislado lógicamente compartido. Este punto de acceso se denomina almacén de copias de seguridad con acceso a la restauración. Este almacén de acceso no almacena datos, sino que se utiliza como punto de acceso o montaje que refleja el contenido del almacén aislado lógicamente de origen pero no contiene datos que puedan modificarse o eliminarse. Por ejemplo, si un cliente realiza el proceso de restauración para un punto de recuperación en un almacén de copias de seguridad con acceso a la restauración, es el punto de recuperación del almacén aislado lógicamente el que se restaura mediante la restauración entre cuentas a través de la cuenta de recuperación.

Para incrementar la seguridad, los clientes utilizan esta cuenta de recuperación para llevar a cabo operaciones protegidas en la cuenta principal, pero solo después de que el [equipo de aprobación asociado haya aprobado dichas operaciones en una sesión de aprobación](#). AWS Una vez que

se envía una solicitud de aprobación, se crea una sesión y esa sesión finaliza cuando un número mínimo de miembros del equipo de aprobación aprueba o deniega la solicitud o cuando ha transcurrido el tiempo de sesión permitido.

Un equipo está formado por aprobadores (es decir, las partes de la aprobación de varias partes) que reciben notificaciones por correo electrónico de las solicitudes de operaciones protegidas. Estos correos electrónicos confirman que se ha iniciado una sesión de aprobación de la solicitud. La aprobación se concede si se alcanza el umbral mínimo de aprobación requerido. Este umbral se puede establecer al crear el equipo de aprobación de varias partes ("Equipo").

Los equipos de aprobación multipartitos se gestionan a través del portal de aprobación multipartita de Organizations («portal»), una aplicación AWS gestionada que proporciona a las identidades una ubicación centralizada donde los miembros del equipo de aprobación pueden recibir y responder a las invitaciones y solicitudes de operación del equipo de aprobación.

Tareas del administrador

Varias tareas que implicaban AWS Backup una visión general multipartita requerían un usuario con permisos de administrador y acceso a la cuenta de administración.

Creación de un equipo de aprobación

Un usuario de tu organización con permisos de administrador para una AWS cuenta debe [configurar la aprobación multipartita](#) (paso 3 de la [descripción general](#)).

Antes de realizar este paso, se recomienda configurar una organización principal y una secundaria (para la recuperación) en AWS Organizations (paso 1 de [Información general](#)).

Consulte [Creación de un equipo de aprobación](#) en la Guía del usuario de aprobación de varias partes para crear el equipo.

Durante la operación `aws mpa create-approval-team`, uno de los parámetros es `policies`. Esta es una lista de ARNs (nombres de recursos de Amazon) para políticas de recursos de aprobación multipartita que definen los permisos que protegen al equipo.

La política que se muestra en el ejemplo de la Guía del usuario de aprobación de varias partes en el procedimiento [Creación de un equipo de aprobación](#) contiene la política `["arn:aws:mpa::aws:policy/backup.amazonaws.com/CreateRestoreAccessVault"]` con varios permisos necesarios.

Siga estos pasos para obtener una lista de las políticas disponibles mediante `mpa list-policies`:

1. Enumerar las políticas:

```
aws mpa list-policies --region us-east-1
```

2. Enumerar todas las versiones de las políticas:

```
aws mpa list-policy-versions --policy-arn arn:aws:mpa:::aws:policy/
backup.amazonaws.com/CreateRestoreAccessVault --region us-east-1
```

3. Obtener información detallada sobre una política:

```
aws mpa get-policy-version --policy-version-arn arn:aws:mpa:::aws:policy/
backup.amazonaws.com/CreateRestoreAccessVault/1 --region us-east-1
```

Amplíe la información siguiente para ver la política que se creará y luego se asociará al equipo de aprobación mediante esta operación:

Restauración de la política de acceso al almacén

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VaultOwnerPermissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Resource": "*",
      "Action": [
        "mpa:StartSession",
        "mpa:CancelSession"
      ],
      "Condition": {
        "StringEquals": {
          "mpa:RequestedOperation": "backup:RevokeRestoreAccessBackupVault",
          "mpa:ProtectedResourceAccount": "${aws:PrincipalAccount}"
        },
        "Bool": {
```

```
    "aws:ViaAWSService": "true"
  }
}
]
```

Comparta un equipo de aprobación multipartito mediante AWS RAM

[Puedes compartir un equipo de aprobación multipartito con otras AWS cuentas mediante AWS Resource Access Manager \(RAM\), paso 4 de la descripción general.](#)

Console

Comparta un equipo de aprobación multipartito mediante AWS RAM

1. Inicie sesión en la [consola de AWS RAM](#).
2. En el panel de navegación, elija Recursos compartidos.
3. Elija Crear recurso compartido.
4. En el campo Nombre, introduzca un nombre descriptivo para el recurso compartido.
5. En Tipo de recurso, seleccione Equipo de aprobación de varias partes en el menú desplegable.
6. En Recursos, seleccione el equipo de aprobación que quiere compartir.
7. En Directores, especifique las AWS cuentas con las que quiere compartir el equipo de aprobación.
8. Para compartir con AWS cuentas específicas, selecciona las AWS cuentas e introduce la cuenta de 12 dígitos. IDs
9. Para compartir con una organización o unidad organizativa, seleccione Organización o Unidad organizativa e introduzca el ID correspondiente.
10. (Opcional) En Etiquetas, añada cualquier etiqueta que quiera asociar a este recurso compartido.
11. Elija Crear recurso compartido.

El estado del recurso compartido se mostrará inicialmente como PENDING. Cuando las cuentas del destinatario acepten la invitación, el estado cambiará a ACTIVE.

CLI

Para compartir un equipo de aprobación multipartito AWS RAM mediante la CLI, utilice los siguientes comandos:

En primer lugar, identifique el ARN del equipo de aprobación que desee compartir:

```
aws mpa list-approval-teams --region us-east-1
```

Cree un recurso compartido mediante el create-resource-share comando:

```
aws ram create-resource-share \  
--name "MPA-Team-Share" \  
--resource-arns "arn:aws:mpa:us-east-1:ACCOUNT_ID:approval-team/TEAM_ID" \  
--principals "ACCOUNT_ID_TO_SHARE_WITH" \  
--permission-arns "arn:aws:ram::aws:permission/AWSRAMMPAApprovalTeamAccess" \  
--region us-east-1
```

Para compartir con una organización en lugar de con cuentas específicas, haga lo siguiente:

```
aws ram create-resource-share \  
--name "MPA-Team-Share" \  
--resource-arns "arn:aws:mpa:us-east-1:ACCOUNT_ID:approval-team/TEAM_ID" \  
--permission-arns "arn:aws:ram::aws:permission/AWSRAMMPAApprovalTeamAccess" \  
--allow-external-principals \  
--region us-east-1
```

Compruebe el estado del recurso compartido:

```
aws ram get-resource-shares \  
--resource-owner SELF \  
--region us-east-1
```

Las cuentas del destinatario deberán aceptar la invitación para el uso compartido de un recurso:

```
aws ram get-resource-share-invitations --region us-east-1
```

Inicie sesión en la cuenta del destinatario para aceptar una invitación:

```
aws ram accept-resource-share-invitation \  

```

```
--resource-share-invitation-arn "arn:aws:ram:REGION:ACCOUNT_ID:resource-share-
invitation/INVITATION_ID" \
--region us-east-1
```

Después de aceptar la invitación, el equipo de aprobación de varias partes ya se podrá usar en la cuenta del destinatario.

AWS ofrece herramientas para compartir el acceso a la cuenta, incluido el [acceso AWS Resource Access Manager directo y multipartito](#). Si decide compartir un almacén aislado lógicamente con otra cuenta, tenga en cuenta los siguientes detalles:

Característica	AWS RAM uso compartido basado	Acceso basado en la aprobación de varias partes
Acceso a almacenes aislados lógicamente	Cuando se haya completado el uso compartido de RAM, se podrá acceder a los almacenes.	Cualquier intento por parte de una cuenta diferente debe ser aprobado por un umbral mínimo de miembros del equipo de aprobación de varias partes. La sesión de aprobación caduca automáticamente 24 horas después de que se inicie la solicitud.
Retirada del acceso	La cuenta propietaria del almacén aislado lógicamente puede poner fin al uso compartido basado en RAM en cualquier momento.	El acceso a un almacén solo se puede eliminar mediante una solicitud al equipo de aprobación de varias partes.
Copia entre cuentas y and/or regiones	No se admite actualmente.	Las copias de seguridad se pueden copiar en la misma cuenta o con otras cuentas de la misma organización que la cuenta de recuperación.
Facturación por transferencia entre regiones		Las transferencias entre regiones se facturan a la

Característica	AWS RAM uso compartido basado	Acceso basado en la aprobación de varias partes
		misma cuenta propietaria del almacén de copias de seguridad con acceso a la restauración.
Uso recomendado	El uso principal es para recuperar datos perdidos y para probar la restauración.	El uso principal es para situaciones en las que se sospecha que el acceso o la seguridad de la cuenta están comprometidos.
Regiones	Disponible en todos los Regiones de AWS lugares donde se admiten bóvedas con huecos lógicos.	Disponible en todos los Regiones de AWS lugares donde se admiten bóvedas con huecos de aire lógicos.
Restaura	Todos los tipos de recurso compatibles se pueden restaurar desde una cuenta compartida.	Todos los tipos de recurso compatibles se pueden restaurar desde una cuenta compartida.
Configuración	El uso compartido se puede realizar tan pronto como la AWS Backup cuenta configure el uso compartido de RAM y la cuenta receptora lo acepte.	El uso compartido requiere que la cuenta de administración primero cree un equipo y, a continuación, configure el uso compartido de RAM. A continuación, la cuenta de administración se suscribe a la aprobación de varias partes y asigna ese equipo a un almacén aislado lógicamente.

Característica	AWS RAM uso compartido basado	Acceso basado en la aprobación de varias partes
Uso compartido	El uso compartido se realiza a través de la RAM dentro de AWS la misma organización o entre AWS organizaciones. El acceso se concede según el modelo “push”, en el que la cuenta propietaria del almacén aislado lógicamente primero concede el acceso. Luego, la otra cuenta acepta el acceso.	El acceso a una bóveda aislada de forma lógica se realiza a través de los equipos de aprobación apoyados por Organizations dentro de la misma AWS organización o entre organizaciones. El acceso se concede siguiendo el modelo “pull”, en el que la cuenta receptora primero solicita el acceso y, a continuación, el equipo de aprobación concede o deniega la solicitud.

Tareas del solicitante

Asocie un equipo de aprobación multipartito a una bóveda cerrada de forma lógica

Solicitante: usuario con acceso a la cuenta propietaria del almacén aislado lógicamente

Puede asociar un equipo de aprobación de varias partes a un almacén aislado lógicamente para permitir la aprobación colaborativa del acceso al almacén (paso 5 de la [Información general](#)).

Console

Asocia un equipo de aprobación multipartito a una bóveda con huecos lógicos

1. [Abra la consola en AWS Backup /backup. https://console.aws.amazon.com](https://console.aws.amazon.com/backup/)
2. Desplácese hasta la sección Almacenes de copia de seguridad en el panel de navegación izquierdo.
3. Seleccione el almacén de copias de seguridad aislado lógicamente que desee asociar a un equipo de MPA.
4. En la página Detalles del almacén, seleccione Asignar equipo de aprobación.

5. En el menú desplegable, seleccione el equipo de aprobación que desea asociar al almacén.
6. Opcional Escriba un comentario donde explique el motivo de la asociación.
7. Seleccione Enviar solicitud para enviar la solicitud de asociación.

Si es el primer equipo de aprobación que se asocia al almacén, el equipo se asociará al almacén. Si el almacén ya tiene un equipo asociado, consulte [Actualización de un equipo de aprobación de varias partes](#) para ver los pasos a seguir.

CLI

Utilice el comando de CLI `associate-backup-vault-mpa-approval-team` modificado con los parámetros siguientes:

```
aws backup associate-backup-vault-mpa-approval-team \
--backup-vault-name VAULT_NAME \
--mpa-approval-team-arn MPA_TEAM_ARN \
--requester-comment "OPTIONAL_COMMENT" \
--region REGION
```

Si es el primer equipo de aprobación que se asocia al almacén, el equipo se asociará al almacén. Si el almacén ya tiene un equipo asociado, consulte [Actualización de un equipo de aprobación de varias partes](#) para ver los pasos a seguir.

Solicitud de acceso a un almacén aislado lógicamente

Solicitante: usuario con acceso a la cuenta de recuperación

Puede solicitar el acceso a un almacén aislado lógicamente en otra cuenta (paso 6 de la [Información general](#)).

Una vez que un equipo de aprobación haya accedido a la solicitud, AWS Backup crea una bóveda de respaldo con acceso de restauración en la cuenta de recuperación designada para que esa cuenta tenga acceso a los puntos de recuperación de la bóveda conectada y aislada de forma lógica.

Console

Solicitud de acceso a un almacén aislado lógicamente

1. [Abre la AWS Backup consola en /backup. https://console.aws.amazon.com](https://console.aws.amazon.com/backup/)

2. Desplácese hasta la sección Almacenes de copia de seguridad en el panel de navegación izquierdo.
3. Seleccione la pestaña Almacenes accesibles a través de MPA.
4. Seleccione Solicitar acceso al almacén.
5. Introduzca el ARN del almacén de copias de seguridad de origen del almacén aislado lógicamente al que desea acceder.
6. Introduzca un nombre opcional para el almacén de copias de seguridad con acceso a la restauración. Si no introduce un nombre, AWS Backup se le asignará uno basado en el nombre de la bóveda con huecos de aire de forma lógica.
7. Puede escribir un comentario opcional del solicitante que explique el motivo de la solicitud de acceso.
8. Seleccione Enviar solicitud para enviar la solicitud de acceso.

Los miembros del equipo de aprobación asociados al almacén de origen recibirán una notificación por correo electrónico para aprobar la solicitud.

Cuando el número requerido de miembros del equipo (“umbral”) apruebe la solicitud, se creará el almacén de copias de seguridad con acceso a la restauración en la cuenta de recuperación.

CLI

Utilice el comando `create-restore-access-backup-vault` CLI:

```
aws backup create-restore-access-backup-vault \
--source-backup-vault-arn SOURCE_VAULT_ARN \
--backup-vault-name OPTIONAL_VAULT_NAME \
--requester-comment "OPTIONAL_COMMENT" \
--region REGION
```

Los miembros del equipo de aprobación MPA asociados al almacén de origen recibirán una notificación por correo electrónico para aprobar la solicitud. Cuando el número requerido de miembros del equipo (“umbral”) apruebe la solicitud, se creará el almacén de copias de seguridad con acceso a la restauración en la cuenta de recuperación.

También puede comprobar el estado del almacén con:

```
aws backup describe-backup-vault \
```

```
--backup-vault-name VAULT_NAME \  
--region REGION
```

Desasociación del equipo de aprobación de varias partes del almacén aislado lógicamente

Solicitante: administrador de la cuenta propietaria del almacén aislado lógicamente

Puede desasociar un equipo de aprobación de varias partes de un almacén aislado lógicamente (paso 7 de la [Información general](#)).

Console

Disocia al equipo de aprobación de la bóveda con espacios vacíos de forma lógica

1. [Abra la consola en AWS Backup /backup. https://console.aws.amazon.com](https://console.aws.amazon.com/backup)
2. Desplácese hasta la sección Almacenes de copia de seguridad en el panel de navegación izquierdo.
3. Seleccione el almacén de copias de seguridad aislado lógicamente desde el que desee desasociar al equipo de aprobación.
4. En la página Detalles del almacén, seleccione Desasociar equipo de aprobación.
5. Puede escribir un comentario opcional del solicitante que explique el motivo de la desasociación.
6. Seleccione Enviar solicitud para enviar la solicitud de desasociación.

Los miembros actuales del equipo de aprobación recibirán una notificación para aprobar la solicitud.

Cuando el número requerido de miembros del equipo lo apruebe, se desasociará al equipo del almacén.

CLI

Utilice el comando `disassociate-backup-vault-mpa-approval-team` CLI:

```
aws backup disassociate-backup-vault-mpa-approval-team \  
--backup-vault-name VAULT_NAME \  
--requester-comment "OPTIONAL_COMMENT" \  
--region REGION
```

Los miembros actuales del equipo de aprobación MPA recibirán una notificación para aprobar la solicitud. Cuando el número requerido de miembros del equipo lo apruebe, se desasociará al equipo del almacén.

Revocación del almacén de copias de seguridad de acceso a la restauración

Solicitante: administrador de la cuenta propietaria del almacén aislado lógicamente

Puede revocar el acceso a un almacén de copias de seguridad con acceso a la restauración desde la cuenta del almacén de origen.

Console

Revocación del almacén de copias de seguridad de acceso a la restauración

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. Desplácese hasta la sección Almacenes de copia de seguridad en el panel de navegación izquierdo.
3. Seleccione el almacén de copias de seguridad aislado lógicamente para el que quiere revocar el acceso.
4. En la página Detalles del almacén, desplácese hacia abajo hasta la sección Acceso mediante aprobación de varias partes.
5. Busque el almacén de copias de seguridad con acceso a la restauración que desea revocar y, a continuación, seleccione Solicitud para eliminar el acceso al almacén.
6. Puede escribir un comentario opcional del solicitante que explique el motivo de la revocación.
7. Seleccione Enviar solicitud para enviar la solicitud de revocación.

Los miembros del equipo de aprobación recibirán una notificación para aprobar la solicitud.

Cuando el número requerido de miembros del equipo apruebe la solicitud, se eliminará el almacén de copias de seguridad con acceso a la restauración de la cuenta de recuperación.

CLI

En primer lugar, enumere los almacenes con acceso a la restauración asociados a su almacén de origen:

```
aws backup list-restore-access-backup-vaults \
--backup-vault-name SOURCE_VAULT_NAME \
```



```
--region REGION
```

A continuación, utilice el comando `revoke-restore-access-backup-vault` de la CLI:

```
aws backup revoke-restore-access-backup-vault \  
--backup-vault-name SOURCE_VAULT_NAME \  
--restore-access-backup-vault-arn RESTORE_ACCESS_VAULT_ARN \  
--requester-comment "OPTIONAL_COMMENT" \  
--region REGION
```

Los miembros del equipo de aprobación recibirán una notificación para aprobar la solicitud. Cuando el número requerido de miembros del equipo apruebe la solicitud, se eliminará el almacén de copias de seguridad con acceso a la restauración de la cuenta de recuperación.

Actualice el equipo de aprobación multipartito asociado a una bóveda con huecos lógicos

Solicitante: administrador de la cuenta propietaria del almacén aislado lógicamente

Puede actualizar el equipo de aprobación de varias partes asociado a un almacén aislado lógicamente (paso 8 de la [Información general](#)).

Console

Actualización del equipo de aprobación asociado a un almacén aislado lógicamente

1. [Abre la consola en AWS Backup /backup. https://console.aws.amazon.com](https://console.aws.amazon.com/backup/)
2. Desplácese hasta la sección Almacenes de copia de seguridad en el panel de navegación izquierdo.
3. Seleccione el almacén de copias de seguridad aislado lógicamente para el que quiere actualizar el equipo de aprobación.
4. En la página Detalles del almacén, seleccione Solicitar cambio de equipo de aprobación.
5. En el menú desplegable, seleccione el nuevo equipo de aprobación que desea asociar al almacén.
6. Puede escribir un comentario opcional del solicitante que explique el motivo del cambio.
7. Seleccione Enviar solicitud para enviar la solicitud de modificación.

Los miembros actuales del equipo de aprobación recibirán una notificación por correo electrónico para aprobar la solicitud.

Cuando el número requerido de miembros del equipo (umbral) del equipo de MPA actual (límite) apruebe la solicitud, el nuevo equipo se asociará al almacén.

CLI

Utilice el comando `associate-backup-vault-mpa-approval-team` de la CLI con el nuevo ARN del equipo:

```
aws backup associate-backup-vault-mpa-approval-team \
--backup-vault-name VAULT_NAME \
--mpa-approval-team-arn NEW_MPA_TEAM_ARN \
--requester-comment "OPTIONAL_COMMENT" \
--region REGION
```

Los miembros actuales del equipo de aprobación recibirán una notificación para aprobar la solicitud. Cuando el número requerido de miembros del equipo (umbral) actual apruebe la solicitud, el nuevo equipo de MPA se asociará al almacén.

Tareas del aprobador

Un usuario que sea miembro de un equipo de aprobación de varias partes puede [aprobar o denegar solicitudes](#) que forman parte de una sesión. Otras tareas pueden ser:

- [Responder a las operaciones solicitadas](#)
- [Visualizar un equipo de aprobación](#)
- [Visualizar el historial de operaciones](#)

Políticas de acceso a almacenes

Con él AWS Backup, puede asignar políticas a las bóvedas de respaldo y a los recursos que contienen. La asignación de políticas le permite hacer cosas como conceder acceso a los usuarios para crear planes de copia de seguridad y copias de seguridad bajo demanda, pero limitar su capacidad de eliminar puntos de recuperación una vez creados.

Para obtener información sobre el uso de políticas para conceder o restringir el acceso a recursos, consulte [Políticas basadas en identidad y políticas basadas en recursos](#) en la Guía del usuario de IAM. También puede controlar el acceso mediante etiquetas.

Puede utilizar las siguientes políticas de ejemplo como guía para limitar el acceso a los recursos cuando trabaje con AWS Backup almacenes. A diferencia de otras políticas basadas en la IAM, las políticas de AWS Backup acceso no admiten el uso de un comodín en la clave. Action

Para obtener una lista de los nombres de recursos de Amazon (ARNs) que puede utilizar para identificar los puntos de recuperación de distintos tipos de recursos, consulte el punto [AWS Backup recurso ARNs](#) de recuperación específico del recurso. ARNs

Las políticas de acceso a Vault solo controlan el acceso de los usuarios a. AWS Backup APIs También se puede acceder a algunos tipos de copias de seguridad, como las instantáneas de Amazon Elastic Block Store (Amazon EBS) y Amazon Relational Database Service (Amazon RDS), mediante estos servicios. APIs Puede crear políticas de acceso independientes en IAM que controlen el acceso a dichas políticas para controlar completamente el acceso APIs a esos tipos de copias de seguridad.

Independientemente de la política de acceso del AWS Backup almacén, se `backup:CopyIntoBackupVault` rechazará el acceso entre cuentas para cualquier acción que no sea la que no sea la del recurso al que se hace referencia. Es decir, se AWS Backup rechazará cualquier otra solicitud de una cuenta que no sea la cuenta del recurso al que se hace referencia.

Temas

- [Denegación del acceso a un tipo de recurso en un almacén de copias de seguridad](#)
- [Denegación del acceso a un almacén de copias de seguridad](#)
- [Denegación del acceso para eliminar puntos de recuperación en un almacén de copias de seguridad](#)

Denegación del acceso a un tipo de recurso en un almacén de copias de seguridad

Esta política deniega el acceso a las operaciones de API especificadas para todas las instantáneas de Amazon EBS de un almacén de copias de seguridad.

Denegación del acceso a un almacén de copias de seguridad

Esta política deniega el acceso a las operaciones de API especificadas dirigidas a un almacén de copias de seguridad.

Denegación del acceso para eliminar puntos de recuperación en un almacén de copias de seguridad

El acceso a los almacenes y la capacidad de eliminar puntos de recuperación almacenados en ellos se determinará en función del acceso que conceda a los usuarios.

Siga estos pasos para crear una política de acceso basada en recursos en un almacén de copias de seguridad que impida la eliminación de todas las copias de seguridad del almacén.

Para crear una política de acceso basada en recursos en un almacén de copias de seguridad

1. Inicie sesión en y abra la Consola de administración de AWS AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación de la izquierda, elija Backup vaults (Almacenes de copias de seguridad).
3. Elija un almacén de copias de seguridad en la lista.
4. En la sección Access policy (Política de acceso), pegue el siguiente ejemplo de JSON. Esta política impide que cualquier persona que no sea la entidad principal elimine un punto de recuperación en el almacén de copias de seguridad de destino.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": "backup:DeleteRecoveryPoint",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:userId": [
            "AIDA1234567890EXAMPLE",
            "ARO1234567890EXAMPLE:my-role-session",
            "ARO1234567890EXAMPLE:*",
            "112233445566"
          ]
        }
      }
    }
  ]
}
```

```
}  
  }  
] }  
}
```

Para permitir que las identidades de IAM de la lista utilicen su ARN, utilice la clave de condición global `aws:PrincipalArn` del siguiente ejemplo.

Para obtener información acerca de cómo obtener un ID único para una entidad de IAM, consulte [Obtener el identificador único](#) en la Guía del usuario de IAM.

Si desea limitar esto a tipos de recursos específicos, en lugar de `"Resource": "*"` , puede incluir explícitamente los tipos de puntos de recuperación que se van a denegar. Por ejemplo, para las instantáneas de Amazon EBS, cambie el tipo de recurso por lo siguiente.

```
"Resource": ["arn:aws:ec2::Region::snapshot/*"]
```

5. Elija Asociar política.

AWS Backup Vault Lock

Note

AWS Backup Cohasset Associates ha evaluado Vault Lock para su uso en entornos sujetos a las normas SEC 17a-4, la CFTC y la FINRA. [Para obtener más información sobre la relación de AWS Backup Vault Lock con estas normas, consulte la evaluación de conformidad de Cohasset Associates.](#)

AWS Backup Vault Lock es una función opcional de las bóvedas de respaldo, que puede resultar útil para proporcionarle seguridad y control adicionales sobre las bóvedas de respaldo. Cuando hay un bloqueo activo en el modo de conformidad y ha transcurrido el tiempo de gracia, el cliente o el account/data propietario no podrá modificar ni eliminar la configuración del almacén AWS mientras contenga puntos de recuperación. Cada almacén puede tener implementado un bloqueo de almacén.

AWS Backup garantiza que sus copias de seguridad estén disponibles para usted hasta que venzan sus períodos de retención. Si algún usuario (incluido el usuario root) intenta eliminar una copia de

seguridad o cambiar las propiedades del ciclo de vida de un almacén bloqueado, AWS Backup denegará la operación.

- Los usuarios con permisos de IAM suficientes pueden eliminar el bloqueo de los almacenes bloqueadas en modo de gobernanza.
- Los almacenes bloqueadas en modo de gobernanza no se pueden eliminar una vez que el periodo de reflexión (“periodo de gracia”) venza si hay puntos de recuperación en el almacén. Durante el periodo de gracia, aún puede eliminar el bloqueo del almacén y cambiar la configuración del bloqueo.

Modos de bloqueo del almacén

Al crear un bloqueo de almacén, puede elegir entre dos modos: el modo de gobernanza o el modo de cumplimiento. El modo de gobernanza está diseñado para permitir que solo usuarios con suficientes privilegios de IAM administren el almacén. El modo de gobernanza ayuda a una organización a cumplir los requisitos de gobernanza, ya que garantiza que solo el personal designado pueda hacer cambios en un almacén de copias de seguridad. El modo de cumplimiento está pensado para almacenes de copias de seguridad en los que se espera que el almacén (y, por extensión, su contenido) no se vaya a eliminar ni modificar nunca hasta que se complete el periodo de retención de datos. Una vez que un almacén en modo de conformidad está bloqueado, es inmutable, lo que significa que el bloqueo no se puede eliminar (el propio almacén se puede eliminar si está vacío y no contiene ningún punto de recuperación).

Los usuarios que dispongan de los permisos de IAM adecuados pueden administrar o eliminar un almacén bloqueado en modo gobernanza.

Un bloqueo de almacén en modo de cumplimiento no puede ser modificado ni eliminado por ningún usuario ni por AWS. Un almacén bloqueado en modo de cumplimiento tiene un periodo de gracia que se establece antes de que se bloquee y los contenidos del almacén pasan a ser inmutables.

Ventajas del bloqueo de almacenes

AWS Backup Vault Lock ofrece varias ventajas, entre las que se incluyen las siguientes:

- Configuración de WORM (escritura única y lectura múltiple) para todas las copias de seguridad que almacene y cree en un almacén de copias de seguridad.
- Una capa de defensa adicional que protege las copias de seguridad (puntos de recuperación) de sus almacenes de copias de seguridad contra eliminaciones involuntarias o malintencionadas.

- Aplica los períodos de retención, lo que evita que los usuarios con privilegios (incluido el usuario Cuenta de AWS root) los eliminen anticipadamente y cumple con las políticas y los procedimientos de protección de datos de la organización.

Bloqueo de un almacén de copias de seguridad mediante la consola

Puede añadir un candado de bóveda a su AWS Backup bóveda mediante la consola Backup.

Para agregar un bloqueo de almacén a su almacén de copias de seguridad:

1. Inicie sesión en y abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
[Consola de administración de AWS](#)
2. En el panel de navegación, elija Almacenes de copia de seguridad. Haga clic en el enlace anidado debajo de Almacenes de copia de seguridad denominado Bloqueos de almacén.
3. En Cómo funcionan los bloqueos de almacén o Bloqueos de almacén, haga clic en + crear bloqueo de almacén.
4. En el panel Detalles del bloqueo de almacén, elija el almacén al que desea que se aplique el bloqueo.
5. En Modo de bloqueo de almacenes, elija el modo en el que desea bloquear su almacén. Para obtener más información sobre cómo elegir los modos, consulte [Modos de bloqueo del almacén](#), que aparece antes en esta página.
6. Para el Periodo de retención, elija los periodos de retención mínimo y máximo (los periodos de retención son opcionales). Los nuevos trabajos de copia y copia de seguridad creados en el almacén darán un error si no se ajustan a los periodos de retención que haya establecido; estos periodos no se aplicarán a los puntos de recuperación que ya estén en el almacén.
7. Si ha elegido el modo de cumplimiento, aparecerá una sección denominada Fecha de inicio del bloqueo de almacén. Si ha elegido el modo de gobernanza, esto no se mostrará y podrá omitir este paso.

En el modo de cumplimiento, un bloqueo de almacén tiene un periodo de reflexión desde su creación hasta que el almacén y su bloqueo se vuelven inmutables e incambiables. Usted elige la duración de este periodo (denominado periodo de gracia), aunque debe ser de al menos 3 días (72 horas).

⚠ Important

Una vez transcurrido el periodo de gracia, el almacén y su bloqueo son inmutables. Ningún usuario ni AWS puede cambiarlo ni eliminarlo.

8. Cuando esté satisfecho con las opciones de configuración, haga clic en Crear bloqueo de almacén.
9. Para confirmar que desea crear este bloqueo en el modo elegido, escriba `confirm` en el cuadro de texto y, a continuación, marque la casilla para confirmar que la configuración es la deseada.

Si los pasos se han completado correctamente, aparecerá un banner en la parte superior de la consola que indica que el proceso se ha realizado correctamente.

Bloqueo de un almacén de copias de seguridad mediante programación

Para configurar AWS Backup Vault Lock, utilice la API [PutBackupVaultLockConfiguration](#). Los parámetros que se incluyan dependerán del modo de bloqueo de almacén que desee utilizar. Si desea crear un bloqueo de almacén en modo de gobernanza, no incluya `ChangeableForDays`. Si incluye este parámetro, el bloqueo del almacén se creará en modo de cumplimiento.

Este es una CLI de ejemplo de creación de un bloqueo de almacén en modo de cumplimiento:

```
aws backup put-backup-vault-lock-configuration \  
  --backup-vault-name my_vault_to_lock \  
  --changeable-for-days 3 \  
  --min-retention-days 7 \  
  --max-retention-days 30
```

Este es una CLI de ejemplo de creación de un bloqueo de almacén en modo de gobernanza:

```
aws backup put-backup-vault-lock-configuration \  
  --backup-vault-name my_vault_to_lock \  
  --min-retention-days 7 \  
  --max-retention-days 30
```

Puede configurar cuatro opciones.

1. **BackupVaultName**

El nombre del almacén que se va a bloquear.

2. **ChangeableForDays** (se incluye solo para el modo de cumplimiento)

Este parámetro indica AWS Backup que se cree el bloqueo del almacén en modo de conformidad. Omite este parámetro si desea crear el bloqueo en el modo de gobernanza.

Este valor se expresa en días. Debe ser un número no inferior a 3 ni superior a 36 500; de lo contrario, se generará un error.

Desde la creación de este bloqueo de almacén hasta el vencimiento de la fecha especificada, el bloqueo de almacén se puede quitar de la bóveda mediante `DeleteBackupVaultLockConfiguration`. Como alternativa, durante este tiempo, puede cambiar la configuración mediante `PutBackupVaultLockConfiguration`.

A partir de la fecha especificada, determinada por este parámetro, el almacén de copias de seguridad será inmutable y no se podrá modificar ni eliminar.

3. **MaxRetentionDays** (opcional)

Es un valor numérico expresado en días. Es el periodo máximo de retención durante el cual el almacén retiene sus puntos de recuperación.

El periodo máximo de retención que elija debe estar en consonancia con las políticas de retención de datos de su organización. Si su organización exige que los datos se retengan durante un periodo determinado, este valor se puede establecer en ese periodo (en días). Por ejemplo, es posible que sea necesario conservar los datos financieros o bancarios durante 7 años (aproximadamente 2557 días, según los años bisiestos).

Si no se especifica, AWS Backup Vault Lock no aplicará un período máximo de retención. Si se especifica, no se podrán realizar copias ni copias de seguridad en este almacén con periodos de retención del ciclo de vida superiores al periodo máximo de retención. Los puntos de recuperación ya guardados en el almacén antes de la creación del bloqueo no se ven afectados. El periodo de retención máximo más largo que puede especificar es de 36 500 días (aproximadamente 100 años).

4. **MinRetentionDays**(opcional; obligatorio para CloudFormation)

Es un valor numérico expresado en días. Es el periodo mínimo de retención durante el cual el almacén retiene sus puntos de recuperación. Esta configuración debe ajustarse a la cantidad de tiempo que su organización está obligada a mantener los datos. Por ejemplo, si la normativa o las

leyes exigen que los datos se conserven durante al menos siete años, el valor en días sería de aproximadamente 2557, según los años bisiestos.

Si no se especifica, AWS Backup Vault Lock no aplicará un período mínimo de retención. Si se especifica, no se podrán realizar copias ni copias de seguridad en este almacén con periodos de retención del ciclo de vida inferiores al periodo mínimo de retención. Los puntos de recuperación que ya estaban guardados en la bóveda antes del bloqueo de la AWS Backup bóveda no se ven afectados. El periodo de retención mínimo más corto que puede especificar es de 1 día.

Revise la configuración de Vault Lock de una AWS Backup bóveda de respaldo

Puede revisar los detalles de AWS Backup Vault Lock de una bóveda en cualquier momento llamando [DescribeBackupVault](#) o [ListBackupVaults](#) APIs.

Para determinar si ha aplicado un bloqueo de almacén a un almacén de copias de seguridad, llama a `DescribeBackupVault` y comprueba la propiedad `Locked`. Si `"Locked": true`, como en el ejemplo siguiente, ha aplicado AWS Backup Vault Lock a su bóveda de respaldo.

```
{
  "BackupVaultName": "my_vault_to_lock",
  "BackupVaultArn": "arn:aws:backup:us-east-1:555500000000:backup-
vault:my_vault_to_lock",
  "EncryptionKeyArn": "arn:aws:kms:us-
east-1:555500000000:key/00000000-1111-2222-3333-000000000000",
  "CreationDate": "2021-09-24T12:25:43.030000-07:00",
  "CreatorRequestId": "ac6ce255-0456-4f84-bbc4-eec919f50709",
  "NumberOfRecoveryPoints": 1,
  "Locked": true,
  "MinRetentionDays": 7,
  "MaxRetentionDays": 30,
  "LockDate": "2021-09-30T10:12:38.089000-07:00"
}
```

El resultado anterior confirma las opciones siguientes:

1. `Locked` es un booleano que indica si ha aplicado AWS Backup Vault Lock a esta bóveda de respaldo. `True` significa que AWS Backup Vault Lock provoca un error en las operaciones

de eliminación o actualización de los puntos de recuperación almacenados en el almacén (independientemente de si aún se encuentra o no en el período de gracia de reflexión).

2. LockDate es la fecha y hora UTC en las que finaliza el periodo de gracia de reflexión. Pasado este tiempo, no podrá eliminar ni cambiar el bloqueo de este almacén. Utilice cualquier conversor de hora disponible al público para convertir esta cadena a su hora local.

Si "Locked": false, como en el ejemplo siguiente, no ha aplicado un bloqueo de almacén (o se ha eliminado uno anterior).

```
{
  "BackupVaultName": "my_vault_to_lock",
  "BackupVaultArn": "arn:aws:backup:us-east-1:555500000000:backup-
vault:my_vault_to_lock",
  "EncryptionKeyArn": "arn:aws:kms:us-
east-1:555500000000:key/00000000-1111-2222-3333-000000000000",
  "CreationDate": "2021-09-24T12:25:43.030000-07:00",
  "CreatorRequestId": "ac6ce255-0456-4f84-bbc4-eec919f50709",
  "NumberOfRecoveryPoints": 3,
  "Locked": false
}
```

Eliminación del bloqueo del almacén durante el periodo de gracia (modo de cumplimiento)

Para eliminar el bloqueo del almacén durante el tiempo de gracia (es decir, después de bloquear el depósito pero antes del tuyoLockDate) mediante la AWS Backup consola,

1. Inicie sesión en y abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
[Consola de administración de AWS](#)
2. En el menú de navegación de la izquierda, en Mi cuenta, haga clic en Almacenes de copia de seguridad y, a continuación, en Bloqueo de almacén de copias de seguridad.
3. Haga clic en el bloqueo del almacén que desee eliminar y, a continuación, en Administrar el bloqueo de almacén.
4. Haga clic en Eliminar el bloqueo de almacén.
5. Aparecerá un cuadro de advertencia en el que se le pedirá que confirme su intención de eliminar el bloqueo del almacén. Escriba **confirm** en el cuadro de texto y, a continuación, haga clic en confirmar.

Cuando todos los pasos se hayan completado correctamente, aparecerá un banner en la parte superior de la pantalla de la consola que indica que el proceso se ha realizado correctamente.

Para eliminar el bloqueo del almacén durante el periodo de gracia mediante un comando de la CLI, utilice [DeleteBackupVaultLockConfiguration](#) como en este ejemplo de CLI:

```
aws backup delete-backup-vault-lock-configuration \  
  --backup-vault-name my_vault_to_lock
```

Cuenta de AWS cierre con una bóveda cerrada

Cuando cierras una Cuenta de AWS que contiene una bóveda de copias de seguridad AWS y AWS Backup suspendes tu cuenta durante 90 días con las copias de seguridad intactas. Si no vuelves a abrir tu cuenta durante esos 90 días, AWS borra el contenido de tu almacén de copias de seguridad, incluso si AWS Backup Vault Lock estaba activado.

Consideraciones adicionales de seguridad

AWS Backup Vault Lock añade un nivel adicional de seguridad a tu defensa en profundidad en materia de protección de datos. El bloqueo de almacenes se puede combinar con estas otras características de seguridad:

- [Cifrado de sus puntos de recuperación](#)
- [AWS Backup políticas de acceso a almacenes y puntos de recuperación](#), que permiten conceder o denegar permisos a nivel de almacén,
- [AWS Backup las mejores prácticas de seguridad](#), incluida su biblioteca de [políticas administradas por el cliente](#) que le permiten conceder o denegar permisos de copia de seguridad y restauración mediante un servicio AWS compatible, y
- [AWS Backup Audit Manager](#), que le permite automatizar las comprobaciones de conformidad de sus copias de seguridad comparándolas [con una lista de controles](#) que usted defina.

Puede trabajar a través de [Creación de marcos mediante la AWS Backup API](#) para [Los recursos están en un plan de respaldo con un AWS Backup Vault Lock](#) de control con AWS Backup Audit Manager para asegurarse de que los recursos deseados estén protegidos con un bloqueo de almacén.

- Los mecanismos que inactivan los recursos pueden afectar a la capacidad de restaurarlos. Si bien todavía no se pueden eliminar en una bóveda cerrada, pueden estar en un estado distinto al activo. Por ejemplo, la configuración de Amazon Elastic Compute Cloud que permite [deshabilitar](#)

[una AMI](#) puede bloquear temporalmente la capacidad de restaurar las copias de seguridad de EC2 las instancias. Esto afecta a todos los puntos de EC2 recuperación, incluso a las copias de seguridad afectadas por un bloqueo del almacén o una retención legal.

Si una EC2 copia de seguridad está deshabilitada, puede [volver a activar una AMI deshabilitada](#). Una vez que se vuelva a activar, podrá restaurarse. Para bloquear la característica de desactivación de la AMI, puede utilizar las políticas de IAM para no permitir `ec2:DisableImage`.

 Note

AWS Backup Vault Lock no es la misma función que [Amazon Glacier Vault Lock](#), que solo es compatible con Amazon Glacier.

Creación, mantenimiento y restauración de copias de seguridad

Una copia de seguridad, o punto de recuperación, representa el contenido de un recurso, por ejemplo un volumen de Amazon Elastic Block Store (Amazon EBS) o una tabla de Amazon DynamoDB, en un momento específico. Punto de recuperación es un término que se refiere generalmente a las distintas copias de seguridad de los AWS servicios, como las instantáneas de Amazon EBS y las copias de seguridad de DynamoDB. Los términos punto de recuperación y copia de seguridad se utilizan indistintamente.

AWS Backup guarda los puntos de recuperación en bóvedas de respaldo, que puede organizar de acuerdo con las necesidades de su empresa. Por ejemplo, puede guardar un conjunto de recursos que contengan información financiera para el ejercicio de 2020. Cuando necesite recuperar un recurso, puede utilizar la AWS Backup consola o el AWS Command Line Interface (AWS CLI) para buscar y recuperar el recurso que necesita.

Cada punto de recuperación tiene un identificador único. El identificador único se encuentra al final del nombre de recurso de Amazon (ARN) del punto de recuperación. Para ver ejemplos de puntos de recuperación ARNs y únicos IDs, consulte la tabla de [Recursos y operaciones](#).

Important

Para evitar cargos adicionales, configure su política de retención con una duración de almacenamiento en caliente de al menos una semana. Para obtener más información, consulte [Medición, costos y facturación de AWS Backup](#).

Las siguientes secciones proporcionan información general acerca de las tareas de administración básicas de copia de seguridad en AWS Backup.

Temas

- [Crear una copia de seguridad bajo demanda mediante AWS Backup](#)
- [Respaldos y point-in-time recuperación continuos \(PITR\)](#)
- [Creación de copias de seguridad por tipo de recurso](#)
- [Copia de seguridad y copia de etiquetas](#)
- [Eliminaciones de las copias de seguridad](#)

- [Ediciones de copia de seguridad y etiquetas](#)
- [Búsqueda de copias de seguridad](#)
- [Backup por niveles](#)
- [Restauración de una copia de seguridad por tipo de recurso](#)
- [Pruebas de restauración](#)
- [Detener un trabajo de copia de seguridad](#)
- [Visualizar copias de seguridad existentes](#)

Crear una copia de seguridad bajo demanda mediante AWS Backup

En la AWS Backup consola, la página Recursos protegidos muestra los recursos de los que se ha hecho una copia de seguridad al AWS Backup menos una vez. Si lo utiliza AWS Backup por primera vez, no hay ningún recurso (como volúmenes de Amazon EBS o bases de datos de Amazon RDS) en esta página. No aparecerán aunque haya asignado un recurso a un plan de copias de seguridad si dicho plan no ha ejecutado un trabajo de copia de seguridad programado al menos una vez.

Nota: Una copia de seguridad bajo demanda comienza a hacer copias de seguridad de su recurso de forma inmediata. Puede elegir una copia de seguridad bajo demanda si desea crear una copia de seguridad en un momento distinto del momento programado definido en un plan de copia de seguridad. Una copia de seguridad bajo demanda se puede utilizar, por ejemplo, para probar la copia de seguridad y su funcionalidad en cualquier momento.

Las copias de seguridad bajo demanda no se pueden usar con la point-in-time recuperación (PITR), ya que una copia de seguridad bajo demanda preserva los recursos en el estado en que se encuentran cuando se realiza la copia de seguridad, pero la PITR usa [copias de seguridad continuas](#), que registran los cambios durante un período de tiempo.

Consideraciones

- Si el rol AWS Backup predeterminado no está presente en tu cuenta, se crea uno para ti con los permisos correctos.
- Cuando las copias de seguridad venzan y estén marcadas para su eliminación como parte de su política de ciclo de vida, AWS Backup las eliminará en un momento elegido al azar durante las 8 horas siguientes. Este intervalo ayuda a garantizar un rendimiento uniforme.

- En el caso de EC2 los recursos de Amazon, copia AWS Backup automáticamente las etiquetas de recursos individuales y grupales existentes, además de las etiquetas que añadidas en este paso.
- AWS Backup realiza EC2 copias de seguridad con el comportamiento predeterminado de «no reiniciar». AWS Backup actualmente admite recursos que se ejecutan en Amazon EC2 y algunos tipos de instancias no son compatibles. Para obtener más información, consulte [Creación de copias de seguridad de Windows VSS](#).

Para crear una copia de seguridad bajo demanda

1. Abre la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel, elija Create an on-demand backup (Crear una copia de seguridad bajo demanda). O bien, en el panel de navegación, elija Protected resources (Recursos protegidos) y, a continuación, Create an on-demand backup (Crear una copia de seguridad bajo demanda).
3. En la página Tipo de recurso, elija el tipo de recurso del que desea crear una copia de seguridad. Por ejemplo, elija DynamoDB para las tablas de Amazon DynamoDB.
4. Elija el nombre o ID del recurso que desea proteger. Por ejemplo, elija el nombre de la tabla de DynamoDB para Amazon DynamoDB.
5. Asegúrese de que la opción Create backup now (Crear copia de seguridad ahora) esté seleccionada.
6. Si el tipo de recurso admite la transición al almacenamiento en frío, el almacenamiento en frío está presente. Para obtener más información, consulte la columna Ciclo de vida al almacenamiento en frío de la tabla [Disponibilidad de características por recurso](#).

Para especificar cuándo se almacenará esta copia de seguridad en frío, seleccione Mover las copias de seguridad del almacenamiento semiactivo al almacenamiento en frío y, a continuación, especifique el tiempo en almacenamiento semiactivo.

7. En Período de retención total, especifique el número de días. Si especificó el tiempo de almacenamiento en frío, el período de retención se divide entre almacenamiento en frío y semiactivo.
8. Elija un almacén de copias de seguridad existente o cree uno nuevo. Al elegir Create new Backup vault (Crear nuevo almacén de copias de seguridad), se abre una nueva página para crear un almacén y, a continuación, vuelve a la página Create on-demand backup (Crear copia de seguridad bajo demanda) cuando termine.
9. En Rol de IAM, seleccione el rol predeterminado o un rol que creó.

10. Para asignar una etiqueta a su copia de seguridad bajo demanda, expanda Etiquetas agregadas a los puntos de recuperación, elija Agregar etiqueta nueva e ingrese una clave y un valor de etiqueta.
11. Las opciones de Configuración avanzada de copia de seguridad varían según el tipo de recurso:
 - Para obtener EC2recursos: para realizar instantáneas coherentes con las aplicaciones mediante Windows Volume Shadow Copy Service (VSS), elija Windows VSS.
 - Para los recursos de Amazon S3: puede optar por excluir las listas de control de acceso (ACLs) de la copia de seguridad dejando las listas de control de acceso de respaldo (ACLs) sin seleccionar.
12. Seleccione Create on-demand backup (Crear copia de seguridad bajo demanda). Esto abre la página Trabajos, donde puede ver una lista de trabajos y ver su estado.

RespalDOS y point-in-time recuperación continuos (PITR)

En el caso de algunos recursos, AWS Backup admite copias de seguridad y point-in-time recuperación continuas (PITR) además de las copias de seguridad instantáneas.

Con las copias de seguridad continuas, puede restaurar el recurso AWS Backup compatible retrocediéndolo hasta el momento específico que elija, con un tiempo de precisión de 1 segundo (retrocediendo un máximo de 35 días). La copia de seguridad continua consiste en crear primero una copia de seguridad completa del recurso y, a continuación, realizar copias de seguridad constantes de los registros de transacciones del recurso. La PITR consiste en acceder a la copia de seguridad completa y reproducir el registro de transacciones hasta el momento en que se le indique a AWS Backup que realice la recuperación.

Como alternativa, se pueden realizar copias de seguridad instantáneas con una frecuencia de hasta una hora. Las copias de seguridad de instantáneas se pueden almacenar hasta un máximo de 100 años. Las instantáneas se pueden copiar para realizar copias de seguridad completas o incrementales.

Dado que las copias de seguridad continuas y las instantáneas ofrecen diferentes ventajas, le recomendamos que proteja sus recursos con reglas de copia de seguridad continuas e instantáneas.

Una copia de seguridad bajo demanda comienza a hacer copias de seguridad de su recurso de forma inmediata. Puede elegir una copia de seguridad bajo demanda si desea crear una copia de seguridad en un momento distinto del momento programado definido en un plan de copia de

seguridad. Una copia de seguridad bajo demanda se puede utilizar, por ejemplo, para probar la copia de seguridad y su funcionalidad en cualquier momento.

No puede usar [copias de seguridad bajo demanda](#) con la PITR, ya que la copia de seguridad bajo demanda conserva los recursos en el estado en que se encontraban cuando se realizó la copia de seguridad, mientras que la PITR utiliza copias de seguridad continuas que registran los cambios a lo largo de un periodo de tiempo.

Puede optar por realizar copias de seguridad continuas para los recursos compatibles al crear un plan de copias de seguridad AWS Backup mediante la AWS Backup consola o la API. El plan de copia de seguridad continuo crea un punto de recuperación continuo y lo actualiza cada vez que se ejecuta el trabajo.

Contenido

- [Point-in-time consideraciones de recuperación](#)
- [Servicios compatibles con las copias de seguridad continuas y la PITR](#)
- [Búsqueda de una copia de seguridad continua](#)
- [Restauración de una copia de seguridad continua](#)
- [Detención o eliminación de copias de seguridad continuas](#)
- [Copiado de copias de seguridad continuas](#)
- [Cambio del periodo de retención](#)
- [Eliminación de la única regla de copia de seguridad continua de un plan de copia de seguridad](#)

Point-in-time consideraciones de recuperación

Tenga en cuenta las siguientes consideraciones para la point-in-time recuperación:

- Recuperación automática a instantáneas: si AWS Backup no puede realizar una copia de seguridad continua, intenta realizar una copia de seguridad instantánea en su lugar.
- No admite las copias de seguridad continuas a pedido: AWS Backup no admite las copias de seguridad continuas a pedido, ya que las copias de seguridad a pedido registran un punto en el tiempo, mientras que las copias de seguridad continuas registran los cambios a lo largo de un período de tiempo.
- No admite la transferencia al almacenamiento en frío: las copias de seguridad continuas no admiten la transferencia al almacenamiento en frío porque la transferencia al almacenamiento en

frío requiere un periodo de transferencia mínimo de 90 días, mientras que las copias de seguridad continuas tienen un periodo de retención máximo de 35 días.

- Restauración de la actividad reciente: la actividad de Amazon RDS permite restauraciones hasta los últimos 5 minutos de actividad; Amazon S3 permite restauraciones hasta los últimos 15 minutos de actividad.

Important

Un único recurso solo puede tener una copia de seguridad continua. Expandir la siguiente sección para obtener información adicional y conocer las prácticas recomendadas.

Copias de seguridad continuas superpuestas en el mismo recurso

Cada recurso (como un bucket de Amazon S3 o una base de datos de Amazon RDS) solo puede tener una copia de seguridad continua (punto de recuperación); las copias de seguridad continuas adicionales son redundantes. Cuando varias políticas, planes o reglas de respaldo indican AWS Backup la creación de múltiples copias de seguridad continuas para el mismo recurso, se aplica el siguiente proceso:

- Si varias reglas especifican que debe haber más de una copia de seguridad continua en un mismo almacén, AWS Backup siga la regla con el período de retención más largo (ciclo de vida) e ignore las reglas adicionales.
- Si varias reglas especifican que debe haber más de una copia de seguridad continua en más de un almacén, AWS Backup crea una copia de seguridad continua de acuerdo con la primera regla procesada. Cada regla posterior que especifique una copia de seguridad continua para un recurso que ya tiene una copia de seguridad continua dará como resultado una copia de seguridad (periódica) de la instantánea en su lugar.

Cuando se duplican los planes de copias de seguridad continuas, las copias de seguridad de instantáneas creadas después del punto de recuperación continuo pueden mostrar el estado `Completed with issues`. La información detallada de este punto de recuperación mostrará un error similar a `"Enabling continuous backup failed, because of the following error: PITR already configured in backup plan: [ARN]"`. Este error indica que al menos hay una copia de seguridad continua configurada (para un punto de recuperación diferente

al que contiene el error). Esa primera copia de seguridad continua (punto de recuperación) se puede utilizar para la restauración en un momento dado (PITR) siempre que tenga el estado COMPLETED.

Para evitar que se creen instantáneas de forma inintencionada con problemas (y mensajes de error), revise la estrategia de copias de seguridad de su organización. Si es necesario, adapte los planes y políticas de copia de seguridad para crear múltiples copias de seguridad continuas del mismo recurso.

Cuando haya realizado los ajustes que den como resultado una sola copia de seguridad continua para un recurso, las copias de seguridad de instantáneas se conservarán de acuerdo con el ciclo de vida especificado del plan que las creó; a continuación, pasarán a tener el estado EXPIRED y se eliminarán. La copia de seguridad continua y su capacidad de point-in-time recuperación se mantendrán de acuerdo con la regla que la creó.

Servicios compatibles con las copias de seguridad continuas y la PITR

AWS Backup admite copias de seguridad y point-in-time recuperación continuas para los siguientes servicios y aplicaciones:

Amazon S3

Para activar la PITR en las copias de seguridad de S3, las copias de seguridad continuas deben formar parte del plan de copia de seguridad.

Si bien esta copia de seguridad original del bucket de origen puede tener la PITR activa, las copias de destino entre regiones o entre cuentas no tendrán PITR, y la restauración a partir de estas copias será en el momento en el que se crearon (las copias serán copias de instantáneas) en lugar de restaurarse en un momento específico.

AWS Backup para S3 se basa en la recepción de eventos de S3 a través de Amazon EventBridge. Si este ajuste está deshabilitado en la configuración de notificaciones del bucket de S3, se detendrán las copias de seguridad continuas de esos buckets con el ajuste desactivado. Para obtener más información, consulte [Uso EventBridge](#).

RDS

Programaciones de backup: cuando un AWS Backup plan cree tanto instantáneas de Amazon RDS como copias de seguridad continuas, AWS Backup programará de forma inteligente las ventanas de backup para coordinarlas con la ventana de mantenimiento de Amazon RDS y evitar conflictos. Para

evitar aún más conflictos, la configuración manual del periodo de copia de seguridad automática de Amazon RDS no está disponible. RDS toma instantáneas una vez al día, incluso si un plan de copia de seguridad tiene una frecuencia de copias de seguridad de instantáneas diferente a una vez al día.

Configuración: después de aplicar una regla de copia de seguridad AWS Backup continua a una instancia de Amazon RDS, no puede crear ni modificar la configuración de copia de seguridad continua de esa instancia en Amazon RDS; las modificaciones deben realizarse a través de la AWS Backup consola o la CLI AWS Backup .

Control de transición de una instancia de Amazon RDS de vuelta a Amazon RDS:

Console

1. [Abra la AWS Backup consola en /backup. https://console.aws.amazon.com](https://console.aws.amazon.com/backup)
2. En el panel de navegación, seleccione Backup plans (Planes de copias de seguridad).
3. Elimine todos los planes de copia de seguridad de Amazon RDS con una copia de seguridad continua que proteja ese recurso.
4. Elija Almacenes de Backup. Elimine el punto de recuperación de la copia de seguridad continua de su almacén de copias de seguridad. O bien, espere a que transcurra su período de retención, lo que provocará que AWS Backup se elimine automáticamente el punto de recuperación.

Después de completar estos pasos, AWS Backup transferirá el control de respaldo continuo de su recurso a Amazon RDS.

AWS CLI

Llame a la operación de la API `DisassociateRecoveryPoint`.

Para obtener más información, consulte [DisassociateRecoveryPoint](#).

Permisos de IAM requeridos para las copias de seguridad continuas de Amazon RDS

- AWS Backup Para configurar copias de seguridad continuas para su base de datos de Amazon RDS, compruebe que el permiso de API `rds:ModifyDBInstance` existe en la función de IAM definida en la configuración del plan de copias de seguridad. Para restaurar las copias de seguridad continuas de Amazon RDS, debe agregar el permiso `rds:RestoreDBInstanceToPointInTime` al rol de IAM que envió para el trabajo de

restauración. Puede utilizar `AWS Backup default service role` para realizar copias de seguridad y restauraciones.

- Para describir el rango de tiempos disponibles para la point-in-time recuperación, AWS Backup llame a `rds:DescribeDBInstanceAutomatedBackups`. En la AWS Backup consola, debes tener el permiso de `rds:DescribeDBInstanceAutomatedBackups` API en tu política gestionada AWS Identity and Access Management (IAM). Puede utilizar las políticas administradas `AWSBackupOperatorAccess` o `AWSBackupFullAccess`. Ambas políticas tienen todos los permisos necesarios. Para obtener más información, consulte [Políticas administradas](#).

Períodos de retención: al cambiar el período de retención de la PITR, AWS Backup llama a [ModifyDBInstance](#) y [aplica ese cambio](#), empezando por la siguiente copia de seguridad que se realice, según se define en la regla de frecuencia establecida en el plan de copia de seguridad.

Copias de seguridad continuas de Amazon RDS:

- Los trabajos de copia de instantáneas incrementales se procesan más rápido que los trabajos de copia de instantáneas completas. Si se mantiene una copia de instantánea anterior hasta que se complete el nuevo trabajo de copia se puede reducir la duración del trabajo de copia. Si decide copiar las instantáneas de las instancias de la base de datos de RDS, es importante tener en cuenta que si elimina primero las copias anteriores, se realizarán copias de instantáneas completas (en lugar de incrementales). Para obtener más información sobre cómo optimizar la copia, consulte [Copias de instantáneas incrementales](#) en la Guía del usuario de Amazon RDS.
- Creación de copias de seguridad continuas de Amazon RDS: no puede crear copias de las copias de seguridad continuas de Amazon RDS porque AWS Backup Amazon RDS no permite copiar los registros de transacciones. En su lugar, AWS Backup crea una instantánea y la copia con la frecuencia especificada en el plan de copias de seguridad.

Restauraciones: puede realizar una point-in-time restauración con Amazon RDS AWS Backup o con Amazon RDS. Para obtener instrucciones sobre AWS Backup la consola, consulte [Restauración de una base de datos de Amazon RDS](#). Para obtener instrucciones sobre Amazon RDS, consulte [Restauración de una instancia de base de datos a un momento especificado](#) en la Guía del usuario de Amazon RDS.

Tip

Una instancia de base de datos con varias zonas de disponibilidad (AZ) establecida en `Always On` no debería tener la retención de copias de seguridad establecida en cero. Si se

producen errores, utilice el AWS CLI comando `disassociate-recovery-point` en lugar de `ydelete-recovery-point`, a continuación, cambie la configuración de retención a 1 en la configuración de Amazon RDS.

Para obtener información general sobre el uso de Amazon RDS, consulte la [Guía del usuario De Amazon RDS](#).

Aurora

Para habilitar la copia de seguridad continua de sus recursos de Aurora, consulte los pasos de la primera sección de esta página.

El procedimiento para restaurar un clúster de Aurora a un momento dado es una [variación de los pasos para restaurar una instantánea de un clúster de Aurora](#).

Al realizar una restauración en un momento dado, la consola muestra una sección de hora de restauración. Consulte Restauración a partir de una copia de seguridad continua más abajo en esta página, en [Uso de copias de seguridad continuas](#).

EC2 Instancias de SAP HANA en Amazon

Puede realizar [copias de seguridad continuas](#), que se pueden utilizar con la point-in-time restauración (PITR) (tenga en cuenta que las copias de seguridad bajo demanda conservan los recursos en el estado en que se toman, mientras que la PITR utiliza copias de seguridad continuas que registran los cambios a lo largo de un período de tiempo).

Con las copias de seguridad continuas, puede restaurar la base de datos de SAP HANA en una EC2 instancia retrocediéndola hasta el momento específico que elija, con una precisión de 1 segundo (con un tiempo máximo de 35 días). La copia de seguridad continua consiste en crear primero una copia de seguridad completa del recurso y, a continuación, realizar copias de seguridad constantes de los registros de transacciones del recurso. La restauración mediante PITR funciona accediendo a la copia de seguridad completa y reproduciendo el registro de transacciones hasta el momento indicado para su recuperación. AWS Backup

Puede optar por realizar copias de seguridad continuas al crear un plan de copias de seguridad AWS Backup mediante la AWS Backup consola o la API.

Para habilitar las copias de seguridad continuas desde la consola

1. Inicie sesión en y abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
[Consola de administración de AWS](#)
2. En el panel de navegación principal, elija Planes de copia de seguridad y, a continuación, elija Crear plan de copia de seguridad.
3. En Reglas de copia de seguridad, elija Agregar regla de copia de seguridad.
4. En la sección Configuración de regla de copia de seguridad, seleccione Habilitar copias de seguridad continuas para los recursos compatibles.

Tras deshabilitar el [PITR \(point-in-time restauración\)](#) para las copias de seguridad de las bases de datos de SAP HANA, se seguirán enviando los registros AWS Backup hasta que caduque el punto de recuperación (el estado es igual a). EXPIRED) Puede cambiar a una ubicación alternativa de copia de seguridad de registros en SAP HANA para detener la transmisión de registros a AWS Backup.

Un punto de recuperación continuo con un estado de STOPPED indica que se ha interrumpido un punto de recuperación continuo; es decir, los registros transmitidos desde SAP HANA a AWS Backup ese punto que muestran los cambios incrementales en una base de datos tienen un vacío. Los puntos de recuperación que se producen dentro de este lapso de tiempo tienen un estado de STOPPED..

Para ver los problemas que pueden surgir durante los trabajos de restauración de copias de seguridad continuas (puntos de recuperación), consulte la sección de solución [Solución de problemas de restauración de SAP HANA](#) de esta guía.

Búsqueda de una copia de seguridad continua

Puede utilizar la AWS Backup consola para buscar su copia de seguridad continua.

Para buscar una copia de seguridad continua mediante la AWS Backup consola

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, elija Almacenes de copia de seguridad y, a continuación, elija el almacén de copias de seguridad de la lista.
3. En la sección Copias de seguridad, orden la columna Tipo de copia de seguridad según los puntos de recuperación Continuos. También puede ordenar según el ID de punto de recuperación para el prefijo continuo.

Restauración de una copia de seguridad continua

Para restaurar una copia de seguridad continua mediante la consola AWS Backup

- Durante el proceso de restauración del PITR, la AWS Backup consola muestra una sección de tiempo de restauración. En esta sección, realice una de las siguientes acciones:
 - Elija restaurar a la Última hora restaurable.
 - Elija Especificar fecha y hora para introducir su propia fecha y hora dentro del periodo de retención.

Para restaurar una copia de seguridad continua mediante la API AWS Backup

1. Para Amazon S3, consulte [Usar la AWS Backup API, la CLI o el SDK para restaurar los puntos de recuperación de S3](#).
2. Para Amazon RDS, consulte [Utilizar la AWS Backup API, la CLI o el SDK para restaurar los puntos de recuperación de Amazon RDS](#).

Detención o eliminación de copias de seguridad continuas

Puede detener la creación de copias de seguridad continuas o eliminar copias de seguridad específicas (point-in-time-recovery o puntos PITR).

Si desea detener las copias de seguridad continuas, debe eliminar la regla de la copia de seguridad continua de su plan de copia de seguridad. Si desea detener las copias de seguridad continuas para uno o más recursos, pero no para todos los recursos, cree un nuevo plan de copia de seguridad con la regla de la copia de seguridad continua para los recursos de los que aún desee realizar copias de seguridad continuas. Si, por el contrario, solo elimina un punto de recuperación de la copia de seguridad continua de su almacén de copias de seguridad, el plan de copia de seguridad seguirá ejecutando la regla de la copia de seguridad continua y se creará un nuevo punto de recuperación.

Sin embargo, incluso después de eliminar la regla de copia de seguridad continua, AWS Backup recuerda el período de retención de la regla de copia de seguridad ahora eliminada. Eliminará automáticamente el punto de recuperación de la copia de seguridad continua del almacén de copias de seguridad en función del periodo de retención especificado.

Al eliminar los puntos de recuperación de Amazon RDS, tenga en cuenta lo siguiente:

- Una instancia de base de datos con varias zonas de disponibilidad (AZ) establecida en Always On no debería tener la retención de copias de seguridad establecida en cero. Si se producen errores, utilice el AWS CLI comando `disassociate-recovery-point` en lugar de `ydelete-recovery-point`, a continuación, cambie la configuración de retención a 1 en la configuración de Amazon RDS.
- Cuando se elimina un punto de point-in-time recuperación (una copia de seguridad creada mediante una copia de seguridad continua) de Amazon RDS, se desencadena el reinicio de la base de datos y se deshabilitan los registros binarios. Para obtener más información, consulte [Periodo de retención de copia de seguridad](#) en la Guía del usuario de Amazon RDS.

Al eliminar los puntos de recuperación de Aurora, tenga en cuenta lo siguiente:

Si se selecciona para un punto de recuperación de Amazon Aurora, AWS Backup establece el período de retención en 1 día. Las copias de seguridad de Aurora no se pueden eliminar por completo hasta que también se haya eliminado el clúster de origen.

Copiado de copias de seguridad continuas

Si una regla de copia de seguridad continua también especifica una copia entre cuentas o regiones y AWS Backup admite la operación para el tipo de recurso, AWS Backup toma una instantánea del recurso y la copia en el almacén de destino. Para obtener más información sobre cómo copiar sus puntos de recuperación entre cuentas y regiones, consulte [Copia de una copia de seguridad](#).

Las copias de seguridad continuas crean copias de seguridad periódicas de acuerdo con la frecuencia establecida en la regla del plan de copias de seguridad en la región de la cuenta and/or de destino.

AWS Backup no admite copias bajo demanda de copias de seguridad continuas.

Cambio del periodo de retención

Puede utilizarla AWS Backup para aumentar o reducir el período de retención de su regla de copia de seguridad continua existente. El periodo mínimo de retención es de 1 día. El periodo máximo de retención es de 35 días. El cambio en el período de retención entrará en vigor cuando se complete la siguiente copia de seguridad después de dicho cambio.

Período de retención por servicio

El comportamiento de retención puede ser específico del tipo de recurso del que se hace una copia de seguridad en el punto de recuperación.

Amazon S3

Cuando un período de retención de un punto de recuperación continuo de Amazon S3 cambie (aumente o disminuya), el estado de ese punto de recuperación pasará a ser STOPPED. Se creará un nuevo punto de recuperación continua con la configuración de retención modificada.

Amazon Aurora y Amazon RDS

Para los puntos de recuperación de los recursos de Aurora y Amazon RDS, solo puede haber un punto de recuperación cada vez. No se crean nuevos puntos de recuperación cuando se cambia un período de retención; en su lugar, AWS Backup actualiza el punto de recuperación existente con las especificaciones de retención del plan de respaldo.

Asegúrese de configurar el período de retención de estas copias de seguridad de manera que su frecuencia sea superior a la de las copias de seguridad para evitar una situación en la que el punto de recuperación pase al estado EXPIRED.

Tip

Una regla de frecuencia de copia de seguridad para una copia de seguridad continua no es lo mismo que una instantánea de copia de seguridad periódica. Cada plan de copia de seguridad, incluso uno que no cree instantáneas, tiene una frecuencia que establece el usuario (horaria, diaria, semanal o mensual, por ejemplo) con fines de mantenimiento y sincronización.

Eliminación de la única regla de copia de seguridad continua de un plan de copia de seguridad

Al crear un plan de respaldo con una regla de respaldo continuo y, a continuación, eliminar esa regla, AWS Backup recuerda el período de retención de la regla ahora eliminada. Eliminará la copia de seguridad continua de su almacén de copias de seguridad cuando haya transcurrido el periodo de retención.

Creación de copias de seguridad por tipo de recurso

Con él AWS Backup, puede crear copias de seguridad automáticamente mediante planes de copia de seguridad o manualmente iniciando una copia de seguridad bajo demanda.

Creación de copias de seguridad automáticas

Cuando se crean copias de seguridad automáticamente mediante planes de copias de seguridad, se configuran con la configuración del ciclo de vida que se define en el plan de copias de seguridad. Están organizadas en el almacén de copias de seguridad especificado en el plan de copia de seguridad. Además, a estas copias de seguridad se les asignarán las etiquetas que se indiquen en el plan. Para obtener más información sobre los planes de copia de seguridad, consulte [Planes de copia de seguridad](#).

Creación de copias de seguridad bajo demanda

Al crear una copia de seguridad bajo demanda, puede configurar esta configuración para la copia de seguridad que se está creando. Cuando se crea una copia de seguridad de forma automática o manual, se inicia un trabajo de copia de seguridad. Para obtener información sobre cómo crear una copia de seguridad bajo demanda, consulte [Crear una copia de seguridad bajo demanda mediante AWS Backup](#).

Nota: Una copia de seguridad bajo demanda crea un trabajo de copia de seguridad; el trabajo de copia de seguridad cambiará al estado Running en el plazo de una hora (o cuando se especifique). Puede elegir una copia de seguridad bajo demanda si desea crear una copia de seguridad en un momento distinto del momento programado definido en un plan de copia de seguridad. Una copia de seguridad bajo demanda se puede utilizar, por ejemplo, para probar la copia de seguridad y su funcionalidad en cualquier momento.

[Las copias de seguridad bajo demanda](#) no se pueden utilizar con la [point-in-timere restauración \(PITR\)](#), ya que una copia de seguridad bajo demanda conserva los recursos en el estado en que se encontraban cuando se realiza la copia de seguridad, mientras que la PITR utiliza [copias de seguridad continuas](#) que registran los cambios a lo largo de un período de tiempo.

Estados de los trabajos de copia de seguridad

Cada trabajo de copia de seguridad tiene un ID único. Por ejemplo, D48D8717-0C9D-72DF-1F56-14E703BF2345.

Puede ver el estado de un trabajo de copia de seguridad en la página Jobs (Trabajos) de la consola de AWS Backup . Los estados de las tareas de copia de seguridad incluyen CREATED, PENDING, RUNNING, ABORTING, ABORTED, COMPLETED, FAILED, EXPIRED y PARTIAL.

Copias de seguridad incrementales

Muchos recursos permiten realizar copias de seguridad incrementales con AWS Backup. Encontrará una lista completa en la sección de copias de seguridad incrementales de la tabla [Disponibilidad de características por recurso](#).

Si bien cada copia de seguridad posterior a la primera (completa) es incremental (lo que significa que solo captura los cambios de la copia de seguridad anterior), todas las copias de seguridad realizadas con ellas AWS Backup conservan los datos de referencia necesarios para permitir una restauración completa. Esto es así incluso si la copia de seguridad original (completa) ha llegado al final de su ciclo de vida y se ha eliminado.

Por ejemplo, si la copia de seguridad (completa) del día 1 se eliminó debido a una política de ciclo de vida de 3 días, aún podrá realizar una restauración completa con las copias de seguridad de los días 2 y 3. AWS Backup mantiene los datos de referencia necesarios desde el primer día para hacerlo.

Regiones y copias de seguridad incrementales

Las copias de seguridad de los recursos que se administran en su totalidad solo AWS Backup pueden ser incrementales si el almacén en el que se crea la copia de seguridad también contiene una copia de seguridad anterior (incremental o completa); otros tipos de recursos (no gestionados por completo AWS Backup) pueden tener copias de seguridad incrementales siempre que un almacén de la misma región tenga una copia de seguridad anterior.

Acceso a los recursos de origen

AWS Backup necesita acceder a sus recursos de origen para realizar copias de seguridad de los mismos. Por ejemplo:

- Para hacer una copia de seguridad de una EC2 instancia de Amazon, la instancia puede estar en el `stopped` estado `running` o, pero no en el `terminated` estado. Esto se debe a que una `stopped` instancia `running` o se puede comunicar con AWS Backup ella, pero una `terminated` instancia no.

- Para hacer una copia de seguridad de una máquina virtual, su hipervisor debe tener el estado de puerta de enlace de copia de seguridad ONLINE. Para obtener más información, consulte [Descripción del estado del hipervisor](#).
- Para hacer una copia de seguridad de una base de datos de Amazon RDS, Amazon Aurora o un clúster de Amazon DocumentDB, esos recursos deben tener el estado AVAILABLE.
- Para hacer una copia de seguridad de un Amazon Elastic File System (Amazon EFS), debe tener el estado AVAILABLE.
- Para hacer una copia de seguridad de un sistema de FSx archivos de Amazon, debe tener este estado AVAILABLE. Si el estado es UPDATING, la solicitud de copia de seguridad queda en cola hasta que el sistema de archivos pase a estar AVAILABLE.

FSx ya que ONTAP no admite la creación de copias de seguridad de determinados tipos de volúmenes, incluidos los volúmenes DP (protección de datos), los volúmenes LS (carga compartida), los volúmenes completos o los volúmenes de sistemas de archivos que están llenos. Para obtener más información, consulte [ONTAP Cómo trabajar con copias FSx de seguridad](#).

AWS Backup conserva las copias de seguridad creadas anteriormente de acuerdo con su política de ciclo de vida, independientemente del estado del recurso de origen.

Temas

- [CloudFormation apile copias de seguridad](#)
- [Copias de seguridad de Amazon Aurora DSQL](#)
- [Copia de seguridad avanzada de DynamoDB](#)
- [Amazon EBS y AWS Backup](#)
- [Copias de seguridad de Amazon Relational Database Service](#)
- [Copias de seguridad de Amazon Redshift](#)
- [Copias de seguridad de Amazon Redshift sin servidor](#)
- [Copias de seguridad de Amazon EKS](#)
- [Respaldo de SAP HANA en Amazon EC2](#)
- [Copias de seguridad de Amazon S3](#)
- [Copias de seguridad de Amazon Timestream](#)
- [Copias de seguridad de máquinas virtuales](#)
- [Creación de copias de seguridad de Windows VSS](#)

CloudFormation apila copias de seguridad

Una CloudFormation pila consta de varios recursos con y sin estado de los que puede hacer copias de seguridad como una sola unidad. En otras palabras, puede hacer copias de seguridad y restaurar una aplicación que contenga varios recursos al hacer una copia de seguridad de una pila y restaurar los recursos que contiene. Todos los recursos de una pila se definen por la plantilla de CloudFormation de la pila.

Cuando se hace una copia de seguridad de una CloudFormation pila, se crean puntos de recuperación para la CloudFormation plantilla y para cada recurso adicional compatible con AWS Backup la pila. Estos puntos de recuperación se agrupan dentro de un punto de recuperación global denominado compuesto.

Este punto de recuperación compuesto no se puede restaurar, pero los puntos de recuperación anidados sí se pueden restaurar. Puede restaurar desde una hasta todas las copias de seguridad anidadas dentro de una copia de seguridad compuesta mediante la consola o la AWS CLI.

CloudFormation terminología de pila de aplicaciones

- Punto de recuperación compuesto: un punto de recuperación que se utiliza para agrupar puntos de recuperación anidados, así como otros metadatos.
- Punto de recuperación anidado: punto de recuperación de un recurso que forma parte de una CloudFormation pila y del que se hace una copia de seguridad como parte del punto de recuperación compuesto. Cada punto de recuperación anidado pertenece a la pila de un punto de recuperación compuesto.
- Trabajo compuesto: trabajo de respaldo, copia o restauración de una CloudFormation pila que puede activar otros trabajos de respaldo para los recursos individuales de la pila.
- Trabajo anidado: trabajo de respaldo, copia o restauración de un recurso de una CloudFormation pila.

CloudFormation apilar tareas de copia de seguridad

El proceso de creación de una copia de seguridad se denomina trabajo de copia de seguridad. Un trabajo de backup CloudFormation apilado tiene un [estado](#). Cuando un trabajo de copia de seguridad ha finalizado, tiene el estado `Completed`. Esto significa que se ha creado un [CloudFormation punto de recuperación](#) (copia de seguridad).

CloudFormation Se puede hacer una copia de seguridad de las pilas mediante la consola o se puede hacer una copia de seguridad mediante programación. Para hacer una copia de seguridad de cualquier recurso, incluida una CloudFormation pila, consulta [Cómo crear una copia](#) de seguridad en otra parte de esta guía AWS Backup para desarrolladores.

CloudFormation Se puede hacer una copia de seguridad de las pilas mediante el comando `StartBackupJob` de la API. Tenga en cuenta que la documentación y la consola hacen referencia a puntos de recuperación compuestos y anidados; el lenguaje de la API utiliza la terminología “puntos de recuperación principales y secundarios” en la misma relación contextual.

CloudFormation [las pilas contienen todos los AWS recursos indicados en tu plantilla. CloudFormation](#) Tenga en cuenta que es posible que la plantilla contenga recursos que aún no son compatibles con AWS Backup. Si la plantilla contiene una combinación de recursos AWS compatibles y recursos no compatibles, AWS Backup seguirá haciendo una copia de seguridad de la plantilla en una pila compuesta, pero Backup solo creará puntos de recuperación de los servicios compatibles con Backup. Todos los tipos de recursos incluidos en la CloudFormation plantilla se incluirán en la copia de seguridad, incluso si no ha optado por un servicio en particular (cambiando un servicio a «Activado» en la configuración de la consola).

CloudFormation punto de recuperación

Estado del punto de recuperación

Cuando finaliza el trabajo de copia de seguridad de una pila (el estado del trabajo es `Completed`), se ha creado una copia de seguridad de la pila. Esta copia de seguridad también se conoce como punto de recuperación compuesto. Un punto de recuperación compuesto puede tener uno de los siguientes estados: `Completed`, `Failed` o `Partial`. Tenga en cuenta que un trabajo de copia de seguridad tiene un estado, y un punto de recuperación (también denominado copia de seguridad) también tiene un estado diferente.

Un trabajo de respaldo completado significa que toda su pila y los recursos que contiene están protegidos por AWS Backup. Un estado de error indica que el trabajo de copia de seguridad no se realizó correctamente; debe volver a crear la copia de seguridad una vez que se haya corregido el problema que provocó el error.

Un estado `Partial` significa que no se realizó una copia de seguridad de todos los recursos de la pila. Esto puede suceder si la CloudFormation plantilla contiene recursos que actualmente no son compatibles AWS Backup o si uno o más de los trabajos de respaldo que pertenecen a los recursos de la pila (recursos anidados) tienen un estado diferente al de. `Completed` Puede crear

manualmente una copia de seguridad bajo demanda para volver a ejecutar cualquier recurso cuyo estado no sea `Completed`. Si esperaba que la pila tuviera el estado de `Completed`, pero en su lugar aparece marcado como `Partial`, compruebe cuál de las condiciones anteriores podría aplicarse a su pila.

Cada recurso anidado dentro del punto de recuperación compuesto tiene su propio punto de recuperación individual, cada uno con su propio estado (`Completed` o `Failed`). Es posible restaurar los puntos de recuperación anidados con un estado de `Completed`.

Administración de los puntos de recuperación

Los puntos de recuperación compuestos (copias de seguridad) se pueden copiar; los puntos de recuperación anidados se pueden copiar, eliminar, disociar o restaurar. No se puede eliminar un punto de recuperación compuesto que contenga copias de seguridad anidadas. Una vez eliminados o disociados los puntos de recuperación anidados dentro de un punto de recuperación compuesto, puede eliminar manualmente el punto de recuperación compuesto o dejar que permanezca hasta que se elimine durante el ciclo de vida del plan de copia de seguridad.

Eliminación de un punto de recuperación

Puede eliminar un punto de recuperación mediante la AWS Backup consola o mediante el AWS CLI

Para eliminar puntos de recuperación mediante la AWS Backup consola,

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. Haga clic en Recursos protegidos en el menú de navegación de la izquierda. En el cuadro de texto, escriba `CloudFormation` para que se muestren solo las CloudFormation pilas.
3. Los puntos de recuperación compuestos se mostrarán en el panel Puntos de recuperación. Puede hacer clic en el signo más (+) situado a la izquierda del identificador de cada punto de recuperación para ampliar cada punto de recuperación compuesto y mostrar todos los puntos de recuperación anidados que contiene el compuesto. Puede marcar la casilla situada a la izquierda de cualquier punto de recuperación para incluirlo en la selección de puntos de recuperación que desee eliminar.
4. Haga clic en el botón Eliminar.

Si utiliza la consola para eliminar uno o más puntos de recuperación compuestos, aparecerá un cuadro de advertencia. Este cuadro de advertencia requiere que confirme su intención de eliminar los puntos de recuperación compuestos, incluidos los puntos de recuperación anidados dentro de las pilas compuestas.

Para eliminar puntos de recuperación mediante la API, use el comando `DeleteRecoveryPoint`.

Si utilizas la API con la, AWS Command Line Interface debes eliminar todos los puntos de recuperación anidados antes de eliminar un punto compuesto. Si envía una solicitud a la API para eliminar una copia de seguridad de pila compuesta (punto de recuperación) que aún contiene puntos de recuperación anidados, la solicitud devolverá un error.

Disociación de un punto de recuperación anidado del punto de recuperación compuesto

Puede disociar un punto de recuperación anidado de un punto de recuperación compuesto (por ejemplo, desea conservar el punto de recuperación anidado pero eliminar el punto de recuperación compuesto). Ambos puntos de recuperación permanecerán, pero dejarán de estar conectados; es decir, las acciones que se realicen en el punto de recuperación compuesto dejarán de aplicarse al punto de recuperación anidado una vez que se haya disociado.

Puede disociar el punto de recuperación mediante la consola o puede llamar a la API `DisassociateRecoveryPointFromParent`. [Tenga en cuenta que las llamadas a la API utilizan el término “principal” para referirse a los puntos de recuperación compuestos].

Copia de un punto de recuperación

Puede copiar un punto de recuperación compuesto o puede copiar un punto de recuperación anidado si el recurso admite la [copia entre cuentas y regiones](#).

Para copiar los puntos de recuperación mediante la AWS Backup consola:

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. Haga clic en Recursos protegidos en el menú de navegación de la izquierda. En el cuadro de texto, escriba `CloudFormation` para que se muestren solo las CloudFormation pilas.
3. Los puntos de recuperación compuestos se mostrarán en el panel Puntos de recuperación. Puede hacer clic en el signo más (+) situado a la izquierda del identificador de cada punto de recuperación para ampliar cada punto de recuperación compuesto y mostrar todos los puntos de recuperación anidados que contiene el compuesto. Puede hacer clic en el botón circular de opción situado a la izquierda de cualquier punto de recuperación para copiarlo.
4. Una vez seleccionado, haga clic en el botón Copiar de la esquina superior derecha del panel.

Al copiar un punto de recuperación compuesto, los puntos de recuperación anidados que no admiten la función de copia no se incluirán en la pila copiada. El punto de recuperación compuesto tendrá un estado de `Partial`.

Preguntas frecuentes

1. “¿Qué se incluye como parte de la copia de seguridad de la aplicación?”

Como parte de cada copia de seguridad de una aplicación definida mediante `CloudFormation`, se hace una copia de seguridad de la plantilla, del valor procesado de cada parámetro de la plantilla y de los recursos anidados AWS Backup compatibles con ella. Se hace una copia de seguridad de un recurso anidado de la misma manera que se hace una copia de seguridad de un recurso individual que no forma parte de una `CloudFormation` pila. Tenga en cuenta que no se realizará una copia de seguridad de los valores de los parámetros marcados como `no-echo`.

2. «¿Puedo hacer una copia de seguridad de mi `CloudFormation` pila que tiene pilas anidadas?»

Sí. Las `CloudFormation` pilas que contienen pilas anidadas pueden estar en la copia de seguridad.

3. “¿Un estado *Partial* significa que se ha producido un error al crear mi copia de seguridad?”

No. Un estado parcial indica que se realizó una copia de seguridad de algunos puntos de recuperación, pero no de otros. Hay tres condiciones que debe comprobar si esperaba un resultado `Completed` de la copia de seguridad:

- ¿Su `CloudFormation` pila contiene recursos que actualmente no son compatibles? AWS Backup
Para ver una lista de los recursos compatibles, consulta los [AWS recursos compatibles y las aplicaciones de terceros](#) en nuestra Guía para desarrolladores.
- Uno o más de los trabajos de copia de seguridad pertenecientes a recursos de la pila no se ha realizado correctamente y hay que volver a ejecutarlo.
- Se eliminó o disoció un punto de recuperación anidado del punto de recuperación compuesto.

4. «¿Cómo excluyo los recursos de la copia de seguridad de mi `CloudFormation` pila?»

Al hacer una copia de seguridad de la `CloudFormation` pila, puede excluir los recursos para que no formen parte de la copia de seguridad. En la consola, durante los procesos de [creación de un plan de copia de seguridad](#) y [actualización de un plan de copia de seguridad](#), hay un paso de [asignación de recursos](#). En este paso, hay una sección de Selección de recurso. Si eliges incluir tipos de recursos específicos y los has incluido `CloudFormation` como recurso para realizar una copia de seguridad, puedes excluir un recurso específico IDs de los tipos de recursos seleccionados. También puede utilizar etiquetas para excluir recursos de la pila.

Mediante la CLI, puede utilizar

- `NotResources` en tu plan de respaldo para excluir un recurso específico de tus CloudFormation pilas.
- `StringNotLike` para excluir elementos mediante etiquetas.

5. “¿Qué tipos de copias de seguridad son compatibles con los recursos anidados?”

Las copias de seguridad de los recursos anidados pueden ser copias de seguridad completas o incrementales, según el tipo de copia de seguridad que admitan AWS Backup estos recursos. Para obtener más información, consulte [Funcionamiento de las copias de seguridad incrementales](#). Sin embargo, tenga en cuenta que los recursos anidados de Amazon S3 y Amazon RDS [no admiten](#) PITR (point-in-time restauración).

6. «¿Se hace una copia de seguridad de los conjuntos de cambios que forman parte de la CloudFormation pila?»

No. Los conjuntos de cambios no se respaldan como parte de la copia de seguridad de la CloudFormation pila.

7. «¿Cómo afecta el estado de la CloudFormation pila a la copia de seguridad?»

El estado de la CloudFormation pila puede afectar a la copia de seguridad. Se puede hacer una copia de seguridad de una pila con un estado que incluya `COMPLETE`, como los estados `CREATE_COMPLETE`, `ROLLBACK_COMPLETE`, `UPDATE_COMPLETE`, `UPDATE_ROLLBACK_COMPLETE`, `IMPORT_COMPLETE` o `IMPORT_ROLLBACK_COMPLETE`.

En caso de que se produzca un error al cargar una plantilla nueva y la pila pase al estado `ROLLBACK_COMPLETE`, se realizará una copia de seguridad de la nueva plantilla, pero las copias de seguridad de los recursos anidados se basarán en los recursos revertidos.

8. “¿En qué se diferencian los ciclos de vida de las pilas de aplicaciones de los ciclos de vida de otros puntos de recuperación?”

Los ciclos de vida de los puntos de recuperación anidados vienen determinados por el plan de copia de seguridad al que pertenecen. El punto de recuperación compuesto está determinado por el ciclo de vida más largo de todos los puntos de recuperación anidados. Cuando el último punto de recuperación anidado restante dentro de un punto de recuperación compuesto se elimina o se disocia, también se eliminará el punto de recuperación compuesto.

9. «¿Cómo se CloudFormation copian las etiquetas de un objeto a los puntos de recuperación?»

Sí. Esas etiquetas se copiarán en cada punto de recuperación anidado respectivo.

10. «¿Hay un orden para eliminar puntos de recuperación compuestos y anidados (copias de seguridad)?»

Sí. Algunas copias de seguridad se deben eliminar antes de poder eliminar otras. Las copias de seguridad compuestas que contienen puntos de recuperación anidados no se pueden eliminar hasta que se hayan eliminado todos los puntos de recuperación del compuesto. Una vez que un punto de recuperación compuesto ya no contiene puntos de recuperación anidados, puede eliminarlo manualmente. De lo contrario, se eliminará de acuerdo con el ciclo de vida de su plan de copia de seguridad.

Restauración de aplicaciones dentro de una pila

Consulte [Cómo restaurar copias de seguridad de pilas de aplicaciones](#) para obtener información sobre la restauración de puntos de recuperación anidados.

Copias de seguridad de Amazon Aurora DSQL

Puede utilizarlos AWS Backup para crear copias de seguridad de sus clústeres de una o varias regiones de Amazon Aurora DSQL. Las copias de seguridad de los clústeres de Amazon Aurora DSQL siempre son copias de seguridad completas.

Para crear las copias de seguridad de los clústeres de Amazon Aurora DSQL se utiliza el proceso de creación de copias de seguridad estándar. Para obtener más información, consulte los siguientes temas:

- [Crear una copia de seguridad bajo demanda mediante AWS Backup](#)
- [Creación de plan de copia de seguridad](#)

AWS Backup Para crear copias de seguridad de sus clústeres DSQL de Amazon Aurora, debe habilitar la protección para Aurora DSQL. Para obtener más información, consulte [Suscripción al servicio](#).

Cuando haga una copia de seguridad de un clúster multirregional, tenga en cuenta lo siguiente:

- Una copia de seguridad de un clúster multirregional requiere una copia de seguridad independiente para cada región del clúster; una copia de seguridad en una región no crea ningún punto de recuperación para todas las regiones de un clúster multirregional.
- Como práctica recomendada, se AWS Backup recomienda crear un punto de recuperación en una región y copiarlo en otra región relacionada. Para la [restauración multirregional](#), necesita un punto de recuperación en una región compatible y una copia de ese punto de recuperación en otra región dentro del mismo trío de regiones.

Se admiten los siguientes tríos. Si hay más regiones, elija tres del mismo grupo.

- Este de EE. UU. (Norte de Virginia); Este de EE. UU. (Ohio); Oeste de EE. UU. (Norte de California)
- Europa (Irlanda); Europa (Londres); Europa (París); Europa (Fráncfort)
- Asia-Pacífico (Tokio); Asia-Pacífico (Seúl); Asia-Pacífico (Osaka)

AWS Backup recomienda añadir la regla de copia de seguridad al plan de copia de seguridad. Si no añade la regla de copia al plan de copia de seguridad, debe copiar manualmente la copia de seguridad en la región requerida en la que vaya a realizar la restauración, lo que aumentará el Objetivo de tiempo de recuperación (RTO).

Para obtener más información sobre la restauración de un punto de recuperación (copia de seguridad) de Aurora DSQL, consulte [Restauración de Amazon Aurora DSQL](#).

Copia de seguridad avanzada de DynamoDB

AWS Backup admite funciones adicionales y avanzadas para sus necesidades de protección de datos en Amazon DynamoDB.

Los clientes que comenzaron a usarlo AWS Backup después de noviembre de 2021 tienen habilitadas de forma predeterminada las funciones de copia de seguridad avanzadas de DynamoDB. En concreto, las características avanzadas de copia de seguridad de DynamoDB están habilitadas de forma predeterminada para los clientes que no hayan creado un almacén de copias de seguridad antes del 21 de noviembre de 2021.

Se recomienda que AWS Backup los clientes actuales habiliten las funciones avanzadas de DynamoDB. Después de activar las características avanzadas, no hay diferencia en los precios del almacenamiento de copias de seguridad en caliente. Puede ahorrar dinero al mover las copias de seguridad en niveles para almacenarlas en frío y optimizar sus costos mediante el uso de etiquetas

de asignación de costos. También puede empezar a aprovechar las funciones AWS Backup de copia y seguridad para distintas regiones y cuentas.

Temas

- [Ventajas de la copia de seguridad avanzada de DDB](#)
- [Consideraciones sobre la copia de seguridad avanzada de DynamoDB](#)
- [Habilitación de copias de seguridad avanzadas de DynamoDB mediante la consola](#)
- [Habilitación de copias de seguridad avanzadas de DynamoDB mediante programación](#)
- [Edición de una copia de seguridad avanzada de DynamoDB](#)
- [Restauración de una copia de seguridad avanzada de DynamoDB](#)
- [Eliminación de una copia de seguridad avanzada de DynamoDB](#)
- [Otros beneficios de la administración completa de AWS Backup cuando se habilita la copia de seguridad avanzada de DynamoDB](#)

Ventajas de la copia de seguridad avanzada de DDB

Después AWS Backup de habilitar las funciones avanzadas en su Región de AWS, desbloqueará las siguientes funciones para todas las copias de seguridad de tablas de DynamoDB nuevas que cree:

- Ahorro de costos y optimización:
 - [Organizar las copias de seguridad en niveles para almacenarlas en frío](#) para reducir los costos de almacenamiento
 - [Etiquetado de asignación de costos para su uso con Cost Explorer](#)
- Opciones de copia adicionales:
 - [Copia entre regiones](#)
 - [Copia entre cuentas](#)
- Seguridad:
 - Las copias de seguridad heredan las etiquetas de sus tablas de DynamoDB de origen, lo que le permite utilizarlas para establecer políticas de control de [servicios y](#) permisos (). SCPs

Consideraciones sobre la copia de seguridad avanzada de DynamoDB

Activar

Las copias de seguridad, incluidas las de los recursos de DDB avanzado, se pueden crear mediante un plan de copias de seguridad, una copia de seguridad a pedido o mediante una política de copias de seguridad. Las copias de seguridad creadas mediante un plan o bajo demanda se incorporarán automáticamente a su cuenta para permitir las copias de seguridad de los recursos de DDB avanzada.

Si su trabajo de copia de seguridad lo crea una política de copias de seguridad, debe optar manualmente por las copias de seguridad avanzadas de DynamoDB, ya sea a través de la [consola de Backup](#) o mediante la [CLI](#).

Políticas y funciones personalizadas

Si usa un rol o una política personalizados en lugar AWS Backup del rol de servicio predeterminado, debe agregar o usar las siguientes políticas de permisos (o agregar sus permisos equivalentes) a su rol personalizado:

- `AWSBackupServiceRolePolicyForBackup` para realizar copias de seguridad avanzadas de DynamoDB.
- `AWSBackupServiceRolePolicyForRestores` para restaurar copias de seguridad avanzadas de DynamoDB.

Para obtener más información sobre las políticas AWS administradas y ver ejemplos de políticas administradas por el cliente, consulte. [Políticas administradas para AWS Backup](#)

Habilitación de copias de seguridad avanzadas de DynamoDB mediante la consola

Puede activar las funciones AWS Backup avanzadas para las copias de seguridad de DynamoDB mediante la consola AWS Backup o la consola de DynamoDB.

Para activar las funciones avanzadas de copia de seguridad de DynamoDB desde la consola: AWS Backup

1. [Abra la AWS Backup consola en /backup. https://console.aws.amazon.com](https://console.aws.amazon.com/backup)
2. En el menú de navegación izquierdo, elija Configuración.
3. En la sección Servicios admitidos, compruebe que DynamoDB esté Habilitado.

Si no es así, elija Activación y habilite DynamoDB como servicio admitido por AWS Backup .

4. En la sección Características avanzadas para copias de seguridad de DynamoDB, elija Habilitar.
5. Elija Enable features (Habilitar características).

Para obtener información sobre cómo habilitar las funciones AWS Backup avanzadas mediante la consola de DynamoDB, [consulte AWS Backup Habilitación](#) de funciones en la Guía del usuario de Amazon DynamoDB.

Habilitación de copias de seguridad avanzadas de DynamoDB mediante programación

También puede activar las funciones AWS Backup avanzadas para las copias de seguridad de DynamoDB mediante la AWS Command Line Interface (CLI). Para habilitar las copias de seguridad avanzadas de DynamoDB, debe establecer los dos valores siguientes en `true`:

Para habilitar mediante programación las funciones AWS Backup avanzadas de las copias de seguridad de DynamoDB:

1. Compruebe si ya ha activado las funciones AWS Backup avanzadas de DynamoDB mediante el siguiente comando:

```
$ aws backup describe-region-settings
```

Si `"DynamoDB":true` en `"ResourceTypeManagementPreference"` y `"ResourceTypeOptInPreference"`, ya ha habilitado la copia de seguridad avanzada de DynamoDB.

Si, como en el siguiente resultado, tiene al menos una instancia de `"DynamoDB":false`, aún no ha habilitado la copia de seguridad avanzada de DynamoDB. Continúe con el siguiente paso.

```
{
  "ResourceTypeManagementPreference":{
    "DynamoDB":false,
    "EFS":true
  }
  "ResourceTypeOptInPreference":{
    "Aurora":true,
    "DocumentDB":false,
    "DynamoDB":false,
    "EBS":true,
    "EC2":true,
    "EFS":true,
    "FSx":true,
    "Neptune":false,
    "RDS":true,
    "Storage Gateway":true
  }
}
```

```
}  
}
```

2. Utilice la siguiente operación [UpdateRegionSettings](#) para configurar "ResourceTypeManagementPreference" y "ResourceTypeOptInPreference" en "DynamoDB":true:

```
aws backup update-region-settings \  
    --resource-type-opt-in-preference DynamoDB=true \  
    --resource-type-management-preference DynamoDB=true
```

Edición de una copia de seguridad avanzada de DynamoDB

Al crear una copia de seguridad de DynamoDB después de AWS Backup activar las funciones avanzadas, puede utilizarla para: AWS Backup

- Copiar una copia de seguridad entre regiones
- Copiar una copia de seguridad entre cuentas
- Cambia el momento en el que se AWS Backup coloca una copia de seguridad en almacenamiento en frío
- Etiquetar la copia de seguridad

Para usar esas características avanzadas en una copia de seguridad existente, consulte [Edición de una copia de seguridad](#).

Si más adelante deshabilita las funciones AWS Backup avanzadas de DynamoDB, podrá seguir realizando esas operaciones en las copias de seguridad de DynamoDB que haya creado durante el período en que activó las funciones avanzadas.

Restauración de una copia de seguridad avanzada de DynamoDB

Puede restaurar las copias de seguridad de DynamoDB realizadas AWS Backup con las funciones avanzadas habilitadas del mismo modo que restaura las copias de seguridad de DynamoDB realizadas antes de activar las funciones avanzadas. AWS Backup Puede realizar una restauración mediante DynamoDB AWS Backup o DynamoDB.

Puede especificar cómo cifrar la tabla recién restaurada con las siguientes opciones:

- Al restaurar en la misma región que la tabla original, si lo desea, puede especificar una clave de cifrado para la tabla restaurada. Si no especifica una clave de cifrado, AWS Backup cifrará automáticamente la tabla restaurada con la misma clave que cifró la tabla original.
- Al restaurar en una región diferente a la de la tabla original, debe especificar una clave de cifrado.

Para restaurar mediante AWS Backup, consulte [Restauración de una tabla de Amazon DynamoDB](#).

Para restaurar con DynamoDB, consulte [Restoring a DynamoDB table from a backup](#) en la Guía del usuario de Amazon DynamoDB.

Eliminación de una copia de seguridad avanzada de DynamoDB

No puede eliminar las copias de seguridad creadas mediante estas características avanzadas de DynamoDB. Debe utilizar AWS Backup para eliminar las copias de seguridad a fin de mantener la coherencia global en todo su entorno de AWS .

Para eliminar una copia de seguridad de DynamoDB, consulte [Eliminaciones de las copias de seguridad](#).

Otros beneficios de la administración completa de AWS Backup cuando se habilita la copia de seguridad avanzada de DynamoDB

Al habilitar las funciones AWS Backup avanzadas de DynamoDB, proporciona una administración completa de las copias de seguridad de DynamoDB a. AWS Backup Al hacer esto, obtendrá los siguientes beneficios adicionales:

Cifrado

AWS Backup cifra automáticamente las copias de seguridad con la clave KMS del almacén de destino. AWS Backup Antes, se cifraban con el mismo método de cifrado que la tabla de DynamoDB de origen. Esto aumenta el número de defensas que puede utilizar para proteger sus datos. Para obtener más información, consulte [Cifrado de copias de seguridad en AWS Backup](#).

Nombre de recurso de Amazon (ARN)

El espacio de nombres de servicio de cada ARN de copia de seguridad es awsbackup. Antes, el espacio de nombres de servicio era dynamodb. Dicho de otro modo, el principio de cada ARN cambiará de `arn:aws:dynamodb` a `arn:aws:backup`. Consulte AWS Backup en [ARNs la](#) Referencia de autorización de servicio.

Con este cambio, usted o su administrador de copias de seguridad pueden crear políticas de acceso para las copias de seguridad mediante el espacio de nombres de servicio awsbackup que ahora se aplica a las copias de seguridad de DynamoDB creadas después de activar las características avanzadas. Al utilizar el espacio de nombres de servicio awsbackup, también puede aplicar políticas a otras copias de seguridad realizadas por AWS Backup. Para obtener más información, consulte [Control de acceso](#).

Ubicación de los cargos en el extracto de facturación

Los cargos por copias de seguridad (incluidos el almacenamiento, las transferencias de datos, las restauraciones y la eliminación anticipada) aparecen en la sección «Respaldo» de tu AWS factura. Antes, los cargos aparecían en la sección “DynamoDB” de la factura.

Este cambio garantiza que puedas utilizar la AWS Backup facturación para supervisar de forma centralizada los costes de las copias de seguridad. Para obtener más información, consulte [Medición, costos y facturación de AWS Backup](#).

Amazon EBS y AWS Backup

El proceso de copia de seguridad de los recursos de Amazon EBS es similar a los pasos que se utilizan para realizar copias de seguridad de otros tipos de recursos:

- [Creación de una copia de seguridad bajo demanda](#)
- [Creación de una copia de seguridad programada](#)

En las siguientes secciones se indica información específica de recursos.

Nivel de archivo de Amazon EBS para almacenamiento en frío

EBS es uno de los recursos que admiten la transición de copias de seguridad a almacenamiento en frío. Para obtener más información, consulte [Ciclo de vida y niveles de almacenamiento](#).

Copias de seguridad de varios volúmenes de Amazon EBS y coherentes ante bloqueos

De forma predeterminada, AWS Backup crea copias de seguridad coherentes con los bloqueos de los volúmenes de Amazon EBS que están adjuntos a una instancia de Amazon EC2. La coherencia de los fallos significa que las instantáneas de cada volumen de Amazon EBS adjunto a la misma EC2 instancia de Amazon se toman exactamente en el mismo momento. Ya no tiene que detener

sus instancias ni coordinar varios volúmenes de Amazon EBS para garantizar que el estado de su aplicación sea coherente ante bloqueos.

Dado que las instantáneas de varios volúmenes consistentes en los bloqueos son una AWS Backup funcionalidad predeterminada, no necesita hacer nada diferente para usar esta función.

EL rol utilizado para crear un punto de recuperación de instantáneas de EBS está asociada a esa instantánea. Este mismo rol debe usarse para eliminar los puntos de recuperación que haya creado o para hacer la transición de los puntos de recuperación de la misma a un nivel de archivo.

Amazon EBS Snapshot Lock y AWS Backup

AWS Backup Las instantáneas de Amazon EBS gestionadas y las instantáneas asociadas a una EC2 AMI de AWS Backup Amazon gestionada que tengan aplicado el bloqueo de instantáneas de Amazon EBS no se pueden eliminar como parte del ciclo de vida del punto de recuperación si la duración del bloqueo de instantáneas supera el ciclo de vida de la copia de seguridad. Por el contrario, estos puntos de recuperación tendrán el estado de EXPIRED. Estos puntos de recuperación se pueden [eliminar manualmente](#) si decide eliminar primero el bloqueo de instantáneas de Amazon EBS.

Restauración de recursos de Amazon EBS

Para restaurar los volúmenes de Amazon EBS, siga los pasos que se indican en [Restauración de un volumen de Amazon EBS](#).

Copias de seguridad de Amazon Relational Database Service

Amazon RDS y AWS Backup

Cuando considere las opciones para realizar copias de seguridad de sus instancias y clústeres de Amazon RDS, es importante que aclare qué tipo de copia de seguridad desea crear y utilizar. Varios recursos de AWS , incluido Amazon RDS, ofrecen sus propias soluciones de copia de seguridad nativas.

Amazon RDS ofrece la opción de realizar [copias de seguridad automáticas](#) y [copias de seguridad manuales](#). En la terminología de Amazon RDS, todos los puntos de recuperación creados por AWS Backup, incluidos los de un plan de respaldo, se consideran copias de seguridad manuales.

Cuando [crea una copia de seguridad](#) (punto de recuperación) de una instancia de Amazon RDS, AWS Backup comprueba si ha utilizado anteriormente Amazon RDS para crear una copia de

seguridad automática. AWS Backup Si existe una copia de seguridad automática, AWS Backup crea una copia instantánea incremental (copy-db-snapshotoperación). Si no existe ninguna copia de seguridad, AWS Backup crea una instantánea de la instancia que usted indique, en lugar de una copia (create-db-snapshotoperación).

La primera instantánea creada por AWS Backup cualquiera de las dos operaciones dará como resultado una instantánea completa. Todas las copias subsiguientes serán copias de seguridad incrementales, siempre que exista la copia de seguridad completa.

Important

Cuando un plan de AWS Backup backup está programado para crear varias instantáneas diarias de una instancia de Amazon RDS y cuando una de esas ventanas programadas de Start Backup coincide con la [ventana Amazon RDS AWS Backup Backup](#), el linaje de datos de las copias de seguridad puede ramificarse en copias de seguridad no idénticas, lo que crea copias de seguridad no planificadas y conflictivas. Para evitarlo, asegúrese de que su plan AWS Backup de respaldo o la ventana de Amazon RDS no coincidan en sus horarios.

Consideraciones

Actualmente, RDS Custom para SQL Server y RDS Custom para Oracle no son compatibles con AWS Backup.

AWS Backup no admite la copia de seguridad y la restauración de RDS en Outposts.

Copias de seguridad continuas y restauraciones en un momento dado (PITR) de Amazon RDS

Las copias de seguridad continuas implican AWS Backup crear una copia de seguridad completa de su recurso de Amazon RDS y, a continuación, capturar todos los cambios en un registro de transacciones. Puede lograr una mayor granularidad si retrocede hasta el punto en el que desea realizar la restauración, en lugar de elegir una instantánea anterior tomada en intervalos de tiempo fijos.

Consulte las [copias de seguridad continuas y los servicios compatibles con el PITR](#) y la [administración de la configuración de las copias de seguridad continuas](#) para obtener más información.

Copias de seguridad en varias zonas de disponibilidad de Amazon RDS

AWS Backup realiza copias de seguridad y es compatible con las opciones de implementación Multi-AZ (zona de disponibilidad) de Amazon RDS for MySQL y PostgreSQL con una instancia de base de datos principal y dos en espera legibles.

Las copias de seguridad en varias zonas de disponibilidad están disponibles en las siguientes regiones: Asia-Pacífico (Sídney), Asia-Pacífico (Tokio), Europa (Irlanda), Este de EE. UU. (Ohio), Oeste de EE. UU. (Oregón), Europa (Estocolmo), Asia-Pacífico (Singapur), Este de EE. UU. (Norte de Virginia) y Europa (Fráncfort).

La opción de implementación Multi-AZ optimiza las transacciones de escritura y es ideal cuando las cargas de trabajo requieren capacidad de lectura adicional, menor latencia de las transacciones de escritura, mayor resiliencia ante la inestabilidad de la red (que afecta a la coherencia de la latencia de las transacciones de escritura) y alta disponibilidad y durabilidad.

Para crear un clúster Multi-AZ, puede elegir MySQL o PostgreSQL como tipo de motor.

En la AWS Backup consola, hay tres opciones de implementación:

- Clúster de base de datos Multi-AZ: crea un clúster de base de datos con una instancia de base de datos principal y dos instancias de base de datos en espera legibles, cada una de las cuales se encuentra en una zona de disponibilidad diferente. Proporciona alta disponibilidad y redundancia de datos y aumenta la capacidad para cargas de trabajo preparadas para el servidor.
- Clúster de base de datos Multi-AZ: crea una instancia de base de datos principal y una instancia de base de datos en espera en una zona de disponibilidad diferente. Esto proporciona alta disponibilidad y redundancia de datos, pero la instancia de base de datos en espera no admite conexiones para cargas de trabajo de lectura.
- Instancia de base de datos única: crea una instancia de base de datos única sin ninguna instancia de base de datos en espera.

Comportamiento de la copia de seguridad con instancias y clústeres

- [Point-in-TimeLa recuperación](#) (PITR) puede admitir instancias, pero no clústeres.
- No se admite la copia de una instantánea de un clúster de base de datos Multi-AZ.
- El Nombre de recurso de Amazon (ARN) de un punto de recuperación de RDS depende de si se utiliza una instancia o un clúster:

Un ARN de instancia de RDS: `arn:aws:rds:region:account:db:name`

Un clúster de varias zonas de disponibilidad de RDS:

`arn:aws:rds:region:account:cluster:name`

Para obtener más información, consulte [Implementaciones de clústeres de base de datos Multi-AZ](#) en la Guía del usuario de Amazon RDS.

Para obtener más información, sobre la [Creación de una instantánea de un clúster de base de datos Multi-AZ](#) en la Guía del usuario de Amazon RDS.

Copias de seguridad de Amazon Redshift

Amazon Redshift es un almacenamiento de datos en la nube escalable y completamente administrado que acelera el tiempo necesario para obtener información mediante análisis rápidos, fáciles y seguros. Puede utilizarla AWS Backup para proteger sus almacenes de datos con copias de seguridad inmutables, políticas de acceso independientes y una gestión organizativa centralizada de las tareas de copia de seguridad y restauración.

Un almacén de datos de Amazon Redshift es un conjunto de recursos informáticos denominados nodos, que se organizan en un grupo denominado clúster. AWS Backup puede hacer copias de seguridad de estos clústeres.

Para obtener información sobre [Amazon Redshift](#), consulte la [Guía de introducción de Amazon Redshift](#), la [Guía para desarrolladores de bases de datos de Amazon Redshift](#) y la [Guía de administración de clústeres de Amazon Redshift](#).

Copia de seguridad de clústeres aprovisionados de Amazon Redshift

Puede proteger sus clústeres de Amazon Redshift mediante la AWS Backup consola o mediante programación mediante API o CLI. Se pueden hacer copias de seguridad de estos clústeres de forma periódica como parte de un plan de copia de seguridad. También se pueden realizar copias de seguridad según sea necesario mediante copias de seguridad bajo demanda.

Puede restaurar una sola tabla (lo que también se conoce como restauración a nivel de elemento) o un clúster completo. Tenga en cuenta que no se pueden hacer copias de seguridad de las tablas por sí mismas; se hacen copias de seguridad de las tablas como parte de un clúster cuando se hace una copia de seguridad del clúster.

AWS Backup El uso le permite ver sus recursos de forma centralizada; sin embargo, si Amazon Redshift es el único recurso que utiliza, puede seguir utilizando el programador automático de instantáneas de Amazon Redshift. Tenga en cuenta que no podrá seguir gestionando la configuración manual de las instantáneas con Amazon Redshift si decide gestionarla a través de AWS Backup.

Puede hacer copias de seguridad de los clústeres de Amazon Redshift a través de la AWS Backup consola o mediante AWS CLI.

Hay dos formas de utilizar la AWS Backup consola para hacer copias de seguridad de un clúster de Amazon Redshift: a pedido o como parte de un plan de copias de seguridad.

Creación de copias de seguridad de Amazon Redshift bajo demanda

Consulte la página [Creación de una copia de seguridad bajo demanda](#) para obtener más información.

Para crear una instantánea manual, deje sin marcar la casilla de verificación de copia de seguridad continua cuando cree un plan de copia de seguridad que incluya recursos de Amazon Redshift.

Creación de copias de seguridad programadas de Amazon Redshift en un plan de copia de seguridad

Las copias de seguridad programadas pueden incluir clústeres de Amazon Redshift si son un recurso protegido. Para optar por la protección de los clústeres de Amazon Redshift:

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, elija Recursos protegidos.
3. Mueva a la posición de activación el conmutador de Amazon Redshift.
4. Consulte [Asignación de recursos mediante la consola](#) para incluir los clústeres de Amazon Redshift en un plan nuevo o existente.

En Administrar planes de copia de seguridad, puede elegir [crear un plan de copia de seguridad](#) e incluir clústeres de Amazon Redshift o [actualizar uno existente](#) para que incluya clústeres de Amazon Redshift. Al añadir el tipo de recurso Amazon Redshift, puede optar por añadir Todos los clústeres de Amazon Redshift o marcar las casillas situadas junto a los clústeres que quiere incluir en su plan de copia de seguridad.

Copia de seguridad mediante programación

También puede definir su plan de copia de seguridad en un documento JSON y proporcionarlo mediante la consola de AWS Backup o la AWS CLI. Consulte [Crear planes de respaldo mediante un documento JSON y la AWS Backup CLI](#) para obtener información sobre cómo crear un plan de respaldo mediante programación.

Puede realizar las siguientes operaciones mediante la API:

- Iniciar un trabajo de copia de seguridad
- Describir un trabajo de copia de seguridad
- Obtener los metadatos de los puntos de recuperación

Note

`BackupSizeInBytes` Los metadatos son compatibles con los siguientes tipos de recursos: volúmenes de Amazon EBS, sistemas de archivos Amazon EFS, bases de datos de Amazon RDS, tablas de DynamoDB, EC2 instancias de Amazon, sistemas de archivos de Amazon y buckets de FSx Amazon S3. Este campo proporciona el tamaño de la copia de seguridad en bytes y está disponible a través de la API `DescribeRecoveryPoint` y de la consola de AWS Backup . En el caso de los tipos de recurso no compatibles, este campo no se rellenará.

- Enumerar los puntos de recuperación por recursos
- Enumerar las etiquetas para el punto de recuperación

Visualización de copias de seguridad de los clústeres de Amazon Redshift

Para ver y modificar las copias de seguridad de las tablas de Amazon Redshift en la consola:

1. [Abra la consola en /backup. AWS Backup https://console.aws.amazon.com](https://console.aws.amazon.com/backup/)
2. Elija Almacenes de Backup. A continuación, haga clic en el nombre del almacén de copias de seguridad que contiene los clústeres de Amazon Redshift.
3. El almacén de copias de seguridad mostrará un resumen y una lista de copias de seguridad. Puede hacer clic en el enlace de la columna ID de punto de recuperación.
4. Para eliminar uno o más puntos de recuperación, marque las casillas que desea eliminar. En el botón Acciones, puede seleccionar Eliminar.

Restauración de un clúster de Amazon Redshift

Para obtener más información, consulte [Restauración de un clúster de Amazon Redshift](#).

Copias de seguridad de Amazon Redshift sin servidor

Descripción general de

AWS Backup ofrece una gestión completa de las copias de seguridad de los espacios de nombres de Amazon Redshift Serverless. De este AWS Backup modo, puede programar y restaurar las instantáneas manuales de Redshift Serverless a través de la consola o mediante la CLI.

La protección de datos sin servidor de Redshift AWS Backup ofrece varias opciones para realizar copias de seguridad y restaurar sus almacenes de datos. Puede crear una instantánea programada o bajo demanda de su espacio de nombres. A continuación, puede optar por restaurar todas las bases de datos de esa instantánea en un clúster aprovisionado por Amazon Redshift o en un espacio de nombres sin servidor. Como alternativa, puede restaurar una sola tabla.

Redshift sin servidor ofrece instantáneas automáticas y manuales. Actualmente, AWS Backup puede utilizarse para administrar instantáneas manuales, pero no las automáticas.

Opciones de copia de seguridad para Redshift sin servidor

Puede usar la AWS Backup consola o la CLI para crear copias de seguridad a pedido o como parte de un plan de copias de seguridad.

Creación de copias de seguridad bajo demanda

Puede crear copias de seguridad bajo demanda de los espacios de nombres de Redshift sin servidor mediante los siguientes pasos:

Console

1. Abra la [consola de AWS Backup](#).
2. En el panel, elija Create an on-demand backup (Crear una copia de seguridad bajo demanda).
3. Elija Redshift sin servidor en el menú desplegable de tipos de recursos.
4. Seleccione el espacio de nombres del que desea hacer una copia de seguridad.
5. Asegúrese de que la opción Crear copia de seguridad ahora esté seleccionada.

6. Especifique el periodo de retención para la copia de seguridad.
7. Elija una copia de seguridad existente o cree una nueva.
8. Seleccione el rol de IAM que desee utilizar en la copia de seguridad.
9. De manera opcional, añada etiquetas a la copia de seguridad. Para asignar una etiqueta a su copia de seguridad bajo demanda, expanda Etiquetas agregadas a los puntos de recuperación, elija Agregar etiqueta nueva e ingrese una clave y un valor de etiqueta.
10. Seleccione Crear copia de seguridad bajo demanda para comenzar el trabajo de copia de seguridad.
11. Una vez iniciado el trabajo, la consola mostrará la pantalla Trabajos. En ella aparece una lista de los trabajos de copia de seguridad y sus estados.

AWS CLI

Utilice el comando `start-backup-job`.

Parámetros necesarios

- `BackupVaultName`
- `IamRoleArn`
- `ResourceArn`

Parámetros opcionales

- `CompleteWindowMinutes`
- `IdempotencyToken`
- `Lifecycle`
- `StartWindowMinutes`

Example Ejemplo

En el siguiente ejemplo se crea una copia de seguridad bajo demanda de un espacio de nombres de Redshift sin servidor.

```
aws backup start-backup-job \  
    --backup-vault-name sample-vault \  
    --resource-arn arn:aws:redshift:us-east-1:123456789012:resourc
```

```
--iam-role-arn arn:aws:iam::account:role/service-role/  
AWSBackupDefaultServiceRole \  
--resource-arn arn:aws:redshift-serverless:region:account:namespace/namespace-  
name-UUID
```

Creación de copias de seguridad programadas de Redshift sin servidor en un plan de copia de seguridad

Puede crear un nuevo plan de copia de seguridad para los espacios de nombres de Redshift sin servidor desde la consola de AWS Backup o la CLI, o bien puede añadir Redshift sin servidor a un plan de copia de seguridad existente.

Las copias de seguridad programadas pueden incluir espacios de nombres de Redshift sin servidor si son un recurso protegido. Para optar por proteger Redshift Serverless en la AWS Backup consola, siga estos pasos:

Console

Para optar por proteger Redshift Serverless en la AWS Backup consola, siga estos pasos:

1. Abra la [consola de AWS Backup](#).
2. En el panel de navegación, elija Recursos protegidos.
3. Active Amazon Redshift sin servidor.
4. Consulte [Seleccione AWS los servicios para realizar una copia de seguridad](#) para incluir los espacios de nombres de Redshift sin servidor en un plan nuevo o existente. Al añadir el tipo de recurso Redshift sin servidor, puede optar por añadir Todos los espacios de nombres de Amazon Redshift o marcar las casillas situadas junto a los espacios de nombres de los que quiere realizar copias de seguridad.

En Administrar planes de Backup, puede:

- [crear un plan de copia de seguridad](#) e incluir Redshift sin servidor,
- [actualizar](#) un plan de copia de seguridad existente para incluir Redshift sin servidor.

AWS CLI

Consulte [Cree planes de respaldo mediante el AWS CLI](#) para obtener instrucciones sobre cómo usar create-backup-plan.

Si desea modificar un plan existente para incluir sus recursos sin servidor, utilice el comando `update-backup-plan`.

El ARN (nombre de recurso de Amazon) de los recursos sin servidor que se van a incluir en "BackupSelection": {"Resources"} tiene el siguiente formato:

```
arn:aws:redshift-serverless:Region:account:snapshot/a12bc34d-567e-890f-123g-h4ijk56l78m9
```

Para obtener más información sobre la restauración de datos de una instantánea en un espacio de nombres sin servidor, consulte [Restauración de Amazon Redshift sin servidor](#).

Copias de seguridad de Amazon EKS

Un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) consta de varios recursos de los que puede hacer copias de seguridad como una sola unidad. Al realizar una copia de seguridad de un clúster de Amazon EKS, AWS Backup crea un punto de recuperación compuesto que incluye tanto el estado del clúster de EKS como las copias de seguridad de volúmenes persistentes.

Cuando se hace una copia de seguridad de un clúster de Amazon EKS, se crean puntos de recuperación para el estado del clúster de Amazon EKS y los volúmenes persistentes compatibles con él AWS Backup. Estos puntos de recuperación se agrupan dentro de un punto de recuperación global denominado compuesto.

Hay dos componentes distintos de una copia de seguridad de Amazon EKS:

- Estado del clúster de Amazon EKS: se trata de una copia de seguridad del estado del clúster de Amazon EKS. Consulte la terminología de backup de Amazon EKS que aparece a continuación para ver qué incluye.
- Almacenamiento persistente: se trata de una copia de seguridad del almacenamiento persistente (Amazon EBS, Amazon S3, Amazon Elastic File System) adjunto al clúster de Amazon EKS mediante Persistent Volume Claims y [compatible con el controlador CSI EKS Add Ons](#).

Terminología de backup de Amazon EKS

Los siguientes términos se utilizan en toda la documentación de respaldo de Amazon EKS. Para obtener información sobre la terminología específica de Amazon EKS, consulte la [documentación de Amazon EKS](#).

Terminología de EKS Backup

- Punto de recuperación compuesto: punto de recuperación que se utiliza para agrupar puntos de recuperación anidados para realizar una copia de seguridad de un clúster de Amazon EKS.
- Punto de recuperación anidado: punto de recuperación de un recurso que forma parte de un clúster de Amazon EKS y del que se hace una copia de seguridad como parte del punto de recuperación compuesto.
- Estado del clúster de EKS: los manifiestos de Kubernetes (archivos YAML o JSON) que definen el estado deseado de los recursos de Kubernetes del clúster. Esto incluye los recursos y despliegues de Kubernetes, como los secretos, los mapas de configuración, los conjuntos con estado, las clases de almacenamiento, los mapas de almacenamiento, los conjuntos de réplicas DaemonSets, las notificaciones de volumen persistentes, las definiciones de recursos personalizadas, las funciones y los enlaces de funciones.
- Punto de recuperación secundario de la configuración del clúster de Amazon EKS: contiene el estado del clúster de Amazon EKS.
- Puntos de recuperación secundaria de volumen persistente: contiene copias de seguridad de volumen persistentes para los tipos de almacenamiento compatibles (EBS, S3, EFS) [compatibles con el controlador CSI adicional de EKS](#).

Estructura de respaldo de Amazon EKS

Las copias de seguridad de Amazon EKS incluyen los siguientes componentes:

- Estado del clúster de Amazon EKS
- Almacenamiento persistente: copias de seguridad de los tipos de almacenamiento compatibles, incluidos Amazon EBS, Amazon EFS y Amazon S3

Amazon EKS Backups no incluirá los siguientes componentes:

- Imágenes de contenedores de repositorios externos (ECR, Docker)
- Componentes de la infraestructura de clústeres de EKS (por ejemplo, subredes VPCs)
- Recursos de EKS generados automáticamente, como nodos, módulos generados automáticamente, eventos, arrendamientos y trabajos.

Configuración y requisitos previos de la copia de seguridad de EKS («Antes de realizar la copia de seguridad»)

- Configuración del clúster EKS:
 - El [modo de autorización](#) del clúster EKS está configurado en API o API_AND_CONFIG_MAP para crear [entradas de acceso AWS Backup para acceder](#) al clúster EKS.
- Permisos:
 - AWS Backup La política gestionada [AWSBackupServiceRolePolicyForBackup](#) contiene los permisos necesarios para hacer copias de seguridad del clúster de Amazon EKS y del almacenamiento persistente de EBS y EFS
 - Si su clúster EKS contiene un bucket de S3, tendrá que asegurarse de que se añadan y activen las siguientes políticas y requisitos previos para su bucket de S3, tal como se indica en la documentación:
 - [AWSBackupServiceRolePolicyForS3 Backup](#)
 - [Requisitos previos para las copias de seguridad de S3](#)
- Cifrado:
 - Los puntos de recuperación secundarios de Amazon EKS se cifrarán con el conjunto de claves de Amazon KMS del Backup Vault de destino.
 - Los puntos de recuperación de almacenamiento persistente se cifrarán según el soporte actual para cada clase de almacenamiento: EBS Snapshots, S3 Backups y EFS Backups. [Consulte Cifrado de copias de seguridad en AWS Backup](#)

Cree una copia de seguridad de Amazon EKS

El proceso de creación de una copia de seguridad se denomina trabajo de copia de seguridad. Un trabajo de copia de seguridad de un clúster de Amazon EKS tiene un estado. Cuando un trabajo de respaldo ha finalizado, tiene el estado Completado. Esto significa que se ha creado un punto de recuperación (una copia de seguridad).

Creación de una copia de seguridad de Amazon EKS bajo demanda

Console

Para crear una copia de seguridad bajo demanda de su clúster de Amazon EKS:

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.

2. En el panel de navegación, elija Protected resources (Recursos protegidos).
3. En Tipo de recurso, seleccione Amazon EKS.
4. Seleccione la casilla de verificación situada junto al clúster de Amazon EKS del que desee hacer una copia de seguridad.
5. Seleccione Create on-demand backup (Crear copia de seguridad bajo demanda).
6. Configure los ajustes de copia de seguridad, incluida la ventana de copia de seguridad, la transición al almacenamiento en frío y el período de retención.
7. Seleccione Create on-demand backup (Crear copia de seguridad bajo demanda).

AWS CLI

Para crear una copia de seguridad bajo demanda de su clúster de Amazon EKS mediante AWS CLI:

Utilice el comando start-backup-job:

```
aws backup start-backup-job \
                                --backup-vault-name my-backup-vault \
                                --resource-arn arn:aws:eks:us-
west-2:123456789012:cluster/my-cluster \
                                --iam-role-arn arn:aws:iam::123456789012:role/
service-role \
                                --region us-west-2
```

Si lo desea, especifique parámetros adicionales, como la configuración del ciclo de vida:

```
aws backup start-backup-job \
                                --backup-vault-name my-backup-vault \
                                --resource-arn arn:aws:eks:us-
west-2:123456789012:cluster/my-cluster \
                                --iam-role-arn arn:aws:iam::123456789012:role/
service-role \
                                --lifecycle
MoveToColdStorageAfterDays=30,DeleteAfterDays=365 \
                                --region us-west-2
```

Supervise el estado del trabajo de respaldo:

```
aws backup describe-backup-job \
```

```
--backup-job-id backup-job-id \  
--region us-west-2
```

Formato ARN de respaldo de Amazon EKS

El punto de recuperación compuesto arn ::backup: :recovery-point:composite:eks/ - *partition region accountId cluster-name timestamp*

Child Recovery Point arn ::backup*partition*: :recovery-point:eks/ - *region accountId cluster-name timestamp*

Puntos de recuperación Amazon EKS

Estado del punto de recuperación

Cuando finaliza el trabajo de copia de seguridad de un clúster de Amazon EKS (el estado del trabajo es `Completed`), se ha creado una copia de seguridad del clúster. Esta copia de seguridad también se conoce como punto de recuperación compuesto. Un punto de recuperación compuesto puede tener uno de los siguientes estados: `Completed`, `Failed` o `Partial`.

Cada copia de seguridad de Amazon EKS crea una tarea de copia de seguridad principal para el punto de recuperación compuesto y una tarea de copia de seguridad secundaria para cada punto de recuperación secundario (configuración de clústeres y volúmenes persistentes).

- Una tarea de copia de seguridad completada significa que todo su clúster de Amazon EKS y los recursos que contiene están protegidos por AWS Backup.
- Un estado de error indica que el trabajo de copia de seguridad no se realizó correctamente; debe volver a crear la copia de seguridad una vez que se haya corregido el problema que provocó el error.
- Un `Partial` estado significa que no se realizó una copia de seguridad de todos los recursos del clúster. Esto puede suceder si uno o más de los trabajos de copia de seguridad que pertenecen a los recursos del clúster (recursos anidados) tienen estados distintos de los siguientes. `Completed` Puede crear manualmente una copia de seguridad bajo demanda para volver a ejecutar cualquier recurso cuyo estado no sea `Completed`.

Cada recurso anidado dentro del punto de recuperación compuesto tiene su propio punto de recuperación individual, cada uno con su propio estado (`Completed` o `Failed`). Es posible restaurar los puntos de recuperación anidados con un estado de `Completed`.

AWS Backup admite las transiciones del ciclo de vida al almacenamiento en frío para puntos de recuperación de volúmenes persistentes. Puede suscribirse a las notificaciones para recibir alertas sobre el estado de las tareas de copia de seguridad.

Administración de los puntos de recuperación

Los puntos de recuperación compuestos (copias de seguridad) se pueden copiar; los puntos de recuperación secundarios de volúmenes persistentes se pueden copiar, eliminar, disociar o restaurar. El punto de recuperación secundario del estado del clúster de Amazon EKS no se puede copiar, eliminar ni disociar, ya que mantiene una relación 1:1 con su punto de recuperación compuesto principal.

No se puede eliminar un punto de recuperación compuesto que contenga copias de seguridad anidadas. Una vez eliminados o disociados los puntos de recuperación anidados dentro de un punto de recuperación compuesto, puede eliminar manualmente el punto de recuperación compuesto o dejar que permanezca hasta que se elimine durante el ciclo de vida del plan de copia de seguridad.

Eliminación de un punto de recuperación

Puede eliminar un punto de recuperación mediante la consola o mediante el AWS CLI.

Para eliminar puntos de recuperación mediante la consola:

Abra la AWS Backup consola en <https://console.aws.amazon.com/backup/>.

1. Haga clic en Recursos protegidos en el menú de navegación de la izquierda. En el cuadro de texto, escriba EKS para mostrar solo los clústeres de Amazon EKS.
2. Los puntos de recuperación compuestos se mostrarán en el panel Puntos de recuperación. Puede hacer clic en el signo más (+) situado a la izquierda del identificador de cada punto de recuperación para ampliar cada punto de recuperación compuesto y mostrar todos los puntos de recuperación anidados que contiene el compuesto. Puede marcar la casilla situada a la izquierda de cualquier punto de recuperación para incluirlo en la selección de puntos de recuperación que desee eliminar.
3. Haga clic en el botón Eliminar.

Si utiliza la consola para eliminar uno o más puntos de recuperación compuestos, aparecerá un cuadro de advertencia. Este cuadro de advertencia requiere que confirme su intención de eliminar los puntos de recuperación compuestos, incluidos los puntos de recuperación anidados dentro de las pilas compuestas.

Para eliminar los puntos de recuperación mediante la API, utilice el `DeleteRecoveryPoint` comando.

Si utiliza la API con la, AWS Command Line Interface debe eliminar todos los puntos de recuperación anidados antes de eliminar un punto compuesto.

Disociación de un punto de recuperación anidado del punto de recuperación compuesto

Puede disociar un punto de recuperación anidado de un punto de recuperación compuesto (por ejemplo, desea conservar el punto de recuperación anidado pero eliminar el punto de recuperación compuesto). Ambos puntos de recuperación permanecerán, pero dejarán de estar conectados; es decir, las acciones que se realicen en el punto de recuperación compuesto dejarán de aplicarse al punto de recuperación anidado una vez que se haya disociado. El punto de recuperación secundario del estado del clúster de Amazon EKS no se puede disociar, ya que mantiene una relación 1:1 con su punto de recuperación compuesto principal.

Puede desasociar el punto de recuperación mediante la consola o puede llamar a la API.

`DisassociateRecoveryPointFromParent`

Copia de un punto de recuperación

Puede copiar un punto de recuperación compuesto o puede copiar un punto de recuperación anidado si el recurso admite la [copia entre cuentas y regiones](#).

Para copiar los puntos de recuperación mediante la AWS Backup consola:

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. Haga clic en Recursos protegidos en el menú de navegación de la izquierda. En el cuadro de texto, escriba EKS para que se muestren solo sus clústeres de Amazon EKS.
3. Los puntos de recuperación compuestos se mostrarán en el panel Puntos de recuperación. Puede hacer clic en el signo más (+) situado a la izquierda del identificador de cada punto de recuperación para ampliar cada punto de recuperación compuesto y mostrar todos los puntos de recuperación anidados que contiene el compuesto. Puede hacer clic en el botón circular de opción situado a la izquierda de cualquier punto de recuperación para copiarlo.
4. Una vez seleccionado, haga clic en el botón Copiar de la esquina superior derecha del panel.

Las copias de seguridad de Amazon EKS admiten todos los tipos de copias:

- Misma región/cuenta
- Entre cuentas

- Entre regiones
- Regiones registradas

Limitaciones

- No se admiten los volúmenes persistentes que utilizan un controlador CSI mediante la migración de CSI, los complementos de almacenamiento en árbol o los controladores ACK.
- No se MountPoints pueden hacer copias de seguridad de los buckets de Amazon S3 con prefijos específicos adjuntos al controlador CSI. Solo se admiten buckets de Amazon S3 como destinos, no prefijos específicos
- Las copias de seguridad de bucket de Amazon S3 que forman parte de una copia de seguridad de un clúster de EKS solo admitirán copias de seguridad instantáneas.
- Amazon FSx mediante el controlador CSI no es compatible con las copias de seguridad de EKS.
- Sujeto a cuotas [de copia de seguridad y restauración](#)

Preguntas frecuentes

1. «¿Qué se incluye como parte de la copia de seguridad de Amazon EKS?»

Como parte de cada copia de seguridad de un clúster de Amazon EKS, se realiza una copia de seguridad del estado del clúster de Amazon EKS y de los volúmenes persistentes AWS Backup compatibles con él. El estado del clúster de Amazon EKS incluye detalles como el nombre del clúster, la función de IAM, la configuración de Amazon VPC, los ajustes de red, el registro, el cifrado, los complementos, las entradas de acceso, los grupos de nodos gestionados, los perfiles de Fargate, las asociaciones de identidad de los pods y los archivos de manifiesto de Kubernetes.

2. “¿Un estado *Partial* significa que se ha producido un error al crear mi copia de seguridad?”

No. Un estado parcial indica que se realizó una copia de seguridad de algunos puntos de recuperación, pero no de otros. Existen dos condiciones para comprobar si esperaba un resultado de copia de seguridad: `Completed`

- a. Uno o más de los trabajos de copia de seguridad que pertenecían a los recursos del clúster no se realizaron correctamente y es necesario volver a ejecutar el trabajo.
- b. Se eliminó o disoció un punto de recuperación anidado del punto de recuperación compuesto.

3. «¿Necesito tener un agente o un complemento de Amazon EKS instalado en mi clúster de Amazon EKS antes de realizar la copia de seguridad?»

No. AWS Backup no requiere la instalación de ningún agente o complemento en su clúster de Amazon EKS. El único requisito previo es tener el [modo de autorización](#) de su clúster EKS configurado en API o API_AND_CONFIG_MAP para poder crear [entradas de acceso para acceder AWS Backup](#) al clúster EKS.

4. «¿Amazon EKS Backups incluye componentes de infraestructura de Amazon EKS o imágenes de Amazon ECR?»

No. Las copias de seguridad de Amazon EKS se centran en el estado del clúster de EKS y en las cargas de trabajo de las aplicaciones, no en los componentes de la infraestructura subyacente ni en las imágenes del contenedor.

5. «¿Puedo pasar el ciclo de vida de mi punto de recuperación compuesto de EKS a almacenamiento en frío?»

Puede hacer la transición al almacenamiento en frío para los puntos de recuperación secundarios subyacentes que admitan los niveles de almacenamiento en frío. Consulte la [matriz de disponibilidad de AWS Backup funciones](#) para ver la lista completa de soporte.

6. «¿Mis copias de seguridad de EKS son incrementales?»

AWS Backup realizará copias de seguridad incrementales de cada punto de recuperación secundario donde sea compatible en la actualidad, lo que incluye los volúmenes de EBS, los sistemas de archivos EFS y los depósitos de S3. El punto de recuperación secundario del estado del clúster de EKS será una copia de seguridad completa. Consulte la [matriz AWS Backup de disponibilidad de funciones](#).

7. «¿Puedo crear un índice y buscar en mis copias de seguridad de EKS?»

No, sin embargo, puede crear índices bajo demanda y buscar volúmenes persistentes cuando el tipo de almacenamiento subyacente admita esta capacidad. AWS Backup Consulte la [matriz de disponibilidad de AWS Backup funciones](#).

Respaldo de SAP HANA en Amazon EC2

Note

[Servicios compatibles con Región de AWS](#) contiene las regiones compatibles actualmente en las que están disponibles las copias de seguridad de bases de datos de SAP HANA en las EC2 instancias de Amazon.

AWS Backup admite copias de seguridad y restauraciones de bases de datos de SAP HANA en EC2 instancias de Amazon.

Temas

- [Descripción general de las bases de datos de SAP HANA con AWS Backup](#)
- [Requisitos previos para realizar copias de seguridad de las bases de datos de SAP HANA mediante AWS Backup](#)
- [Operaciones de copia de seguridad de SAP HANA en la consola de AWS Backup](#)
- [Visualización de copias de seguridad de las bases de datos de SAP](#)
- [Úselo AWS CLI para las bases de datos de SAP HANA con AWS Backup](#)
- [Solución de problemas de copias de seguridad de las bases de datos de SAP HANA](#)
- [Glosario de términos de SAP HANA utilizados AWS Backup](#)
- [AWS Backup soporte de bases de datos de SAP HANA en EC2 instancias, notas de la versión](#)

Descripción general de las bases de datos de SAP HANA con AWS Backup

Además de la capacidad de crear copias de seguridad y restaurar bases de datos, la AWS Backup integración con Amazon EC2 Systems Manager for SAP permite a los clientes identificar y etiquetar las bases de datos de SAP HANA.

AWS Backup está integrado con AWS Backint Agent para realizar copias de seguridad y restauraciones de SAP HANA. Para obtener más información, consulte [AWS Backint](#).

Requisitos previos para realizar copias de seguridad de las bases de datos de SAP HANA mediante AWS Backup

Se deben cumplir varios requisitos previos antes de poder realizar las actividades de copia de seguridad y restauración. Tenga en cuenta que necesitará acceso administrativo a su base de datos

de SAP HANA y permisos para crear nuevas funciones y políticas de IAM en su AWS cuenta para llevar a cabo estos pasos.

Complete [estos requisitos previos en Amazon EC2 Systems Manager](#).

1. [Configure los permisos necesarios para la EC2 instancia de Amazon que ejecute la base de datos SAP HANA](#)
2. [Registre las credenciales en AWS Secrets Manager](#)
3. [Instale AWS Backup y AWS Systems Manager para los agentes de SAP](#)
4. [Verifique el agente SSM](#)
5. [Verifique los parámetros](#)
6. [Registre la base de datos de SAP HANA](#)

Se recomienda registrar cada instancia de HANA solo una vez. Los registros múltiples pueden resultar en varios ARNs para la misma base de datos. Mantener un único ARN y registro simplifica la creación y el mantenimiento del plan de copia de seguridad y también puede ayudar a reducir la duplicación no planificada de copias de seguridad.

Operaciones de copia de seguridad de SAP HANA en la consola de AWS Backup

Una vez que se hayan completado los requisitos previos y el SSM para las configuraciones de SAP, podrá realizar copias de seguridad de su SAP HANA en las bases de datos y restaurarlas. EC2

Activación de la protección de los recursos de SAP HANA

Para poder proteger AWS Backup sus bases de datos de SAP HANA, SAP HANA debe estar activado como uno de los recursos protegidos. Para ello:

1. [Abra la AWS Backup consola en /backup. https://console.aws.amazon.com](#)
2. En el panel de navegación izquierdo, elija Configuración.
3. En Activación del servicio, seleccione Configurar recursos.
4. Suscríbase a SAP HANA en Amazon EC2. .
5. Haga clic en Confirmar.

La suscripción al servicio SAP HANA en Amazon ahora EC2 estará habilitada.

Creación de una copia de seguridad programada de las bases de datos de SAP HANA

Puede [editar un plan de copia de seguridad existente](#) y agregarle recursos de SAP HANA, o puede [crear un nuevo plan de copia de seguridad](#) solo para los recursos de SAP HANA.

Si decide crear un nuevo plan de copia de seguridad, tendrá tres opciones:

1. Opción 1: comience con una plantilla

1. Elija una plantilla de plan de copia de seguridad.
2. Especifique un nombre de plan de copia de seguridad.
3. Haga clic en Crear plan.

2. Opción 2: cree un plan nuevo

1. Especifique un nombre de plan de copia de seguridad.
2. Si lo desea, especifique las etiquetas que se agregarán al plan de copia de seguridad.
3. Especifique la configuración de la regla de copia de seguridad.
 - a. Especifique un nombre para la regla de copia de seguridad.
 - b. Seleccione un almacén de copias de seguridad existente o cree uno nuevo. Aquí es donde se guardan las copias de seguridad.
 - c. Especifique la frecuencia de las copias de seguridad.
 - d. Especifique un intervalo de copia de seguridad.

Tenga en cuenta que actualmente no se admite la transferencia al almacenamiento en frío.

- e. Especifique el periodo de retención.

Actualmente no se admite la copia al destino

- f. (Opcional) Especifique las etiquetas que desee agregar a los puntos de recuperación.
4. Haga clic en Crear plan.

3. Opción 3: defina un plan con JSON

1. Para especificar el JSON de su plan de copia de seguridad, modifique la expresión JSON de un plan de copia de seguridad existente o cree una nueva expresión.
2. Especifique un nombre de plan de copia de seguridad.
3. Haga clic en Validar JSON.

Una vez que el plan de copia de seguridad se haya creado correctamente, puede asignar recursos al plan de copia de seguridad en el siguiente paso.

Sea cual sea el plan que utilice, asegúrese de [asignar recursos](#). Puede elegir qué bases de datos de SAP HANA desea asignar, incluidas bases de datos del sistema y de inquilinos. También tiene la opción de excluir un recurso IDs específico.

Creación de una copia de seguridad bajo demanda de las bases de datos de SAP HANA

Puede [crear una copia de seguridad completa bajo demanda](#) que se ejecute inmediatamente después de su creación. Tenga en cuenta que las copias de seguridad bajo demanda de las bases de datos de SAP HANA en EC2 las instancias de Amazon son copias de seguridad completas; no se admiten las copias de seguridad incrementales.

La copia de seguridad bajo demanda ya está creada. Comenzará a hacer copias de seguridad de los recursos especificados. La consola lo llevará a la página de Trabajos de copia de seguridad, donde podrá ver el progreso del trabajo. Tome nota del identificador del trabajo de copia de seguridad en el banner azul situado en la parte superior de la pantalla, ya que lo necesitará para encontrar fácilmente el estado del trabajo de copia de seguridad. Cuando se complete la copia de seguridad, el estado pasará a Completed. Las copias de seguridad pueden tardar varias horas.

Actualice la Lista de trabajos de copia de seguridad para ver el cambio de estado. También puede buscar y hacer clic en el ID de trabajo de copia de seguridad para ver el estado detallado del trabajo.

Copias de seguridad continuas de las bases de datos de SAP HANA

Puede realizar [copias de seguridad continuas](#), que se pueden utilizar con la point-in-time restauración (PITR) (tenga en cuenta que las copias de seguridad bajo demanda conservan los recursos en el estado en que se utilizan, mientras que la PITR utiliza copias de seguridad continuas que registran los cambios a lo largo de un período de tiempo).

Con las copias de seguridad continuas, puede restaurar la base de datos de SAP HANA en una EC2 instancia retrocediéndola hasta el momento específico que elija, con una precisión de 1 segundo (con un tiempo máximo de 35 días). La copia de seguridad continua consiste en crear primero una copia de seguridad completa del recurso y, a continuación, realizar copias de seguridad constantes de los registros de transacciones del recurso. La restauración mediante PITR funciona accediendo a la copia de seguridad completa y reproduciendo el registro de transacciones hasta el momento indicado para su recuperación. AWS Backup

Puede optar por realizar copias de seguridad continuas al crear un plan de copias de seguridad AWS Backup mediante la AWS Backup consola o la API.

Para habilitar las copias de seguridad continuas desde la consola

1. Inicie sesión en y abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
[Consola de administración de AWS](#)
2. En el panel de navegación principal, elija Planes de copia de seguridad y, a continuación, elija Crear plan de copia de seguridad.
3. En Reglas de copia de seguridad, elija Agregar regla de copia de seguridad.
4. En la sección Configuración de regla de copia de seguridad, seleccione Habilitar copias de seguridad continuas para los recursos compatibles.

Tras deshabilitar el [PITR \(point-in-time restauración\)](#) para las copias de seguridad de las bases de datos de SAP HANA, se seguirán enviando los registros AWS Backup hasta que caduque el punto de recuperación (el estado es igual a). EXPIRED) Puede cambiar a una ubicación alternativa de copia de seguridad de registros en SAP HANA para detener la transmisión de registros a AWS Backup.

Un punto de recuperación continuo con un estado de STOPPED indica que se ha interrumpido un punto de recuperación continuo; es decir, los registros transmitidos desde SAP HANA a AWS Backup ese punto que muestran los cambios incrementales en una base de datos tienen un vacío. Los puntos de recuperación que se producen dentro de este lapso de tiempo tienen un estado de STOPPED..

Para ver los problemas que pueden surgir durante los trabajos de restauración de copias de seguridad continuas (puntos de recuperación), consulte la sección de solución [Solución de problemas de restauración de SAP HANA](#) de esta guía.

Visualización de copias de seguridad de las bases de datos de SAP

Consulte el estado de los trabajos de copia de seguridad:

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, seleccione Trabajos.
3. Elija trabajos de copia de seguridad, trabajos de restauración o trabajos de copia para ver la lista de sus trabajos.
4. Busque el ID del trabajo y haga clic en él para ver los estados detallados de los trabajos.

Consulte todos los puntos de recuperación de un almacén:

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, elija Backup vaults (Almacenes de copia de seguridad).
3. Busque un almacén de copias de seguridad y haga clic en él para ver todos los puntos de recuperación dentro del almacén.

Consulte los detalles de los recursos protegidos:

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, elija Protected resources (Recursos protegidos).
3. También puede filtrar por tipo de recurso para ver todas las copias de seguridad de ese tipo de recurso.

Úselo AWS CLI para las bases de datos de SAP HANA con AWS Backup

Cada acción de la consola de copia de seguridad tiene una llamada a la API correspondiente.

Para configurar AWS Backup y gestionar sus recursos mediante programación, utilice la llamada [StartBackupJob](#) la API para hacer una copia de seguridad de una base de datos de SAP HANA en una EC2 instancia.

Utilice `start-backup-job` como el comando de la CLI.

Solución de problemas de copias de seguridad de las bases de datos de SAP HANA

Si encuentra errores durante su flujo de trabajo, consulte los siguientes ejemplos de errores y soluciones sugeridas:

Requisitos previos de Python

- Error: error de Zypper relacionado con la versión de Python desde SSM para SAP y requiere AWS Backup Python 3.6, pero SUSE 12 es compatible de SP5 forma predeterminada con Python 3.4.

Solución: instale varias versiones de SUSE12 SP5 Python siguiendo estos pasos:

1. Ejecute un comando `update-alternatives` para crear un enlace simbólico para Python 3 en `/usr/local/bin/` instead of directly using `/usr/bin/python` Estos comandos establecerán Python 3.4 como la versión por defecto. El comando es:

```
# sudo update-alternatives --install /usr/local/bin/python3 python3 /usr/bin/python3.4 5.
```

2. Añada Python 3.6 a la configuración de alternativas ejecutando el siguiente comando: `# sudo update-alternatives --install /usr/local/bin/python3 python3 /usr/bin/python3.6 2`
3. Cambie la configuración alternativa a Python 3.6 ejecutando el siguiente comando: `# sudo update-alternatives --config python3`

Debería mostrarse el siguiente resultado:

```
There are 2 choices for the alternative python3 (providing /usr/local/bin/python3).
Selection Path Priority Status
* 0 /usr/bin/python3.4 5 auto mode
  1 /usr/bin/python3.4 5 manual mode
  2 /usr/bin/python3.6 2 manual mode
Press enter to keep the current choice[*], or type selection number:
```

4. Introduzca el número correspondiente a Python 3.6.
5. Compruebe la versión de Python y confirme que se está utilizando Python 3.6.
6. (Opcional, pero recomendado) Compruebe que los comandos de Zypper funcionan según lo esperado.

Descubrimiento y registro de Amazon EC2 Systems Manager para SAP

- Error: SSM para SAP no pudo detectar la carga de trabajo debido al bloqueo del acceso a un terminal público para AWS Secrets Manager SSM.

Solución: compruebe si se puede acceder a los puntos de conexión desde su base de datos de SAP HANA. Si no se puede acceder a ellos, puede crear puntos de conexión de Amazon VPC para AWS Secrets Manager y SSM para SAP.

1. Pruebe el acceso a Secrets Manager desde el EC2 host de Amazon para HANA DB ejecutando el siguiente comando: `aws secretsmanager get-secret-value --secret-id hanaeccsbx_hbx_database_awsbkp`. Si el comando no devuelve un valor, el firewall bloquea el acceso al punto de conexión del servicio Secrets Manager. El registro se detendrá en el paso “Recuperación de secretos de Secrets Manager”.
2. Ejecute el comando `aws ssm-sap list-registration` para probar la conectividad con SSM para el punto de conexión de SAP. Si el comando no devuelve un valor, el firewall bloquea el acceso a SSM para el punto de conexión de SAP.

Ejemplo de error: Connection was closed before we received a valid response from endpoint URL: "https://ssm-sap.us-west-2.amazonaws.com/register-application"

Hay dos opciones para continuar si no se puede acceder a los puntos de conexión.

- Abra los puertos del firewall para permitir el acceso al punto de conexión del servicio público para Secrets Manager y SSM para SAP; o,
- Cree puntos de conexión de VPC para Secrets Manager y SSM para SAP y, a continuación:
 - Asegúrese de que Amazon VPC esté habilitada para DNSSupport y. DNSHostname
 - Asegúrese de que su punto de conexión de VPC haya habilitado la opción Permitir nombre de DNS privado.
 - Si la detección de SSM para SAP se completó correctamente, el registro mostrará que se ha descubierto el host.
- Error: AWS Backup y la conexión de Backint falla debido al bloqueo del acceso a los puntos finales públicos AWS Backup del servicio. aws-backint-agent.log puede mostrar errores similares a este: time="2024-01-03T11:39:15-08:00" level=error msg="Storage configuration validation failed: missing backup data plane Id" o. level=fatal msg="Error performing backup missing backup data plane Id. Además, la consola de AWS Backup puede mostrar Fatal Error: An internal error occurred.

Solución: abra los puertos del firewall para permitir el acceso a los puntos de conexión de servicio público (HTTPS). Una vez utilizada esta opción, el DNS resolverá las solicitudes a AWS los servicios a través de direcciones IP públicas.

- Error: el registro de SSM para SAP falla debido a que la contraseña de HANA contiene caracteres especiales. Los ejemplos de errores pueden incluir Error connecting to database HBX/HBX when validating its credentials. o Discovery failed because credentials for HBX/SYSTEMDB either not provided or cannot be validated. después de probar una conexión utilizando hdbsql systemdb y tenantdb que se probó desde la EC2 instancia Amazon de la base de datos HANA.

En la AWS Backup consola de la página de trabajos, los detalles del trabajo de respaldo pueden mostrar el estado del FAILED error Miscellaneous: b' * 10: authentication failed SQLSTATE: 28000\n'.

Solución: asegúrese de que la contraseña no contenga caracteres especiales, como \$.

- Error: **b'* 447: backup could not be completed: [110507] Backint exited with exit code 1 instead of 0. console output: time...**

Solución: es posible que la instalación del AWS BackInt agente para SAP HANA no se haya completado correctamente. Vuelva a intentar el proceso para implementar el [AWS Backint Agent](#) y el Amazon [EC2 Systems Manager Agent](#) en su servidor de aplicaciones SAP.

- Error: la consola no coincide con los archivos de registro tras el registro.

El registro de detección muestra un error de registro al intentar conectarse a HANA DB debido a que la contraseña contiene caracteres especiales, aunque la consola SSM para SAP Application Manager para SAP indica que el registro se ha realizado correctamente. No confirma que el registro se haya realizado correctamente. Si la consola muestra un registro correcto pero los registros no, las copias de seguridad fallarán.

Confirme el estado del registro:

1. Inicie sesión en la [consola de SSM](#)
2. En el panel de navegación izquierda, seleccione Ejecutar comando.
3. En el campo de texto Historial de comandos, introduzca Instance ID:Equal:, con un valor igual al de la instancia que utilizó para el registro. Esto filtrará el historial de comandos.
4. Use la columna de identificador de comandos para buscar comandos con estado Failed. A continuación, busque el nombre del documento de. AWSSystemsManagerSAP-Discovery
5. En AWS CLI, ejecute el comando `aws ssm-sap register-application status`. Si se devuelve el valor Error, significa que el registro no se ha realizado correctamente.

Solución: asegúrese de que la contraseña de HANA no contenga caracteres especiales (como '\$').

Crear una copia de seguridad de una base de datos de SAP HANA

- Error: AWS Backup la consola muestra el mensaje «Error grave» cuando se crea una copia de seguridad bajo demanda para SystemDB o TenantDB. Esto ocurre porque no se puede acceder al punto de conexión público. Esto se debe a un firewall del lado del cliente que bloquea el acceso a este punto de conexión.

`aws-backint-agent.log` puede mostrar errores como `level=error msg="Storage configuration validation failed: missing backup data plane Id"` o `level=fatal msg="Error performing backup missing backup data plane Id."`

Solución: abra el acceso mediante firewall al punto de conexión público.

- Error: Database cannot be backed up while it is stopped.

Solución: asegúrese de que la base de datos de la que se va a hacer la copia de seguridad esté activa. Solo se puede hacer una copia de seguridad de los datos y registros de la base de datos cuando la base de datos está en línea.

- Error: Getting backup metadata failed. Check the SSM document execution for more details.

Solución: asegúrese de que la base de datos de la que se va a hacer la copia de seguridad esté activa. Solo se puede hacer una copia de seguridad de los datos y registros de la base de datos cuando la base de datos está en línea.

Supervisión de los registros de copia de seguridad

- Error: Encountered an issue with log backups, please check SAP HANA for details.

Solución: compruebe SAP HANA para asegurarse de que las copias de seguridad de los registros se envíen AWS Backup desde SAP HANA.

- Error: One or more log backup attempts failed for recovery point.

Solución: consulte SAP HANA para obtener más información. Asegúrese de que las copias de seguridad de los registros se envíen AWS Backup desde SAP HANA.

- Error: Unable to determine the status of log backups for recovery point.

Solución: consulte SAP HANA para obtener más información. Asegúrese de que las copias de seguridad de los registros se envíen AWS Backup desde SAP HANA.

- Error: Log backups for recovery point %s were interrupted due to a restore operation on the database.

Solución: espere a que se complete el trabajo de restauración. Las copias de seguridad de los registros deberían reanudarse.

Glosario de términos de SAP HANA utilizados AWS Backup

Tipos de copias de seguridad de datos: SAP HANA admite dos tipos de copias de seguridad de datos: completas e INC (incrementales). AWS Backup optimiza el tipo que se utiliza durante cada operación de respaldo.

Copias de seguridad del catálogo: SAP HANA mantiene su propio manifiesto denominado catálogo. AWS Backup interactúa con este catálogo. Cada nueva copia de seguridad creará una entrada en el catálogo.

Copia de seguridad continua de registros (registros de transacciones): para las funciones de recuperación en un momento dado (PITR), SAP HANA hace un seguimiento de todas las transacciones a partir de la copia de seguridad más reciente.

Copia del sistema: un trabajo de restauración en el que la base de datos de destino de la restauración es diferente de la base de datos de origen a partir de la cual se creó el punto de recuperación.

Restauración destructiva: una restauración destructiva es un tipo de trabajo de restauración durante el cual una base de datos restaurada elimina o sobrescribe la base de datos de origen o existente.

COMPLETA: una copia de seguridad completa es una copia de seguridad completa de una base de datos.

INC: una copia de seguridad incremental es una copia de seguridad de todos los cambios en una base de datos de SAP HANA desde la copia de seguridad anterior.

AWS Backup soporte de bases de datos de SAP HANA en EC2 instancias, notas de la versión

Algunas funcionalidades no son compatibles en este momento:

- Las copias de seguridad continuas (que utilizan registros de transacciones) no se pueden copiar a otras regiones o cuentas. Las copias de seguridad instantáneas se pueden copiar a las regiones y cuentas compatibles a partir de copias de seguridad completas.
- No se admite Backup Audit Manager ni la generación de informes.
- [Servicios compatibles con Región de AWS](#) contiene las regiones actualmente compatibles para las copias de seguridad de bases de datos de SAP HANA en EC2 instancias de Amazon.

Copias de seguridad de Amazon S3

Descripción general de

AWS Backup admite la copia de seguridad y la restauración centralizadas de aplicaciones que almacenan datos solo en S3 o junto con otros AWS servicios de bases de datos, almacenamiento y computación. Hay muchas [características disponibles para las copias de seguridad de S3](#), incluido Backup Audit Manager.

Puede utilizar una única política de copias de seguridad AWS Backup para automatizar de forma centralizada la creación de copias de seguridad de los datos de sus aplicaciones. AWS Backup organiza automáticamente las copias de seguridad de diferentes AWS servicios y aplicaciones de terceros en una ubicación centralizada y cifrada (conocida como [bóveda de copias de seguridad](#)) para que pueda gestionar las copias de seguridad de toda la aplicación mediante una experiencia centralizada. En el caso de S3, puede crear copias de seguridad continuas y restaurar los datos de las aplicaciones almacenados en S3, así como restaurar las copias de seguridad a una point-in-time ubicación única con un solo clic.

Backup por niveles

Amazon S3 es el único recurso que admite la organización de copias de seguridad en niveles en un nivel de almacenamiento en caliente de menor coste. Para obtener más información, consulte Organización de [copias de seguridad en niveles](#).

Requisitos previos para las copias de seguridad de S3

Permisos y políticas para la copia de seguridad y restauración de Amazon S3

Para realizar copias de seguridad, copiar y restaurar los recursos de S3, debe tener las políticas correctas en su rol. Para agregar estas políticas, vaya a [Políticas administradas de AWS](#). Añada [AWSBackupServiceRolePolicyForS3Backup](#) y [AWSBackupServiceRolePolicyForS3Restore](#) a las funciones que pretende utilizar para realizar copias de seguridad y restaurar depósitos de S3.

Si no tiene suficientes permisos, solicite al administrados de la cuenta administrativa (admin) de su organización que agregue las políticas a los roles previstos.

Para obtener más información, consulte [Políticas administradas y políticas insertadas](#) en la Guía del usuario de IAM.

Copias de seguridad y control de versiones

Debe [habilitar el control de versiones de S3 en su bucket de S3](#) AWS Backup para usarlo en Amazon S3.

Se recomienda [establecer un periodo de vencimiento del ciclo de vida](#) para sus versiones de S3.

Cuando comience la copia de seguridad, todos los objetos (incluidas todas las versiones) del bucket se almacenarán en el punto de recuperación (copia de seguridad completada). Puede ser la versión actual de cada objeto, versiones anteriores, los marcadores de eliminación y los objetos pendientes de realizar acciones durante su ciclo de vida.

El costo de almacenamiento se calculará para todos los objetos de la copia de seguridad, incluidos los objetos cuya eliminación esté programada (objetos que caducarán). Puede usar la CLI o los scripts para eliminar la inclusión de objetos cuya caducidad está programada.

Para obtener más información sobre cómo configurar las políticas del ciclo de vida de S3, siga las instrucciones de [esta página](#).

Consideraciones sobre las copias de seguridad de Amazon S3

Tenga en cuenta lo siguiente cuando haga copias de seguridad de recursos de S3:

- Soporte de metadatos de objetos específicos: AWS Backup admite los siguientes metadatos: etiquetas, listas de control de acceso (ACLs), metadatos definidos por el usuario, fecha de creación original e ID de versión. También puede restaurar todos los datos y metadatos de la copia de seguridad, excepto la fecha de creación original, el ID de la versión, la clase de almacenamiento y las etiquetas electrónicas.
- Al restaurar un objeto de S3, AWS Backup aplica un valor de suma de comprobación, incluso si el objeto original no utilizaba la función de suma de comprobación.
- El nombre de clave de un objeto de S3 puede estar compuesto por la mayoría de las cadenas codificables en UTF-8. Se admiten los siguientes caracteres Unicode: #x9 | #xA | #xD | #x20 to #xD7FF | #xE000 to #xFFFD | #x10000 to #x10FFFF.

Los nombres de clave de objeto que incluyen caracteres que no figuran en esta lista podrían quedar excluidos de las copias de seguridad.

- Transición al almacenamiento en frío: utilice una política de administración AWS Backup del ciclo de vida para definir el plazo de caducidad del backup. No se admite la transición al almacenamiento en frío de las copias de seguridad de S3.

- En el caso de las copias de seguridad periódicas, AWS Backup hace todo lo posible por realizar un seguimiento de todos los cambios en los metadatos de los objetos. Sin embargo, si actualiza una etiqueta o una ACL varias veces en un minuto, es posible que AWS Backup no capture todos los estados intermedios.
- AWS Backup no admite copias de seguridad de [SSE-C-encrypted](#) objetos. AWS Backup tampoco admite copias de seguridad de las configuraciones de los buckets, incluidas las políticas, los ajustes, los nombres o los puntos de acceso de los buckets.
- AWS Backup no admite copias de seguridad de S3 en adelante AWS Outposts.
- CloudTrail registro: si registra eventos de lectura de datos, debe enviar los CloudTrail registros a un depósito de destino diferente. Si guardas CloudTrail los registros en el depósito que ellos registran, se produce un bucle infinito que puede provocar cargos inesperados.

Para obtener más información, consulte [Eventos de datos](#) en la Guía del usuario de CloudTrail .

- Registro de acceso al servidor: si habilita el registro de acceso al servidor, debe enviar los registros a un bucket de destino diferente. Si guarda estos registros en el bucket en el que se registran, se crea un bucle infinito. Para obtener más información, consulte [Habilitación del registro de acceso al servidor de Amazon S3](#).

Tipos y cantidades de buckets admitidos

AWS Backup admite la copia de seguridad y la restauración de depósitos S3 de uso general. Por el momento no se admiten los buckets de directorio.

El límite máximo de la cantidad de un recurso (denominado cuota), como un bucket, permitido en una cuenta de AWS depende del servicio. Las [cuotas de Amazon S3](#) son diferentes de las [cuotas de AWS Backup](#).

En cada AWS cuenta, puede crear copias de seguridad de hasta 100 depósitos de forma predeterminada. Puede solicitar un aumento de cuota de hasta 1000 buckets.

Las cuentas con más de 1000 buckets están sujetas a límites de cuota; si las solicitudes superan la cuota, es posible que los trabajos generen errores. Se recomienda limitar una cuenta a 1000 buckets.

Clases de almacenamiento de S3 compatibles

AWS Backup le permite hacer copias de seguridad de los datos de S3 almacenados en las siguientes [clases de almacenamiento de S3](#):

- S3 Standard
- S3 Standard - Acceso infrecuente
- S3 One Zone-IA
- S3 Glacier Instant Retrieval
- S3 Intelligent-Tiering (S3 INT)

Las copias de seguridad de un objeto de la clase de almacenamiento [S3 Intelligent-Tiering \(INT\)](#) acceden a esos objetos. Este acceso hace que S3 Intelligent-Tiering mueva automáticamente esos objetos a Acceso frecuente.

Las copias de seguridad que acceden a los niveles de acceso infrecuente, incluidas las clases S3 Standard-Infrequent Access (IA) y S3 One Zone-IA, se transfieren al cargo de almacenamiento de S3 de acceso frecuente (se aplica a los niveles de Infrequent Access o Archive Instant Access).

No se admiten las clases de almacenamiento archivadas S3 Glacier Flexible Retrieval y S3 Glacier Deep Archive.

Para obtener más información acerca de los precios de almacenamiento para Amazon S3, consulte [Precios de Amazon S3](#).

Tipos de copia de seguridad de S3

Con él AWS Backup, puede crear los siguientes tipos de copias de seguridad de sus depósitos de S3, incluidos los datos de objetos, las etiquetas, las listas de control de acceso (ACLs) y los metadatos definidos por el usuario:

- Las copias de seguridad continuas le permiten realizar una restauración a cualquier momento de los últimos 35 días. Las copias de seguridad continuas de un bucket de S3 solo deben configurarse en un plan de copia de seguridad.

Consulte [Recuperación en un momento dado](#) para obtener una lista de los servicios compatibles e instrucciones sobre cómo utilizar AWS Backup para realizar copias de seguridad continuas.

- Las copias de seguridad periódicas utilizan instantáneas de sus datos para que pueda retenerlos durante un periodo especificado de hasta 99 años. Puede programar copias de seguridad periódicas en frecuencias de 1 hora, 12 horas, 1 día, 1 semana o 1 mes. AWS Backup realiza copias de seguridad periódicas durante el intervalo de copia de seguridad que defina en su [plan de copia de seguridad](#).

Consulte [Crear un plan de respaldo](#) para entender cómo AWS Backup se aplica el plan de respaldo a sus recursos.

Hay copias entre cuentas y regiones disponibles para las copias de seguridad de S3, pero las copias de las copias de seguridad continuas no tienen capacidades de point-in-time restauración.

Las copias de seguridad continuas y periódicas de los buckets de S3 deben residir en el mismo almacén de copias de seguridad.

AWS Backup para S3 se basa en la recepción de eventos de S3 a través de Amazon EventBridge. Si este ajuste está deshabilitado en la configuración de notificaciones del bucket de S3, se detendrán las copias de seguridad continuas de esos buckets con el ajuste desactivado. Para obtener más información, consulte [Uso EventBridge](#).

Para ambos tipos de copia de seguridad, la primera es una copia de seguridad completa, mientras que las copias de seguridad posteriores son incrementales a nivel de objeto.

Comparación de tipos de copia de seguridad de S3

Su estrategia de copia de seguridad de los recursos de S3 puede incluir solo copias de seguridad continuas, solo copias de seguridad periódicas (instantáneas) o una combinación de ambas. La siguiente información puede ayudarle a elegir lo que mejor se adapte a su organización:

Solo copias de seguridad continuas:

- Una vez finalizada la primera copia de seguridad completa de los datos existentes, se realiza un seguimiento de los cambios en los datos del bucket de S3 a medida que se producen.
- Los cambios registrados le permiten utilizar la PITR (point-in-time restauración) durante el período de retención de la copia de seguridad continua. Para realizar un trabajo de restauración, elija el momento al que desee realizar la restauración.
- El periodo de retención de cada copia de seguridad continua es de un máximo de 35 días.
- Para los planes de copia de seguridad que cree mediante CLI, la configuración de copia de seguridad avanzada para Amazon S3 (que incluye la opción de incluir etiquetas y ACLs en la copia de seguridad) está activada de forma predeterminada. Si lo desea, puede excluirla de las opciones de copia de seguridad. Para ver un ejemplo de sintaxis, consulte [Configuración avanzada de las copias de seguridad de Amazon S3](#).

Solo copias de seguridad periódicas (instantáneas), programadas o bajo demanda:

- AWS Backup escanea todo el depósito de S3, recupera la ACL y las etiquetas de cada objeto e inicia una solicitud Head para cada objeto que estaba en la instantánea anterior pero que no se encontró en la instantánea que se está creando.
- La copia de seguridad es coherente point-in-time.
- La fecha y la hora de la copia de seguridad registradas son la hora en la que se AWS Backup completa el recorrido del depósito, no la hora en que se creó la tarea de copia de seguridad.
- La primera copia de seguridad de un bucket es una copia de seguridad completa. Cada copia de seguridad posterior es incremental y representa el cambio en los datos desde la última instantánea.
- La instantánea realizada por la copia de seguridad periódica puede tener un periodo de retención de hasta 99 años.

Copias de seguridad continuas combinadas con periodic/snapshot copias de seguridad:

- Una vez finalizada la primera copia de seguridad completa de los datos existentes (cada bucket), se realiza un seguimiento de los cambios en el bucket a medida que se producen.
- Puede realizar una point-in-time restauración desde un punto de recuperación continua.
- Las instantáneas son point-in-time coherentes.
- Las instantáneas se toman directamente del punto de recuperación continuo, lo que elimina la necesidad de volver a escanear un bucket para facilitar procesos más rápidos.
- Las instantáneas y los puntos de recuperación continuos comparten un linaje de datos; el almacenamiento de datos entre puntos de recuperación continuos e instantáneas no se duplica.
- Cuando la configuración avanzada de las copias de seguridad de Amazon S3, como incluir etiquetas y ACLs en una copia de seguridad, se cambia por un continuous punto de recuperación, AWS Backup se detiene ese punto de recuperación y se crea uno nuevo con las configuraciones actualizadas.

Si se está ejecutando un trabajo de copia de seguridad continuo para un bucket de S3, puede iniciar igualmente los trabajos de copia de seguridad periódicos (instantáneas). Sin embargo, se aplica el siguiente comportamiento:

- Los trabajos de copia de seguridad instantánea utilizarán las mismas opciones de copia de seguridad (ACLs y la misma configuración de etiquetas de objetos) que la copia de seguridad continua existente.

- Si especifica opciones de copia de seguridad para el trabajo de instantánea distintas a las que utiliza la copia de seguridad continua, el trabajo de instantánea seguirá utilizando la configuración de la copia de seguridad continua y aparecerá el estado Completado con errores.

Cuando ocurra esto, verá el siguiente mensaje de estado: "Periodic/snapshot backup for bucket <bucket name> has different backup options than the continuous backup. When using continuous backups along with snapshot backups for the same bucket, the snapshot will use the same settings for backing up ACLs and Object tags as the continuous backup."

La siguiente tabla muestra cuándo es necesario realizar un análisis completo al cambiar BackupOptions los puntos de recuperación continua existentes:

Comportamiento del escaneo completo cuando BackupOptions se modifica

Anterior BackupOptions	Nuevo BackupOptions	Análisis completo
copia de seguridad ACLs y backupObjectTags activado	copia de seguridad ACLs y backupObjectTags deshabilitado	No
copia de seguridad ACLs y backupObjectTags activado	copia de seguridad ACLs habilitada; backupObjectTags deshabilitada	No
copia de seguridad ACLs y backupObjectTags activado	copia de seguridad ACLs deshabilitada; backupObjectTags habilitada	No
copia de seguridad ACLs y backupObjectTags deshabilitado	copia de seguridad ACLs y backupObjectTags activado	Sí
copia de seguridad ACLs habilitada; backupObjectTags deshabilitada	copia de seguridad ACLs y backupObjectTags activado	Sí

Anterior BackupOptions	Nuevo BackupOptions	Análisis completo
copia de seguridad ACLs deshabilitada; backupObjectTags habilitada	copia de seguridad ACLs y backupObjectTags activado	Sí

Intervalos de conclusión de la copia de seguridad de S3

La siguiente tabla muestra ejemplos de buckets de varios tamaños para ayudarle a estimar el tiempo de conclusión de la copia de seguridad completa inicial de un bucket de S3. Los tiempos de copias de seguridad variarán según el tamaño, el contenido, la configuración y los ajustes de cada bucket.

Tamaño del bucket	Número de objetos	Tiempo estimado para completar la copia de seguridad inicial
425 GB (gigabytes)	135 millones	31 horas
800 TB (terabytes)	670 millones	38 horas
6 PB (petabytes)	5000 millones	100 horas
370 TB (terabytes)	7500 millones	180 horas

Prácticas recomendadas y consideraciones de costos de las copias de seguridad de S3

Prácticas recomendadas con buckets grandes

Para buckets con más de 300 millones de objetos:

- En el caso de los buckets con más de 300 millones de objetos, la velocidad de copia de seguridad puede alcanzar hasta 17 000 objetos por segundo durante la copia de seguridad completa inicial del bucket (las copias de seguridad incrementales tendrán una velocidad diferente); las copias de seguridad de los buckets que contengan menos de 300 millones de objetos tendrán una velocidad cercana a los 1000 objetos por segundo.
- Se recomienda realizar copias de seguridad continuas.

- Si está previsto que el ciclo de vida de las copias de seguridad sea de más de 35 días, también puede habilitar copias de seguridad instantáneas para el bucket en el mismo almacén en el que se almacenan las copias de seguridad continuas.

Optimización de la estrategia de copia de seguridad

- En el caso de las cuentas que realizan copias de seguridad al menos a diario o con mayor frecuencia, puede ser beneficioso desde el punto de vista económico el uso de copias de seguridad continuas si los datos de las copias de seguridad sufren cambios mínimos entre las copias de seguridad.
- Los buckets más grandes que no cambian con frecuencia pueden beneficiarse de las copias de seguridad continuas, ya que esto puede reducir los costos cuando los escaneos de todo el bucket junto con numerosas solicitudes por objeto no necesitan realizarse en objetos preexistentes (objetos que permanecen inalterados desde la copia de seguridad anterior).
- Los buckets que contengan más de 100 millones de objetos y que tengan una tasa de eliminación pequeña en comparación con el tamaño total de la copia de seguridad pueden beneficiarse desde el punto de vista económico de un plan de copia de seguridad que incluya tanto una copia de seguridad continua con un periodo de retención de 2 días como instantáneas con una retención más prolongada.
- El tiempo de copia de seguridad periódica (instantánea) se alinea con el inicio del proceso de copia de seguridad cuando no es necesario escanear los buckets. No es necesario realizar escaneos en un bucket que contenga copias de seguridad continuas e instantáneas, ya que en estos casos las instantáneas se toman desde un punto de recuperación continua.

Ciclo de vida de los objetos y eliminación de marcadores

- Las políticas de ciclo de vida de S3 incluyen una característica opcional denominada Eliminar marcadores de eliminación de objetos vencidos. Cuando esta característica está desactivada, los marcadores de eliminación, que a veces son millones, vencen sin un plan de depuración. Cuando se hace una copia de seguridad de los buckets sin esta característica, hay dos problemas que afectan al tiempo y al costo:
 - Se hacen copias de seguridad de los marcadores de eliminación, al igual que de los objetos. El tiempo de copia de seguridad y el tiempo de restauración pueden verse afectados en función de la proporción entre objetos y marcadores de eliminación.

- Cada objeto y marcador del que se haga una copia de seguridad tiene un costo mínimo. Cada marcador de eliminación se cobra igual que un objeto de 128 KB.

Consideraciones de costos de las clases de almacenamiento

- Para cada objeto de un solo S3-GIR (Amazon S3 Glacier Instant Retrieval), AWS Backup realiza varias llamadas, lo que generará gastos de recuperación cuando se realice una copia de seguridad.

Se aplican costos de recuperación similares a los buckets con objetos de las clases de almacenamiento S3-IA y S3 One Zone-IA.

AWS optimización del costo del servicio

- El uso de funciones de AWS KMS Amazon CloudWatch y Amazon GuardDuty como parte de su estrategia de respaldo puede generar costos adicionales más allá del almacenamiento de datos en cubos de S3. CloudTrail Para obtener más información sobre cómo ajustar estas características, consulte lo siguiente:
 - [Reducción del costo de SSE-KMS con las claves de bucket de Amazon S3](#) en la Guía del usuario de Amazon S3.
- Puede reducir CloudTrail los costos excluyendo los AWS KMS eventos y deshabilitando los eventos de datos de S3:
 - Excluir AWS KMS eventos: en la Guía del CloudTrail usuario, al [crear una ruta en la consola \(selectores de eventos básicos\)](#), se ofrece la opción de excluir AWS KMS eventos para filtrarlos de la ruta (la configuración predeterminada incluye todos los eventos de KMS):
 - La opción para registrar o excluir eventos de KMS solo se encuentra disponible si registra eventos de administración en su registro de seguimiento. Si elige no registrar eventos de administración, no se registran eventos de KMS y no podrá cambiar la configuración del registro de eventos de KMS.
 - AWS KMS acciones como Encrypt, por ejemplo Decrypt, y GenerateDataKey suelen generar un gran volumen (más del 99%) de eventos. Estas acciones se registran ahora como eventos de lectura. Las acciones relevantes y de bajo volumen de KMS, como Disable, Delete y ScheduleKey (que normalmente representan menos del 0,5 % del volumen de eventos de KMS), se registran como eventos de Escritura.

- Para excluir eventos de gran volumen como Encrypt, Decrypt y GenerateDataKey, y seguir registrando eventos relevantes como Disable, Delete y ScheduleKey, elija registrar eventos de administración de Escritura y desmarque la casilla de verificación Excluir eventos de AWS KMS .
- Deshabilitar eventos de datos de S3: de forma predeterminada, los registros y los almacenes de datos de eventos no registran eventos de datos. Deshabilite los eventos de datos de S3 antes de la copia de seguridad inicial para reducir los costos.
- Para reducir CloudWatch los costes, puedes dejar de enviar CloudTrail eventos a CloudWatch los registros al actualizar un registro para deshabilitar la configuración de CloudWatch los registros.
- [Estimación GuardDuty del coste de uso](#) en la Guía del GuardDuty usuario de Amazon.

Mensajes de copia de seguridad de S3

Si un trabajo de copia de seguridad se completa o genera un error, puede aparecer el siguiente mensaje. La siguiente tabla puede ayudarlo a determinar la posible causa del mensaje de estado.

Escenario	Estado del trabajo	Mensaje	Ejemplo
No se ha podido realizar la copia de seguridad de todos los objetos para realizar una instantánea o una copia de seguridad continua inicial	FAILED	«No se realizó una copia de seguridad de ningún objeto desde el depósito <i>BucketName</i> de origen. To get notified of these failures, enable SNS event notifications”.	El rol de copia de seguridad no tiene permisos para obtener la ACL de la versión del objeto. Por lo tanto, no se hace ninguna copia de seguridad de ninguno de los objetos.
No se ha podido realizar la copia de seguridad de todos los objetos para realizar una copia de seguridad continua subsiguiente.	COMPLETED	«No se hizo una copia de seguridad de ningún objeto desde el depósito de origen <i>BucketName</i> . To get notified of these	

Escenario	Estado del trabajo	Mensaje	Ejemplo
		failures, enable SNS event notifications”.	

Configuración avanzada de las copias de seguridad de Amazon S3

AWS Backup proporciona ajustes avanzados para controlar los metadatos que se incluyen en las copias de seguridad de Amazon S3. Si lo desea, puede excluir las listas de control de acceso (ACLs) y las etiquetas de objetos, lo que puede resultar útil si los objetos están ACLs configurados sin etiquetas de objetos. En otras palabras, si no utiliza etiquetas de objetos ACLs o etiquetas para sus recursos de S3, puede resultarle útil excluirlas de las copias de seguridad.

Configurar la copia de seguridad de las etiquetas de objetos ACLs y las etiquetas

Puede configurar las opciones de copia de seguridad de las ACL y las etiquetas de objetos mediante la AWS Backup consola o mediante el AWS CLI.

Console

Configuración de las opciones de las ACL y las etiquetas mediante la consola

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup/>.
2. En el panel de navegación principal, elija Planes de copia de seguridad y, a continuación, elija Crear plan de copia de seguridad.
3. En la configuración de su plan de copia de seguridad, expanda Configuración avanzada de copia de seguridad.
4. Para los recursos de Amazon S3, configure las siguientes opciones:
 - Hacer copia de seguridad ACLs: seleccione la casilla de verificación para incluirlas ACLs o déjela sin seleccionar para excluirlas.

Copia de seguridad de las etiquetas de objetos: seleccione la casilla de verificación para incluir las etiquetas de objetos en la copia de seguridad.

5. Complete la configuración del plan de copia de seguridad y elija Crear plan.

AWS CLI

Puede incluir o excluir de forma selectiva las listas de control de acceso (ACLs) y las etiquetas de objetos de sus copias de seguridad de Amazon S3 mediante las siguientes opciones de copia de seguridad:

Backup ACLs

Controla si los objetos ACLs se incluyen en la copia de seguridad. `disabled` Configúrelo en Excluir ACLs. Valor predeterminado: `enabled`

BackupObjectTags

Controla si las etiquetas de los objetos se incluyen en la copia de seguridad. Configúrelo en `disabled` para excluir las etiquetas. Valor predeterminado: `enabled`

Configure las opciones de ACL y de etiqueta mediante AWS CLI

Para configurar las opciones de copia de seguridad de la ACL y las etiquetas de objetos mediante el AWS CLI, utilice el `update-backup-plan` comando con la configuración de copia de seguridad avanzada:

```
aws backup update-backup-plan \
  --backup-plan-id "your-backup-plan-id" \
  --backup-plan '{
    "BackupPlanName": "MyS3BackupPlan",
    "Rules": [{
      "RuleName": "MyS3BackupRule",
      "TargetBackupVaultName": "MyBackupVault",
      "ScheduleExpression": "cron(0 2 ? * * *)",
      "Lifecycle": {
        "DeleteAfterDays": 30
      },
      "RecoveryPointTags": {},
      "CopyActions": [],
      "EnableContinuousBackup": false
    }],
    "AdvancedBackupSettings": [{
      "ResourceType": "S3",
      "BackupOptions": {
        "BackupACLs": "disabled",
```

```
        "BackupObjectTags": "disabled"
    }
  ]
}'
```

Los parámetros BackupOptions controlan la inclusión de los metadatos:

- "BackupACLs": "disabled"- Excluye de las copias ACLs de seguridad
- "BackupObjectTags": "disabled": excluye las etiquetas de objetos de las copias de seguridad
- "BackupACLs": "enabled"- Se incluye ACLs en las copias de seguridad (predeterminado)
- "BackupObjectTags": "enabled": incluye las etiquetas de objetos en las copias de seguridad (opción predeterminada)

Copias de seguridad de Amazon Timestream

Amazon Timestream es una base de datos de serie temporal escalable que permite almacenar y analizar hasta billones de puntos de datos de serie temporal por día. Timestream se ha optimizado para ahorrar costos y tiempo, ya que mantiene los datos recientes en la memoria y almacena los datos históricos en un nivel de almacenamiento con costos optimizados de acuerdo con sus políticas.

Una base de datos de Timestream tiene tablas. Estas tablas contienen registros y cada registro es un único punto de datos de una serie temporal. Una serie temporal es una secuencia de registros registrados durante un intervalo de tiempo, como el precio de una acción, el nivel de uso de la memoria de una EC2 instancia de Amazon o una lectura de temperatura. AWS Backup puede realizar copias de seguridad y restaurar de forma centralizada las tablas de Timestream. Puede copiar estas copias de seguridad de las tablas a otras cuentas y a varias más Regiones de AWS de la misma organización.

Actualmente, Timestream no ofrece servicios nativos de copia de seguridad y restauración, por lo que AWS Backup utilizarlos para crear copias seguras de las tablas de Timestream puede añadir un nivel adicional de seguridad y resiliencia a sus recursos.

Copia de seguridad de tablas de Timestream

Puede hacer copias de seguridad de las tablas de Timestream a través de la consola o mediante. AWS Backup AWS CLI

Hay dos formas de utilizar la AWS Backup consola para hacer copias de seguridad de una tabla de Timestream: a pedido o como parte de un plan de copia de seguridad.

Creación de copias de seguridad de Timestream bajo demanda

1. [Abra la AWS Backup consola en /backup. https://console.aws.amazon.com](https://console.aws.amazon.com/backup)
2. En el panel de navegación, elija Recursos protegidos y Crear copia de seguridad bajo demanda.
3. En la página Crear copia de seguridad bajo demanda, elija Amazon Timestream.
4. Elija el Tipo de recurso Timestream y, a continuación, elija el nombre de la tabla de la que desea hacer una copia de seguridad.
5. En la ventana de copia de seguridad, asegúrese de que Crear copia de seguridad ahora esté seleccionado. De esta manera, se inicia una copia de seguridad de inmediato y puede ver antes los clústeres en la página Recursos protegidos.
6. En el menú desplegable Transferir al almacenamiento en frío, puede configurar los ajustes de transferencia.
7. En Periodo de retención, puede elegir durante cuánto tiempo desea conservar la copia de seguridad.
8. Elija un almacén de copias de seguridad existente o cree uno nuevo. Al elegir Create new backup vault (Crear nuevo almacén de copias de seguridad) se abre una nueva página para crear un almacén y a continuación, vuelve a la página Create on-demand backup (Crear copia de seguridad bajo demanda) cuando termine.
9. En Función de IAM, selecciona Función predeterminada (si la función AWS Backup predeterminada no está presente en tu cuenta, se creará automáticamente con los permisos correctos).
10. Si lo desea, puede agregar etiquetas a su punto de recuperación. Si desea asignar una o varias etiquetas a su copia de seguridad bajo demanda, introduzca una key (clave) y un value (valor) opcional y elija Add tag (Añadir etiqueta).
11. Seleccione Create on-demand backup (Crear copia de seguridad bajo demanda). Esto le lleva a la página Jobs (Trabajos), donde verá una lista de trabajos.
12. Elija el ID de trabajo de copia de seguridad del clúster para ver los detalles de ese trabajo. Mostrará un estado de Completed, In Progress o Failed. Haga clic en el botón de actualización para actualizar el estado.

Creación de copias de seguridad programadas de Timestream en un plan de copia de seguridad

Las copias de seguridad programadas pueden incluir tablas de Timestream si son un recurso protegido. Para optar por la protección de las tablas de Amazon Timestream:

1. Abre la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, elija Recursos protegidos.
3. Mueva a la posición de activación el conmutador de Amazon Timestream.
4. Consulte [Asignación de recursos mediante la consola](#) para incluir las tablas de Timestream en un plan nuevo o existente.

En Administrar planes de copia de seguridad, puede elegir [crear un plan de copia de seguridad](#) e incluir tablas de Timestream o [actualizar uno existente](#) para que incluya tablas de Timestream. Al agregar el tipo de recurso Timestream, puede optar por agregar Todas las tablas de Timestream o marcar las casillas situadas junto a las tablas que desee agregar en Seleccionar tipos de recursos específicos.

La primera copia de seguridad que se haga con tablas de Timestream será una copia de seguridad completa. Las copias de seguridad posteriores serán copias de seguridad incrementales.

Una vez que haya creado o modificado su plan de copia de seguridad, vaya a Planes de copia de seguridad en el menú de navegación de la izquierda. El plan de copia de seguridad que especificó debe mostrar sus clústeres en Asignaciones de recursos.

Copia de seguridad mediante programación

También puede utilizar la operación denominada `start-backup-job`. Incluya los siguientes parámetros:

```
aws backup start-backup-job \  
--backup-vault-name backup-vault-name \  
--resource-arn arn:aws:timestream:region:account:database/database-name/table/table-name \  
--iam-role-arn arn:aws:iam::account:role/role-name \  
--region Región de AWS \  
--endpoint-url URL
```

Visualización de las copias de seguridad de las tablas de Timestream

Para ver y modificar las copias de seguridad de las tablas de Timestream en la consola:

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. Elija Almacenes de Backup. A continuación, haga clic en el nombre del almacén de copias de seguridad que contiene las tablas de Timestream.
3. El almacén de copias de seguridad mostrará un resumen y una lista de copias de seguridad.
 - a. Puede hacer clic en el enlace de la columna ID de punto de recuperación, o
 - b. Puede marcar la casilla situada a la izquierda del ID de punto de recuperación y hacer clic en Acciones para eliminar los puntos de recuperación que ya no sean necesarios.

Restauración de una tabla de Timestream

Consulte cómo [restaurar una tabla de Timestream](#).

Copias de seguridad de máquinas virtuales

AWS Backup admite la protección de datos centralizada y automatizada para las máquinas VMware virtuales locales (VMs) junto con las aplicaciones VMs In the VMware Cloud™ (VMC) on AWS y VMware Cloud™ (VMC) on. AWS Outposts Puede realizar copias de seguridad desde sus máquinas virtuales locales y de VMC hasta. AWS Backup A continuación, puede realizar la restauración de AWS Backup forma local VMs, VMs en el VMC o en el VMC activado. AWS Outposts

AWS Backup también le proporciona funciones de gestión de copias de seguridad de máquinas virtuales AWS nativas y totalmente gestionadas, como la detección de máquinas virtuales, la programación de copias de seguridad, la gestión de la retención, un nivel de almacenamiento de bajo coste, copia entre regiones y entre cuentas, compatibilidad con AWS Backup Vault Lock y Audit Manager AWS Backup , cifrado independiente de los datos de origen y políticas de acceso a las copias de seguridad. Consulte la tabla [Disponibilidad de características por recurso](#) para obtener una lista completa de capacidades y detalles.

[Puede utilizarlas AWS Backup para proteger sus máquinas virtuales en Cloud™ onVMware . AWS Outposts](#) AWS Backup almacena las copias de seguridad de sus máquinas virtuales en la Región de AWS que AWS Outposts está conectado su VMware Cloud™ on. Puedes usarlo AWS Backup para proteger tu VMware Cloud™ on AWS Backup VMs cuando usas VMware Cloud™ on AWS Outposts para satisfacer tus necesidades de procesamiento de datos local y de baja latencia para los datos de tus aplicaciones. En función de tus requisitos de residencia de datos, puedes optar por AWS Backup almacenar las copias de seguridad de los datos de tu aplicación en el servidor principal Región de AWS al que estés conectado AWS Outposts .

Compatible VMs

AWS Backup puede realizar copias de seguridad y restaurar máquinas virtuales administradas por una instancia VMware vCenter.

Se admite actualmente:

- vSphere 8, 7.0 y 6.7
- Tamaños de disco virtual que son múltiplos de 1 KiB
- Almacenes de datos de NFS, VMFS y VSAN en las instalaciones y en VMC en AWS
- Modos de transporte SCSI Hot-Add y Network Block Device Secure Sockets Layer (NBDSSL) para copiar datos del origen a otros de forma local VMs AWS VMware
- Modo Hot-Add para proteger en Cloud On VMs VMware AWS

No se admiten actualmente:

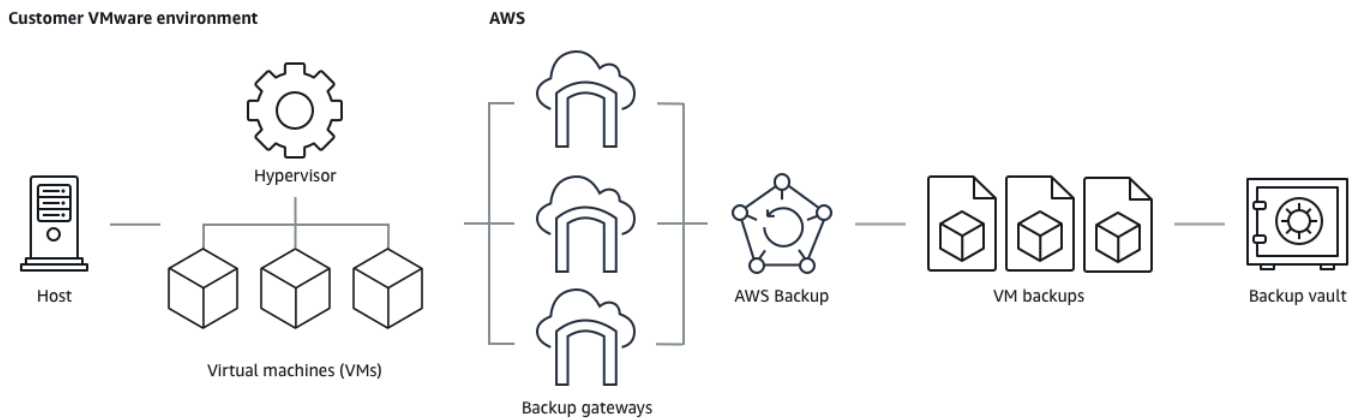
- Discos o NVMe controladores RDM (mapeo de discos sin procesar) y sus discos
- Máquinas virtuales con modos de disco independiente-persistente e independiente-no persistente

Coherencia de la copia de seguridad

AWS Backup, de forma predeterminada, captura copias de seguridad coherentes con las aplicaciones cuando se VMs utiliza la configuración de inactividad de las VMware herramientas en la máquina virtual. Sus copias de seguridad son coherentes con las aplicaciones si estas son compatibles con Tools. VMware Si la función de inactividad no está disponible, AWS Backup captura copias de seguridad consistentes en caso de fallos. Pruebe sus restauraciones para comprobar que las copias de seguridad cumplan con las necesidades de la organización.

Puerta de enlace de copia de seguridad

Backup Gateway es un AWS Backup software descargable que puede implementar en su VMware infraestructura para conectarse VMware VMs a ella AWS Backup. La puerta de enlace se conecta a su servidor de administración de máquinas virtuales para detectarlas VMs VMs, descubrirlas, cifrarlas y transferirlas de manera eficiente. AWS Backup El siguiente diagrama ilustra cómo Backup Gateway se conecta a su VMs:



Para descargar el software de puerta de enlace de copia de seguridad, siga el procedimiento para [Uso de puertas de enlace](#).

Descargue el software VM

Backup Gateway se distribuye como una plantilla de OVF (Open Virtualization Format) que puede implementar en su VMware infraestructura. El software de puerta de enlace VMware VMs lo conecta AWS Backup descubriendo VMs, cifrando datos y transfiriéndolos de manera eficiente. AWS Backup

Para obtener la plantilla OVF, utilice la AWS Backup consola:

1. Inicie sesión en la consola AWS de administración y abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación izquierdo, en Recursos externos, selecciona Puertas de enlace.
3. Seleccione Crear puerta de enlace.
4. En la sección Configurar puerta de enlace, descargue la plantilla de OVF e impleméntela en su VMware entorno.

[Para obtener información sobre los puntos finales de VPC \(nube privada virtual\), consulte AWS Backup conectividad. AWS PrivateLink](#)

La puerta de enlace de copia de seguridad incluye su propia API, que se mantiene por separado de la API de AWS Backup . Para ver una lista de las acciones de la API de la puerta de enlace de copia de seguridad, consulte [Acciones de la puerta de enlace de copia de seguridad](#). Para ver una lista de los tipos de datos de la API de la puerta de enlace de copia de seguridad, consulte [Tipos de datos de la puerta de enlace de copia de seguridad](#).

Puntos de conexión

Los usuarios existentes que actualmente utilizan un punto de conexión público y que desean cambiar a un punto de conexión de VPC (nube privada virtual) pueden [crear una nueva puerta de enlace con un punto de conexión de VPC](#) mediante [AWS PrivateLink](#), asociar el hipervisor existente a la puerta de enlace y, a continuación, [eliminar la puerta de enlace](#) que contiene el punto de conexión público.

Configuración de la infraestructura para usar una puerta de enlace de copia de seguridad

La puerta de enlace de copia de seguridad requiere las siguientes configuraciones de red, firewall y hardware para realizar copias de seguridad y restaurar las máquinas virtuales.

Configuración de red

La puerta de enlace de copia de seguridad requiere que se permita el funcionamiento de determinados puertos. Permita los siguientes puertos:

1. TCP 443 saliente

- Origen: puerta de enlace de copia de seguridad
- Destino: AWS
- Uso: Permite que Backup Gateway se comunique con AWS.

2. TCP 80 entrante

- Fuente: el host que utiliza para conectarse al Consola de administración de AWS
- Destino: puerta de enlace de copia de seguridad
- Uso: usado por los sistemas locales para obtener la clave de activación de la puerta de enlace de copia de seguridad. El puerto 80 solo se usa durante la activación de Backup Gateway. AWS Backup no requiere que el puerto 80 sea de acceso público. El nivel de acceso exigido al puerto 80 depende de la configuración de la red. Si activa la puerta de enlace desde el Consola de administración de AWS, el host desde el que se conecta a la consola debe tener acceso al puerto 80 de la puerta de enlace.

3. UDP 53 saliente

- Origen: puerta de enlace de copia de seguridad
- Destino: servidor del servicio de nombres de dominio (DNS)
- Uso: permite que la puerta de enlace de copia de seguridad se comunique con el DNS.

4. TCP 22 saliente

- Origen: puerta de enlace de copia de seguridad
- Destino: Soporte
- Uso: permite acceder Soporte a su puerta de enlace para ayudarlo con los problemas. No necesita abrir este puerto para el funcionamiento normal de la puerta de enlace, pero es necesario para la solución de problemas.

5. UDP 123 saliente

- Origen: cliente NTP
- Destino: servidor NTP
- Uso: utilizado por los sistemas locales para sincronizar la hora de la VM con la hora del host.

6. TCP 443 saliente

- Origen: puerta de enlace de copia de seguridad
- Destino: VMware vCenter
- Uso: permite que Backup Gateway se comunice con VMware vCenter.

7. TCP 443 saliente

- Origen: puerta de enlace de copia de seguridad
- Destino: hosts ESXi
- Uso: permite que Backup Gateway se comunice con ESXi los hosts.

8. TCP 902 saliente

- Origen: puerta de enlace de copia de seguridad
- Destino: VMware ESXi anfitriones
- Uso: se utiliza para la transferencia de datos a través de la puerta de enlace de copia de seguridad.

Los puertos anteriores son necesarios para Backup Gateway. Consulte [Creación de un punto de conexión de VPC](#) para obtener más información sobre cómo configurar los puntos de conexión de Amazon VPC para AWS Backup.

Configuración del firewall

Backup Gateway requiere acceso a los siguientes puntos finales de servicio para poder comunicarse con Amazon Web Services ellos. Si utiliza un firewall o un router para filtrar o limitar el tráfico de red, debe configurar el firewall y el router para dar permiso a los puntos de conexión de servicio para

mantener comunicaciones de salida con AWS. No se admite el uso de un proxy HTTP entre la puerta de enlace de copia de seguridad y los puntos de servicio.

Tipos de terminales

Puntos finales estándar: Support IPv4 tráfico entre su dispositivo de puerta de enlace y AWS.

Los siguientes puntos de conexión de servicio son necesarios para todas las puertas de enlace para operaciones de ruta de control (anon-cp, client-cp y proxy-app) y de ruta de datos (dp-1).

```
anon-cp.backup-gateway.region.amazonaws.com:443  
client-cp.backup-gateway.region.amazonaws.com:443  
proxy-app.backup-gateway.region.amazonaws.com:443  
dp-1.backup-gateway.region.amazonaws.com:443
```

Terminales de doble pila: Support tanto como el IPv6 tráfico entre su dispositivo de puerta de enlace IPv4 y. AWS

Todas las puertas de enlace requieren los siguientes puntos de conexión de servicio de doble pila para las operaciones de ruta de control (activación, plano de control y proxy) y de ruta de datos (plano de datos).

```
activation-backup-gateway.region.api.aws:443  
controlplane-backup-gateway.region.api.aws:443  
proxy-backup-gateway.region.api.aws:443  
dataplane-backup-gateway.region.api.aws:443
```

Configure su puerta de enlace para múltiples entradas NICs VMware

Puede mantener redes separadas para el tráfico interno y externo conectando varias conexiones de interfaz de red virtual (NICs) a la puerta de enlace y, a continuación, dirigiendo el tráfico interno (de la puerta de enlace al hipervisor) y el tráfico externo (de la puerta de enlace a AWS) por separado.

De forma predeterminada, las máquinas virtuales conectadas a la AWS Backup puerta de enlace tienen un adaptador de red (`eth0`). Esta red incluye el hipervisor, las máquinas virtuales y la puerta de enlace de red (Backup Gateway) que se comunica con el resto de Internet.

A continuación, se muestra un ejemplo de una configuración con varias interfaces de red virtuales:

```
eth0:
```

```
- IP: 10.0.3.83
- routes: 10.0.3.0/24

eth1:
- IP: 10.0.0.241
- routes: 10.0.0.0/24
- default gateway: 10.0.0.1
```

- En este ejemplo, la conexión es a un hipervisor con IP 10.0.3.123, la puerta de enlace utilizará eth0 ya que la IP del hipervisor forma parte del bloque 10.0.3.0/24
- Para conectarse a un hipervisor con IP 10.0.0.234, la puerta de enlace utilizará eth1
- Para conectarse a una IP fuera de las redes locales (p. ej. 34.193.121.211), la puerta de enlace volverá a la puerta de enlace predeterminada, 10.0.0.1, que está en el bloque 10.0.0.0/24 y, por lo tanto, pasará por eth1

La primera secuencia para agregar un adaptador de red adicional se produce en el cliente de vSphere:

1. En el cliente VMware vSphere, abra el menú contextual (haciendo clic con el botón derecho) de la máquina virtual de puerta de enlace y seleccione Editar configuración.
2. En la pestaña Virtual Hardware del cuadro de diálogo Virtual Machine Properties, abra el menú Add New Device y seleccione Network Adapter para agregar un nuevo adaptador de red.
3.
 - a. Amplíe los detalles de New Network para configurar el nuevo adaptador.
 - b. Asegúrese de que la opción Connect At Power On esté seleccionada.
 - c. Para obtener información sobre el tipo de adaptador, consulte Tipos de adaptadores de red en [ESXi la documentación de vCenter Server](#).
4. Haga clic en Okay para guardar la nueva configuración del adaptador de red.

La siguiente secuencia de pasos para configurar un adaptador adicional se realiza en la consola de AWS Backup puerta de enlace (tenga en cuenta que no es la misma interfaz que la consola de AWS administración, donde se administran las copias de seguridad y otros servicios).

Una vez que se agregue la nueva NIC a la máquina virtual de puerta de enlace, debe

- Ir a Command Prompt y encender los nuevos adaptadores.
- Configure la estática IPs para cada NIC nueva

- Establecer la NIC preferida como predeterminada

Para ello:

1. En el cliente VMware vSphere, seleccione la máquina virtual de puerta de enlace e inicie Web Console para acceder a la consola local de Backup Gateway.
 - Para obtener más información sobre cómo acceder a una consola local, consulte [Acceder a la consola local de Gateway](#) con VMware ESXi
2. Salga de la línea de comandos y vaya a Configuración de red > Configurar IP estática y siga las instrucciones de configuración para actualizar la tabla de enrutamiento.
 - a. Asigne una IP estática dentro de la subred del adaptador de red.
 - b. Establezca una máscara de red.
 - c. Elija la dirección IP de la puerta de enlace de aparece por defecto. Esta es la puerta de enlace de red que se conecta a todo el tráfico fuera de la red local.
3. Seleccione Establecer adaptador predeterminado para designar el adaptador que se conectará a la nube como dispositivo predeterminado.
4. Todas las direcciones IP de la puerta de enlace se pueden mostrar tanto en la consola local como en la página de resumen de la máquina virtual en VMware vSphere.

VMware permisos

En esta sección se enumeran los VMware permisos mínimos necesarios para su uso AWS Backup gateway. Estos permisos son necesarios para que la puerta de enlace de copia de seguridad detecte, realice copias de seguridad y restaure máquinas virtuales.

Para usar Backup Gateway con VMware Cloud™ activado AWS o VMware Cloud™ activado AWS Outposts, debe usar el usuario administrador predeterminado `cloudadmin@vmc.local` o asignar la CloudAdmin función a su usuario dedicado.

Para usar Backup Gateway con VMware máquinas virtuales locales, cree un usuario dedicado con los permisos que se indican a continuación.

Global

- Deshabilitar métodos
- Habilitar métodos

- Licencias
- Registrar eventos
- Administrar atributos personalizados
- Establecer atributos personalizados

Etiquetar vSphere

- Asignar o anular la asignación de etiquetas de vSphere

DataStore

- Asignar espacio
- Explorar el almacén de datos
- Configurar el almacén de datos (para el almacén de datos de vSAN)
- Operaciones de archivos de bajo nivel
- Actualizar los archivos de la máquina virtual

Host

- Configuración
 - Configuración avanzada
 - Configuración de la partición de almacenamiento

Carpeta

- Crear carpeta

Network

- Asignar red

Grupo de dvPort

- Crear

- Eliminar

Recurso

- Asignar una máquina virtual al grupo de recursos

Máquina virtual

- Cambio de configuración
 - Adquirir un arrendamiento de disco
 - Agregar un disco existente
 - Agregar un disco nuevo
 - Configuración avanzada
 - Cambiar la configuración del .
 - Configurar dispositivo sin procesar
 - Modificar la configuración del dispositivo
 - Eliminar un disco
 - Establecer anotación
 - Activar el seguimiento de cambios de disco
- Editar inventario
 - Crear desde elemento existente
 - Crear nuevo
 - Regístrese
 - Quitar
 - Anular registro
- Interacción
 - Apagar
 - Encender
- Aprovisionar
 - Permitir acceso al disco
 - Permitir acceso de solo lectura al disco
 - Permitir la descarga de la máquina virtual

- Administración de instantáneas
 - Crear una instantánea
 - Eliminar instantánea
 - Revertir a la instantánea

Uso de puertas de enlace

Para realizar copias de seguridad y restaurar sus máquinas virtuales (VMs) mediante AWS Backup, primero debe instalar una puerta de enlace de respaldo. Una puerta de enlace es un software en forma de plantilla OVF (Open Virtualization Format) que conecta Amazon Web Services Backup con su hipervisor, lo que le permite detectar automáticamente sus máquinas virtuales y le permite realizar copias de seguridad y restaurarlas.

Una sola puerta de enlace puede ejecutar hasta 4 trabajos de copia de seguridad o restauración a la vez. Para ejecutar más de 4 trabajos a la vez, cree más puertas de enlace y asócielas al hipervisor.

Creación de una puerta de enlace

Puede crear una puerta de enlace de respaldo mediante dos enfoques:

- Método de consola (estándar): crea puertas IPv4 de enlace exclusivas a través de la AWS Backup consola con activación automática
- Método manual: admite tanto la obtención IPv4 de claves IPv6 de activación como el uso de comandos AWS CLI

Ambos métodos requieren descargar e implementar primero la plantilla de OVF (consulte [Descargue el software VM](#)).

Método de consola (IPv4 únicamente)

Utilice este método para crear una IPv4 puerta de enlace estándar a través de la AWS Backup consola con activación automática.

Para crear una puerta de enlace:

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación de la izquierda, en la sección Recursos externos, elija Puertas de enlace.

3. Seleccione Crear puerta de enlace.
4. En la sección Configurar puerta de enlace, siga estas instrucciones para descargar e implementar la plantilla de OVF.

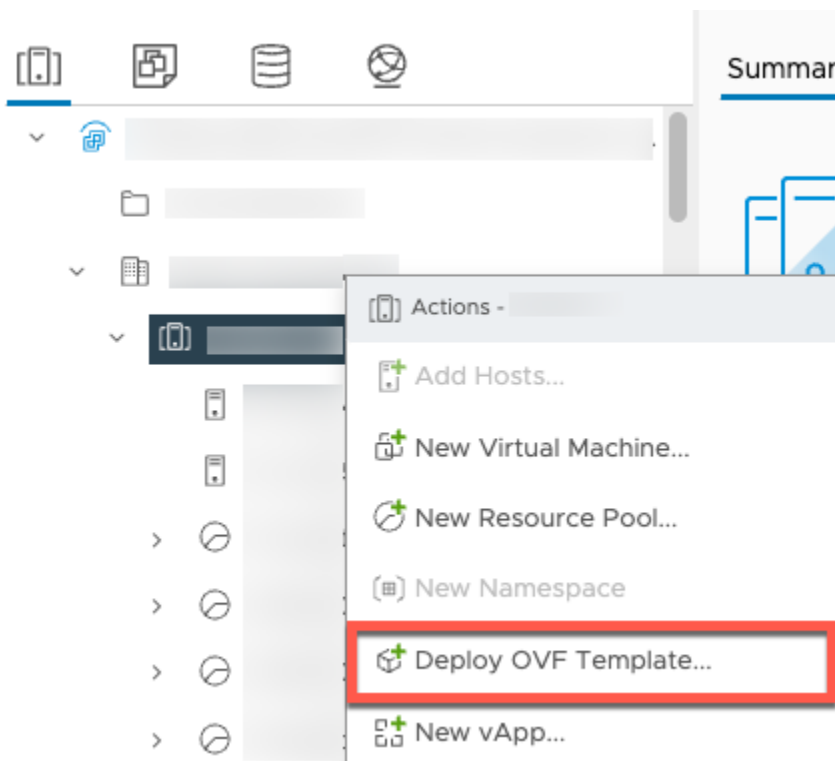
Descargando software VMware

Conexión con el hipervisor

Las pasarelas AWS Backup se conectan al hipervisor para que pueda crear y almacenar copias de seguridad de sus máquinas virtuales. Para configurar su puerta de enlace VMware ESXi, descargue la plantilla [de OVF](#). El proceso de descarga puede llevar unos 10 minutos.

Una vez que se haya completado, continúe con los siguientes pasos:

1. Conéctese al hipervisor de su máquina virtual mediante VMware vSphere.
2. Haga clic con el botón derecho en un objeto principal de una máquina virtual y seleccione Implementar plantilla de OVF.



3. Elija Archivo local y cargue el aws-appliance-latestarchivo.ova que descargó.

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

☐ URL

☒ Local file

aws-appliance-latest.ova

4. Siga los pasos del asistente de implementación para implementarlo. En la página Seleccionar almacenamiento, seleccione el formato de disco virtual Thick Provision Lazy Zeroed.

Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- Select storage**
- Select networks
- Ready to complete

Select storage

Select the storage for the configuration and disk files

Select virtual disk format

VM Storage Policy

☐ Disable Storage DRS for this VM

☒ Thick Provision Lazy Zeroed

☐ Thin Provision

☐ Thick Provision Eager Zeroed

Default

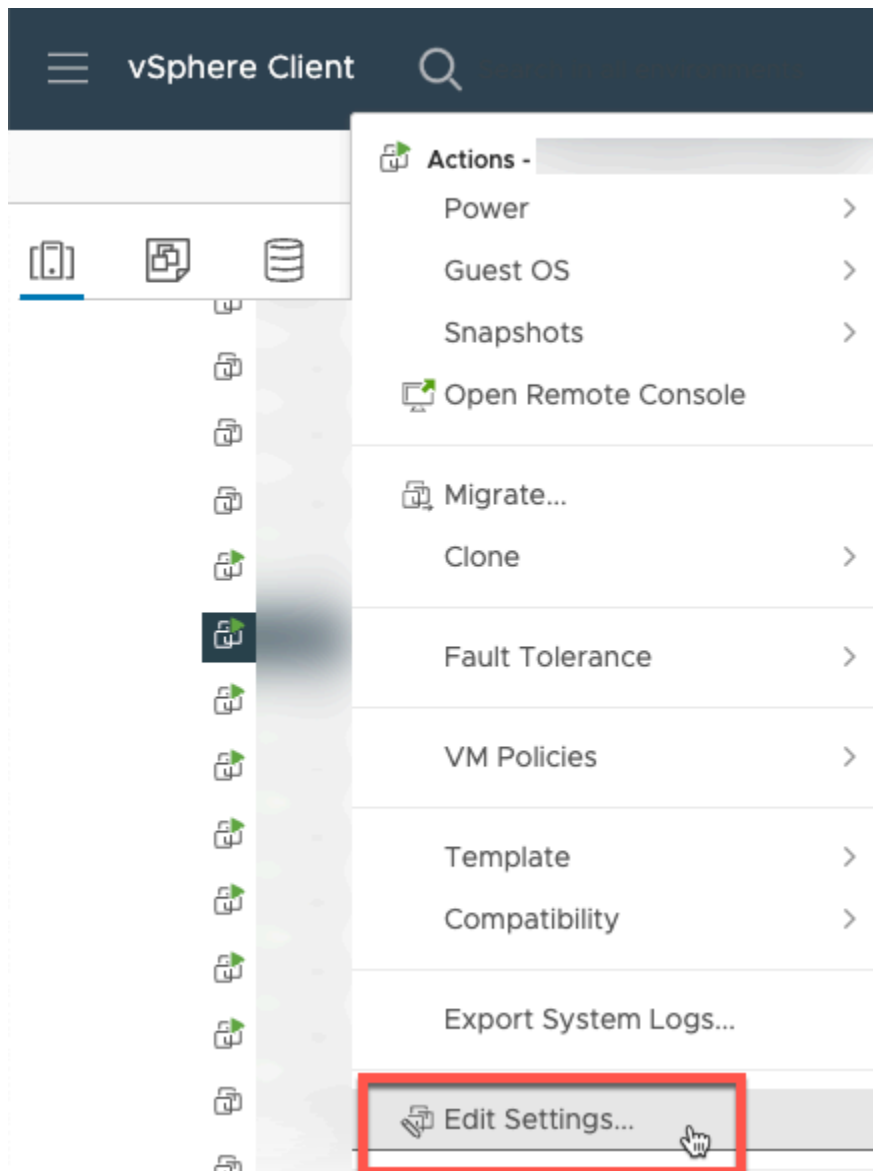
	Name	Storage Compatibility	Capacity	Provisioned	Free	Type	Placement
☐	vsanDatastore	--	20.74 TB	8.72 TB	13.37 TB	vSAN	Local
☐	WorkloadDatasto...	--	20.74 TB	67.44 TB	13.37 TB	vSAN	Local

2 Items

Compatibility

CANCEL BACK NEXT

- Tras implementar el OVF, haga clic con el botón derecho en la puerta de enlace y elija Editar configuración.



- a. En Opciones de máquina virtual, vaya a Herramientas de máquina virtual.
- b. Asegúrese de que en Sincronizar la hora con el host, esté seleccionada la opción Sincronizar al inicio y al reanudar.

Edit Settings

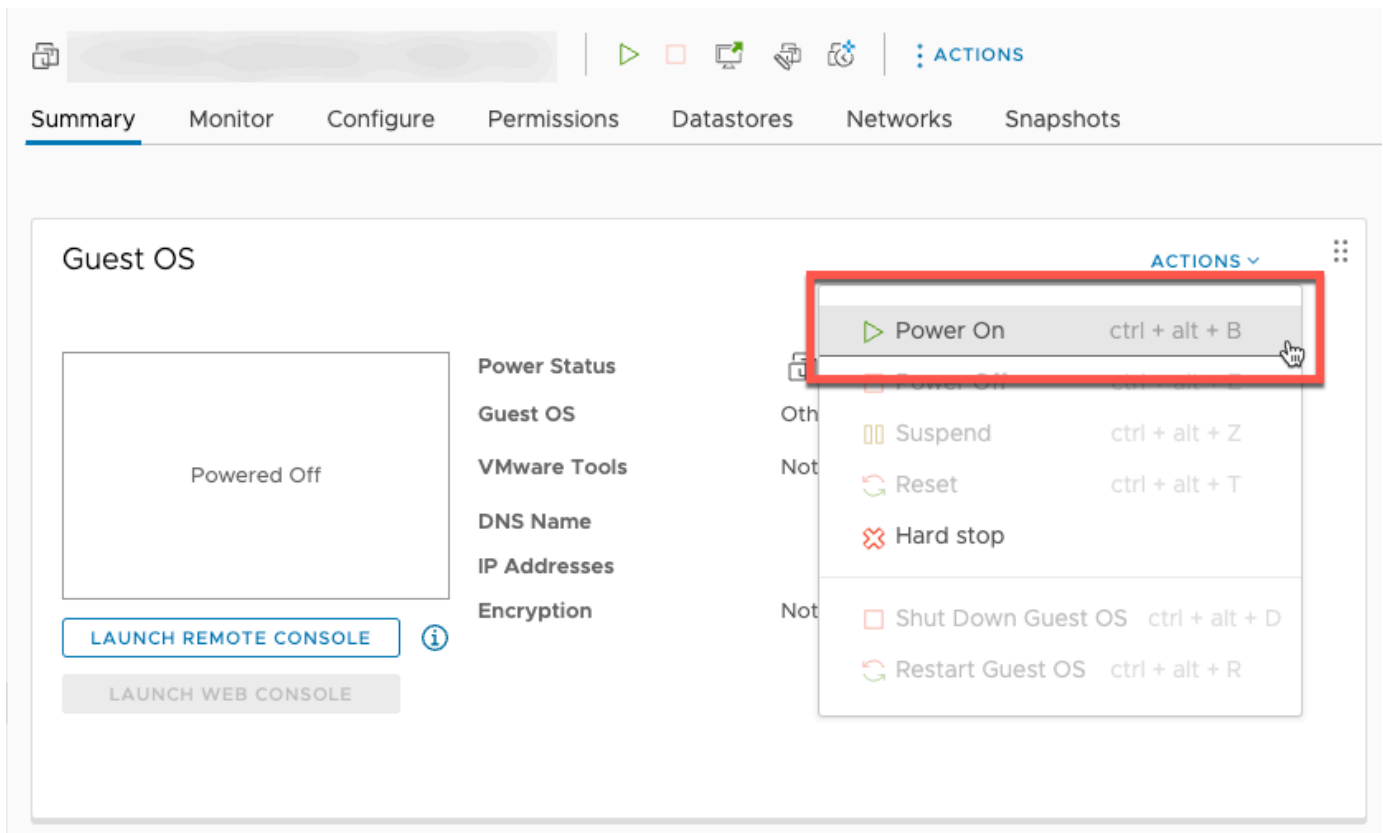
Virtual Hardware | **VM Options**

> General Options	VM Name:
VMware Remote Console Options	☐
>	Lock the guest operating system when the last remote user disconnects
> Encryption	Expand for encryption settings
> Power management	Expand for power management settings
▼ VMware Tools	
Power Operations	▶ Power On / Resume VM ◻ Shut Down Guest (Default) ▼ ⏸ Suspend (Default) ▼ ↺ Restart Guest (Default) ▼
Tools Upgrades	☐ Check and upgrade VMware Tools before each power on
Synchronize Time with Host ⓘ	☒ Synchronize at startup and resume (recommended) ☐ Synchronize time periodically
Run VMware Tools Scripts	☒ After powering on ☒ After resuming ☒ Before suspending ☒ Before shutting down guest

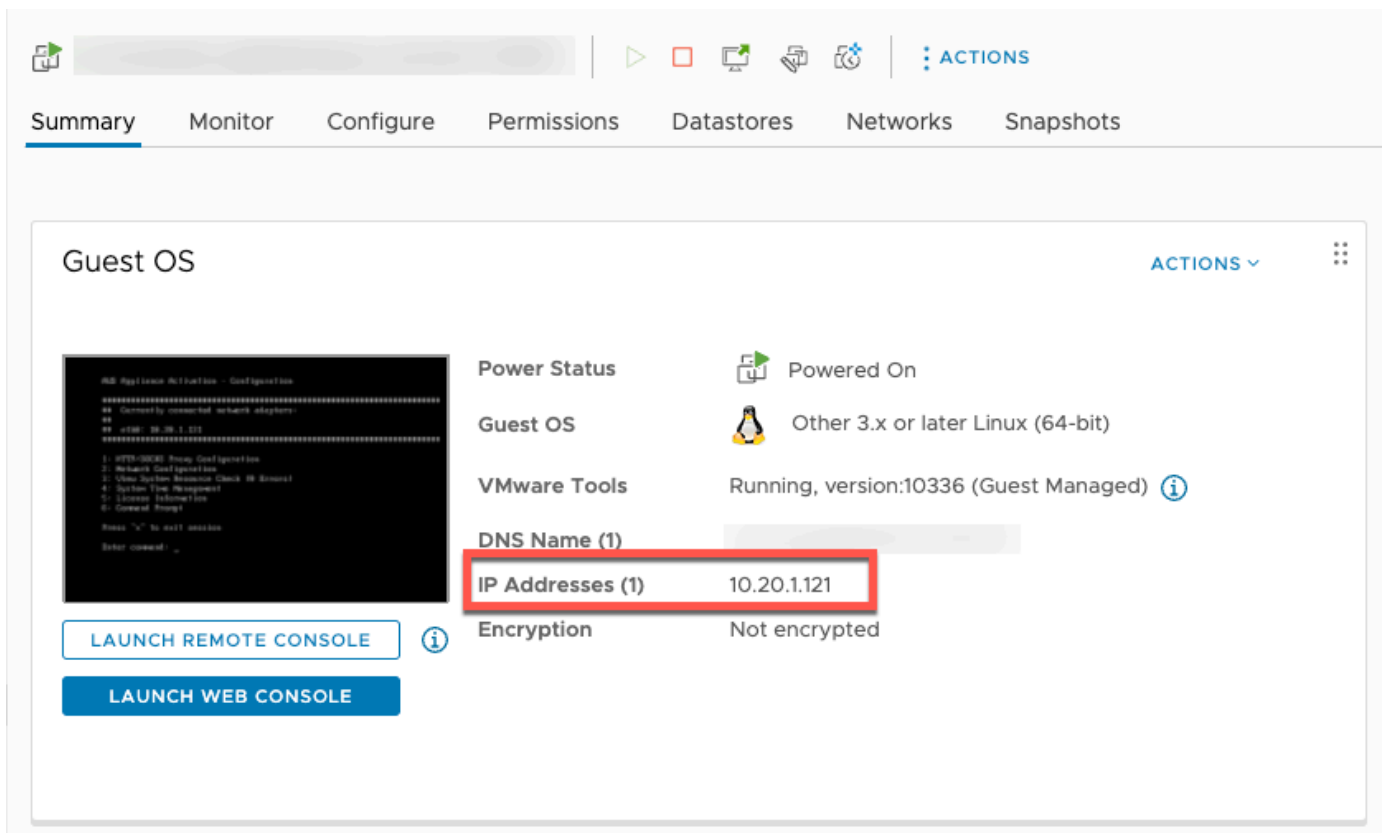
CANCEL

OK

6. Encienda la máquina virtual con la opción de encender en el menú Acciones.



7. Copie la dirección IP del resumen de la máquina virtual e introdúzcala a continuación.



Una vez descargado el VMWare software, complete los siguientes pasos:

1. En la sección Conexión de la puerta de enlace, escriba la dirección IP de la puerta de enlace.
 - a. Para buscar esta dirección IP, vaya a vSphere Client.
 - b. Seleccione su puerta de enlace en la pestaña Resumen.
 - c. Copie la dirección IP y péguela en la barra de texto de la AWS Backup consola.
2. En la sección Configuración de puerta de enlace,
 - a. Escriba el Nombre de la puerta de enlace.
 - b. Compruebe la AWS región.
 - c. Elija si el punto de conexión es de acceso público o está alojado en su nube privada virtual (VPC).
 - d. Según el punto de conexión elegido, introduzca el nombre de DNS del punto de conexión de la VPC.

Para obtener más información, consulte [Creación de un punto de conexión de VPC](#).

3. [Opcional] En la sección Etiquetas de puerta de enlace, puede asignar etiquetas si introduce la clave y el valor opcional. Para agregar más de una etiqueta, haga clic en Agregar otra etiqueta.
4. Para completar el proceso, haga clic en Crear puerta de enlace, que lo llevará a la página de detalles de la puerta de enlace.

Creación manual de puertas de enlace (IPv4 y IPv6)

Para obtener IPv6 asistencia, cree puertas de enlace manualmente con las claves de activación.

IPv6 [el soporte requiere la versión 2.x+ del dispositivo de puerta de enlace y una configuración de firewall adicional en los puntos finales de doble pila.](#)

Important

IPv6 requisito de hipervisor: si su puerta de enlace está activada a través de ella IPv6, debe crear un hipervisor con una dirección. IPv6 Por ejemplo, utilice 2607:fda8:1001:210::252 en lugar de 10.0.0.252. Si asocia una IPv6 puerta de enlace a un IPv4 hipervisor, es probable que se produzcan errores en las tareas de copia de seguridad y restauración.

Obtención de una clave de activación

Para recibir una clave de activación para la puerta de enlace, realice una solicitud web a la máquina virtual (VM) de la puerta de enlace o utilice la consola local de la puerta de enlace. La máquina virtual de la puerta de enlace devuelve una respuesta que contiene la clave de activación, que luego se transfiere como uno de los parámetros para que la CreateGateway API especifique la configuración de la puerta de enlace.

Tip

Las claves de activación de la puerta de enlace caducan en 30 minutos si no se utilizan.

Obtener una clave de activación mediante una solicitud web

Los siguientes ejemplos muestran cómo obtener una clave de activación mediante una solicitud HTTP. Puede utilizar un navegador web o un curl de Linux o un comando equivalente de la siguiente URLs manera.

Note

Sustituya las variables resaltadas por valores reales de la puerta de enlace. Los valores aceptables son los siguientes:

- *gateway_ip_address*- La IPv4 dirección de su puerta de enlace, por ejemplo 172.31.29.201
- *region_code*- La región en la que quieres activar tu puerta de enlace. Consulte [Puntos de conexión regionales](#) en la Guía de referencia general de AWS . Si no se especifica este parámetro o si el valor proporcionado está mal escrito o no coincide con una región válida, el comando utilizará la región us-east-1 de forma predeterminada.

Terminales de doble pila (compatibles) IPv6

IPv4:

```
curl "http://gateway_ip_address?  
activationRegion=region_code&gatewayType=BACKUP_VM&endpointType=DUALSTACK&ipVersion=ipv4&no_red
```

IPv6:

```
curl "http://gateway_ip_address?  
activationRegion=region_code&gatewayType=BACKUP_VM&endpointType=DUALSTACK&ipVersion=ipv6&no_red
```

Obtener una clave de activación mediante la consola local

Los siguientes ejemplos muestran cómo obtener una clave de activación mediante la consola local del host de la puerta de enlace

1. Inicie sesión en la consola de su máquina virtual.
2. En el menú principal Activación y configuración del AWS dispositivo, seleccione 0 Obtener la clave de activación
3. Seleccione 2 Backup Gateway como opción de familia de puertas de enlace
4. Introduzca la AWS región en la que desea activar la puerta de enlace
5. Para el tipo de red, introduzca 1 para punto final público o 2 VPC
6. Para el tipo de punto final, introduzca 1 para punto final estándar o punto final 2 de doble pila
 - Para el punto final de doble pila, seleccione 1 para o para IPv4 2 IPv6
7. La clave de activación se rellenará automáticamente

Creando la puerta de enlace

Utilice AWS CLI para crear la puerta de enlace después de obtener una clave de activación:

1. Obtenga la clave de activación mediante los comandos curl o el método de la consola local
2. Cree una puerta de enlace utilizando AWS CLI, para obtener más información, consulte [CreateGateway](#) la Referencia de la API de Backup Gateway.

```
aws backup-gateway create-gateway \  
    --region region_code \  
    --activation-key activation_key \  
    --gateway-display-name gateway_name \  
    --gateway-type BACKUP_VM
```

3. Compruebe que la puerta de enlace aparezca en AWS Backup la consola en Recursos externos
→ Puertas de enlace

Edición o eliminación de una puerta de enlace

Para editar o eliminar una puerta de enlace:

1. En el panel de navegación de la izquierda, en la sección Recursos externos, elija Puertas de enlace.
2. En la sección Puertas de enlace, elija una puerta de enlace por su Nombre de puerta de enlace.
3. Para editar el nombre de la puerta de enlace, elija Editar.
4. Para eliminar la puerta de enlace, elija Eliminar y, a continuación, elija Eliminar puerta de enlace.

No puede reactivar una puerta de enlace eliminada. Si desea volver a conectarse al hipervisor, siga el procedimiento que se indica en [Creación de una puerta de enlace](#).

5. Para conectarse a un hipervisor, en la sección Hipervisor conectado, elija Conectar.

Cada puerta de enlace se conecta a un único hipervisor. Sin embargo, puede conectar varias puertas de enlace al mismo hipervisor para aumentar el ancho de banda entre ellas por encima del ancho de banda de la primera puerta de enlace.

6. Para asignar, editar o administrar etiquetas, en la sección Etiquetas, elija Administrar etiquetas.

Limitación del ancho de banda de Backup Gateway

Note

Esta característica estará disponible en las nuevas puertas de enlace que se implementen después del 15 de diciembre de 2022. Para las puertas de enlace existentes, esta nueva capacidad estará disponible mediante una actualización automática del software a más tardar el 30 de enero de 2023. Para actualizar manualmente la puerta de enlace a la última versión, utilice el AWS CLI comando [UpdateGatewaySoftwareNow](#).

Puede limitar el rendimiento de carga desde su puerta de enlace AWS Backup para controlar la cantidad de ancho de banda de red que utiliza la puerta de enlace. De forma predeterminada, una puerta de enlace activada no tiene límites de carga o descarga.

Puede configurar un programa de límite de velocidad de ancho de banda mediante la AWS Backup consola o mediante la AWS CLI API mediante (). [PutBandwidthRateLimitSchedule](#) Cuando utiliza una programación de límite de velocidad de ancho de banda, puede configurar los límites para que cambien automáticamente a lo largo del día o de la semana.

La limitación de la velocidad de ancho de banda funciona equilibrando el rendimiento de todos los datos que se cargan, promediado en cada segundo. Si bien es posible que las cargas superen brevemente el límite de velocidad de ancho de banda durante un microsegundo o milisegundo determinado, esto no suele provocar picos importantes durante periodos de tiempo más prolongados.

Puede agregar un máximo de 20 intervalos. El valor máximo de la velocidad de carga es de 8 000 000 Mbps.

Consulta y edita el programa de límite de velocidad de ancho de banda de tu puerta de enlace mediante la consola. AWS Backup

En esta sección, se describe cómo ver y editar la programación de límite de velocidad de ancho de banda de su puerta de enlace.

Para ver y editar la programación de límite de velocidad de ancho de banda

1. [Abra la AWS Backup consola en /backup. https://console.aws.amazon.com](https://console.aws.amazon.com/backup)
2. En el panel de navegación izquierdo, seleccione Puertas de enlace. En el panel Puertas de enlace, se muestran las puertas de enlace por nombre. Haga clic en el botón de opción situado junto al nombre de la puerta de enlace que desee administrar.
3. Una vez que haya seleccionado un botón de opción, podrá hacer clic en el menú desplegable Acción. Haga clic en Acciones y, a continuación, en Editar programación de límite de velocidad de ancho de banda. Aparece la programación actual. De forma predeterminada, una puerta de enlace nueva o sin editar no tiene límites de velocidad de ancho de banda definidos.

 Note

También puede hacer clic en Administrar programación en la página de detalles de la puerta de enlace para ir a la página Editar ancho de banda.

4. (Opcional) Seleccione Agregar intervalo para agregar un nuevo intervalo configurable a la programación. Para cada intervalo, introduzca la siguiente información:
 - a. Días de la semana: seleccione el día o los días periódicos a los que desee que se aplique el intervalo. Cuando los elija, los días de aparece en el menú desplegable. Para eliminarlos, haga clic en la X situada junto al día.

- b. Hora de inicio: introduzca la hora de inicio del intervalo de ancho de banda con el formato HH:MM de 24 horas. La hora debe especificarse de acuerdo con el horario universal coordinado (UTC).

Nota: El bandwidth-rate-limit intervalo comienza al principio del minuto especificado.

- c. Hora de finalización: introduzca la hora de finalización del intervalo de ancho de banda con el formato HH:MM de 24 horas. La hora debe especificarse de acuerdo con el horario universal coordinado (UTC).

 Important

El bandwidth-rate-limit intervalo finaliza al final del minuto especificado. Para programar un intervalo que finalice al final de una hora, introduzca 59. Para programar intervalos continuos consecutivos, con transferencia al principio de la hora, sin interrupción entre los intervalos, introduzca 59 para el minuto final del primer intervalo. Introduzca 00 para el minuto de inicio del siguiente intervalo.

- d. Velocidad de carga: introduzca el límite de velocidad de carga, en megabits por segundo (Mbps). El valor mínimo es de 102 megabytes por segundo (Mbps).
5. (Opcional) Repita el paso anterior como desee hasta completar la programación de límite de velocidad de ancho de banda. Si necesita eliminar un intervalo de la programación, elija Eliminar.

 Important

Los intervalos de límite de velocidad de ancho de banda no se pueden superponer. La hora de inicio de un intervalo debe producirse después de la hora de finalización del intervalo anterior y antes de la hora de inicio del intervalo siguiente; la hora de finalización debe producirse antes de la hora de inicio del intervalo siguiente.

6. Cuando haya terminado, haga clic en el botón Guardar cambios.

Consulte y edite la programación de límite de velocidad de ancho de banda de su puerta de enlace mediante la AWS CLI

La acción [GetBandwidthRateLimitSchedule](#) se puede utilizar para ver la programación de limitación del ancho de banda de una puerta de enlace concreta. Si no se ha definido una

programación, esta será una lista vacía de intervalos. A continuación, se muestra un ejemplo en el AWS CLI que se utiliza para obtener el programa de ancho de banda de una puerta de enlace:

```
aws backup-gateway get-bandwidth-rate-limit-schedule --gateway-arn "arn:aws:backup-gateway:region:account-id:gateway/bgw-gw id"
```

Para editar la programación de limitación del ancho de banda de una puerta de enlace, puedes usar la acción [PutBandwidthRateLimitSchedule](#). Tenga en cuenta que solo puede actualizar la programación de una puerta de enlace en su conjunto, en lugar de modificar, agregar o eliminar intervalos individuales. Al llamar a esta acción, se sobrescribirá la programación anterior de limitación del ancho de banda de la puerta de enlace.

```
aws backup-gateway put-bandwidth-rate-limit-schedule --gateway-arn "arn:aws:backup-gateway:region:account-id:gateway/gw-id" --bandwidth-rate-limit-intervals ...
```

Uso de hipervisores

Cuando termine [Creación de una puerta de enlace](#), puede conectarlo a un hipervisor para que pueda AWS Backup trabajar con las máquinas virtuales administradas por ese hipervisor. Por ejemplo, el hipervisor para VMware VMs es VMware vCenter Server. Asegúrese de que el hipervisor esté configurado con los [permisos necesarios para AWS Backup](#).

Adición de un hipervisor

Para agregar un hipervisor:

1. En el panel de navegación de la izquierda, en la sección Recursos externos, elija Hipervisores.
2. Seleccione Agregar hipervisor.
3. En la sección Configuración del hipervisor, escriba un Nombre del hipervisor.
4. Para Host del servidor vCenter, utilice el menú desplegable para seleccionar la dirección IP o el FQDN (nombre de dominio completo). Escriba el valor correspondiente.
5. AWS Backup Para permitir la detección de las máquinas virtuales en el hipervisor, introduzca el nombre de usuario y la contraseña del hipervisor.
6. Cifre la contraseña. Para [especificar este cifrado](#), seleccione una clave de KMS específica administrada por el servicio o una clave de KMS administrada por el cliente mediante el menú desplegable o a través de Crear clave de KMS. Si no selecciona una clave específica, AWS Backup cifrará su contraseña con una clave propiedad del servicio.

7. En la sección Conexión con la puerta de enlace, utilice la lista desplegable para especificar la puerta de enlace que desee conectar al hipervisor.
8. Seleccione Probar la conexión de la puerta de enlace para verificar las entradas anteriores.
9. Si lo desea, en la sección Etiquetas de hipervisor, puede agregar etiquetas al hipervisor mediante Añadir nueva etiqueta.
10. [Asignación de VMware etiquetas](#) opcional: puede añadir hasta 10 VMware etiquetas que utilice actualmente en sus máquinas virtuales para generar AWS etiquetas.
11. En el panel de configuración del grupo de registros, puede optar por integrarlo con [Amazon CloudWatch Logs](#) para mantener los registros de su hipervisor (se aplicará el [precio estándar de CloudWatch Logs](#) en función del uso). Cada hipervisor puede pertenecer a un grupo de registro.
 - a. Si aún no ha creado un grupo de registro, seleccione el botón de opción Crear un nuevo grupo de registro. El hipervisor que está editando se asociará a este grupo de registro.
 - b. Si ha creado anteriormente un grupo de registro para un hipervisor diferente, puede usar ese grupo de registro para este hipervisor. Seleccione Utilizar un grupo de registro existente.
 - c. Si no desea CloudWatch registrar, seleccione Desactivar el registro.
12. Elija Agregar hipervisor para acceder a su página de detalles.

 Tip

Puede utilizar Amazon CloudWatch Logs (consulte el paso 11 anterior) para obtener información sobre el hipervisor, incluida la supervisión de errores, la conexión de red entre la puerta de enlace y el hipervisor y la información de configuración de la red. Para obtener información sobre los grupos de CloudWatch registros, consulte [Trabajar con grupos de registros y transmisiones de registros](#) en la Guía del CloudWatch usuario de Amazon.

Visualización de máquinas virtuales administradas por un hipervisor

Para ver las máquinas virtuales en un hipervisor:

1. En el panel de navegación de la izquierda, en la sección Recursos externos, elija Hipervisores.
2. En la sección Hipervisores, elija un hipervisor en Nombre del hipervisor para ir a su página de detalles.

3. En la sección titulada Resumen del hipervisor, elija la pestaña Máquinas virtuales.
4. En la sección Máquinas virtuales conectadas, se rellena automáticamente una lista de máquinas virtuales.

Visualización de las puertas de enlace conectadas a un hipervisor

Par ver las puertas de enlace conectadas al hipervisor:

1. Seleccione la pestaña Puertas de enlace.
2. En la sección Puertas de enlace conectadas, se rellena automáticamente una lista de puertas de enlace.

Conexión de un hipervisor a puertas de enlace adicionales

Las velocidades de copia de seguridad y restauración pueden estar limitadas por el ancho de banda de la conexión entre la puerta de enlace y el hipervisor. Para aumentar estas velocidades, puede conectar una o más puertas de enlace adicionales al hipervisor. Puede hacerlo en la sección Puertas de enlace conectadas de la siguiente manera:

1. Elija Conectar.
2. Seleccione otra puerta de enlace mediante el menú desplegable. También puede elegir Crear puerta de enlace para crear una nueva puerta de enlace.
3. Elija Conectar.

Edición de la configuración de un hipervisor

Si no utiliza la característica Probar la conexión de la puerta de enlace, podría agregar un hipervisor con un nombre de usuario o contraseña incorrectos. En ese caso, el estado de conexión del hipervisor es siempre Pending. Como alternativa, puede rotar el nombre de usuario o la contraseña para acceder al hipervisor. Actualice esta información mediante el siguiente procedimiento.

Para editar un hipervisor ya agregado:

1. En el panel de navegación de la izquierda, en la sección Recursos externos, elija Hipervisores.
2. En la sección Hipervisores, elija un hipervisor en Nombre del hipervisor para ir a su página de detalles.
3. Seleccione Editar.

4. El panel superior se denomina Configuración del hipervisor.
 - a. En Host del servidor vCenter, también puede editar el FQDN (nombre de dominio completo) o la dirección IP.
 - b. Si lo desea, introduzca el Nombre de usuario y la Contraseña del hipervisor.
5. En el panel de configuración del grupo de registros, puede optar por integrarlo con [Amazon CloudWatch](#) para mantener los registros de su hipervisor (se aplicará un [CloudWatch precio](#) estándar en función del uso). Cada hipervisor puede pertenecer a un grupo de registro.
 - a. Si aún no ha creado un grupo de registro, seleccione el botón de opción Crear un nuevo grupo de registro. El hipervisor que está editando se asociará a este grupo de registro.
 - b. Si ha creado anteriormente un grupo de registro para un hipervisor diferente, puede usar ese grupo de registro para este hipervisor. Seleccione Utilizar un grupo de registro existente.
 - c. Si no desea CloudWatch registrar, seleccione Desactivar el registro.

 Tip

Puede utilizar Amazon CloudWatch Logs (consulte el paso 5 anterior) para obtener información sobre el hipervisor, incluida la supervisión de errores, la conexión de red entre la puerta de enlace y el hipervisor y la información de configuración de la red. Para obtener información sobre los grupos de CloudWatch registros, consulte [Trabajar con grupos de registros y transmisiones de registros](#) en la Guía del CloudWatch usuario de Amazon.

Para actualizar un hipervisor mediante programación, utilice el comando de CLI [update-hypervisor](#) y la llamada a la API. [UpdateHypervisor](#)

Eliminación de la configuración de un hipervisor

Si necesita eliminar un hipervisor ya agregado, elimine la configuración del hipervisor y agregue otra. Esta operación de eliminación se aplica a la configuración para conectarse al hipervisor. No elimina el hipervisor.

Para eliminar la configuración para conectarse a un hipervisor ya agregado:

1. En el panel de navegación de la izquierda, en la sección Recursos externos, elija Hipervisores.

2. En la sección Hipervisores, elija un hipervisor en Nombre del hipervisor para ir a su página de detalles.
3. Elija Eliminar, y, a continuación, elija Eliminar hipervisor.
4. Opcional: sustituya la configuración del hipervisor eliminada mediante el procedimiento para [Adición de un hipervisor](#).

Descripción del estado del hipervisor

A continuación se describen cada uno de los posibles estados del hipervisor y, si corresponde, los pasos de corrección. El estado ONLINE es el estado normal del hipervisor. Un hipervisor debe tener este estado todo el tiempo o la mayor parte del tiempo que esté en uso para realizar copias de seguridad y recuperación o cuando esté gestionado por el hipervisor. VMs

Estados del hipervisor

Status	Significado y corrección
ONLINE	Ha agregado un hipervisor AWS Backup, lo ha asociado a una puerta de enlace y puede conectarse a esa puerta de enlace a través de la red para realizar copias de seguridad y recuperación de las máquinas virtuales administradas por el hipervisor. Puede realizar copias de seguridad programadas y bajo demanda de esas máquinas virtuales en cualquier momento.
PENDING	Ha agregado un hipervisor, pero: AWS Backup • No está asociado a ninguna puerta de enlace, o • Está asociado a una o más puertas de enlace, pero todas esas puertas de enlace se eliminaron o no están activas por algún otro motivo.

Status	Significado y corrección
OFFLINE	Para cambiar el estado de un hipervisor de PENDING a ONLINE, cree una puerta de enlace y conecte el hipervisor a esa puerta de enlace. Ha agregado un hipervisor AWS Backup y lo ha asociado a una puerta de enlace, pero la puerta de enlace no puede conectarse al hipervisor a través de la red. Para cambiar el estado de un hipervisor de OFFLINE a ONLINE, compruebe que la configuración de red sea correcta. Si el problema persiste, compruebe que la dirección IP o el nombre de dominio completo del hipervisor sean correctos. Si son incorrectos, vuelva a agregar el hipervisor con la información correcta y pruebe la conexión de la puerta de enlace.
ERROR	Ha agregado un hipervisor AWS Backup y lo ha asociado a una puerta de enlace, pero la puerta de enlace no puede comunicarse con el hipervisor. Para cambiar el estado de un hipervisor de ERROR a ONLINE, compruebe que el nombre de usuario y la contraseña del hipervisor sean correctos. Si son incorrectos, edite la configuración del hipervisor.

Pasos siguientes

Para hacer una copia de seguridad de las máquinas virtuales en el hipervisor, consulte [Copia de seguridad de máquinas virtuales](#).

Copia de seguridad de máquinas virtuales

Después de [Adición de un hipervisor](#), la puerta de enlace de copia de seguridad muestra automáticamente las máquinas virtuales. Para ver sus máquinas virtuales, seleccione Hipervisores o Máquinas virtuales en el panel de navegación izquierdo.

- Elija Hipervisores para ver solo las máquinas virtuales administradas por un hipervisor concreto. Con esta vista, puede trabajar con una máquina virtual a la vez.
- Elija Máquinas virtuales para ver todas las máquinas virtuales de todos los hipervisores que haya agregado a su Cuenta de AWS. Con esta vista, puede trabajar con algunas o todas sus máquinas virtuales en varios hipervisores.

Independientemente de la vista que elija, para realizar una operación de copia de seguridad en una máquina virtual específica, elija el Nombre de máquina virtual para abrir su página de detalles. La página de detalles de la máquina virtual es el punto de partida de los siguientes procedimientos.

Creación de una copia de seguridad bajo demanda de una máquina virtual

Una copia de seguridad [bajo demanda](#) es una copia de seguridad completa y única que se inicia manualmente. Puede utilizar copias de seguridad bajo demanda para probar las capacidades AWS Backup de copia de seguridad y restauración.

Para crear una copia de seguridad bajo demanda de una máquina virtual:

1. Seleccione Create on-demand backup (Crear copia de seguridad bajo demanda).
2. [Configure la copia de seguridad bajo demanda.](#)
3. Seleccione Create on-demand backup (Crear copia de seguridad bajo demanda).
4. Compruebe si su trabajo de copia de seguridad tiene el estado Completed. En el panel de navegación izquierdo, elija Trabajos.
5. Elija el ID de trabajo de copia de seguridad para ver la información del trabajo de copia de seguridad, como el Tamaño de copia de seguridad y el tiempo transcurrido entre la fecha de Fecha de creación y la Fecha de finalización.

Copias de seguridad incrementales de máquinas virtuales

VMware Las versiones más recientes incluyen una función llamada [Seguimiento de bloques modificados](#), que realiza un seguimiento de los bloques de almacenamiento de las máquinas

virtuales a medida que cambian con el tiempo. Cuando se hace una copia de seguridad de una máquina virtual, se AWS Backup intenta utilizar los datos CBT si están disponibles. AWS Backup utiliza datos CBT para acelerar el proceso de copia de seguridad; sin datos CBT, los trabajos de copia de seguridad suelen ser más lentos y utilizan más recursos del hipervisor. La copia de seguridad aún se puede completar correctamente incluso si los datos de CBT no son válidos o no están disponibles. Por ejemplo, es posible que los datos CBT no sean válidos o no estén disponibles si la máquina virtual o el ESXi host se apagan bruscamente.

En los casos en que los datos de CBT no sean válidos o no estén disponibles, el estado de la copia de seguridad aparecerá con un mensaje `Successful`. En estos casos, el mensaje indicará que, en ausencia de datos CBT, AWS Backup utilizó su propio mecanismo patentado de detección de cambios para completar la copia de seguridad en lugar de utilizar los datos CBT. Las copias de seguridad posteriores volverán a intentar utilizar los datos de CBT y, en la mayoría de los casos, los datos de CBT serán válidos y estarán disponibles correctamente. Si el problema persiste, consulta [VMware Solución de problemas](#) para ver los pasos a seguir.

Para que el CBT funcione de forma correcta, debe cumplirse lo siguiente:

- El host debe ser ESXi 4.0 o posterior
- La máquina virtual propietaria de los discos debe tener la versión de hardware 7 o posterior
- CBT debe estar habilitada para la máquina virtual (está habilitado de forma predeterminada)

Para comprobar si un disco virtual tiene CBT habilitado:

1. Abra vSphere Client y seleccione una máquina virtual apagada.
2. Haga clic con el botón derecho en la máquina virtual y vaya a Edit Settings > Options > Advanced/General > Configuration Parameters.
3. La opción `ctkEnabled` debe ser `True`.

Automatización de la copia de seguridad de la máquina virtual mediante la asignación de recursos a un plan de copia de seguridad

Un [plan de copia de seguridad](#) es una política de protección de datos definida por el usuario que automatiza la protección de datos en muchos servicios de AWS y aplicaciones de terceros. Primero debe crear su plan de copia de seguridad en el que especificará la frecuencia de copia de seguridad, el periodo de retención, la política de ciclo de vida y muchas otras opciones. Para crear un plan de copia de seguridad, consulte el tutorial de introducción.

Después de crear el plan de respaldo, debe asignar los recursos AWS Backup compatibles, incluidas las máquinas virtuales, a ese plan de respaldo. AWS Backup ofrece [muchas formas de asignar recursos](#), incluida la asignación de todos los recursos de su cuenta, la inclusión o exclusión de recursos específicos individuales, o la adición de recursos con determinadas etiquetas.

Además de las funciones de asignación de recursos existentes, la AWS Backup compatibilidad con máquinas virtuales presenta varias funciones nuevas que le ayudarán a asignar rápidamente las máquinas virtuales a los planes de respaldo. Desde la página Máquinas virtuales, puede asignar etiquetas a varias máquinas virtuales o utilizar la nueva característica Asignar recursos para planificar. Utilice estas funciones para asignar las máquinas virtuales ya descubiertas por AWS Backup Gateway.

Si prevé detectar y asignar máquinas virtuales adicionales en el futuro y desea automatizar el paso de asignación de recursos para incluir esas máquinas virtuales futuras, utilice la nueva característica Crear asignación de grupo.

VMware Etiquetas

Las [etiquetas](#) son pares clave-valor que puede utilizar para administrar, filtrar y buscar sus recursos.

Una VMware etiqueta se compone de una categoría y un nombre de etiqueta. VMware las etiquetas se utilizan para agrupar máquinas virtuales. Un nombre de etiqueta es una etiqueta asignada a una máquina virtual. Una categoría es una colección de nombres de etiquetas.

En las AWS etiquetas, puede usar caracteres entre letras, números, espacios y caracteres especiales en UTF-8. + - = . _ : /

Si utiliza etiquetas en sus máquinas virtuales, puede agregar hasta 10 etiquetas coincidentes en AWS Backup para ayudar con la organización. Puede asignar hasta 10 VMware etiquetas a AWS etiquetas. En la [AWS Backup consola](#), se encuentran en Recursos externos > Máquinas virtuales > AWS VMware etiquetas o rótulos.

VMware mapeo de etiquetas

Si utiliza etiquetas en sus máquinas virtuales, puede agregar hasta 10 etiquetas coincidentes en AWS Backup para aumentar la claridad y la organización. Las asignaciones se aplican a cualquier máquina virtual del hipervisor.

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En la consola, vaya a Editar hipervisor (haga clic en Recursos externos, luego en Hipervisores, luego en el nombre del hipervisor y, a continuación, en Administrar asignaciones).

3. El último panel, el mapeo de VMware etiquetas, contiene cuatro campos de cuadro de texto en los que puede introducir la información de las VMware etiquetas en las etiquetas correspondientes AWS . Los cuatro campos son la categoría de etiqueta de VMware, VMware el nombre de la AWS etiqueta, la clave de la AWS etiqueta y el valor de la etiqueta (por ejemplo: Categoría = SO; nombre de etiqueta = Windows; clave de AWS etiqueta = OS-Windows y valor de AWS etiqueta = Windows).
4. Una vez que haya introducido sus valores preferidos, haga clic en Agregar mapeo. Si comete un error, puede hacer clic en Eliminar para eliminar la información ingresada.
5. Tras añadir los mapas, especifique la función de IAM que piensa utilizar para aplicar estas AWS etiquetas a las máquinas VMware virtuales.

La política [AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync](#) contiene todos los permisos necesarios. Puede asociar esta política al rol que utilice (o pedir a un administrador que lo haga) o puede crear una política personalizada para el rol que se utilice.

6. Por último, haga clic en Agregar hipervisor o en Guardar.

La relación de confianza entre los roles de IAM debe modificarse para agregar los servicios backup-gateway.amazonaws.com y backup.amazonaws.com. Sin este servicio, es probable que se produzca un error al asignar etiquetas. Para editar la relación de confianza para un rol existente,

1. Inicie sesión en la [consola de IAM](#).
2. En el panel de navegación de la consola, elija Roles .
3. Elija el nombre del rol que desea modificar y seleccione la pestaña Relaciones de confianza en la página de detalles.
4. En Documento de política, pegue lo siguiente:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "backup.amazonaws.com",
          "backup-gateway.amazonaws.com"
        ]
      }
    }
  ]
}
```

```
    ]
  },
  "Action": "sts:AssumeRole"
}
]
```

5. Elija Actualizar política de confianza.

Consulte [Editing the trust relationship for an existing role](#) en la Guía de administración de AWS Directory Service para obtener más detalles.

Vea las asignaciones VMware de etiquetas

En la [Consola de AWS Backup](#), haga clic en Recursos externos, luego en Hipervisores y, a continuación, en el enlace con el nombre del hipervisor para ver las propiedades del hipervisor seleccionado. En el panel de resumen, hay cuatro pestañas, la última de las cuales es la asignación de VMware etiquetas. Tenga en cuenta que si aún no tiene mapeos, «No hay VMware mapeos de etiquetas». .

Desde aquí, puede sincronizar los metadatos de las máquinas virtuales detectadas por el hipervisor, copiar las asignaciones a sus hipervisores, añadir las etiquetas asignadas a las AWS etiquetas a la selección de copias de seguridad de un plan de copia de seguridad o gestionar las asignaciones. VMware

En la consola, para ver qué etiquetas se aplican a una máquina virtual seleccionada, haga clic en Máquinas virtuales, luego en el nombre de la máquina virtual y, por último, en etiquetas o rótulos.AWS VMware Puede ver las etiquetas asociadas a esta máquina virtual y, además, puede administraras.

Asigne máquinas virtuales a la planificación mediante asignaciones de VMware etiquetas

Para asignar máquinas virtuales a un plan de copia de seguridad mediante asignaciones de etiquetas, haga lo siguiente:

1. [Abra la AWS Backup consola en /backup. https://console.aws.amazon.com](#)
2. En la consola, vaya a las asignaciones de VMware etiquetas en la página de detalles del hipervisor (haga clic en Recursos externos, luego en Hipervisores y, a continuación, en el nombre del hipervisor).

3. Seleccione la casilla de verificación situada junto a varias etiquetas asignadas para asignarlas al mismo plan de copia de seguridad.
4. Haga clic en Agregar a la asignación de recursos.
5. Elija un Plan de copia de seguridad existente de la lista desplegable. También puede elegir Crear plan de copia de seguridad para crear un plan nuevo.
6. Haga clic en Confirmar. Esto abre la página Asignar recursos con la opción Ajustar la selección mediante etiquetas con valores rellenos previamente.

VMware etiqueta utilizando el AWS CLI

AWS Backup utiliza la llamada [PutHypervisorPropertyMappings](#) a la API para asignar las propiedades de la entidad del hipervisor local a las propiedades de. AWS

En el AWS CLI, utilice la operación: `put-hypervisor-property-mappings`

```
aws backup-gateway put-hypervisor-property-mappings \
--hypervisor-arn arn:aws:backup-gateway:region:account:hypervisor/hypervisorId \
--vmware-to-aws-tag-mappings List of VMware to AWS tag mappings \
--iam-role-arn arn:aws:iam::account:role/roleName \
--region AWSRegion
--endpoint-url URL
```

A continuación se muestra un ejemplo:

```
aws backup-gateway put-hypervisor-property-mappings \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--vmware-to-aws-tag-mappings VmwareCategory=OS,VmwareTagName=Windows,AwsTagKey=OS-
Windows,AwsTagValue=Windows \
--iam-role-arn arn:aws:iam::123456789012:role/SyncRole \
--region us-east-1
```

También se puede utilizar [GetHypervisorPropertyMappings](#) para obtener información de asignación de propiedades. En el AWS CLI, utilice la operación `get-hypervisor-property-mappings`. A continuación, se muestra una plantilla de ejemplo:

```
aws backup-gateway get-hypervisor-property-mappings --hypervisor-arn HypervisorARN
--region AWSRegion
```

A continuación se muestra un ejemplo:

```
aws backup-gateway get-hypervisor-property-mappings \  
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \  
--region us-east-1
```

Sincronice los metadatos de las máquinas virtuales descubiertas por el hipervisor AWS mediante API, CLI o SDK

Puede sincronizar los metadatos de las máquinas virtuales. Cuando lo haga, se sincronizarán las VMware etiquetas presentes en la máquina virtual que forman parte de las asignaciones. Además, las AWS etiquetas asignadas a las VMware etiquetas presentes en la máquina virtual se aplicarán al recurso de la AWS máquina virtual.

AWS Backup utiliza la llamada [StartVirtualMachinesMetadataSync](#) la API para sincronizar los metadatos de las máquinas virtuales descubiertas por el hipervisor. Para sincronizar los metadatos de las máquinas virtuales detectadas por el hipervisor mediante la AWS CLI, utilice la operación `start-virtual-machines-metadata-sync`.

Ejemplo de plantilla:

```
aws backup-gateway start-virtual-machines-metadata-sync \  
--hypervisor-arn Hypervisor ARN \  
--region AWSRegion
```

Ejemplo:

```
aws backup-gateway start-virtual-machines-metadata-sync \  
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \  
--region us-east-1
```

También puede utilizar [GetHypervisor](#) para obtener información del hipervisor, como el host, el estado o el estado de la última sincronización de metadatos, y también para recuperar la hora de la última sincronización correcta de los metadatos. En el AWS CLI, utilice la operación `get-hypervisor`

Ejemplo de plantilla:

```
aws backup-gateway get-hypervisor \  
--hypervisor-arn Hypervisor ARN
```

```
--region AWSRegion
```

Ejemplo:

```
aws backup-gateway get-hypervisor \  
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \  
--region us-east-1
```

Para obtener más información, consulte la documentación de la API [VmwareTagy VmwareToAwsTagMapping](#).

Esta característica estará disponible en las nuevas puertas de enlace que se implementen después del 15 de diciembre de 2022. Para las puertas de enlace existentes, esta nueva capacidad estará disponible mediante una actualización automática del software a más tardar el 30 de enero de 2023. Para actualizar la puerta de enlace a la última versión de forma manual, usa AWS CLI el comando [UpdateGatewaySoftwareNow](#).

Ejemplo:

```
aws backup-gateway update-gateway-software-now \  
--gateway-arn arn:aws:backup-gateway:us-east-1:123456789012:gateway/bgw-12345 \  
--region us-east-1
```

Asignación de máquinas virtuales mediante etiquetas

Puede asignar las máquinas virtuales que encuentre actualmente AWS Backup, junto con otros AWS Backup recursos, asignándoles una etiqueta que ya haya asignado a uno de sus planes de backup existentes. También puede crear un [nuevo plan de copia de seguridad](#) y una nueva [asignación de recursos basada en etiquetas](#). Los planes de copia de seguridad comprueban los recursos recién asignados cada vez que ejecutan un trabajo de copia de seguridad.

Para etiquetar varias máquinas virtuales con la misma etiqueta:

1. En el panel de navegación izquierdo, elija Máquinas virtuales.
2. Seleccione la casilla de verificación situada junto al Nombre de máquina virtual para elegir todas las máquinas virtuales. También puede seleccionar la casilla de verificación situada junto a los nombres de las máquinas virtuales que desee etiquetar.
3. Elija Add tags (Añadir etiquetas).
4. Escriba una Clave de etiqueta.

5. Recomendado: escriba un Valor de etiqueta.
6. Elija Confirmar.

Asignación de máquinas virtuales mediante la característica Asignar recursos para planificar

Puede asignar las máquinas virtuales descubiertas actualmente AWS Backup a un plan de respaldo nuevo o existente mediante la función Asignar recursos al plan.

Para asignar máquinas virtuales mediante la característica Asignar recursos para planificar:

1. En el panel de navegación izquierdo, elija Máquinas virtuales.
2. Seleccione la casilla de verificación situada junto al Nombre de máquina virtual para elegir todas las máquinas virtuales. También puede seleccionar la casilla de verificación situada junto a varios nombres de máquinas virtuales para asignarlas al mismo plan de copia de seguridad.
3. Seleccione Asignaciones y, a continuación, elija Asignar recursos para planificar.
4. Escriba un Nombre de asignación de recursos.
5. Elija una rol de IAM en la asignación de recursos para crear copias de seguridad y administrar los puntos de recuperación. Si no desea utilizar un rol de IAM específico, le recomendamos el Rol predeterminado, que tiene los permisos correctos.
6. En la sección Plan de copia de seguridad, elija un Plan de copia de seguridad existente de la lista desplegable. También puede elegir Crear plan de copia de seguridad para crear un plan nuevo.
7. Elija Asignar recursos.
8. De forma opcional, para comprobar que sus máquinas virtuales están asignadas a un plan de copia de seguridad, seleccione Ver plan de copia de seguridad. A continuación, en la sección Asignaciones de recursos, elija el Nombre de la asignación de recursos.

Asignación de máquinas virtuales mediante la característica Crear asignación de grupo

A diferencia de las dos funciones de asignación de recursos anteriores para máquinas virtuales, la función Crear asignación de grupos no solo asigna las máquinas virtuales detectadas actualmente AWS Backup, sino también las máquinas virtuales descubiertas en el futuro en una carpeta o hipervisor que defina.

Además, no tiene que seleccionar ninguna casilla de verificación para utilizar la característica Crear asignación de grupo.

Para asignar máquinas virtuales mediante la característica Asignar recursos para planificar:

1. En el panel de navegación izquierdo, elija Máquinas virtuales.
 2. Elija Asignaciones y, a continuación, elija Crear asignación de grupo.
 3. Escriba un Nombre de asignación de recursos.
 4. Elija una rol de IAM en la asignación de recursos para crear copias de seguridad y administrar los puntos de recuperación. Si no desea utilizar un rol de IAM específico, le recomendamos el Rol predeterminado, que tiene los permisos correctos.
 5. En la sección Grupo de recursos, seleccione el menú desplegable Tipo de grupo. Las opciones son Carpeta o Hipervisor.
 - a. Elija Carpeta para asignar todas las máquinas virtuales de una carpeta en un hipervisor. Seleccione Nombre del grupo de carpetas, por ejemplo `datacenter/vm`, mediante el menú desplegable. También puede optar por incluir Subcarpetas.
-  **Note**

Para realizar asignaciones basadas en carpetas, durante el proceso de detección, AWS Backup etiqueta las máquinas virtuales con la carpeta en la que las encuentra durante el proceso de detección. Si más adelante mueve una máquina virtual a una carpeta diferente, AWS Backup no podrá actualizar la etiqueta por usted debido a las prácticas recomendadas de AWS etiquetado. Este método de asignación puede dar lugar a que se sigan realizando copias de seguridad de las máquinas virtuales que haya sacado de la carpeta asignada.
- b. Elija Hipervisor para asignar todas las máquinas virtuales administradas por un hipervisor. Seleccione un Nombre del grupo de ID de hipervisor mediante el menú desplegable.
 6. En la sección Plan de copia de seguridad, elija un Plan de copia de seguridad existente de la lista desplegable. También puede elegir Crear plan de copia de seguridad para crear un plan nuevo.
 7. Elija Crear asignación de grupo.
 8. De forma opcional, para comprobar que sus máquinas virtuales están asignadas a un plan de copia de seguridad, seleccione Ver plan de copia de seguridad. En la sección Asignaciones de recursos, elija el Nombre de la asignación de recursos.

Pasos siguientes

Para restaurar una máquina virtual, consulte [Restaure una máquina virtual mediante AWS Backup](#).

Información sobre componentes de origen de terceros para la puerta de enlace de copia de seguridad

En esta sección, encontrará información sobre las herramientas y licencias de terceros de las que dependemos para ofrecer la funcionalidad de puerta de enlace de copia de seguridad.

El código fuente de algunos componentes de software de código abierto que se incluyen con el software de la puerta de enlace de copia de seguridad se puede descargar en las siguientes ubicaciones:

- [Para las puertas de enlace implementadas en VMware ESXi, descargue sources.tgz](#).

[Este producto incluye software desarrollado por el proyecto OpenSSL para su uso en el kit de herramientas OpenSSL \(<https://www.openssl.org/>\)](#).

Este producto incluye software desarrollado por VMware® vSphere Software Development Kit () <https://www.vmware.com>.

Para obtener las licencias pertinentes para todas las herramientas de terceros dependientes, consulte [Licencias de terceros](#).

Componentes de código abierto para AWS Appliance

Se utilizan varias herramientas y licencias de terceros para ofrecer la funcionalidad de puerta de enlace de copia de seguridad.

Utilice los siguientes enlaces para descargar el código fuente de determinados componentes de software de código abierto que se incluyen con el software de AWS Appliance:

- [Para las puertas de enlace implementadas en VMware ESXi, descargue sources.tar](#)

[Este producto incluye software desarrollado por el proyecto OpenSSL para su uso en el kit de herramientas OpenSSL \(<https://www.openssl.org/>\)](#). Para obtener las licencias pertinentes para todas las herramientas de terceros dependientes, consulte [Licencias de terceros](#).

Solución de problemas de máquinas virtuales

Problemas y mensajes relacionados con copias de seguridad incrementales o CBT

Mensaje de error: "The VMware Change Block Tracking (CBT) data was invalid during this backup, but the incremental backup was successfully completed with our proprietary change detection mechanism."

Si este mensaje continúa, [restablezca la CBT](#) como se indica en. VMware

El mensaje indica que la CBT no estaba activada o no estaba disponible: «El seguimiento de bloques de VMware cambios (CBT) no estaba disponible para esta máquina virtual, pero la copia de seguridad incremental se completó correctamente con nuestro mecanismo de cambios patentado».

Asegúrese de que el CBT esté activado. Para comprobar si un disco virtual tiene CBT habilitado:

1. Abra vSphere Client y seleccione una máquina virtual apagada.
2. Haga clic con el botón derecho en la máquina virtual y vaya a Edit Settings > Options > Advanced/General > Configuration Parameters.
3. La opción ctkEnabled debe ser True.

Si está activado, asegúrese de que está utilizando up-to-date VMware las funciones. El host debe ser ESXi 4.0 o posterior y la máquina virtual propietaria de los discos que se van a rastrear debe ser de la versión de hardware 7 o posterior.

Si el CBT está activado (habilitado) y el software y el hardware están actualizados, apague la máquina virtual y vuelva a encenderla. Asegúrese de que el CBT esté activado. A continuación, vuelva a realizar la copia de seguridad.

VMware error de copia de seguridad

Cuando se produce un error en una VMware copia de seguridad, puede estar relacionado con uno de los siguientes motivos:

Mensaje de error: "Failed to process backup data. Aborted backup job." o "Error opening disk on the virtual machine".

Causas posibles: este error puede deberse a un problema de configuración o a que la VMware versión o el disco no sean compatibles.

Solución 1: asegúrese de que su infraestructura esté configurada para usar una puerta de enlace y asegúrese de que todos los puertos necesarios estén abiertos.

1. Acceda a la [consola de Backup Gateway](#). Tenga en cuenta que es diferente de la consola de AWS Backup .
2. En la página de configuración de Backup Gateway, introduzca la opción 3 para probar la conectividad de la red.
3. Si la prueba de red es correcta, escriba X.
4. Vuelva a la página de configuración de Backup Gateway.
5. Introduzca 7 para acceder al símbolo del sistema.
6. Para comprobar la conectividad de red, ejecute los siguientes comandos:

```
ncport -d ESXi Host -p 902
```

```
ncport -d ESXi Host -p 443
```

Solución 2: use versiones de [Compatible VMs](#).

Solución 3: si un dispositivo de puerta de enlace está configurado con servidores DNS incorrectos, se produce un error en la copia de seguridad. Siga estos pasos para comprobar la configuración de DNS:

1. Acceda a la [consola de Backup Gateway](#).
2. En la página de configuración de Backup Gateway, introduzca la opción 2 para ir a la conectividad de la red.
3. En Configuración de red, escriba 7 para ver la configuración de DNS.
4. Las direcciones IP del servidor del DNS. Si la dirección IP del servidor DNS es incorrecta, aparece la petición para volver a Configuración de red.
5. En Configuración de red, escriba 6 para editar la configuración de DNS.
6. Introduzca las direcciones IP del servidor DNS correctas. A continuación, introduzca X para completar la configuración de la red.

Para obtener más información sobre el hipervisor, como los errores y la configuración y conexión de la red, consulte Cómo configurar el hipervisor [Edición de la configuración de un hipervisor](#) para que se integre con Amazon CloudWatch Logs.

Fallos de copia de seguridad debidos a problemas de conexión de red

Mensaje de error: "Failed to upload backup during data ingestion. Aborted backup job." o "Cloud network request timed out during data ingestion".

Causas posibles: este error puede producirse si la conexión de red no es suficiente para administrar la carga de datos. Si el ancho de banda de la red es bajo, el enlace entre la máquina virtual y la máquina virtual AWS Backup puede congestionarse y provocar errores en las copias de seguridad.

El ancho de banda de la red necesario depende de varios factores, como el tamaño de la máquina virtual, los datos incrementales generados para cada copia de seguridad de la máquina virtual, el periodo de copia de seguridad y los requisitos de restauración.

Solución: las mejores prácticas y recomendaciones incluyen tener un ancho de banda de carga mínimo de 1000 Mbps para las VMs conexiones locales a. AWS Backup Una vez confirmado el ancho de banda, vuelva a intentar el trabajo de copia de seguridad.

Trabajo de copia de seguridad cancelado

Mensaje de error: "Failed to create backup during snapshot creation. Aborted backup job."

Causa posible: es posible que el VMware host en el que se encuentra el dispositivo de puerta de enlace tenga un problema.

Solución: compruebe la configuración de su VMware host y revísela para ver si hay problemas. Para obtener información adicional, consulta [Edición de la configuración de un hipervisor](#).

No hay puertas de enlace disponibles

Mensaje de error: "No gateways available to work on job."

Causa posible: todas las puertas de enlace conectadas están ocupadas realizando otras tareas. Cada puerta de enlace tiene un límite de cuatro tareas simultáneas (copia de seguridad o restauración).

Para obtener información sobre las soluciones, consulte la siguiente sección para conocer los pasos para aumentar el número de puertas de enlace y los pasos para aumentar la duración del plan de copia de seguridad.

VMware error en el trabajo de respaldo

Mensaje de error: "Abort signal detected"

Causas posibles:

- Bajo ancho de banda de la red: un ancho de banda de la red insuficiente puede impedir que se completen las copias de seguridad dentro del plazo de finalización. Si el trabajo de copia de seguridad requiere más ancho de banda del disponible, se puede producir un error y provocar el error “Se ha detectado una señal de interrupción”.
- Número inadecuado de puertas de enlace de respaldo: si el número de puertas de enlace de respaldo no es suficiente para gestionar la rotación de respaldo de todas las configuraciones VMs, es posible que el trabajo de respaldo falle. Esto puede ocurrir cuando el plazo del plan de copia de seguridad para completar las copias de seguridad es demasiado corto o si la cantidad de puertas de enlace de copia de seguridad no es suficiente.
- El periodo de finalización del plan de copia de seguridad es demasiado pequeña.

Remedios:

Aumente el ancho de banda: considere aumentar la capacidad de la red entre el entorno local AWS y el entorno local. Este paso proporcionará más ancho de banda para el proceso de copia de seguridad, lo que permitirá que los datos se transfieran eficientemente sin que se produzca un error. Se recomienda disponer de un ancho de banda de al menos 100 Mbps AWS para realizar copias de seguridad en VMware VMs las instalaciones. AWS Backup

Si se configura un límite de velocidad de ancho de banda para la puerta de enlace de copia de seguridad, esto puede restringir el flujo de datos y provocar errores de copia de seguridad. Aumentar el límite de velocidad de ancho de banda para garantizar una capacidad de transferencia de datos suficiente puede ayudar a reducir las fallas. Este ajuste puede mitigar la aparición del error “Se ha detectado una señal de cancelación”. Para obtener más información, consulte [Limitación del ancho de banda de Backup Gateway](#).

Aumente la cantidad de puertas de enlace de copia de seguridad: una sola puerta de enlace de copia de seguridad puede procesar hasta 4 trabajos de copia de seguridad y restauración a la vez. Los trabajos adicionales se pondrán en cola y esperarán a que la puerta de enlace se libere hasta que pase el periodo de inicio de la copia de seguridad. Si se agota el periodo de copia de seguridad y las tareas en cola no se han iniciado, esas tareas de copia de seguridad fallarán y se detectará una señal de cancelación. Puede aumentar la cantidad de puertas de enlace de copia de seguridad para reducir la cantidad de trabajos fallidos. Consulte [Uso de puertas de enlace](#) para más detalles.

Aumente la duración del período de copia de seguridad del plan de copia de seguridad: puede aumentar la duración total del período de copia de seguridad en su plan de copia de seguridad. Consulte [Opciones y configuración del plan de copia de seguridad](#) para más detalles.

Para obtener ayuda para resolver estos problemas, consulte el [AWS Knowledge Center](#).

Creación de copias de seguridad de Windows VSS

Con AWS Backup, puede realizar copias de seguridad y restaurar aplicaciones de Windows habilitadas para VSS (Volume Shadow Copy Service) que se ejecuten en instancias de Amazon EC2 . Si la aplicación tiene un grabador VSS registrado en Windows VSS, AWS Backup crea una instantánea que sea coherente con esa aplicación.

Puede realizar restauraciones consistentes y, al mismo tiempo, usar el mismo servicio de respaldo administrado que se usa para proteger otros AWS recursos. Con las copias de seguridad de Windows compatibles con las aplicaciones EC2, obtendrá la misma configuración de coherencia y el mismo conocimiento de las aplicaciones que las herramientas de copia de seguridad tradicionales.

Note

AWS Backup solo admite copias de seguridad coherentes con las aplicaciones de los recursos que se ejecutan en Amazon EC2, específicamente en escenarios de copia de seguridad en los que los datos de la aplicación se pueden restaurar sustituyendo una instancia existente por una nueva creada a partir de la copia de seguridad. No todos los tipos de instancia o aplicaciones son compatibles con las copias de seguridad de Windows VSS.

Para obtener más información, consulte [Crear instantáneas basadas en VSS](#) en la Guía del EC2 usuario de Amazon.

Para realizar copias de seguridad y restaurar los recursos de Windows habilitados para VSS que EC2 ejecutan Amazon, sigue estos pasos para completar las tareas previas requeridas. Para obtener instrucciones, consulte [Requisitos previos para crear instantáneas de EBS basadas en Windows VSS en la Guía del usuario](#) de Amazon. EC2

1. Descargue, instale y configure el agente SSM en. AWS Systems Manager Este paso es necesario. Para obtener instrucciones, consulte Cómo [trabajar con el agente SSM en EC2 instancias de Windows Server](#) en la Guía del AWS Systems Manager usuario.

2. Añada una política de IAM a la función de IAM y asocie la función a la EC2 instancia de Amazon antes de realizar la copia de seguridad de Windows VSS (Volume Shadow Copy Service). Para obtener instrucciones, consulte [Utilizar una política gestionada por IAM para conceder permisos para instantáneas basadas en VSS en](#) la Guía del usuario de Amazon EC2 . Para ver una política de IAM de ejemplo, consulte [Políticas administradas para AWS Backup](#).
3. [Descargar e instalar los componentes de VSS](#) en la instancia de Windows on Amazon EC2
4. Habilite VSS en: AWS Backup
 1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
 2. En el panel, elija el tipo de copia de seguridad que desea crear, ya sea Crear una copia de seguridad bajo demanda o Administrar planes de Backup. Proporcione la información necesaria para el tipo de copia de seguridad.
 3. Cuando asigne recursos, elija. EC2 Actualmente, las copias de seguridad de Windows VSS solo se admiten en EC2 instancias.
 4. En la sección Configuración avanzada, elija Windows VSS. Esto le permite realizar copias de seguridad de Windows VSS coherentes con la aplicación.
 5. Cree su copia de seguridad.

Un trabajo de copia de seguridad con un estado Completed no garantiza que la parte de VSS se realice correctamente; la inclusión de VSS se realiza sobre la base del mejor esfuerzo. Siga los siguientes pasos para determinar si una copia de seguridad es coherente con la aplicación, coherente ante bloqueos o no ha tenido éxito:

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En Mi cuenta, en el menú de navegación de la izquierda, haz clic en Trabajos.
3. Un estado Completed indica que el trabajo se ha realizado correctamente y es coherente con la aplicación (VSS).

Un estado Completed with issues indica que la operación de VSS ha tenido errores, por lo que solo se ha realizado correctamente una copia de seguridad coherente ante bloqueos. Este estado también tendrá un mensaje emergente "Windows VSS Backup Job Error encountered, trying for regular backup".

Si la copia de seguridad no se realizó correctamente, el estado será Failed.

4. Para ver detalles adicionales del trabajo de copia de seguridad, haga clic en el trabajo individual. Por ejemplo, los detalles pueden indicar `Windows VSS Backup attempt failed because of timeout on VSS enabled snapshot creation`.

Las copias de seguridad compatibles con VSS con un objetivo que no sea Windows o que no sea Windows con un componente de VSS que funcione correctamente serán coherentes ante bloqueos sin VSS.

Instancias de Amazon EC2 no compatibles

Los siguientes tipos de EC2 instancias de Amazon no son compatibles con las copias de seguridad de Windows habilitadas para VSS porque son instancias pequeñas y es posible que no realicen la copia de seguridad correctamente.

- t3.nano
- t3.micro
- t3a.nano
- t3a.micro
- t2.nano
- t2.micro

Copia de seguridad y copia de etiquetas

Para la mayoría de los tipos de recursos, puede copiar las copias de seguridad Regiones de AWS en varias Cuentas de AWS copias de seguridad, a pedido o automáticamente como parte de un plan de copias de seguridad programadas, aunque las copias de seguridad almacenadas en frío o en capas de archivo no se pueden copiar. Consulte [the section called “Disponibilidad de características por recurso”](#) y [Cifrado para obtener una copia de seguridad en una cuenta o Región de AWS diferentes](#) obtener más información.

También puede automatizar una secuencia de copias entre cuentas y entre regiones para la mayoría de los recursos compatibles, excepto Amazon RDS y Aurora. Para las instantáneas de Amazon RDS y Aurora, AWS Backup solo admite la automatización de copias entre cuentas o entre regiones debido a la forma en que esos servicios crean sus claves de cifrado (no se admite la copia de una instantánea de un clúster de base de datos Multi-AZ).

Algunos tipos de recursos tienen capacidades de copia de seguridad continua y copia entre regiones y entre cuentas. Cuando se realiza una copia entre regiones o entre cuentas de una copia de seguridad continua, el punto de recuperación copiado (copia de seguridad) se convierte en una copia de seguridad de instantánea (periódica) (no disponible para todos los tipos de recursos compatibles con ambos tipos de copias de seguridad). Según el [tipo de recurso](#), las instantáneas pueden ser una copia incremental o una copia completa. El PITR (Point-in-Time restauración) no está disponible para estas copias.

Important

Las copias conservan su configuración de origen, incluidas las fechas de creación y el periodo de retención. La fecha de creación se refiere al momento en que se creó la fuente, no al momento en que se creó la copia. Puede anular el periodo de retención.

La configuración de la copia de seguridad de origen que se está copiando anula la configuración de caducidad de la copia si el periodo de retención de copias se establece en Siempre en la AWS Backup consola (o el [DeleteAfterDays](#) valor se establece -1 en la solicitud de API); es decir, una copia con una configuración de retención establecida para que no caduque nunca conservará la fecha de caducidad de su punto de recuperación de origen.

Si desea que la nueva copia de seguridad no venza nunca, configure las copias de seguridad de origen para que nunca venzan o especifique que la nueva copia venza 100 años después de su creación.

Reintento de los trabajos de copia

AWS Backup implementa la siguiente estrategia de reintento para los trabajos de copia: si AWS Backup se detecta algún error en el sistema, el trabajo de copia entra en una fase de reintento que dura 2 horas. Durante este tiempo, el estado del trabajo de copia permanece en ese estado CREATED mientras el sistema intenta iniciar el trabajo de forma periódica. Si el trabajo se inicia correctamente en ese período, pasa al estado RUNNING.

Si los problemas persisten más allá del período de reintento de 2 horas, el equipo de AWS Backup servicio recibe una alerta automática. A continuación, el equipo investigará y abordará cualquier problema subyacente. Una vez resuelto, se vuelve a intentar realizar la copia manualmente, comprobando que los trabajos de copia se completen según lo solicitado.

El proceso de reintento del trabajo de copia es diferente del proceso de reintento del trabajo de copia de seguridad, que utiliza un período de inicio definido con reintentos periódicos hasta que se ejecute correctamente o hasta que caduque. El mecanismo de trabajos de copia proporciona un nivel adicional de fiabilidad al incorporar la intervención directa del equipo de servicio en caso de problemas persistentes.

Contenido

- [Creación de copias de seguridad en Regiones de AWS](#)
- [Creación de copias de las copias de seguridad entre Cuentas de AWS](#)
- [Copia de etiquetas en copias de seguridad](#)

Creación de copias de seguridad en Regiones de AWS

Con él AWS Backup, puede copiar copias de seguridad Regiones de AWS en varias copias de seguridad a pedido o automáticamente como parte de un plan de copias de seguridad programado. La replicación entre regiones resulta especialmente útil si hay requisitos de continuidad del negocio o de conformidad que exigen que las copias de seguridad deben almacenarse a una distancia mínima de los datos de producción. Para ver un tutorial de vídeo, consulte [Managing cross-Region copies of backups](#).

Cuando copia una copia de seguridad en una nueva Región de AWS por primera vez, AWS Backup copia la copia de seguridad completa. En general, si un servicio admite copias de seguridad incrementales, las copias posteriores de esa copia de seguridad incluidas en el mismo Región de AWS serán incrementales. AWS Backup volverá a cifrar su copia con la clave gestionada por el cliente de su almacén de destino.

Una excepción es Amazon EBS, pues si se cambia el estado de cifrado de una instantánea durante una operación de copia, [podría generarse una copia completa \(no incremental\)](#).

Requisitos

- La mayoría de los recursos AWS Backup compatibles admiten copias de seguridad entre regiones. Para obtener información detallada, consulte [Disponibilidad de características por recurso](#).
- La mayoría de AWS las regiones admiten copias de seguridad entre regiones. Para obtener información detallada, consulte [Disponibilidad de las funciones por Región de AWS](#).
- AWS Backup no admite copias entre regiones para su almacenamiento en capas frías.

Cifrado de copias entre regiones

Consulte [Cifrado para obtener una copia de seguridad en una cuenta o Región de AWS](#) para obtener más información sobre el funcionamiento del cifrado en los trabajos de copia.

Consideraciones de copia entre regiones con recursos específicos

Amazon RDS

No puede [copiar un grupo de opciones](#) a otro Región de AWS. Si lo intenta, puede aparecer un error como: “La instantánea requiere un grupo de opciones de destino con las siguientes opciones: ...”

Debe introducir los mismos grupos de opciones en el destino Región de AWS al crear una nueva copia entre regiones de una instantánea de Amazon RDS.

Realización de copias de seguridad entre regiones bajo demanda

Para replicar una copia de seguridad existente bajo demanda

1. [Abra la AWS Backup consola en /backup. https://console.aws.amazon.com](#)
2. Elija Almacenes de Backup.
3. Elija el almacén que contenga el punto de recuperación que desee copiar.
4. En la sección Copias de seguridad, seleccione el punto de recuperación que desee copiar.
5. Con el botón desplegable Acciones, elija Copiar.
6. Escriba los siguientes valores:

Copiar al destino

Elija el destino Región de AWS de la copia. Puede agregar una nueva regla a cada copia que se realice en un nuevo destino.

Almacén de copias de seguridad de destino

Elija el almacén de copia de seguridad de destino de la copia.

Transferir al almacenamiento en frío

Elija cuándo realizar la transferencia de una copia de la copia de seguridad al almacenamiento en frío. Las copias de seguridad que se han migrado al almacenamiento en frío deben permanecer en él durante un mínimo de 90 días. Este valor no se puede modificar una vez que la copia se ha migrado al almacenamiento en frío.

Para ver la lista de recursos que puede transferir al almacenamiento en frío, consulte la sección “Ciclo de vida al almacenamiento en frío” de la tabla [Disponibilidad de características por recurso](#). La expresión de almacenamiento en frío se omite para otros recursos.

Periodo de retención

Especifica el número de días que deben transcurrir desde la creación hasta que se elimina la copia. Este valor debe ser 90 días superior al valor de Transferir al almacenamiento en frío.

rol de IAM

Elija la función de IAM que AWS Backup se utilizará al crear la copia. El rol también debe AWS Backup figurar como entidad de confianza, lo que AWS Backup permite asumirlo. Si selecciona Predeterminado y el rol AWS Backup predeterminado no está presente en su cuenta, se le creará uno con los permisos correctos.

7. Elija Copiar.

Programación de la copia de seguridad entre regiones

Puede utilizar un plan de copia de seguridad programadas para copiar las copias de seguridad en Regiones de AWS.

Para copiar una copia de seguridad mediante un plan de copia de seguridad programadas

1. Abre la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En Mi cuenta, elija Planes de copia de seguridad y, a continuación, elija Crear plan de copia de seguridad.
3. En la página Crear plan de copia de seguridad, elija Crear un nuevo plan.
4. En Nombre del plan de copia de seguridad, introduzca un nombre para su plan de copia de seguridad.
5. En la sección Configuración de regla de copia de seguridad, agregue una regla de copia de seguridad que defina una programación de copia de seguridad, un intervalo de copia de seguridad y reglas de ciclo de vida. Puede agregar más reglas de copia de seguridad más adelante.
 - a. En Nombre, ingrese un nombre para la regla.

- b. Para Almacén de copia de seguridad, elija un almacén de la lista. Los puntos de recuperación de esta copia de seguridad se guardarán en este almacén. También puede crear un almacén de copias de seguridad nuevo.
- c. En Frecuencia de copia de seguridad, elija la frecuencia con la que desea realizar copias de seguridad.
- d. Para los servicios compatibles con el PITR, si desea utilizar esta función, seleccione **Habilitar las copias de seguridad continuas para la point-in-time recuperación (PITR)**. Para ver una lista de los servicios que admiten la PITR, consulta esa sección de la tabla [Disponibilidad de características por recurso](#).
- e. En Intervalo de copia de seguridad, elija Usar valores predeterminados de intervalo de copia de seguridad (recomendado). Puede personalizar el intervalo de copia de seguridad.
- f. En Copiar en el destino, elija la Región de AWS de destino de la copia de la copia de seguridad. La copia de seguridad se copiará en esta región. Puede agregar una nueva regla a cada copia que se realice en un nuevo destino. A continuación, ingrese los siguientes valores:

Copiar en el almacén de otra cuenta

No active esta opción. Para obtener más información sobre la copia multicuenta, consulta [Cómo crear](#) copias de seguridad en varias cuentas Cuentas de AWS

Almacén de copias de seguridad de destino

Elija el almacén de copias de seguridad de la región de destino donde se AWS Backup copiará la copia de seguridad.

Si desea crear un nuevo almacén de copias de seguridad para realizar copias entre regiones, elija **Crear nuevo almacén de copia de seguridad**. Ingrese la información en el asistente. A continuación, elija **Crear almacén de copia de seguridad**.

6. Elija **Crear plan**.

Creación de copias de las copias de seguridad entre Cuentas de AWS

Con él AWS Backup, puede realizar copias de seguridad de hasta varias Cuentas de AWS copias a pedido o automáticamente como parte de un plan de copias de seguridad programado. Utilice una copia de seguridad multicuenta si desea copiar sus copias de seguridad de forma segura a una o más personas Cuentas de AWS de su organización por motivos operativos o de seguridad. Si la

copia de seguridad original se elimina accidentalmente, puede copiar la copia de seguridad de su cuenta de destino a su cuenta de origen y, a continuación, iniciar la restauración. Para poder hacerlo, debe tener dos cuentas que pertenezcan a la misma organización en el servicio AWS Organizations . Para obtener más información, consulte [Tutorial: Creación y configuración de una organización](#) en la Guía del usuario de Organizations.

En su cuenta de destino, debe crear un almacén de copias de seguridad. A continuación, debe asignar una clave gestionada por el cliente para cifrar las copias de seguridad en la cuenta de destino y una política de acceso basada en los recursos para permitir el acceso AWS Backup a los recursos que desee copiar. En la cuenta de origen, si sus recursos están cifrados con una clave administrada por el cliente, debe compartir esta clave con la cuenta de destino. A continuación, puede crear un plan de copia de seguridad y elegir una cuenta de destino que forme parte de su unidad organizativa en AWS Organizations.

Al copiar una copia de seguridad en varias cuentas por primera vez, la AWS Backup copia de seguridad completa. En general, si un servicio admite copias de seguridad incrementales, las copias posteriores de esa copia de seguridad en la misma cuenta son incrementales. AWS Backup vuelve a cifrar la copia con la clave gestionada por el cliente de la bóveda de destino.

Requisitos

- Antes de administrar los recursos Cuentas de AWS en varias entradas AWS Backup, sus cuentas deben pertenecer a la misma organización del AWS Organizations servicio.
- La mayoría de los recursos compatibles AWS Backup admiten la copia de seguridad entre cuentas. Para obtener información detallada, consulte [Disponibilidad de características por recurso](#).
- La mayoría de AWS las regiones admiten la copia de seguridad entre cuentas. Para obtener información detallada, consulte [Disponibilidad de las funciones por Región de AWS](#).
- AWS Backup no admite copias multicuenta para su almacenamiento en niveles inactivos.

Configuración de la copia de seguridad entre cuentas

¿Qué necesita para crear copias de seguridad entre cuentas?

- Una cuenta de origen

La cuenta de origen es la cuenta en la que residen AWS los recursos de producción y las copias de seguridad principales.

El usuario de la cuenta de origen inicia la operación de copia de seguridad entre cuentas. El usuario o rol de la cuenta de origen debe tener los permisos de API adecuados para iniciar la operación. Los permisos adecuados pueden ser la política AWS gestionada `AWSBackupFullAccess`, que permite el acceso total a AWS Backup las operaciones, o una política gestionada por el cliente que permite realizar acciones como `ec2:ModifySnapshotAttribute`. Para obtener más información sobre los tipos de políticas, consulte [Políticas administradas por AWS Backup](#).

- Una cuenta de destino

La cuenta de destino es la cuenta en la que desea guardar una copia de su copia de seguridad. Puede elegir más de una cuenta de destino. La cuenta de destino debe estar en la misma organización que la cuenta de origen en AWS Organizations.

Debe “permitir” la política de acceso `backup:CopyIntoBackupVault` para su almacén de copias de seguridad de destino. La ausencia de esta política impedirá los intentos de copia en la cuenta de destino.

- Una cuenta de administración en AWS Organizations

La cuenta de administración es la cuenta principal de su organización, tal como la define AWS Organizations, que se utiliza para administrar las copias de seguridad entre cuentas entre sus Cuentas de AWS. Para utilizar la copia de seguridad entre cuentas, también debe habilitar la confianza en el servicio. Tras habilitar la confianza en el servicio, puede usar cualquier cuenta de la organización como cuenta de destino. Desde la cuenta de destino, puede elegir qué almacenes va a usar para realizar copias de seguridad entre cuentas.

- Habilite la copia de seguridad entre cuentas en la consola de AWS Backup

Para obtener información acerca de la seguridad, consulte [Consideraciones de seguridad para la copia de seguridad entre cuentas](#).

Para utilizar la copia de seguridad entre cuentas, debe habilitar la característica de copia de seguridad entre cuentas. A continuación, debe “permitir” la política de acceso `backup:CopyIntoBackupVault` a su almacén de copias de seguridad de destino.

[EC2 Se permiten EC2](#) ofertas de Amazon AMIs. Si esta configuración está habilitada en su cuenta, añada el ID de su cuenta de origen a la lista de permitidos. De lo contrario, la operación de copia fallará y aparecerá un mensaje de error como “Source AMI not found in Region”.

Habilitar la copia de seguridad entre cuentas

1. Inicie sesión con las credenciales AWS Organizations de su cuenta de administración. La copia de seguridad entre cuentas solo se puede habilitar o deshabilitar con estas credenciales.
2. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
3. En Mi cuenta, elija Configuración.
4. Para Copia de seguridad entre cuentas, elija Habilitar.
5. En Almacenes de copia de seguridad, elija su almacén de destino.

En el caso de las copias entre cuentas, la bóveda de origen y la bóveda de destino se encuentran en cuentas diferentes. Cambie a la cuenta propietaria de la cuenta de destino, según sea necesario.

6. En la sección Política de acceso, seleccione “Permitir” `backup:CopyIntoBackupVault`. Por ejemplo, elija Agregar permisos y, a continuación, Permitir el acceso a un almacén de copias de seguridad desde la organización. Se rechazará cualquier acción entre cuentas que no sea `backup:CopyIntoBackupVault`.
7. Ahora, cualquier cuenta de su organización puede compartir el contenido de su almacén de copias de seguridad con cualquier otra cuenta de su organización. Para obtener más información, consulte [Intercambio de un almacén de copias de seguridad con una cuenta de AWS diferente](#). Para limitar las cuentas que pueden recibir el contenido de los almacenes de copias de seguridad de otras cuentas, consulte [Configuración de la cuenta como cuenta de destino](#).

Programación de copias de seguridad entre cuentas

Puede utilizar un plan de copia de seguridad programadas para copiar las copias de seguridad en Cuentas de AWS.

Para copiar una copia de seguridad mediante un plan de copia de seguridad programadas

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En Mi cuenta, elija Planes de copia de seguridad y, a continuación, elija Crear plan de copia de seguridad.
3. En la página Crear plan de copia de seguridad, elija Crear un nuevo plan.
4. En Nombre del plan de copia de seguridad, introduzca un nombre para su plan de copia de seguridad.

5. En la sección Configuración de regla de copia de seguridad, agregue una regla de copia de seguridad que defina una programación de copia de seguridad, un intervalo de copia de seguridad y reglas de ciclo de vida. Puede agregar más reglas de copia de seguridad más adelante.

En Nombre de la regla, ingrese un nombre para la regla.

6. En la sección Programar, en Frecuencia, elija con qué frecuencia quiere que se realice la copia de seguridad.
7. En Intervalo de copia de seguridad, elija Usar valores predeterminados de intervalo de copia de seguridad (recomendado). Puede personalizar el intervalo de copia de seguridad.
8. Para Almacén de copia de seguridad, elija un almacén de la lista. Los puntos de recuperación de esta copia de seguridad se guardarán en este almacén. También puede crear un almacén de copias de seguridad nuevo.
9. En la sección Generar copia (opcional), ingrese los siguientes valores:

Región de destino

Elija el destino de Región de AWS la copia de seguridad. La copia de seguridad se copiará en esta región. Puede agregar una nueva regla a cada copia que se realice en un nuevo destino.

Copiar en el almacén de otra cuenta

Mueva el conmutador para elegir esta opción. La opción aparece en color azul cuando se selecciona. Aparecerá la opción ARN del almacén externo.

ARN del almacén externo

Ingrese el nombre de recurso de Amazon (ARN) de la cuenta de destino. El ARN es una cadena que contiene el ID de la cuenta y su. Región de AWS AWS Backup copiará la copia de seguridad a la bóveda de la cuenta de destino. La lista Región de destino se actualiza automáticamente a la región del ARN del almacén externo.

En Permitir el acceso al almacén de copias de seguridad, elija Permitir. A continuación, elija Permitir en el asistente que se abre.

AWS Backup necesita permisos para acceder a la cuenta externa y copiar la copia de seguridad al valor especificado. El asistente muestra el siguiente ejemplo de política que proporciona este acceso.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAccountCopyIntoBackupVault",
      "Effect": "Allow",
      "Action": "backup:CopyIntoBackupVault",
      "Resource": "*",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      }
    }
  ]
}
```

Transferir al almacenamiento en frío

Elija cuándo desea transferir la réplica de la copia de seguridad al almacenamiento en frío y cuándo va a caducar (se va a eliminar). Las copias de seguridad que se transfieran a cámaras frigoríficas deben almacenarse en cámaras frigoríficas durante un mínimo de 90 días. Este valor no se puede modificar una vez que la copia se ha migrado al almacenamiento en frío.

Para ver la lista de recursos que puede transferir al almacenamiento en frío, consulte la sección “Ciclo de vida al almacenamiento en frío” de la tabla [Disponibilidad de características por recurso](#). La expresión de almacenamiento en frío se omite para otros recursos.

Vencimiento especifica el número de días que deben transcurrir desde la creación hasta que se elimina la copia. Este valor debe ser 90 días superior al valor de Transferir al almacenamiento en frío.

Note

Cuando las copias de seguridad caduquen y estén marcadas para su eliminación como parte de su política de ciclo de vida, las AWS Backup eliminará en un momento

elegido al azar durante las 8 horas siguientes. Este intervalo ayuda a garantizar un rendimiento uniforme.

10. Elija Etiquetas agregadas a puntos de recuperación para agregar etiquetas a sus puntos de recuperación.
11. Para configurar las copias de seguridad avanzadas, elija Windows VSS para habilitar las instantáneas compatibles con las aplicaciones del software de terceros seleccionado en el que se esté ejecutando. EC2
12. Elija Crear plan.

Realización de copias de seguridad entre cuentas bajo demanda

Si lo desea, puede copiar una copia de seguridad en otro sitio. Cuenta de AWS

Para copiar una copia de seguridad bajo demanda

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En Mi cuenta, elija Almacén de copia de seguridad para ver todos tus almacenes de copias de seguridad en la lista. Puede filtrar por nombre o etiqueta del almacén de copias de seguridad.
3. Elija el ID de punto de recuperación de la copia de seguridad que desee copiar.
4. Elija Copiar.
5. Amplíe Detalles de la copia de seguridad para ver información sobre el punto de recuperación que está copiando.
6. En la sección Copiar configuración, elija una opción de la lista Región de destino.
7. Elija Copiar en el almacén de otra cuenta. La opción aparece en color azul cuando se selecciona.
8. Ingrese el nombre de recurso de Amazon (ARN) de la cuenta de destino. El ARN es una cadena que contiene el ID de la cuenta y su. Región de AWS AWS Backup copiará la copia de seguridad a la bóveda de la cuenta de destino. La lista Región de destino se actualiza automáticamente a la región del ARN del almacén externo.
9. En Permitir el acceso al almacén de copias de seguridad, elija Permitir. A continuación, elija Permitir en el asistente que se abre.

Para crear la copia, AWS Backup necesita permisos para acceder a la cuenta de origen. El asistente muestra un ejemplo de política que proporciona este acceso. Esta política se muestra a continuación:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAccountCopyIntoBackupVault",
      "Effect": "Allow",
      "Action": "backup:CopyIntoBackupVault",
      "Resource": "*",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      }
    }
  ]
}
```

10. En Transferir al almacenamiento en frío, elija cuándo desea transferir la copia de la copia de seguridad al almacenamiento en frío y cuándo va a vencer (se va a eliminar) la copia. Las copias de seguridad que se transfieran al almacenamiento en frío deben almacenarse en un almacenamiento en frío durante un mínimo de 90 días. Este valor no se puede modificar una vez que la copia se ha migrado al almacenamiento en frío.

Para ver la lista de recursos que puede transferir al almacenamiento en frío, consulte la sección “Ciclo de vida al almacenamiento en frío” de la tabla [Disponibilidad de características por recurso](#). La expresión de almacenamiento en frío se omite para otros recursos.

Vencimiento especifica el número de días que deben transcurrir desde la creación hasta que se elimina la copia. Este valor debe ser 90 días superior al valor de Transferir al almacenamiento en frío.

11. Para el rol de IAM, especifique el rol de IAM (por ejemplo, el rol predeterminado) que tiene los permisos necesarios para que la copia de seguridad esté disponible para su copia. El acto de copiar lo realiza el rol vinculado al servicio de la cuenta de destino.
12. Elija Copiar. Según el tamaño del recurso que está copiando, este proceso puede tardar varias horas en completarse. Cuando se complete el trabajo de copia, verá la copia en la pestaña Trabajos de copia del menú Trabajos.

Claves de cifrado y copias entre cuentas

Consulte [Cifrado para obtener una copia de seguridad en una cuenta o Región de AWS](#) para obtener más información sobre el funcionamiento del cifrado en un trabajo de copia.

Si necesita ayuda adicional para solucionar errores de copia entre cuentas, consulte el [AWS Knowledge Center](#).

Restaurar una copia de seguridad de una Cuenta de AWS a otra

AWS Backup no admite la recuperación de recursos de uno Cuenta de AWS a otro. Sin embargo, puede copiar una copia de seguridad desde una cuenta a otra diferente y, a continuación, restaurarla en esa cuenta. Por ejemplo, no puede restaurar una copia de seguridad de la cuenta A a la cuenta B, pero puede copiar una copia de seguridad de la cuenta A a la cuenta B y, a continuación, restaurarla en la cuenta B.

La restauración de una copia de seguridad de una cuenta a otra es un proceso de dos pasos.

Para restaurar una copia de seguridad de una cuenta a otra

1. Copie la copia de seguridad del origen Cuenta de AWS a la cuenta en la que desee restaurarla. Para obtener instrucciones, consulte [Configuración de la copia de seguridad entre cuentas](#).
2. Utilice las instrucciones correspondientes a su recurso para restaurar la copia de seguridad.

Intercambio de un almacén de copias de seguridad con una cuenta de AWS diferente

AWS Backup le permite compartir un almacén de copias de seguridad con una o varias cuentas, o con toda su organización AWS Organizations. Puede compartir un almacén de copias de seguridad de destino con una cuenta de AWS , un usuario o un rol de IAM de origen.

Para compartir un almacén de copias de seguridad de destino

1. Elija y AWS Backup y, a continuación, elija Almacenes de copia de seguridad.
2. Elija el nombre del almacén de copias de seguridad que desea compartir.
3. En el panel Política de acceso, elija el menú desplegable Agregar permisos.
4. Elija Permitir el acceso de nivel de cuenta a un almacén de copias de seguridad. O bien, puede optar por permitir el acceso a nivel de organización o de rol.
5. Ingrese el AccountID de la cuenta que quiere compartir con este almacén de copias de seguridad de destino.

6. Elija Guardar política.

Puede utilizar las políticas de IAM para compartir su almacén de copias de seguridad.

Compartir un almacén de copias de seguridad de destino con una Cuenta de AWS o rol de IAM

La siguiente política comparte un almacén de copias de seguridad con el número de cuenta 444455556666 y el rol de IAM SomeRole en el número de cuenta 111122223333.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam:444455556666:root",
          "arn:aws:iam:111122223333:role/SomeRole"
        ]
      },
      "Action": "backup:CopyIntoBackupVault",
      "Resource": "*"
    }
  ]
}
```

Comparte una bóveda de respaldo de destino en la que se encuentre una unidad organizativa AWS Organizations

La siguiente política comparte un almacén de copias de seguridad con las unidades organizativas que utilizan su PrincipalOrgPaths.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```

{
  "Effect": "Allow",
  "Principal": "*",
  "Action": "backup:CopyIntoBackupVault",
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringLike": {
      "aws:PrincipalOrgPaths": [
        "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbbb/",
        "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbbb/ou-jkl0-awsdddddd/"
      ]
    }
  }
}

```

Comparta una bóveda de respaldo de destino con una organización en AWS Organizations

La siguiente política comparte un almacén de copias de seguridad con la organización con un PrincipalOrgID de “o-a1b2c3d4e5”.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "backup:CopyIntoBackupVault",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgID": [
            "o-a1b2c3d4e5"
          ]
        }
      }
    }
  ]
}

```

```
}
```

Configuración de la cuenta como cuenta de destino

La primera vez que habilita las copias de seguridad multicuenta con su cuenta de AWS Organizations administración, cualquier usuario de una cuenta de miembro puede configurar su cuenta para que sea una cuenta de destino. Te recomendamos configurar una o más de las siguientes políticas de control de servicios (SCPs) AWS Organizations para limitar tus cuentas de destino. Para obtener más información sobre cómo adjuntar políticas de control de servicios a AWS Organizations los nodos, consulte [Adjuntar y separar políticas de control de servicios](#).

Limitar las cuentas de destino mediante etiquetas

Cuando se vincula a una cuenta AWS Organizations raíz, OU o individual, esta política limita las copias de los destinos de esa raíz, unidad organizativa o cuenta a solo aquellas cuentas con bóvedas de respaldo que hayas etiquetado. `DestinationBackupVault` El permiso `"backup:CopyIntoBackupVault"` controla el comportamiento del almacén de copias de seguridad y, en este caso, qué almacenes de copias de seguridad de destino son válidos. Utilice esta política, junto con la etiqueta correspondiente que se aplica a los almacenes de destino aprobados, para controlar el destino de las copias entre cuentas únicamente a las cuentas y almacenes de copia de seguridad aprobados.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "backup:CopyIntoBackupVault",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/DestinationBackupVault": "true"
        }
      }
    }
  ]
}
```


Limitar las cuentas de destino mediante números de cuenta y nombres de almacén

Cuando se vincula a una cuenta AWS Organizations raíz, OU o cuenta individual, esta política limita las copias que se originen en esa raíz, unidad organizativa o cuenta a solo dos cuentas de destino. El permiso "backup:CopyFromBackupVault" controla el comportamiento de un punto de recuperación del almacén de copias de seguridad y, en este caso, los destinos a los que se puede copiar ese punto de recuperación. El almacén de origen solo permitirá realizar copias en la primera cuenta de destino (112233445566) si uno o varios nombres del almacén de copias de seguridad de destino comienzan por cab-. El almacén de origen solo permitirá realizar copias en la segunda cuenta de destino (123456789012) si el destino es un almacén de copias de seguridad único llamado fort-knox.

Limite las cuentas de destino mediante unidades organizativas en AWS Organizations

Cuando estén asociadas a una AWS Organizations raíz o unidad organizativa que contenga su cuenta de origen, o cuando estén asociadas a su cuenta de origen, la siguiente política limita las cuentas de destino a aquellas cuentas que estén dentro de las dos especificadas OUs.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "backup:CopyFromBackupVault",
      "Resource": "*",
      "Condition": {
        "ForAllValues:StringNotLike": {
          "backup:CopyTargetOrgPaths": [
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbbb/",
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbbb/ou-jkl0-awsdddddd/"
          ]
        }
      }
    }
  ]
}
```

Consideraciones de seguridad para la copia de seguridad entre cuentas

Tenga en cuenta lo siguiente cuando realice copias de seguridad entre cuentas en AWS Backup:

- El almacén de destino no puede ser el almacén predeterminado. Esto se debe a que el almacén predeterminado está cifrado con una clave que no se puede compartir con otras cuentas.
- Es posible que las copias de seguridad entre cuentas sigan ejecutándose durante 15 minutos después de que deshabilite la copia de seguridad entre cuentas. Esto se debe a la coherencia futura y puede provocar que algunos trabajos entre cuentas se inicien o finalicen incluso después de deshabilitar la copia de seguridad entre cuentas.
- Si la cuenta de destino abandona la organización más adelante, esa cuenta retendrá las copias de seguridad. Para evitar una posible filtración de datos, incluya un permiso de denegación en el permiso `organizations:LeaveOrganization` en una política de control de servicio (SCP) asociada a la cuenta de destino. Para obtener información detallada al respecto SCPs, consulte [Eliminar una cuenta de miembro de su organización](#) en la Guía del usuario de Organizations.
- Si eliminas una función de copia durante una copia multicuenta, no AWS Backup podrás dejar de compartir las instantáneas de la cuenta de origen cuando se complete la tarea de copia. En este caso, el trabajo de copia de seguridad finaliza, pero el estado del trabajo de copia aparece como `Failed to unshare snapshot`.

Copia de etiquetas en copias de seguridad

En general, AWS Backup copia las etiquetas de los recursos que protege a sus puntos de recuperación. Para obtener más información sobre cómo copiar etiquetas durante una restauración, consulte [Copia de etiquetas durante una restauración](#).

Por ejemplo, cuando haces una copia de seguridad de un EC2 volumen de Amazon, AWS Backup copia sus etiquetas de recursos individuales y de grupo en la instantánea resultante, de acuerdo con lo siguiente:

- Para obtener una lista de permisos específicos de recursos que son necesarios para guardar etiquetas de metadatos en copias de seguridad, consulte [Permisos necesarios para asignar etiquetas a copias de seguridad](#).
- Las etiquetas que se asociaron originalmente a un recurso y las etiquetas que se asignaron durante la copia de seguridad se asignan a los puntos de recuperación almacenados en una bóveda de copias de seguridad, hasta un máximo de 50 (esta es una AWS limitación). Las

etiquetas asignadas durante la copia de seguridad tienen prioridad y ambos conjuntos de etiquetas se copian en orden alfabético.

- DynamoDB no admite la asignación de etiquetas a las copias de seguridad a menos que habilite primero la [Copia de seguridad avanzada de DynamoDB](#).
- Los volúmenes de Amazon EBS que se adjuntan a las EC2 instancias de Amazon son recursos anidados. Las etiquetas de los volúmenes de Amazon EBS que se adjuntan a las EC2 instancias de Amazon son etiquetas anidadas. Si no AWS Backup se pueden copiar las etiquetas anidadas, se produce un error en el trabajo de copia de seguridad.
- Cuando una EC2 copia de seguridad de Amazon crea un punto de recuperación de imágenes y un conjunto de instantáneas, AWS Backup copia las etiquetas en la AMI resultante. Si no AWS Backup se pueden copiar las etiquetas de los volúmenes asociados a la EC2 instancia de Amazon a las instantáneas resultantes, se produce un error en el trabajo de copia de seguridad.

Si copias la copia de seguridad en otra Región de AWS, AWS Backup copia todas las etiquetas de la copia de seguridad original en el destino Región de AWS.

Eliminaciones de las copias de seguridad

Le recomendamos que utilice AWS Backup para eliminar automáticamente las copias de seguridad que ya no necesite configurando su ciclo de vida al crear su plan de copias de seguridad. Por ejemplo, si configuras el ciclo de vida de tu plan de copias de seguridad para conservar los puntos de recuperación durante un año, se AWS Backup eliminarán automáticamente el 1 de enero de 2022 los puntos de recuperación que haya creado el 1 de enero de 2021 o en un plazo de varias horas. (distribuye sus eliminaciones de AWS Backup forma aleatoria dentro de las 8 horas siguientes a la expiración del punto de recuperación para mantener el rendimiento). Para obtener más información sobre cómo configurar su política de retención del ciclo de vida, consulte [Creación de un plan de copia de seguridad](#).

Sin embargo, es posible que desee eliminar manualmente uno o más puntos de recuperación. Por ejemplo:

- Tiene puntos de recuperación EXPIRED. Estos puntos de recuperación no AWS Backup se pudieron eliminar automáticamente porque eliminaste o modificaste la política de IAM original que utilizaste para crear tu plan de respaldo. Cuando AWS Backup intentó eliminarlos, no tenía permiso para hacerlo.

También se pueden crear puntos de recuperación caducados si un punto de EC2 recuperación de Amazon EBS o Amazon AWS gestionado tiene aplicado un bloqueo de instantáneas de Amazon EBS y AWS Backup no puede completar el proceso de ciclo de vida que normalmente provocaría la eliminación del punto de recuperación. Tenga en cuenta que estos puntos de recuperación caducados se pueden restaurar desde la EC2 consola y la [API](#) de Amazon o desde la consola y la [API](#) de Amazon EBS.

 Warning

Seguirá almacenando los puntos de recuperación vencidos en su cuenta. Esto podría aumentar los costos de almacenamiento.

Después del 6 de agosto de 2021, AWS Backup mostrará el punto de recuperación objetivo como Expirado en su bóveda de copias de seguridad. Si coloca el ratón sobre el estado rojo Vencido, aparecerá un mensaje de estado emergente en el que se explica por qué no se ha podido eliminar la copia de seguridad. También puede elegir Actualizar para obtener la información más reciente.

- Ya no desea que un plan de copia de seguridad funcione de la forma en que lo configuró. La actualización del plan de copia de seguridad afecta a los puntos de recuperación futuros que creará, pero no afecta al punto de recuperación que ya haya creado. Para obtener más información, consulte [Actualización de un plan de copia de seguridad](#).
- Tiene que depurar después de terminar una prueba o un tutorial.

Eliminación de las copias de seguridad manualmente

Para eliminar manualmente los puntos de recuperación

1. En la AWS Backup consola, en el panel de navegación, seleccione Backup Vaults.
2. En la página Backup vaults (Almacenes de copias de seguridad), elija el almacén de copias de seguridad donde almacenó las copias de seguridad.
3. Elija los puntos de recuperación y, a continuación, seleccione Acciones y Eliminar.
4. 1. Si la lista contiene una copia de seguridad continua, elija una de las siguientes opciones. Cada copia de seguridad continua tiene un único punto de recuperación.
 - Eliminar permanentemente mis datos de copia de seguridad o Eliminar punto de recuperación. Al seleccionar una de estas opciones, detendrá las copias de seguridad

continuas futuras y también eliminará los datos de las copias de seguridad continuas existentes.

 Note

Consulte [RespalDOS y point-in-time recuperación continuos \(PITR\)](#) para obtener información acerca de las consideraciones sobre el copia de seguridad continuo de Amazon S3, Amazon RDS y Aurora.

- Conservar mis datos de copia de seguridad continua o Desasociar el punto de recuperación. Al seleccionar una de estas opciones, detendrá las copias de seguridad continuas futuras, pero retendrá los datos de copia de seguridad continua existentes hasta que venzan, según lo definido por su periodo de retención.

Un punto de recuperación continua (copia de seguridad) de Amazon S3 disociado permanecerá en su almacén de copias de seguridad, pero su estado pasará a STOPPED.

2. Para eliminar todos los puntos de recuperación seleccionados, escriba delete y, a continuación, elija Eliminar puntos de recuperación.
3. AWS Backup comienza a enviar los puntos de recuperación para su eliminación y muestra una barra de progreso. Mantenga abierta la pestaña del navegador y no salga de esta página durante el proceso de envío.
4. Al final del proceso de envío, AWS Backup aparece un estado en el banner. El estado puede ser:
 - Enviado correctamente. Puede elegir Ver el progreso del estado de eliminación de cada punto de recuperación.
 - Obtiene un error de envío. Puede elegir Ver el progreso del estado de eliminación de cada punto de recuperación o Volver a intentar el envío.
 - Un resultado mixto, en el que algunos puntos de recuperación se enviaron correctamente y otros no.
5. Si elige Ver el progreso, puede revisar el Estado de eliminación de cada copia de seguridad. Si el estado de eliminación es Error o Vencido, puede hacer clic en ese estado para ver el motivo. También puede optar por Volver a intentar las eliminaciones con errores.

Solución de problemas de eliminaciones manuales

En raras ocasiones, es AWS Backup posible que no se complete la solicitud de eliminación. AWS Backup usa la función vinculada al servicio [AWSServiceRoleForBackup](#) para realizar eliminaciones.

Si la solicitud de eliminación tiene como resultado un error, compruebe que su rol de IAM tenga permiso para crear roles vinculados a servicios. En concreto, compruebe que su rol de IAM tenga la acción `iam:CreateServiceLinkedRole`. Si no la tiene, agregue este permiso al rol utilizado para crear una copia de seguridad. Al añadir este permiso, se pueden AWS Backup realizar eliminaciones manuales.

Si, tras confirmar que su rol de IAM incluye la acción `iam:CreateServiceLinkedRole`, los puntos de recuperación siguen estancados en el estado `DELETING`, es probable que estemos investigando el problema. Complete la eliminación de forma manual con los siguientes pasos:

1. Configure un recordatorio para regresar en 2 o 3 días.
2. Transcurridos 2 o 3 días, compruebe si hay puntos de eliminación `EXPIRED` recientes que hayan sido el resultado de su primera operación de eliminación manual.
3. Elimine manualmente esos puntos de recuperación `EXPIRED`.

Para obtener más información sobre roles, consulte [Uso de roles vinculados a servicios](#) y [Adición y eliminación de permisos de identidad de IAM](#).

Ediciones de copia de seguridad y etiquetas

Después de crear una copia de seguridad mediante AWS Backup, puede cambiar el ciclo de vida o las etiquetas de la copia de seguridad. El ciclo de vida define el momento en que se migra una copia de seguridad al almacenamiento en frío y cuándo dicho recurso vence. AWS Backup migra y da por vencidas automáticamente las copias de seguridad en función del ciclo de vida que se defina.

Para ver la lista de recursos que puede transferir al almacenamiento en frío, consulte la sección “Ciclo de vida al almacenamiento en frío” de la tabla [Disponibilidad de características por recurso](#). La expresión de almacenamiento en frío se omite para otros recursos.

 Note

La edición de las etiquetas de una copia de seguridad mediante la AWS Backup consola solo se admite para las copias de seguridad de los sistemas de archivos Amazon Elastic File System (Amazon EFS) y Amazon DynamoDB avanzado.

Las etiquetas que se agregaron al punto de recuperación al crear otros recursos seguirán apareciendo, pero aparecerán atenuadas y no se podrán editar. Aunque estas etiquetas no se pueden editar en la AWS Backup consola, puede editar las etiquetas de las copias de seguridad de estos otros servicios mediante la consola o la API del servicio.

Las copias de seguridad que se han migrado al almacenamiento en frío deben permanecer en él durante un mínimo de 90 días. Por lo tanto, el valor de retención debe tener 90 días más que el valor del número de días tras los cuales se transferirá al almacenamiento en frío. Al actualizar la configuración de “transition to cold after days” (número de días tras los cuales migrará a almacenamiento en frío), el valor debe tener como mínimo la edad de la copia de seguridad más un día. El valor de “número de días tras los cuales migrará a almacenamiento en frío” no puede cambiarse una vez que se ha migrado una copia de seguridad al almacenamiento en frío.

A continuación se muestra un ejemplo de cómo actualizar el ciclo de vida de una copia de seguridad.

Para editar el ciclo de vida de una copia de seguridad

1. [Inicie sesión en y abra Consola de administración de AWS la AWS Backup consola en https://console.aws.amazon.com/backup.](https://console.aws.amazon.com/backup)
2. En el panel de navegación, elija Backup vaults (Almacenes de copia de seguridad).
3. En la sección Backups (Copias de seguridad), elija una copia de seguridad.
4. En la página de detalles de copia de seguridad, elija Edit (Editar).
5. Configure los ajustes del ciclo de vida y, a continuación, seleccione Save (Guardar).

Búsqueda de copias de seguridad

Descripción general de

Con AWS Backup, puede crear copias de seguridad de los AWS recursos, también conocidas como puntos de recuperación. Puede buscar copias de seguridad de determinados tipos de

recursos, como Amazon S3 y Amazon EBS, así como los elementos y archivos incluidos en esas copias de seguridad mediante la AWS Backup consola o la línea de comandos.

AWS Backup le permite buscar en los metadatos de las copias de seguridad de los tipos de recursos compatibles de forma pormenorizada archivos u objetos que coincidan con las propiedades que ha definido en la búsqueda, como el tamaño, la fecha de creación y el tipo de recurso. Puede profundizar aún más definiendo las propiedades de los elementos que desea localizar.

En primer lugar, debe crear un índice de copia de seguridad que quiera incluir en una búsqueda futura. La creación del índice de copia de seguridad se puede automatizar mediante un plan de copia de seguridad o puede crear uno manualmente para cualquier punto de recuperación existente. Cuando quiera realizar la búsqueda, defina las propiedades de la copia de seguridad y del elemento que desee ver en los resultados de la búsqueda. También puede restaurar la copia de seguridad o el elemento que ha buscado en la búsqueda.

En este documento se describen los pasos para crear un índice de copias de seguridad, buscar copias de seguridad indexadas, realizar restauraciones a partir de los resultados de búsqueda y solucionar cualquier problema relacionado con las funciones de índice y búsqueda de las mismas.

AWS Backup

Casos de uso para índices y búsquedas de copias de seguridad

Usted puede ser un administrador que desea recuperar un archivo u objeto específicos. En lugar de identificar o adivinar manualmente qué copias de seguridad contienen los datos, puede buscar en los metadatos de los puntos de recuperación y restaurar las copias de seguridad, los archivos o los objetos exactos que necesita.

Restaurar una copia de seguridad completa tan solo para encontrar el elemento específico que podría contener puede llevar horas o días. En su lugar, la búsqueda de copias de seguridad le permite encontrar y restaurar únicamente el archivo u objeto específicos que necesita.

Las búsquedas de copias de seguridad son útiles para los administradores de copias de seguridad, los operadores de copias de seguridad, los propietarios de datos y otros profesionales de TI que interactúan con la copia de seguridad, la restauración y el cumplimiento de los datos.

Acceso

Antes de crear un índice y una búsqueda, su cuenta debe tener los permisos necesarios para realizar las operaciones.

Permisos de índice

Para las operaciones de indexación, las AWS Backup autenticaciones se basan en la función de IAM y no en las credenciales de usuario (para obtener información específica sobre el usuario y la función de IAM, consulte). [Autenticación](#)

Se requieren los siguientes permisos para crear un índice de una copia de seguridad de EBS. Estos permisos se incluyen en la política gestionada: [AWSBackupServiceRolePolicyForIndexing](#)

- `ec2:DescribeSnapshots`
- `ebs:ListSnapshotBlocks`
- `ebs:GetSnapshotBlock`
- `kms:Decrypt`

No se requieren permisos de índice para crear un índice de S3.

Permisos en búsquedas

Los siguientes permisos son obligatorios para crear una búsqueda. Estos permisos se incluyen en la política administrada [AWSBackupSearchOperatorAccess](#):

- `backup:ListIndexedRecoveryPointsForSearch`
- `backup:SearchRecoveryPoint`

Si decide cifrar los resultados de la búsqueda con una AWS KMS clave gestionada por el cliente, asegúrese de que la clave contenga los siguientes permisos:

- `kms:GenerateDataKey`
- `kms:Decrypt`

Flujo de procesos

Una búsqueda de copia de seguridad consta de tres pasos, además de un cuarto paso de restauración opcional para cuando quiera restaurar los elementos que devuelve la búsqueda.

Indexar las copias de seguridad: active la indexación en sus planes de copia de seguridad o cree manualmente un índice de copias de seguridad mediante la consola o la CLI para cada copia de seguridad (punto de recuperación) existente que desee que se pueda incluir en las búsquedas.

Buscar los metadatos de las copias de seguridad para un punto de recuperación, archivo u objeto: especifique las propiedades de las copias de seguridad y los elementos que desea encontrar en la búsqueda, por ejemplo, si busca en los buckets de S3 creados entre el 2 y el 6 de abril con etiquetas de `Administration` y para objetos de más de 100 MB y cuyo nombre de la clave contenga `Admin`.

Revisar los resultados de la búsqueda: si encuentra el punto de recuperación o el elemento que buscaba, tiene la opción de restaurarlo. Si no ha encontrado el punto de recuperación o el elemento, puede refinar las propiedades de la copia de seguridad y las propiedades del elemento y, a continuación, iniciar una nueva búsqueda.

Restaurar elementos específicos (opcional): especifique las rutas de los archivos o los elementos que desee restaurar, así como las condiciones de restauración.

Índices de copia de seguridad

Para poder realizar búsquedas, una copia de seguridad (punto de recuperación) debe tener primero un índice correspondiente.

La creación de índices de copia de seguridad se puede activar en un plan de copia de seguridad para que cada copia de seguridad futura también tenga un índice de copia de seguridad asociado. También puede crear un índice al crear una copia de seguridad bajo demanda.

También puedes crear un índice de forma retroactiva para un punto de recuperación existente, ya sea desde la pantalla de detalles del punto de recuperación de Vault de la AWS Backup consola o a través de ella. AWS CLI

Los puntos de recuperación de los tipos de recursos compatibles pueden tener un índice de copia de seguridad si se guardan en un almacén de copias de seguridad estándar (los puntos de recuperación de un almacén aislado lógicamente no admiten actualmente los índices de copia de seguridad).

Índices de copia de seguridad de S3

Una copia de seguridad de S3 puede ser periódica y programarse en un intervalo fijo de acuerdo con su plan de copia de seguridad. Cada vez que se crea una copia de seguridad periódica, se genera un índice de copias de seguridad para ella. Una copia de seguridad de S3 también puede ser continua, donde se registra cada cambio en la copia de seguridad. Dado que pueden producirse numerosos cambios a diario, solo se crea un índice de copias de seguridad por día para una copia de seguridad continua.

El primer índice de copias de seguridad que se crea para un punto de recuperación de S3 continuo está lleno; los índices posteriores para el mismo punto de recuperación pueden ser incrementales.

Índices de copia de seguridad de EBS

Cada índice de copias de seguridad creado para un punto de recuperación de EBS está lleno (no es incremental).

AWS Backup intenta reparar automáticamente los problemas de las instantáneas durante la creación de un índice de respaldo. Si un sistema de archivos estaba en mal estado cuando se creó el punto de recuperación, AWS Backup intentará recuperarlo automáticamente. Si esta recuperación genera un error, también se producirá un error en el trabajo de creación del índice.

La naturaleza de la instantánea determina si se puede indexar:

Se pueden indexar:

- Sistemas de archivos: ext2, ext3, ext4, vfat, xfs y ntfs

No se pueden indexar:

- Instantáneas en el archivo (almacenamiento en frío)
- RAID y otras opciones de almacenamiento en varios discos
- Enlaces simbólicos
- Enlaces duros

Pasos para la creación del índice de copias de seguridad

Console

Añada la creación de un índice de copias de seguridad a su plan de copia de seguridad.

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. Seleccione Planes de copia de seguridad en Mi cuenta en la barra de navegación izquierda.
3. Seleccione el enlace en el panel Planes de copia de seguridad con el nombre del plan en el que desee añadir la creación de índices.
4. En el segundo panel Reglas de copia de seguridad, seleccione Agregar regla de copia de seguridad.
5. Desplácese hacia abajo hasta el panel Índices de copias de seguridad. Marque la casilla junto a los tipos de recurso para los que desea crear un índice.

Con cada nueva copia de seguridad que cree este plan, también se creará simultáneamente el índice correspondiente para ese punto de recuperación.

Creación de un índice para un punto de recuperación existente

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. Seleccione Almacén en la barra de navegación izquierda.
3. Seleccione el enlace que aparece debajo de la columna denominada Almacén en el que se almacena la copia de seguridad en la que desea crear un índice de copias de seguridad.
4. Coloque una marca de verificación junto al punto de recuperación para el que desea crear un índice de copias de seguridad.
5. Seleccione el botón Acción y, a continuación, Crear índice.

Mientras se crea el índice, este tendrá el estado In progress. Cuando el estado cambie a Available, ya se podrá incluir el punto de recuperación en una búsqueda.

Cree un índice al crear una copia de seguridad bajo demanda.

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. Consulte los pasos de [Crear una copia de seguridad bajo demanda mediante AWS Backup](#) Creación de una copia de seguridad bajo demanda con AWS Backup.
3. En Configuración, si ha elegido un tipo de recurso que admite el índice y la búsqueda, se mostrará el elemento de línea Índice de búsqueda de copias de seguridad. Active el índice Crear un búsqueda de copias de seguridad para que se cree un índice de forma simultánea con esta copia de seguridad bajo demanda.

AWS CLI

Creación de un índice de copias de seguridad desde la CLI

Utilice el AWS CLI comando [create-backup-plan](#) para crear un nuevo plan de copias de seguridad. O bien, utilice [update-backup-plan](#) para modificar un plan existente.

Para cualquiera de dichas operaciones, incluya IndexActions en el parámetro `--backup-plan -rules`.

Para obtener más información, consulte [IndexActions](#) en [BackupRuleInput](#) en la Guía de referencia de la API de AWS Backup .

Cuando un punto de recuperación tenga un índice, ya podrá actualizar su configuración.

Ejemplo:

```
aws backup update-recovery-point-index-settings
--recovery-point-arn arn:aws:ec2:us-west-2::snapshot/snap-012345678901234567

--backup-vault-name [vaultname] //
--index ENABLED
--endpoint-url [URL]
--iam-role-arn arn:aws:iam::012345678901:role/Admin
```

Búsquedas

Una vez que tenga una o más copias de seguridad con un índice, puede buscar esas copias de seguridad indexadas a través de la AWS Backup consola o mediante AWS CLI.

Al crear una búsqueda, seleccionará un tipo de recurso. Los resultados solo devolverán puntos de recuperación que contengan ese tipo de recurso, como buckets de S3 o instantáneas de EBS.

Especifique las propiedades de las copias de seguridad (puntos de recuperación) que desea incluir en la búsqueda. Puede especificar hasta nueve propiedades. Los tipos de propiedad incluidos más de una vez devolverán resultados que coincidan con todos los valores incluidos.

Especifique las propiedades de los elementos que desea encontrar dentro de los puntos de recuperación devueltos, como el nombre de bucket o el tamaño de archivo. Limite sus resultados mediante la inclusión de varias propiedades.

Si se incluye un valor para una propiedad de elemento al crear una búsqueda a través de la consola de AWS Backup , los resultados devolverán solo los elementos que coincidan con esa propiedad de elemento (lógica AND). Si repite la misma propiedad de elemento, pero con valores diferentes, los resultados devolverán todos los elementos que coincidan con alguno de los valores incluidos (lógica OR). Por ejemplo, si incluye dos rutas de archivo de EBS, todos los elementos de los puntos de recuperación que se incluyan en la búsqueda y que coincidan con cualquiera de las rutas de archivo aparecerán en los resultados de la búsqueda.

- Las propiedades de los elementos de S3 incluyen la hora de creación, las ETags, la clave del objeto, el tamaño del objeto y el ID de versión.
- Las propiedades de los elementos de EBS que puede utilizar para filtrar la búsqueda son la hora de creación, la ruta del archivo, la hora de la última modificación y el tamaño.

Si lo desea, puede incluir un identificador AWS KMS clave para cifrar los resultados. Si no incluye una clave, AWS Backup utilizará una clave propiedad del servicio para cifrar los resultados.

Console

Búsqueda de elementos en sus copias de seguridad

Existen varias rutas para crear una búsqueda de copias de seguridad indexadas:

Para encontrar su punto de recuperación preferido, vaya a Almacenes de copia de seguridad y seleccione el punto de recuperación específico que desee buscar. Luego, seleccione Buscar. También puede iniciar una búsqueda desde la página Detalles del punto de recuperación.

Durante una restauración en la que desee incluir elementos específicos, puede buscar en las copias de seguridad para localizar las direcciones URL o las rutas de archivo que contengan los elementos.

Para buscar en más de una copia de seguridad, siga estos pasos:

1. [Abra la AWS Backup consola en /backup. https://console.aws.amazon.com](https://console.aws.amazon.com/backup)
2. En el menú de navegación izquierdo, vaya a Buscar.
3. Seleccione Crear búsqueda en la sección Historial de búsquedas.
4. Seleccione un tipo de recurso. Debe seleccionar un tipo de recurso para cada búsqueda. Si cambia el tipo de recurso después de introducir campos adicionales, las entradas se perderán y tendrá que volver a introducirlas.
5. Seleccione entre una y nueve propiedades de copia de seguridad para reducir los puntos de recuperación que devolverá la búsqueda.

AWS Backup escaneará todas las copias de seguridad que tengan un índice. Solo devolverá los puntos de recuperación que coincidan con todas las propiedades de copia de seguridad diferentes. Por ejemplo, `backup tag = "savings"` y `backup creation date = May 20, 2019 through May 23, 2019 inclusive`.

Puede incluir varios valores de la misma propiedad, como tres etiquetas diferentes. Si la propiedad se repite con valores diferentes, la búsqueda devolverá todos los elementos que coincidan con alguno de los valores especificados (lo que se conoce como lógica OR). Por ejemplo, `backup tag = "savings"; backup tag = "checking"; backup creation date = May 20, 2019 through May 23, 2019, inclusive; y backup creation date = May 20, 2020 through May 23, 2020, inclusive.`

El intervalo de fechas de creación de una copia de seguridad cuenta como una propiedad de la copia de seguridad. Solo se puede incluir un intervalo de fechas de creación de la copia de seguridad como propiedad de la copia de seguridad.

6. Elija entre una y nueve propiedades de elemento para reducir aún más los resultados de la búsqueda.

Puede incluir varios valores de la misma propiedad. Si la propiedad se repite con valores diferentes, la búsqueda devolverá todos los elementos que coincidan con alguno de los valores especificados.

7. Opcional: para cifrar los resultados de la búsqueda, puede especificar una AWS KMS clave existente en el menú desplegable o en el ARN, o puede crear una nueva clave de KMS.
8. AWS Backup recomienda crear un nombre de trabajo de búsqueda único.
9. Seleccione Iniciar búsqueda.

Es posible que vea una advertencia que indica que la búsqueda puede incluir un gran número de puntos de recuperación. La práctica recomendada es volver a las propiedades de la copia de seguridad y seleccionar criterios adicionales para limitar la búsqueda. Si hay menos copias de seguridad en una búsqueda, es posible que los costos sean menores.

AWS CLI

Utilice el AWS CLI comando [start-search-job](#).

Parámetros requeridos:

```
--search-scope // defines the backup properties you wish to include in the search
```

Parámetros opcionales:

```
--client-token // string
```

```
--encryption-key-arn // if not included, AWS Backup uses service-owned key to
encrypt results
--item-filters // accepted keys and values depend on which resource type is included
in the search
--name // If not included, AWS Backup auto-assigns a name
```

Los filtros de elementos de S3 aceptados son:

```
--object-keys // string
--sizes // long condition
--creation-times // time condition
--version-ids // string
--etags // string
```

Los filtros de elementos de EBS aceptados son:

```
--file-paths //
--sizes //
--creation-times //
--last-modification-time //
```

Detención de una búsqueda

Solo puede detener un trabajo de búsqueda si tiene el estado RUNNING.

Un trabajo de búsqueda continuará hasta que alcance el estado COMPLETED (o el estado FAILED si se produce un error). Puede interrumpir un trabajo de búsqueda con el estado RUNNING si desea finalizar un trabajo de búsqueda en curso, lo que puede ser conveniente si ha encontrado la copia de seguridad o el elemento que buscaba antes de completar el trabajo.

- En la AWS Backup consola, seleccione el botón Detener la búsqueda de trabajos.
- En la CLI, envíe la operación `stop-search-job` con el identificador del trabajo de búsqueda que desea detener.

Resultados de la búsqueda

Cuando se inicie el trabajo de búsqueda, empezará a agregar los resultados aunque tenga el estado Running. Mientras se esté ejecutando un trabajo de búsqueda y hasta que se complete, habrá disponibles resultados parciales:

- En la consola, los resultados se mostrarán a medida que se vayan obteniendo durante la búsqueda. Los resultados no se actualizan automáticamente, pero puede ver los últimos resultados si selecciona el botón de actualización. Para ver los resultados más allá de los primeros 1000 elementos, seleccione Exportar resultados.
- Las operaciones de CLI [get-search-job](#) [list-search-jobs](#) devuelven los estados de los trabajos de búsqueda. Si el estado del trabajo es RUNNING, la operación devuelve una lista incompleta.

Los resultados de un trabajo de búsqueda están disponibles en la consola y a través de la CLI durante siete días cuando la búsqueda se detiene o se completa. Durante este tiempo, puede exportar los resultados a su bucket de Amazon S3 preferido para poder acceder a los resultados una vez transcurrido este período de tiempo.

Cada trabajo de búsqueda contiene información detallada, disponible en la consola o mediante la CLI, incluidos los puntos de recuperación que se han buscado, el nombre y el estado de la búsqueda, su descripción, la fecha y hora de creación y finalización, e información sobre los objetos o elementos devueltos, así como el número de elementos y puntos de recuperación analizados.

Si los resultados no contienen el punto de recuperación, el elemento o el objeto que buscaba, puede crear una nueva búsqueda con diferentes propiedades de copia de seguridad y de elemento. Cada búsqueda se cobra de forma individual.

Cada tipo de recurso tiene consideraciones únicas en relación con los resultados que arroja la búsqueda:

- Una búsqueda en los puntos de recuperación de S3 no devolverá marcadores de eliminación como parte del resultado de la búsqueda, incluso si esos objetos coinciden con las propiedades del elemento especificado en la búsqueda.
- Los resultados de una búsqueda en EBS pueden tener un valor nulo para indicar el tiempo de creación en los sistemas de archivos en los que ese campo no es compatible. Estos sistemas de archivos pueden ser, entre otros, vfat, ext2/3 y versiones de XFS anteriores a la 5.

Exportación de los resultados de búsqueda a un bucket de S3

AWS Backup conserva los resultados de la búsqueda durante 7 días, a partir de la fecha y hora de finalización. Estos resultados se pueden ver en la AWS Backup consola o se pueden recuperar mediante la operación CLI. `list-search-job-results`

Se recomienda exportar los resultados de la búsqueda a un bucket de S3 para conservar los resultados una vez transcurridos los siete días de retención. El trabajo de exportación creará una carpeta denominada `Export Job ID` en el bucket designado y, a continuación, exportará los resultados a esa carpeta. Cuando los resultados se exporten allí, estarán disponibles mientras conserve el bucket.

Puede exportar los resultados de la búsqueda de cualquier tipo de recurso compatible, no solo de una búsqueda en S3.

Console

1. [Abra la AWS Backup consola en /backup. https://console.aws.amazon.com](https://console.aws.amazon.com/backup/)
2. Vaya a Trabajos > Trabajos de búsqueda.
3. Seleccione Resultados del trabajo de búsqueda.
4. Coloque una marca de verificación junto a los resultados que desee exportar.
5. Seleccione Exportar a S3.
6. Elija el bucket de S3 de destino para el trabajo de exportación.
7. Después de configurar todos los campos, seleccione Exportar.

La acción de exportación crea un trabajo de exportación. Se pueden ver en Trabajos > Trabajos de exportación. Cuando un trabajo de exportación alcanza el estado `COMPLETED`, la información de los resultados de la búsqueda está disponible en el bucket de S3 desde donde se puede descargar como uno o más archivos `.csv`.

AWS CLI

Use el AWS CLI comando [start-search-result-export-job](#).

Parámetros requeridos:

```
--search-job-identifier  
--export-specification
```

Parámetros opcionales:

```
--client-token  
--role-arn  
--tags
```

La operación devolverá `ExportJobArn` y `ExportJobIdentifier`.

Utilice [list-search-result-export-jobs](#) para recuperar los estados de los trabajos de exportación.

Consideraciones y prácticas recomendadas sobre los costos

Cada creación de un índice de copias de seguridad y cada trabajo de búsqueda incurre un cargo. Cada índice de copias de seguridad tiene un cargo por almacenamiento. Se cobra cada restauración realizada a partir de los resultados de búsqueda (como ocurre con todos los demás trabajos de restauración). Puede consultar más información en [Precios de AWS Backup](#).

Para limitar los posibles resultados devueltos por un trabajo de búsqueda, incluya varias propiedades de copia de seguridad y de elemento; esto puede reducir el costo en comparación con una búsqueda que abarque todos los puntos de recuperación posibles.

Restauración a partir de una búsqueda

Muchos clientes optan por buscar en sus copias de seguridad (y en los objetos o archivos que contienen) para encontrar un punto de recuperación específico o elementos que restaurar. Para obtener información general sobre la restauración, consulte [Restauración de una copia de seguridad por tipo de recurso](#).

Para restaurar desde los resultados de la búsqueda en la AWS Backup consola, vaya a Trabajos > Buscar resultados de trabajo > Restaurar. Para realizar una restauración AWS CLI completa, [start-restore-job](#) utilízala con metadatos específicos del tipo de recurso, el punto de recuperación y los elementos involucrados en la restauración.

Consulte [Restaure los datos de S3 mediante AWS Backup](#) para obtener más información sobre cómo restaurar un punto de recuperación con datos de S3, un bucket de S3 o hasta cinco objetos o carpetas con un bucket de S3.

Consulte [Restauración de un volumen de Amazon EBS](#) para obtener información sobre cómo restaurar una instantánea de EBS en un volumen nuevo que se conecte a una EC2 instancia.

Backup por niveles

Descripción general de

AWS Backup ofrece un nivel de almacenamiento en caliente más económico para las copias de seguridad de Amazon S3 que reduce los costes de almacenamiento a largo plazo hasta en un 30% y, al mismo tiempo, mantiene las capacidades de protección y recuperación de nivel empresarial. El nivel de bajo coste ofrece el mismo rendimiento y las mismas características que el nivel de almacenamiento en caliente. Puede configurar la organización en niveles para mover los datos de backup de S3 a un almacenamiento rentable en función de la antigüedad de los objetos de sus almacenes de backup.

AWS Backup La organización en niveles permite optimizar los costes de almacenamiento de los datos de backup de S3 que se conservan durante períodos prolongados debido a la conformidad normativa, la preparación para casos de desastre y las estrategias de protección contra el ransomware. Puede configurar la organización en niveles para todas las copias de seguridad de S3 de todos los almacenes de una cuenta o crear configuraciones específicas para almacenes y recursos protegidos específicos.

En primer lugar, cree una configuración de organización en niveles que especifique qué recursos de S3 deben organizarse en niveles y después de cuántos días (60 días como mínimo). Las configuraciones de organización en niveles se pueden automatizar para aplicarlas a todos los respaldos o se pueden destinar a recursos específicos. Cuando los datos de respaldo alcanzan el umbral de antigüedad especificado, pasan al nivel de almacenamiento de menor costo y mantienen las mismas capacidades de restauración.

Este documento describe los pasos para crear configuraciones por niveles, administrar los datos de respaldo por niveles, monitorear los ahorros de costos y solucionar cualquier problema relacionado con la función de organización en niveles. AWS Backup

Important

Consideraciones de costos para la organización de copias de seguridad en niveles:

- La organización en niveles de Backup tiene tres componentes de costo: nivel de almacenamiento en caliente, nivel de almacenamiento en caliente de bajo costo y costos de transición. Cuando los datos de backup pasen al nivel de menor costo, se le cobrará una tarifa única de transición por objeto, en función de la cantidad de objetos aptos para la organización en niveles.

- En el caso de conjuntos de datos grandes con muchos objetos, los costes de transición pueden ser importantes al principio, pero suelen compensarse con el ahorro continuo de almacenamiento de los datos que se conservan más allá del límite mínimo de 60 días.

Configuraciones por niveles

La organización en niveles de respaldo de S3 implica la creación de una configuración de organización en niveles que especifique qué recursos deben organizarse en niveles y el número de días antes de la transición (60 días como mínimo) al nivel de menor costo. Para permitir la optimización de los costos, los datos de respaldo deben estar cubiertos por una configuración por niveles.

La creación de configuraciones por niveles se puede configurar para que se aplique ampliamente a las copias de seguridad de todos los recursos de S3 de su cuenta, o bien puede orientarse a almacenes y recursos específicos. Puede crear varias configuraciones para gestionar diferentes requisitos de retención de datos y optimización de costes.

Las configuraciones por niveles se aplican tanto a los datos de copia de seguridad existentes en los almacenes como a las nuevas copias de seguridad creadas una vez establecida la configuración.

Las configuraciones de organización por niveles de respaldo de S3 especifican:

- Alcance de los recursos: todos los recursos de todos los almacenes, todos los recursos de un almacén específico o recursos individuales seleccionados. La configuración por niveles que se aplica a todos los almacenes y a todos los recursos se considera la configuración predeterminada.
- Tiempo de transición: 60 días como mínimo antes de que los datos pasen al nivel de menor coste
- Asignación de bóvedas: a qué bóvedas de respaldo se aplica la configuración (para todas las bóvedas o para un nombre de bóveda específico)
- Selección de recursos: hasta 5 reglas de selección de recursos diferentes por configuración

Restricciones de configuración:

- Una configuración por almacén: cada almacén solo puede tener una configuración de niveles aparte de la configuración predeterminada
- Máximo de 5 selecciones de recursos: la configuración específica de Vault admite hasta 5 grupos de recursos diferentes y los ajustes de estratificación correspondientes

- Máximo de 100 recursos: se pueden seleccionar hasta 100 recursos específicos de todos los grupos de recursos por configuración
- Prioridad del almacén: si existen «todos los depósitos» y configuraciones de almacén específicas, la configuración del almacén específica tiene prioridad

Creación de configuraciones por niveles

Creación de configuraciones de estratificación

Console

Para crear una configuración de estratificación para todos los almacenes (predeterminada)

1. [Abra la AWS Backup consola en /backup. https://console.aws.amazon.com](https://console.aws.amazon.com/backup)
2. En el panel de navegación, elija S3 Backup Tiering.
3. Seleccione Crear configuración.
4. Para el nombre de la configuración, introduzca un nombre descriptivo único.
5. Elija Todos los recursos de S3 en todos los almacenes.
6. Para organizar la configuración por niveles en días, introduzca el número de días (60 como mínimo) antes de que los datos pasen al nivel de menor coste.
7. (Opcional) Agregue etiquetas.
8. Seleccione Crear configuración.

Para crear una configuración de estratificación de almacenes específica

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, elija S3 Backup Tiering.
3. Seleccione Crear configuración.
4. Para el nombre de la configuración, introduzca un nombre descriptivo único.
5. Elija los recursos de S3 en un almacén específico.
6. Para seleccionar un almacén, seleccione un almacén de respaldo específico en el menú desplegable.
7. Para seleccionar los recursos, elija una de las siguientes opciones:

- a. Todos los recursos de S3 de este almacén para aplicarlos a todos los recursos de S3 del almacén
 - b. Recursos de S3 específicos en este almacén para seleccionar depósitos de S3 individuales
8. Si selecciona recursos específicos:
 - a. Elija recursos S3 individuales (hasta 100 en total en todos los grupos de recursos de una configuración)
 - b. Establezca la configuración de organización por niveles en días para cada grupo de recursos
 - c. Seleccione Añadir configuración de niveles para crear reglas adicionales (hasta 5 en total)
9. (Opcional) Agregue etiquetas.
10. Seleccione Crear configuración.

AWS CLI

Para crear una configuración de estratificación de todos los almacenes (predeterminada) mediante el AWS CLI

```
aws backup create-tiering-configuration \
--tiering-configuration '{
  "TieringConfigurationName": "MyTieringConfig",
  "BackupVaultName": "*",
  "ResourceSelection": [{
    "Resources": ["*"],
    "TieringDownSettingsInDays": 60,
    "ResourceType": "S3"
  }]
}'
```

Administrar las configuraciones de estratificación

Visualización de las configuraciones de estratificación

Puede ver las configuraciones de organización en niveles existentes a través de la AWS Backup consola o la AWS CLI API REST.

Console

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, elija S3 Backup Tiering.
3. Vea la lista de configuraciones con su alcance, configuración de transición y estado.

AWS CLI

Para obtener una lista de todas las configuraciones de organización en niveles mediante el AWS CLI

```
aws backup list-tiering-configurations --max-results 50
```

Para obtener detalles específicos de la configuración de estratificación

```
aws backup get-tiering-configuration --tiering-configuration-name "MyTieringConfig"
```

Modificación de las configuraciones de estratificación

Puede actualizar las configuraciones de estratificación existentes para cambiar el tiempo de transición, la selección de recursos o las asignaciones de los almacenes.

Console

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, elija la organización de copias de seguridad en niveles de S3.
3. Seleccione la configuración que desee modificar.
4. Seleccione Editar.
5. Actualice los ajustes deseados.
6. Para organizar la configuración por niveles en días, introduzca el número de días (60 como mínimo) antes de que los datos pasen al nivel de menor coste.
7. Seleccione Save changes (Guardar cambios).

AWS CLI

Para actualizar una configuración de organización por niveles mediante el AWS CLI


```
aws backup update-tiering-configuration \  
--tiering-configuration-name "MyTieringConfig" \  
--tiering-configuration '{  
  "BackupVaultName": "*",  
  "ResourceSelection": [{  
    "Resources": ["*"],  
    "TieringDownSettingsInDays": 60,  
    "ResourceType": "S3"  
  }]  
'
```

Eliminar configuraciones de estratificación

Puede eliminar las configuraciones de estratificación cuando ya no sean necesarias.

Console

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, elija la organización de copias de seguridad en niveles de S3.
3. Seleccione la configuración que desee eliminar.
4. Elija Eliminar.
5. Introduzca el nombre de la configuración de estratificación para confirmar la eliminación.
6. Elija Eliminar la configuración de estratificación.

AWS CLI

Para eliminar una configuración de estratificación mediante el AWS CLI

```
aws backup delete-tiering-configuration \  
--tiering-configuration-name "MyTieringConfig"
```

Nota: Al eliminar una configuración de organización por niveles, se mantienen los datos existentes en el nivel de menor coste, pero se evita que los datos nuevos se agrupen por niveles.

Cómo se aplican las configuraciones de organización por niveles de backup de S3

AWS Backup evalúa los objetos de las copias de seguridad para determinar si son aptos para organizarlos en niveles en función de su antigüedad. El servicio comprueba la antigüedad de los objetos a diario y transfiere los objetos aptos al nivel de menor coste en función de sus ajustes de configuración. La evaluación por niveles se realiza automáticamente en segundo plano. Cuando los objetos de una copia de seguridad alcanzan el límite de antigüedad especificado (60 días como mínimo), pueden ser objeto de transición durante el siguiente ciclo de evaluación.

Tanto los objetos de las copias de seguridad existentes como los objetos de copia de seguridad recién creados están sujetos a configuraciones por niveles. Si tiene varias configuraciones que podrían aplicarse a los mismos objetos de copia de seguridad, las configuraciones específicas de los almacenes tienen prioridad sobre las configuraciones que se aplican a todos los almacenes. El proceso de organización en niveles es irreversible: una vez que los objetos pasan al nivel de menor coste, permanecen allí hasta que se elimine la copia de seguridad, de acuerdo con sus políticas de retención.

Estructura de costos y monitoreo

Modelo de precios

La organización por niveles de backup de S3 utiliza una estructura de precios optimizada en cuanto a costos:

- Coste de almacenamiento: menor coste por GB/mes en comparación con el nivel cálido estándar
- Tarifa de transición: tarifa única por objeto si se pasa a un nivel de menor coste
- Coste de restauración: se cobra por GB al restaurar los datos, igual que en la restauración en el nivel cálido
- Sin cargos de recuperación: no hay cargos de recuperación adicionales

Supervisión de costos

Supervise sus ahorros en los costos de estratificación mediante:

- AWS Cost Explorer: tipos de uso separados para cada nivel de almacenamiento
- AWS Informes de costos y uso: desglose detallado con etiquetas de asignación de costos

- AWS Consola de Backup: información de configuración

Ejemplo de ahorro de costes

En el caso de un bucket S3 de 500 TB con mil millones de objetos, del que el 60% puede organizarse en niveles:

- Antes de la estratificación: 25 600\$ al mes
- Después de la división en niveles: 21 000\$ al mes
- Ahorro mensual: 4.600\$ al mes (reducción del 18%)
- Cuota de transición única: 6.000\$

Ejemplos de configuraciones

Ejemplo 1: Organización por niveles en toda la cuenta

Aplice la organización por niveles a todos los recursos de S3 en todos los almacenes de respaldo:

```
{
  "TieringConfigurationName": "MyTieringConfig",
  "BackupVaultName": "*",
  "ResourceSelection": [
    {
      "Resources": ["*"],
      "TieringDownSettingsInDays": 60,
      "ResourceType": "S3"
    }
  ]
}
```

Ejemplo 2:

Clasifica todos los recursos en una bóveda de MyBackupVault 4 niveles:

```
{
  "TieringConfigurationName": "MyTieringConfig",
  "BackupVaultName": "MyBackupVault4",
  "ResourceSelection": [
    {
      "Resources": ["*"],
```

```

    "TieringDownSettingsInDays":60,
    "ResourceType":"S3"
  }
]
}

```

Ejemplo 3:

Niveles específicos de niveles con reglas diferentes:

```

{
  "TieringConfigurationName":"MyTieringConfig",
  "BackupVaultName":"MyBackupVault",
  "ResourceSelection":[
    {
      "Resources": ["arn:aws:s3:::mybucket1", "arn:aws:s3:::mybucket2"],
      "TieringDownSettingsInDays": 60,
      "ResourceType": "S3"
    },
    {
      "Resources": ["arn:aws:s3:::mybucket3"],
      "TieringDownSettingsInDays": 120,
      "ResourceType": "S3"
    }
  ]
}

```

Ejemplo 4:

Establezca la regla para no estratificar un depósito (establezca la estratificación en 36500):

```

{
  "TieringConfigurationName":"MyTieringConfig",
  "BackupVaultName":"*",
  "ResourceSelection":[
    {
      "Resources":["arn:aws:s3:::mybucket7", "arn:aws:s3:::mybucket8"],
      "TieringDownSettingsInDays":36500,
      "ResourceType":"S3"
    }
  ]
}

```

Características y limitaciones compatibles

Características admitidas

- Tipos de backup: respaldos continuos y periódicos
- Tipos de bóvedas: bóvedas de respaldo estándar y bóvedas con huecos lógicos
- Bloqueo de bóveda: compatibilidad total con bóvedas de respaldo bloqueadas
- Entre regiones o cuentas: se copian datos por niveles (las copias se alojan en el nivel estándar en el lugar de destino)
- Capacidades de restauración: Point-in-time recuperación y restauraciones a nivel de elemento
- Búsqueda e indexación: compatibilidad total con la funcionalidad de búsqueda de copias de seguridad
- Cumplimiento: mantiene todas las capacidades de cumplimiento y auditoría

Limitaciones

- Tiempo mínimo de transición: 60 días antes de que los datos se puedan mover a un nivel de menor costo
- Límite de recursos: hasta 100 recursos específicos por configuración
- Límite de configuración: hasta 5 reglas de selección de recursos diferentes por configuración
- Una configuración por almacén: cada almacén solo puede tener una configuración de estratificación específica, aparte de la predeterminada
- Transición unidireccional: los datos trasladados a un nivel de menor coste permanecen allí hasta que se eliminan

Resolución de problemas

Problemas comunes

La configuración no se aplica a las copias de seguridad existentes

- Compruebe que la configuración esté correctamente asignada a los almacenes correctos
- Compruebe que los recursos estén correctamente seleccionados en las configuraciones de destino
- Asegúrese de que los datos de respaldo cumplan con el requisito de edad mínima (60 días)

AlreadyExistsException crear la configuración

- Asegúrese de que el nombre de la configuración por niveles sea único en su cuenta
- Compruebe si el almacén de destino ya tiene una configuración de estratificación activa

Errores de LimitExceededException

- Compruebe que no ha superado el máximo de 5 grupos de selección de recursos por configuración
- Compruebe que no ha seleccionado más de 100 recursos específicos

Costes de transición superiores a los esperados

- Revise la cantidad de objetos que se van a realizar la transición
- Tenga en cuenta el impacto de la tarifa de transición si los datos cambian con frecuencia
- Evalúe si la configuración del umbral mínimo es adecuada para su caso de uso

Restauración de una copia de seguridad por tipo de recurso

Cómo restaurar

Para ver las instrucciones de restauración de la consola y los enlaces a la documentación AWS Backup de cada tipo de recurso compatible, consulta los enlaces al final de esta página.

Para restaurar una copia de seguridad mediante programación, utilice la operación de API [StartRestoreJob](#).

Los valores de configuración (“restaurar metadatos”) que necesita para restaurar el recurso varían en función del recurso que desee restaurar. Para obtener los metadatos de configuración con los que se creó la copia de seguridad, puede llamar a [GetRecoveryPointRestoreMetadata](#). También hay ejemplos de restauración de metadatos en los enlaces al final de esta página.

La restauración desde el almacenamiento en frío suele tardar 4 horas más que la restauración desde el almacenamiento en caliente.

Para cada restauración, se crea un trabajo de restauración con un identificador de trabajo único, por ejemplo, 1323657E-2AA4-1D94-2C48-5D7A423E7394.

 Note

AWS Backup no proporciona ningún acuerdo de nivel de servicio (SLAs) durante el tiempo de restauración. Los tiempos de restauración pueden variar en función de la carga y la capacidad del sistema, incluso en el caso de restauraciones que contengan los mismos recursos.

Restauraciones no destructivas

Cuando se utiliza AWS Backup para restaurar una copia de seguridad, se crea un nuevo recurso con la copia de seguridad que se está restaurando. Esto sirve para evitar que la actividad de restauración destruya los recursos existentes.

Pruebas de restauración

Puede realizar pruebas en sus recursos para simular una experiencia de restauración. De este modo podrá determinar si cumple el objetivo de tiempo de restauración (RTO) de su organización y prepararse para futuras necesidades de restauración.

Para obtener más información, consulte [Pruebas de restauración](#).

Copia de etiquetas durante una restauración

 Note

Las restauraciones de Amazon DynamoDB, Amazon S3, SAP HANA en instancias de EC2 Amazon, máquinas virtuales y recursos de Amazon Timestream actualmente no tienen esta función disponible.

Introducción

Puede copiar etiquetas a medida que restaura un recurso si las etiquetas pertenecían al recurso protegido en el momento de la copia de seguridad. Las etiquetas, que son etiquetas que contienen un par de clave-valor, pueden ayudarle a identificar y buscar recursos. Al iniciar un trabajo de restauración, las etiquetas que pertenecían a los recursos originales de los que se hizo una copia de seguridad se pueden agregar al recurso que restaura.

Si decide incluir etiquetas durante un trabajo de restauración, este paso puede reemplazar la sobrecarga y el trabajo que supone aplicar etiquetas manualmente a los recursos una vez finalizado el trabajo de restauración. Tenga en cuenta que esto es distinto de agregar etiquetas nuevas a los recursos restaurados.

Al restaurar una copia de seguridad en el flujo de la consola, las etiquetas de origen se copian de forma predeterminada. En la consola, quite la marca de la casilla si quiere dejar de copiar las etiquetas a un recurso restaurado.

En la operación de la API `StartRestoreJob`, el parámetro `CopySourceTagsToRestoredResource` está configurado en `false` de forma predeterminada, lo que excluirá las etiquetas originales del recurso que está restaurando. Si desea incluir las etiquetas originales, configúrelo en `True`.

Consideraciones

- Un recurso puede tener hasta 50 etiquetas, incluidos los recursos restaurados. Consulte [Tagging your AWS resources](#) para obtener más información sobre los límites del etiquetado.
- Asegúrese de que el rol utilizado para restaurar o copiar etiquetas tenga los permisos correctos. El rol predeterminado para las restauraciones contiene los permisos necesarios. Un rol personalizado debe incluir permisos adicionales para etiquetar los recursos.
- Los siguientes recursos no son compatibles actualmente para restaurar la inclusión de etiquetas: VMware Cloud™ on AWS, VMware Cloud™ on, sistemas locales AWS Outposts, SAP HANA en EC2 instancias de Amazon, Timestream, DynamoDB, Advanced DynamoDB y Amazon S3.
- En el caso de las copias de seguridad continuas, se copiarán en el recurso restaurado las etiquetas del recurso original, a partir de la copia de seguridad más reciente.
- Las etiquetas no se copiarán en las restauraciones a nivel de elemento.
- Las etiquetas que se agregaron a una copia de seguridad después de que se completase el trabajo de copia de seguridad, pero que no estaban presentes en el recurso original antes de la copia de seguridad, no se copiarán en el recurso restaurado. Solo las copias de seguridad creadas después del 22 de mayo de 2023 son elegibles para la copia de etiquetas en la restauración.

Interacción de las etiquetas con recursos específicos

- Amazon EC2
 - Las etiquetas aplicadas a las EC2 instancias de Amazon restauradas también se aplican a los volúmenes de Amazon EBS restaurados adjuntos.

- Las etiquetas aplicadas a los volúmenes de EBS adjuntos a las instancias de origen no se copian en los volúmenes adjuntos a las instancias restauradas. Si tiene políticas de IAM que permiten o deniegan a los usuarios el acceso a los volúmenes de EBS en función de sus etiquetas, debe reasignar manualmente las etiquetas necesarias a los volúmenes restaurados para garantizar que sus políticas sigan vigentes.
- Al restaurar un recurso de Amazon EFS, debe copiarlo en un nuevo sistema de archivos. Las etiquetas no se pueden copiar en las restauraciones en un sistema de archivos existente.
- Amazon RDS
 - Si el clúster de RDS del que se hizo la copia de seguridad sigue activo, se copiarán las etiquetas de este clúster.
 - Si el clúster original ya no está activo, en su lugar, se copiarán las etiquetas de la instantánea del clúster.
 - Las etiquetas que estaban presentes en el recurso en el momento de la copia de seguridad se copiarán durante la restauración, independientemente de si el parámetro booleano para `CopySourceTagsToRestoredResource` está establecido en `True` o `False`. Sin embargo, si la instantánea no contiene etiquetas, se utilizará la configuración booleana anterior.
- De forma predeterminada, los clústeres de Amazon Redshift siempre incluyen etiquetas durante un trabajo de restauración.

Copia de etiquetas mediante la consola

1. Abra la [consola de AWS Backup](#).
2. En el panel de navegación, elija Recursos protegidos y seleccione el ID del recurso de Amazon S3 que desee restaurar.
3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID del recurso seleccionado. Para restaurar un recurso:
 - a. En el panel Copia de seguridad, elija el ID del punto de recuperación del recurso.
 - b. En la esquina superior derecha del panel, elija Restaurar (también puede ir al almacén de copias de seguridad, buscar el punto de recuperación, hacer clic en Acciones y, a continuación, hacer clic en Restaurar).
4. En la página Restaurar copia de seguridad, localice el panel denominado Restaurar con etiquetas. Para incluir todas las etiquetas del recurso original, mantenga marcada la casilla

de verificación (tenga en cuenta que en la consola esta casilla está marcada de forma predeterminada).

5. Haga clic en Restaurar copia de seguridad una vez que haya seleccionado todos los ajustes y roles que prefiera.

Para incluir etiquetas mediante programación

Use la operación de la API `StartRestoreJob`. Asegúrese de que el siguiente parámetro booleano esté establecido en `True`.

```
CopySourceTagsToRestoredResource = true
```

Si el parámetro booleano es `CopySourceTagsToRestoredResource = True`, el trabajo de restauración copiará las etiquetas de los recursos originales al material restaurado.

Important

El trabajo de restauración fallará si se incluye este parámetro para un recurso no compatible (sistemas locales VMware AWS Outposts, SAP HANA en EC2 instancias, Timestream, DynamoDB, Advanced DynamoDB y Amazon S3).

```
{
  "RecoveryPointArn": "arn:aws:ec2:us-east-1::image/ami-1234567890a1b234",
  "Metadata": {
    "InstanceInitiatedShutdownBehavior": "stop",
    "DisableApiTermination": "false",
    "EbsOptimized": "false",
    "InstanceType": "t1.micro",
    "SubnetId": "subnet-123ab456cd7efgh89",
    "SecurityGroupIds": "[\"sg-0a1bc2d345ef67890\"]",
    "Placement": "{\"GroupName\":null,\"Tenancy\": \"default\"}",
    "HibernationOptions": "{\"Configured\":false}",
    "IamInstanceProfileName": "UseBackedUpValue",
    "aws:backup:request-id": "1a2345b6-cd78-90e1-2345-67f890g1h2ij"
  },
  "IamRoleArn": "arn:aws:iam::123456789012:role/EC2Restore",
  "ResourceType": "EC2",
  "IdempotencyToken": "34ab5678-9012-3c4d-5678-efg9h01f23i4",
}
```

```
"CopySourceTagsToRestoredResource": true
}
```

Solución de problemas de restauración de etiquetas

ERROR: permisos insuficientes

SOLUCIÓN: asegúrese de tener los permisos necesarios en su rol de restauración para poder incluir etiquetas en el recurso restaurado. La política de roles de servicio [AWS administrado](#) predeterminada para las restauraciones contiene los permisos necesarios para esta tarea [AWSBackupServiceRolePolicyForRestores](#).

Si decide usar un rol personalizado, asegúrese de que estén presentes los siguientes permisos:

- `elasticfilesystem:TagResource`
- `storagegateway:AddTagsToResource`
- `rds:AddTagsToResource`
- `ec2:CreateTags`
- `cloudformation:TagResource`

Para obtener más información, consulte [Permisos de API](#).

Estados de los trabajos de restauración

Puede ver el estado de un trabajo de restauración en la página Trabajos de la consola de AWS Backup . Los estados de los trabajos de restauración incluyen pendiente, en ejecución, anulado, completado y error.

Temas

- [Restauración de un clúster de Amazon Aurora](#)
- [Restauración de Amazon Aurora DSQL](#)
- [Restaure las pilas CloudFormation](#)
- [Restauración de un clúster de DocumentDB](#)
- [Restauración de una tabla de Amazon DynamoDB](#)
- [Restauración de un volumen de Amazon EBS](#)
- [Restaurar una EC2 instancia de Amazon](#)

- [Restauración de un sistema de archivos de Amazon EFS](#)
- [Restaurar un clúster de Amazon EKS](#)
- [Restaure un sistema FSx de archivos](#)
- [Restauración de un clúster de Neptune](#)
- [Restauración de una base de datos de RDS](#)
- [Restauración de un clúster de Amazon Redshift](#)
- [Restauración de Amazon Redshift sin servidor](#)
- [Restaurar una base de datos SAP HANA en una EC2 instancia de Amazon](#)
- [Restaure los datos de S3 mediante AWS Backup](#)
- [Restauración de un volumen de Storage Gateway](#)
- [Restauración de una tabla de Amazon Timestream](#)
- [Restaure una máquina virtual mediante AWS Backup](#)

Restauración de un clúster de Amazon Aurora

Usa la AWS Backup consola para restaurar los puntos de recuperación de Aurora

AWS Backup restaura su clúster de Aurora; no crea ni adjunta una instancia de Amazon RDS a su clúster. En los siguientes pasos, creará y asociará una instancia de Amazon RDS al clúster de Aurora restaurado mediante la CLI.

La restauración de un clúster de Aurora requiere que especifique varias opciones de restauración. Para obtener información acerca de estas opciones, consulte [Información general de copias de seguridad y restauración de un clúster de base de datos Aurora](#) en la Guía del usuario de Amazon Aurora. Las especificaciones de las opciones de restauración se encuentran en la guía de la API de [RestoreDBClusterFromSnapshot](#).

Para restaurar un clúster de Amazon Aurora

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, elija Recursos protegidos y el ID del recurso de Aurora que desee restaurar.
3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID de recurso seleccionado. Para restaurar un recurso, en el panel Copias de seguridad, active el

botón de opción situado junto al ID del punto de recuperación del recurso. En la esquina superior derecha del panel, elija Restaurar.

4. En el panel Especificaciones de instancias, acepte los valores predeterminados o especifique las opciones de configuración de Motor de base de datos, Versión del motor de base de datos y Tipo de capacidad.

 Note

Si se selecciona el tipo de capacidad Serverless (Sin servidor), aparecerá el panel Capacity settings (Ajustes de capacidad). Especifique las opciones de configuración de Minimum Aurora capacity unit (Unidad mínima de capacidad de Aurora) y Maximum Aurora capacity unit (Unidad máxima de capacidad de Aurora) o elija diferentes opciones en la sección Additional scaling configuration (Configuración de escalado adicional).

5. En el panel de configuración, especifique un nombre que sea exclusivo para todas las instancias de clústeres de bases de datos que le pertenezcan Cuenta de AWS en la región actual.
6. En el panel Red y seguridad, acepte los valores predeterminados o especifique las opciones de configuración de Nube privada virtual (VPC), Grupo de subredes y Zona de disponibilidad.
7. En el panel Opciones de base de datos, acepte los valores predeterminados o especifique las opciones de configuración de Puerto de base de datos, Grupo de parámetros de clúster de base de datos e Autenticación de base de datos de IAM habilitada.
8. En el panel Backup (Copia de seguridad), acepte el valor predeterminado o especifique la opción de configuración de Copy tags to snapshots (Copiar etiquetas en instantáneas).
9. En el panel Backtrack (Rastreo), acepte el valor predeterminado o especifique las opciones de configuración de Enable Backtrack (Habilitar rastreo) o Disable Backtrack (Deshabilitar rastreo).
10. En el panel Encryption (Cifrado), acepte el valor predeterminado o especifique las opciones de configuración de Enable encryption (Habilitar cifrado) o Disable encryption (Deshabilitar cifrado).
11. En el panel Exportaciones de registros, elija los tipos de registro que desee publicar en Amazon CloudWatch Logs. El rol de IAM ya se ha definido.
12. En el panel Restore role (Restaurar rol), elija el rol de IAM que AWS Backup asumirá para esta restauración.
13. Después de especificar todos los ajustes, elija Restore backup (Restaurar copia de seguridad).

Aparecerá el panel Trabajos de restauración. En la parte superior de la página, aparecerá un mensaje con información sobre el trabajo de restauración.

14. Una vez finalizada la restauración, asocie el clúster de Aurora restaurado a una instancia de Amazon RDS.

Uso de la AWS CLI:

- Para Linux, macOS o Unix:

```
aws rds create-db-instance --db-instance-identifier sample-instance \  
    --db-cluster-identifier sample-cluster --engine aurora-mysql --db-  
instance-class db.r4.large
```

- Para Windows:

```
aws rds create-db-instance --db-instance-identifier sample-instance ^  
    --db-cluster-identifier sample-cluster --engine aurora-mysql --db-  
instance-class db.r4.large
```

Consulte las [copias de seguridad y la point-in-time restauración continuas \(PITR\)](#) para obtener información sobre las copias de seguridad continuas y la restauración en un momento determinado.

Utilice la AWS Backup API, la CLI o el SDK para restaurar los puntos de recuperación de Amazon Aurora

Utilice [StartRestoreJob](#). Los metadatos que puede incluir en un trabajo de restauración dependen de si va a restaurar una copia de seguridad continua a un momento dado (PITR) o de si va a restaurar una instantánea.

Restauración de un clúster desde una instantánea

Puede especificar los siguientes metadatos para un trabajo de restauración de instantáneas de Aurora. Consulte [RestoreDBClusterFromSnapshot](#) en la Referencia de la API de Amazon Relational Database Service para obtener más información y los valores aceptados.

```
// Required metadata:  
dbClusterIdentifier // string  
engine // string  
  
// Optional metadata:  
availabilityZones // array of strings  
backtrackWindow // long  
copyTagsToSnapshot // Boolean
```

```

databaseName // string
dbClusterParameterGroupName // string
dbSubnetGroupName // string
enableCloudwatchLogsExports // array of strings
enableIAMDatabaseAuthentication // Boolean
engineMode // string
engineVersion // string
kmsKeyId // string
optionGroupName // string
port // integer
scalingConfiguration // object
vpcSecurityGroupIds // array of strings

```

Ejemplo:

```

"restoreMetadata":{"EngineVersion":"5.6.10a","KmsKeyId":"arn:aws:kms:us-east-1:234567890123:key/45678901-ab23-4567-8cd9-012d345e6f7","EngineMode":"serverless","AvailabilityZones":["us-east-1b","us-east-1e","us-east-1c"],"Port":3306,"DatabaseName":"","DBSubnetGroupName":"default-vpc-05a3b07cf6e193e1g","VpcSecurityGroupIds":["sg-012d52c68c6e88f00"],"ScalingConfiguration":{"MinCapacity":2,"MaxCapacity":64,"AutoPause":true,"SecondsUntilAutoPause":300,"TimeoutAction":{"RollbackCapacityChange"},"EnableIAMDatabaseAuthentication":false,"DBClusterParameterGroupName":"default.aurora5.6","CopyTagsToSnapshot":true,"Engine":"aurora","EnableCloudwatchLogsExports":[]}}

```

Restauración de un clúster a un momento dado (PITR)

Cuando desee restaurar una copia de seguridad continua de Aurora (punto de recuperación) a un momento dado (PITR), especifique los siguientes metadatos. Consulte [RestoreDBClusterToPointInTime](#) en la Referencia de la API de Amazon Relational Database Service para obtener más información y los valores aceptados.

```

// Required metadata:
dbClusterIdentifier // string
engine // string
restoreToTime // timestamp; must be specified if UseLatestRestorableTime parameter isn't provided

// Optional metadata:
backtrackWindow // long
copyTagsToSnapshot // Boolean

```

```
dbClusterParameterGroupName // string
dbSubnetGroupName // string
enableCloudwatchLogsExports // array of strings
enableIAMDatabaseAuthentication // Boolean
engineMode // string
engineVersion // string
kmsKeyId // string
optionGroupName // string
port // integer
scalingConfiguration // object
vpcSecurityGroupIds // array of strings
```

Restauración de Amazon Aurora DSQL

Temas

- [Descripción general de](#)
- [Restauración de un clúster en una sola región de Aurora DSQL](#)
- [Restauración de un clúster multirregional de Aurora DSQL](#)
- [Solución de problemas de restauración de Aurora DSQL](#)
- [Preguntas frecuentes sobre la restauración de Aurora DSQL](#)

Descripción general de

Para restaurar un clúster de región única de Amazon Aurora DSQL, utilice la AWS Backup consola o la CLI para seleccionar el punto de recuperación (copia de seguridad) que desea restaurar. Para restaurar un clúster multirregional Aurora DSQL, ahora puede usar la AWS Backup consola o la CLI.

Para la restauración en una sola región, incluya el nombre, el cifrado del clúster y la protección contra la eliminación y, a continuación, inicie la restauración en un clúster recién creado.

Para la restauración multirregional, tendrá que especificar parámetros adicionales, como una región testigo, regiones homólogas y ajustes de la configuración regional. La restauración multirregional crea un clúster que abarca varias regiones de AWS, lo que proporciona una mayor disponibilidad y capacidades de recuperación ante desastres.

Restauración de un clúster en una sola región de Aurora DSQL

Puede restaurar un clúster DSQL de Aurora en una sola región mediante la AWS Backup consola o AWS CLI.

Console

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. Seleccione el botón Restaurar situado junto al punto de recuperación que desea restaurar.
3. Configure los ajustes del nuevo clúster en el que se restaurará el punto de recuperación.
 - a. De forma predeterminada, la AMK (clave AWS gestionada) se utilizará para cifrar los datos restaurados. También puede especificar una clave diferente.
 - b. La [protección contra la eliminación](#) de los clústeres de Aurora está habilitada de forma predeterminada, pero desmarque la casilla para desactivar la opción.
4. Revise la configuración y, cuando esté de acuerdo, seleccione el botón Restaurar copia de seguridad.

AWS Backup creará un nuevo clúster Aurora DSQL.

AWS CLI

Restauración en una sola región

1. Utilice el comando `aws backup start-restore-job` de la CLI para restaurar un clúster de Aurora desde el punto de recuperación especificado.
2. Incluya los metadatos necesarios para el trabajo de restauración. Ejemplo:

Example

```
aws backup start-restore-job \
  --recovery-point-arn "arn:aws:dsql:us-east-1:123456789012:cluster/example-
cluster/backup/example-backup" \
  --iam-role-arn "arn:aws:iam::123456789012:role/service-role/
AWSBackupDefaultServiceRole" \
  --metadata '{"regionalConfig":[{"region\":"us-east-1",
\isDeletionProtectionEnabled\:true,\kmsKeyId\":"my_key\"}]}' \
  --copy-source-tags-to-restored-resource
```

Restauración de un clúster multirregional de Aurora DSQL

La restauración de clústeres multirregionales Aurora DSQL se produce dentro de un triplete de regiones cerrado, que es un grupo de tres pares. Regiones de AWS La restauración multirregional

requiere que las regiones que especifique en la operación formen parte de un trío. Para obtener más información acerca de los clústeres multirregionales, consulte [Configuración de clústeres multirregionales](#).

Se admiten tríos de los siguientes grupos. Si hay más regiones, elija tres del mismo grupo.

- Este de EE. UU. (Norte de Virginia); Este de EE. UU. (Ohio); Oeste de EE. UU. (Norte de California)
- Europa (Irlanda); Europa (Londres); Europa (París); Europa (Fráncfort)
- Asia-Pacífico (Tokio); Asia-Pacífico (Seúl); Asia-Pacífico (Osaka)

Para completar la restauración multirregional, asegúrese de que dispone de los siguientes permisos:

- `backup:StartRestoreJob`
- `dsq1:UpdateCluster`
- `dsq1:AddPeerCluster`
- `dsq1:RemovePeerCluster`

Puede restaurar una copia de seguridad de un clúster de Aurora DSQL en varias regiones mediante la consola de AWS Backup o los comandos de la CLI.

Tip

Si tiene un plan de copia de seguridad con una regla que crea automáticamente una copia entre regiones en una de las regiones indicadas, la copia creada se puede utilizar para esta restauración multirregional.

La restauración multirregional comienza con su región actual. También necesitará:

- Una región homóloga con una copia idéntica entre regiones del punto de recuperación de su región actual
- Región testigo, una región designada Región de AWS que participa en configuraciones de clústeres multirregionales al permitir la escritura únicamente de registros de transacciones sin consumir espacio de almacenamiento para los datos reales. Para obtener más información sobre las regiones testigo, consulte [Creación de un clúster multirregional](#).

Los pasos individuales se muestran a continuación:

Console

La AWS Backup consola ahora admite la restauración multirregional para los clústeres DSQL de Aurora, lo que proporciona un proceso simplificado para crear clústeres que abarquen varias regiones. Para obtener más información acerca de los clústeres multirregionales, consulte [Configuración de clústeres multirregionales](#).

1. [Inicie sesión en la consola de AWS administración y abra la consola en AWS Backup / backup. https://console.aws.amazon.com](https://console.aws.amazon.com/backup)
2. En el panel de navegación, elija Backup vaults (Almacenes de copia de seguridad).
3. Elija el almacén de copias de seguridad que contenga el punto de recuperación de Aurora DSQL que desee restaurar.
4. Seleccione el punto de recuperación que desee restaurar y, a continuación, elija Restaurar.
5. En la página de restauración, en Opciones de restauración, seleccione Añadir regiones homólogas para activar la restauración multirregional.
6. Seleccione una Región de clúster homóloga en el menú desplegable. Esta región debe estar dentro del mismo trío que su región actual y también debe contener una copia entre regiones del punto de recuperación de la (primera) región actual.
7. Seleccione una Región testigo en el menú desplegable. Esta región también debe estar dentro del mismo trío.
8. Defina la Configuración del clúster para los clústeres de regiones principales y homólogas:
 - a. Para el clúster principal, configure:
 - Cifrado de clúster (opcional): seleccione una clave de KMS para el cifrado.
 - Protección contra eliminaciones: permite activar o desactivar la protección contra eliminaciones.
 - b. Para el clúster de regiones homólogas, configure:
 - Cifrado de clúster en regiones homólogas (opcional): seleccione una clave de KMS para el cifrado.
 - Protección contra eliminaciones del clúster en regiones homólogas: permite activar o desactivar la protección contra eliminaciones.
9. Revisa la configuración y seleccione Restaurar copia de seguridad.

10. La consola iniciará el proceso de restauración multirregional, que crea clústeres en ambas regiones y los vincula automáticamente.

AWS CLI

La restauración multirregional ahora se puede lograr mediante los nuevos metadatos de restauración orquestada con comandos AWS Backup CLI. Este enfoque simplifica el proceso al gestionar la vinculación de clústeres de forma automática. Para obtener más información sobre la creación de clústeres multirregionales mediante programación, consulte [Configuración de clústeres multirregionales](#) en la Guía del usuario de Aurora DSQL.

Important

Tanto el clúster principal como el clúster homólogo deben estar en regiones del mismo grupo. La operación fallará si los clústeres se encuentran en regiones que no forman parte del grupo. Los grupos admitidos son:

- Este de EE. UU. (Norte de Virginia); Este de EE. UU. (Ohio); Oeste de EE. UU. (Norte de California)
- Europa (Irlanda); Europa (Londres); Europa (París); Europa (Fráncfort)
- Asia-Pacífico (Tokio); Asia-Pacífico (Seúl); Asia-Pacífico (Osaka)

Restauración multirregional mediante el AWS CLI uso de metadatos de restauración orquestada

1. Cree un trabajo de restauración con el comando `aws backup start-restore-job` de la CLI con los nuevos metadatos de orquestación multirregionales:

Example

```
aws backup start-restore-job \  
--recovery-point-arn "arn:aws:backup:us-east-1:123456789012:recovery-  
point:abcd1234" \  
--iam-role-arn "arn:aws:iam::123456789012:role/service-role/  
AWSBackupDefaultServiceRole" \  
--metadata '{  
    "witnessRegion":"us-west-1",  
    "useMultiRegionOrchestration":"true",  
    "peerRegion":["us-east-2"]',
```

```
"regionalConfig":[{"region":"us-east-1","isDeletionProtectionEnabled":true,"kmsKeyId":"arn:aws:kms:us-east-1:123456789012:key/ba4b3773-4bb8-4a7a-994c-46ede70202f5"},{"region":"us-west-2","isDeletionProtectionEnabled":true,"kmsKeyId":"arn:aws:kms:us-west-2:123456789012:key/ba4b3773-4bb8-4a7a-994c-46ede70202f5"}]'\
--copy-source-tags-to-restored-resource
```

La estructura de metadatos incluye:

- **witnessRegion**: región que servirá de testigo para el clúster multirregional. Para obtener más información, consulte [Resiliencia en Amazon Aurora DSQL](#).
- **useMultiRegionOrchestration**: fíjela en `true` para activar la orquestación multirregional.
- **peerRegion**: matriz que contiene las regiones con clústeres homólogos en el clúster multirregional. Para obtener más información, consulte [MultiRegionProperties](#) la Referencia de la API DSQL de Aurora.
- **regionalConfig**: matriz que contiene la configuración de cada región:
 - **region**: El Región de AWS identificador.
 - **isDeletionProtectionEnabled**: Bandera booleana para protección contra enable/disable eliminaciones. Para obtener más información, consulte [CreateCluster](#) la Referencia de la API DSQL de Aurora.
 - **kmsKeyId**: ARN de la clave de KMS para el cifrado (opcional).

Si no se especifican las propiedades `regionalConfig`, se aplicarán los valores predeterminados: el cifrado predeterminado y `isDeletionProtectionEnabled = TRUE`.

2. Supervise el estado del trabajo de restauración con el comando `aws backup describe-restore-job`:

```
aws backup describe-restore-job --restore-job-id job-12345678
```

3. Cuando se complete el trabajo de restauración, puede verificar la configuración del clúster multirregional mediante la CLI de Aurora DSQL:

```
aws dsql describe-cluster --cluster-identifier your-cluster-id
```

Para obtener más información sobre las operaciones de clústeres multirregionales, consulte [UpdateCluster](#) la Referencia de la API Aurora DSQL.

Solución de problemas de restauración de Aurora DSQL

ERROR: permisos insuficientes

Causa posible: si intenta copiar un punto de recuperación de Aurora DSQL en una cuenta (copia entre cuentas) que nunca ha interactuado con la API de DSQL, es posible que se produzca un error de emisión de permisos, ya que el rol vinculado al servicio de DSQL no está configurado en la cuenta de destino.

Solución: adjunte la [política gestionada de DSQL](#), que incluye la función vinculada al servicio de DSQL [AuroraDsqlServiceLinkedRolePolicy](#), a una función de la cuenta de destino.

Si tiene algún otro problema con el proceso de copia de seguridad o restauración, puede comprobar el estado de las tareas de copia de seguridad y restauración en la AWS Backup consola o mediante la AWS CLI. Además, puede revisar los AWS CloudTrail registros para ver si hay mensajes de error o eventos relevantes relacionados con sus AWS Backup operaciones.

Preguntas frecuentes sobre la restauración de Aurora DSQL

1. «¿Puedo usarlo AWS Backup para Aurora DSQL desde la consola Aurora DSQL?»

No, solo puede realizar copias de seguridad y restauraciones, así como administrar las copias de seguridad, desde la consola, el SDK o la CLI de AWS Backup .

2. “¿Qué nivel de detalle de copia de seguridad está disponible para Aurora DSQL? ¿Puedo hacer copias de seguridad de tablas o bases de datos específicas de mi clúster?”

Solo puede realizar copias de seguridad y restaurar un clúster de Aurora DSQL completo.

3. “¿Las copias de seguridad de Aurora DSQL son copias de seguridad completas o incrementales?”

Los puntos de recuperación de los clústeres de Aurora DSQL (copias de seguridad) son copias de seguridad completas de sus clústeres.

4. “¿Puedo crear copias de seguridad para mis clústeres multirregionales de Aurora DSQL?”

Sí, puede crear copias de seguridad para cada clúster en clústeres multirregionales si sigue los mismos pasos que para crear una copia de seguridad de un solo clúster en una sola región.

AWS Backup recomienda crear una copia regional de la copia de seguridad en la otra región desde la que planea restaurar el clúster multirregional, ya que la restauración multirregional requiere una copia idéntica del mismo punto de recuperación [si es idéntico en esta operación, los puntos de recuperación tienen el mismo nombre de recurso y la misma hora de creación].

5. “¿Mi clúster restaurado sobrescribirá el clúster existente?”

No. Al restaurar los datos de Aurora DSQL, AWS Backup crea un nuevo clúster a partir de las instantáneas; el clúster restaurado no sobrescribirá el clúster de origen.

Restaurar las pilas CloudFormation

Una copia de seguridad CloudFormation compuesta es una combinación de una CloudFormation plantilla y todos los puntos de recuperación anidados asociados. Se puede restaurar cualquier número de puntos de recuperación anidados, pero el punto de recuperación compuesto (que es el punto de recuperación de nivel superior) no se puede restaurar.

Al restaurar un punto de recuperación de una CloudFormation plantilla, se crea una pila nueva con un conjunto de cambios que representa la copia de seguridad.

Restaurar CloudFormation con la AWS Backup consola

Desde la [CloudFormation consola](#) puedes ver la nueva pila y el conjunto de cambios. Para obtener más información sobre los conjuntos de cambios, consulte [Updating stacks using change sets](#) en la Guía del usuario de CloudFormation .

Determina los puntos de recuperación anidados desde los que deseas realizar la restauración con tu CloudFormation pila y, a continuación, restaúralos con la AWS Backup consola.

1. Abre la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. Vaya a Almacenes de copia de seguridad, seleccione el almacén de copias de seguridad que contenga el punto de recuperación deseado y, a continuación, haga clic en Puntos de recuperación.
3. Restaurar el punto CloudFormation de recuperación de la plantilla.

- a. Haga clic en el punto de recuperación compuesto que contiene los puntos de recuperación anidados que desea restaurar para que aparezca la página de detalles del punto de recuperación compuesto.
 - b. En Puntos de recuperación anidados, se mostrarán los puntos de recuperación anidados. Cada punto de recuperación tendrá un identificador de punto de recuperación, un estado, un identificador de recurso, un tipo de recurso, un tipo de copia de seguridad y la hora en que se creó el punto de recuperación. Haga clic en el botón de radio situado junto al punto de CloudFormation recuperación y, a continuación, haga clic en Restaurar. Asegúrese de seleccionar el punto de recuperación que tenga el tipo de recurso: CloudFormation y el tipo de copia de seguridad: copia de seguridad.
4. Cuando se complete el trabajo de restauración de la CloudFormation plantilla, la CloudFormation plantilla restaurada estará visible en la [CloudFormation consola](#), en Stacks.
 5. En Nombres de pilas, encontrará la plantilla restaurada con el estado REVIEW_IN_PROGRESS.
 6. Haga clic en el nombre de la pila para ver los detalles de la pila.
 7. Hay pestañas debajo del nombre de la pila. Haga clic en Conjuntos de cambios.
 8. Ejecute el conjunto de cambios.
 9. Tras este proceso, los recursos de la pila original se volverán a crear en la nueva pila. Los recursos con estado se volverán a crear vacíos. Para recuperar los recursos activos, vuelve a la lista de puntos de recuperación de la AWS Backup consola, selecciona el punto de recuperación que necesitas e inicia una restauración.

Restaura CloudFormation con AWS CLI

En la interfaz de línea de comandos, [start-restore-job](#) permite restaurar una CloudFormation pila.

La siguiente lista contiene los metadatos aceptados para restaurar un CloudFormation recurso.

```
// Mandatory metadata:
ChangeSetName // This is the name of the change set which will be created
StackName // This is the name of the stack that will be created by the new change set

// Optional metadata:
ChangeSetDescription // This is the description of the new change set
StackParameters // This is the JSON of the stack parameters required by the stack
aws:backup:request-id
```


Restauración de un clúster de DocumentDB

Utilice la AWS Backup consola para restaurar los puntos de recuperación de Amazon DocumentDB

La restauración de un clúster de Amazon DocumentDB requiere que especifique varias opciones de restauración. Para obtener información sobre estas opciones, consulte [Restoring from a Cluster Snapshot](#) en la Guía para desarrolladores de Amazon DocumentDB.

Para restaurar un clúster de Amazon DocumentDB

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, elija Recursos protegidos y el ID del recurso de Amazon DocumentDB que desee restaurar.
3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID de recurso seleccionado. Para restaurar un recurso, en el panel Copias de seguridad, active el botón de opción situado junto al ID del punto de recuperación del recurso. En la esquina superior derecha del panel, elija Restaurar.
4. Asegúrese de estar en la página de la consola Restauración de instantáneas del clúster de Amazon DocumentDB.
5. En el panel Especificaciones de instancias, seleccione un motor de base de datos para la instancia.
6. En el panel Configuración, introduzca un nombre único para el identificador del clúster de base de datos.

Puede usar letras, números y guiones, aunque no puede haber dos guiones consecutivos y el nombre no puede terminar con un guion. El nombre definitivo estará en minúsculas.

7. En el panel Red y seguridad, seleccione una zona de disponibilidad o deje que elijamos una por usted.
8. En el panel Opciones de base de datos, seleccione el puerto de la base de datos.

Este es el TCP/IP puerto que utilizará la instancia de base de datos o el clúster para las conexiones de las aplicaciones. La cadena de conexión de cualquier aplicación que se conecte a la instancia de base de datos o al clúster debe especificar su número de puerto. El grupo de seguridad aplicado a la instancia de base de datos o clúster y los firewalls de la organización deben permitir las conexiones al puerto. Todas las instancias de base de datos de un clúster de base de datos utilizan el mismo puerto.

9. En el panel Opciones de base de datos, seleccione el grupo de parámetros de clúster de base de datos.

Se trata del grupo de parámetros asociado al clúster de base de datos de esta instancia. El grupo de parámetros del clúster de base de datos funciona como un contenedor para los valores de configuración del motor que se aplican a cada instancia de base de datos en el clúster.

10. En el panel Cifrado, seleccione la clave que se utilizará para cifrar el volumen de esta base de datos. El valor predeterminado es `aws/rds`. Como alternativa, puede utilizar una clave administrada por el cliente (CMK).
11. En el panel Exportaciones de registros, elija los tipos de registro que desee publicar en Amazon CloudWatch Logs. El rol de IAM ya se ha definido.
12. En el panel Rol de restauración, elija el rol de IAM predeterminado para el trabajo de restauración o un rol de IAM diferente.
13. En el panel Etiquetas del recurso protegido, si lo desea, puede optar por copiar las etiquetas de la copia de seguridad en el clúster de base de datos restaurado.
14. Después de especificar todos los ajustes, elija `Restore backup` (Restaurar copia de seguridad).

Aparecerá el panel Trabajos de restauración. En la parte superior de la página, aparecerá un mensaje con información sobre el trabajo de restauración.

15. Una vez finalizada la restauración, asocie el clúster de Amazon DocumentDB restaurado a una instancia de Amazon RDS.

Utilice la AWS Backup API, la CLI o el SDK para restaurar los puntos de recuperación de Amazon DocumentDB

En primer lugar, restaure el clúster. Utilice [StartRestoreJob](#). Puede especificar los siguientes metadatos durante las restauraciones de Amazon DocumentDB:

```
availabilityZones
backtrackWindow
copyTagsToSnapshot // Boolean
databaseName // string
dbClusterIdentifier // string
dbClusterParameterGroupName // string
dbSubnetGroupName // string
enableCloudwatchLogsExports // string
enableIAMDatabaseAuthentication // Boolean
```

```
engine // string
engineMode // string
engineVersion // string
kmsKeyId // string
port // integer
optionGroupName // string
scalingConfiguration
vpcSecurityGroupIds // string
```

A continuación, asocie el clúster de Amazon DocumentDB restaurado a una instancia de Amazon RDS mediante `create-db-instance`.

- Para Linux, macOS o Unix:

```
aws docdb create-db-instance --db-instance-identifier sample-instance /
                             --db-cluster-identifier sample-cluster --engine docdb --db-
instance-class db.r5.large
```

- Para Windows:

```
aws docdb create-db-instance --db-instance-identifier sample-instance ^
                             --db-cluster-identifier sample-cluster --engine docdb --db-
instance-class db.r5.large
```

Restauración de una tabla de Amazon DynamoDB

Utilice la AWS Backup consola para restaurar los puntos de recuperación de DynamoDB

Para restaurar una tabla de DynamoDB

1. [Abra la AWS Backup consola en /backup. https://console.aws.amazon.com](https://console.aws.amazon.com/backup)
2. En el panel de navegación, elija Recursos protegidos y el ID del recurso de DynamoDB que desee restaurar.
3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID de recurso seleccionado. Para restaurar un recurso, en el panel Copias de seguridad, active el

botón de opción situado junto al ID del punto de recuperación del recurso. En la esquina superior derecha del panel, elija Restaurar.

4. En Settings (Configuración), en el campo de texto New table name (Nuevo nombre de tabla), escriba un nuevo nombre de tabla.
5. En la función de restauración, elija la función de IAM que AWS Backup asumirá para esta restauración.
6. Para Configuración de cifrado:
 - a. Si DynamoDB administra la copia de seguridad (su ARN comienza por) AWS Backup , cifra la tabla restaurada `arn:aws:dynamodb` con una clave propia. AWS

Para elegir una clave diferente para cifrar la tabla restaurada, puede utilizar la AWS Backup [StartRestoreJob](#) operación o realizar la restauración desde la consola de [DynamoDB](#).

- b. Si la copia de seguridad admite la AWS Backup administración completa (su ARN comienza por `arn:aws:backup`), puede elegir cualquiera de las siguientes opciones de cifrado para proteger la tabla restaurada:
 - (Predeterminada) Clave de KMS propiedad de DynamoDB (sin cargo adicional por el cifrado)
 - Clave de KMS administrada por DynamoDB (se aplican cargos de KMS)
 - Clave de KMS administrada por el cliente (se aplican cargos de KMS)

Las claves “propiedad de DynamoDB” y “administradas por DynamoDB” son las mismas que las claves “propiedad de AWS” y “administradas por AWS”, respectivamente. Para obtener más información, consulte [Cifrado en reposo: cómo funciona](#) en la Guía para desarrolladores de Amazon DynamoDB.

Para obtener más información sobre la AWS Backup administración completa, consulte [Copia de seguridad avanzada de DynamoDB](#).

Note

La siguiente guía solo se aplica si restaura una copia de seguridad y desea cifrar la tabla restaurada con la misma clave que utilizó para cifrar la tabla original.

Al restaurar una copia de seguridad entre regiones, para cifrar la tabla restaurada con la misma clave que utilizó para cifrar la tabla original, la clave debe ser multirregional.

AWS-las claves propias y AWS administradas no son claves multirregionales. Para obtener más información, consulte [Multi-Region keys](#) en la Guía para desarrolladores de AWS Key Management Service .

Al restaurar una copia de seguridad multicuenta, para cifrar la tabla restaurada con la misma clave que utilizaste para cifrar la tabla original, debes compartir la clave de la cuenta de origen con la de destino. AWS-las claves propias y AWS administradas no se pueden compartir entre cuentas. Para obtener más información, consulte [Allowing users in other accounts to use a KMS key](#) en la Guía para desarrolladores de AWS Key Management Service .

7. Seleccione Restaurar copia de seguridad.

Aparecerá el panel Trabajos de restauración. En la parte superior de la página, aparecerá un mensaje con información sobre el trabajo de restauración.

Utilice la AWS Backup API, la CLI o el SDK para restaurar los puntos de recuperación de DynamoDB

Utilice [StartRestoreJob](#). Puede especificar los siguientes metadatos durante las restauraciones de DynamoDB: Los metadatos no distinguen entre mayúsculas y minúsculas.

```
targetTableName
encryptionType
kmsMasterKeyArn
aws:backup:request-id
```

A continuación, se muestra un ejemplo del argumento `restoreMetadata` de una operación `StartRestoreJob` en la CLI:

```
aws backup start-restore-job \
--recovery-point-arn "arn:aws:backup:us-east-1:123456789012:recovery-point:abcdef12-
g3hi-4567-8cjk-012345678901" \
--iam-role-arn "arn:aws:iam::123456789012:role/YourIamRole" \
--metadata
'TargetTableName=TestRestoreTestTable,EncryptionType=KMS,kmsMasterKeyArn=arn:aws:kms:us-
east-1:123456789012:key/abcdefg' \
--region us-east-1 \
--endpoint-url https://endpointurl.com
```

En el ejemplo anterior, se cifra la tabla restaurada con una AWS clave propia. La parte de los metadatos de restauración que especifica el cifrado mediante la clave AWS propiedad es:

```
"encryptionType": "Default", "kmsMasterKeyArn": "Not Applicable"
```

Para cifrar la tabla restaurada con una clave AWS administrada, especifique los siguientes metadatos de restauración: "encryptionType": "KMS", "kmsMasterKeyArn": "Not Applicable"

Para cifrar la tabla restaurada con una clave administrada por el cliente, especifique los siguientes metadatos de restauración: "encryptionType": "KMS", "kmsMasterKeyArn": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab".

Restauración de un volumen de Amazon EBS

Al restaurar una instantánea de Amazon Elastic Block Store (EBS), puede optar por restaurarla como un volumen de EBS, restaurarla en un volumen o restaurar los elementos seleccionados de él en un bucket de Amazon S3. AWS Storage Gateway

Restauración en un volumen de EBS

Al restaurar una instantánea (copia de seguridad periódica de los datos de EBS) en un volumen nuevo, debe especificar el tipo de volumen, el tamaño en GiB y una zona de disponibilidad. Si lo desea, puede optar por cifrar el nuevo volumen con una clave nueva o existente. AWS KMS

Restauración en un volumen de puerta de enlace

Cuando restaure en un volumen de puerta de enlace, tendrá que especificar una puerta de enlace en un estado accesible, elegir el nombre de destino de iSCSI y elegir un ID de disco si la puerta de enlace tiene un volumen almacenado o una capacidad igual o superior a la de la instantánea si la puerta de enlace está en caché por volumen.

Restauración de archivos en un bucket de Amazon S3

Antes de iniciar un trabajo de restauración de los recursos de EBS en un bucket de Amazon S3, revise [Permisos de EBS](#) y [Permisos de restauración de Amazon S3](#) para conocer los requisitos de acceso. Los permisos necesarios se incluyen en la política gestionada [AWSBackupServiceRolePolicyForItemRestores](#) y deben incluirse en la [función de IAM](#) utilizada para la operación de restauración.

Todas las cargas de objetos nuevos, incluidos los datos restaurados, a un bucket de S3 se cifran automáticamente. Cuando elija este tipo de restauración, especifique SSE-S3 (clave administrada de Amazon S3 del lado del servidor) o SSE-KMS (clave administrada del lado del servidor). AWS KMS SSE-S3 es el valor predeterminado.

Puede introducir hasta cinco rutas al restaurar desde la AWS Backup consola; puede especificar varias rutas a través de la línea de comandos. Una ruta debe tener una longitud inferior a 1024 bytes en cadenas codificadas en UTF-8, incluidos los prefijos designados y designados por el usuario AWS Backup

Si la instantánea contiene varias particiones, especifique el identificador del sistema de archivos de la partición que contenga los datos que quiere restaurar. Para buscar este identificador, use [Búsqueda de copias de seguridad](#). Se trata del mismo de UUID o del ID de disco del sistema de archivos.

	Al nuevo volumen de EBS	A la puerta de enlace	Restauración de archivos en un bucket de S3
Cifrado	Opcional. Puede elegir una AWS KMS clave existente o crear una clave KMS nueva.		Obligatorio. Elija entre SSE-S3, SSE-KMS o el cifrado de bucket de destino predeterminado ¹ .
Permisos y funciones	Elija el rol existente; si no existe ninguno, se crea el rol predeterminado con los permisos correctos.	Elija el rol existente; si no existe ninguno, se crea el rol predeterminado con los permisos correctos.	La elección del rol debe tener EBS y Permisos de restauración de Amazon S3 suficientes.
Restauración desde un almacenamiento en frío (nivel de archivo de EBS)	Disponible	No disponible	No disponible
Configuración a especificar	Tipo de volumen; tamaño (GiB); zona	Puerta de enlace (en un estado accesible)	Tipo de restauración, que incluye: nombre

	Al nuevo volumen de EBS	A la puerta de enlace	Restauración de archivos en un bucket de S3
	de disponibilidad; rendimiento	); nombre de destino de iSCSI; ID de disco (para puertas de enlace almacenadas por volumen); capacidad (para puertas de enlace con volumen en caché)	del bucket de destino; rutas a restaurar; tipo de cifrado; ID de clave de KMS de restauración de archivos si se ha establecido SSE-KMS como tipo de cifrado

¹ En la AWS Backup consola, selecciona una de las tres opciones de cifrado; si utiliza CLI para restaurar, omite `encryptionType` para restaurar el cifrado del bucket de destino predeterminado.

Restauración de una instantánea de EBS con la consola de AWS Backup

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, elija Recursos protegidos y el ID del recurso de EBS que desee restaurar.
3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID de recurso seleccionado. Para restaurar un recurso, en el panel Copias de seguridad, active el botón de opción situado junto al ID del punto de recuperación del recurso. En la esquina superior derecha del panel, elija Restaurar.
4. Especifique los parámetros de restauración del recurso. Los parámetros de restauración establecidos son específicos del tipo de recurso seleccionado.

En Tipo de recurso, elija el AWS recurso que se va a crear al restaurar esta copia de seguridad.

5. Si elige EBS volume (Volumen de EBS), proporcione los valores de Volume type (Tipo de volumen) y Size (GiB) (Tamaño [GiB]) y seleccione una zona de disponibilidad. Después del Rendimiento, aparecerá una casilla de verificación opcional para Cifrar este volumen. Esta opción permanecerá activa si el punto de recuperación de EBS está cifrado. . Puede especificar una clave KMS o puede crear una AWS KMS clave.

Si elige Volumen de Storage Gateway, elija una Puerta de enlace en un estado accesible. Elija también el Nombre de destino iSCSI. Para las puertas de enlace del Volumen almacenado, elija

un ID de disco. Para las puertas de enlace del Volumen en caché, elija una capacidad que sea al menos tan grande como el recurso protegido.

Si elige la restauración de archivos, puede incluir hasta cinco objetos o carpetas de la instantánea. Puede buscar el nombre o la ruta del archivo [en las copias de seguridad indexadas](#).

- Entrada de las rutas de archivos.
 - Elija entre utilizar un bucket de Amazon S3 existente o crear un bucket nuevo para el destino en el que se restaurarán los objetos o las carpetas.
 - Configure el cifrado de los objetos restaurados. Elija entre SSE-S3, SSE-KMS o el cifrado de bucket de destino predeterminado. Para obtener más información, consulte [Restaura los datos de S3 mediante AWS Backup](#).
6. En la función de restauración, elija la función de IAM que AWS Backup asumirá para esta restauración. Si la función AWS Backup predeterminada no está presente en su cuenta, se creará una función predeterminada para usted con los permisos correctos. Puede eliminar este rol predeterminado o inutilizarlo.
 7. Seleccione Restaurar copia de seguridad (se muestra Restaurar elementos para la restauración de archivos).

Aparecerá el panel Trabajos de restauración. En la parte superior de la página, aparecerá un mensaje con información sobre el trabajo de restauración.

Restauración desde instantáneas de EBS archivadas

La restauración de una instantánea de EBS archivada la mueve temporalmente de almacenamiento en frío a almacenamiento en caliente para crear un nuevo volumen de EBS. Este tipo de restauración conlleva un cargo de recuperación único. Los costos de almacenamiento tanto en caliente como en frío se facturan durante este periodo de restauración.

Tip

Los volúmenes de EBS en almacenamiento en frío no se pueden restaurar en un volumen de puerta de enlace ni restaurar en el nivel de archivo.

Puede restaurar una instantánea de EBS archivada en almacenamiento en frío mediante la [consola de AWS Backup](#) o la línea de comandos. Una restauración desde almacenamiento en frío puede

tardar hasta 72 horas. Para obtener más información, consulte [Archivar instantáneas de Amazon EBS](#) en la Guía del usuario de Amazon EBS.

Console

1. Abre la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. Vaya a Backup Vaults > *Vault* > Restaurar una instantánea de EBS archivada.
3. En la sección Configuración, introduzca un valor de 0 a 180, ambos inclusive, que especifique el número de días para restaurar temporalmente una instantánea archivada.
4. Introduzca otros ajustes: tipo de volumen, tamaño, IOPS, zona de disponibilidad, rendimiento y cifrado.
5. Elija su rol de restauración.
6. Seleccione Restaurar copia de seguridad. En la ventana emergente de confirmación, confirme las instantáneas y el tipo de restauración. A continuación, seleccione Restaurar instantánea.

AWS CLI

1. Uso de [start-restore-job](#)
2. Incluya los parámetros necesarios para la restauración de las instantáneas de EBS archivadas:

```
--recovery-point-arn arn:aws:backup:region:account-id:recovery-point:recovery-point-id
--metadata
'{"temporaryRestoreDays":"value","volumeType":"value","volumeSize":"value","availabilityZone":"value"}'
--iam-role-arn arn:aws:iam::account-id:role/service-role/AWSBackupDefaultServiceRole
--resource-type EBS
```

3. Especifique la duración de la restauración temporal (de 0 a 180 días) en el parámetro `temporaryRestoreDays`. Esto determina cuánto tiempo estará disponible la instantánea archivada en el almacenamiento en caliente.
4. Configure los nuevos ajustes de volumen de EBS, incluidos `volumeType` (gp2, gp3, io1, io2, st1 o sc1), `volumeSize` en GiB y `availabilityZone` de destino.

- Supervise el estado del trabajo de restauración con el [describe-restore-job](#) con el ID del trabajo de restauración devuelto. Las restauraciones de archivos pueden durar hasta 72 horas.

Restauración de una instantánea de EBS mediante AWS CLI

Para restaurar Amazon EBS mediante la API o la CLI, utilice [StartRestoreJob](#). Puede especificar los siguientes metadatos para una restauración de Amazon EBS:

```
aws:backup:request-id
availabilityZone
encrypted // if set to true, encryption will be enabled as volume is restored
iops
kmsKeyId // if included, this key will be used to encrypt the restored volume instead
of default KMS Key Id
restoreType // include for file level restore - see details below
throughput
temporaryRestoreDays
volumeType
volumeSize
```

Ejemplo:

```
"restoreMetadata": "{\"encrypted\": \"false\", \"volumeId\": \"vol-04cc95f3490b5ceea\", \"availabilityZone\": null}"
```

Especificaciones de restauración de archivos

El `restoreType` es obligatorio para la restauración de archivos. Para este tipo de restauración, se requieren los siguientes metadatos unívocos:

```
destinationBucketName //
pathsToRestore //
encryptionType // You can specify SSE-S3 or SSE-KMS; do not include if you want to
restore to default encryption
kmsKeyId //
```

El identificador del sistema de archivos es opcional para las instantáneas de una sola partición. Si no se transmite esta información, solo se aceptará la ruta absoluta sin el separador ":" (por ejemplo, {"/data/process/abc.txt", "/data/departament/xyz.txt"}).

Restaurar una EC2 instancia de Amazon

Al restaurar una EC2 instancia, AWS Backup crea una imagen de máquina de Amazon (AMI), una instancia, el volumen raíz de Amazon EBS, los volúmenes de datos de Amazon EBS (si el recurso protegido tenía volúmenes de datos) y las instantáneas de Amazon EBS. Puede personalizar algunos ajustes de la instancia mediante la AWS Backup consola o un mayor número de ajustes mediante el AWS CLI SDK o un SDK. AWS

A la hora de restaurar EC2 instancias, se tienen en cuenta las siguientes consideraciones:

- AWS Backup configura la instancia restaurada para que use el mismo par de claves que el recurso protegido usó originalmente. No puede especificar un par de claves diferente para la instancia restaurada durante el proceso de restauración.
- AWS Backup no realiza copias de seguridad ni restaura los datos de usuario que se utilizan al lanzar una EC2 instancia de Amazon.
- Al configurar la instancia restaurada, puede elegir entre usar el mismo perfil de instancia que el recurso protegido usó originalmente o lanzarla sin un perfil de instancia. Esto es para evitar la posibilidad de que se produzcan escalamientos de privilegios. Puedes actualizar el perfil de la instancia restaurada mediante la EC2 consola de Amazon.

Si usa el perfil de instancia original, debe conceder AWS Backup los siguientes permisos, donde el ARN del recurso es el ARN del rol de IAM asociado al perfil de instancia.

```
{
  "Effect": "Allow",
  "Action": "iam:PassRole",
  "Resource": "arn:aws:iam::account-id:role/role-name"
},
```

role-name Sustitúyalo por el nombre del rol del perfil de EC2 instancia que se adjuntará a la instancia restaurada. EC2 No se trata de la función de AWS Backup servicio, sino de la función de IAM que proporciona permisos a las aplicaciones que se ejecutan en la EC2 instancia.

- Durante una restauración, se aplican todas EC2 las cuotas y restricciones de configuración de Amazon.
- Si la bóveda que contiene tus puntos de EC2 recuperación de Amazon tiene un candado, consulta [Consideraciones adicionales de seguridad](#) para obtener más información.

Usa la AWS Backup consola para restaurar los puntos de EC2 recuperación de Amazon

Puedes restaurar una EC2 instancia de Amazon completa desde un único punto de recuperación, incluidos el volumen raíz, los volúmenes de datos y algunos ajustes de configuración de la instancia, como el tipo de instancia y el key pair.

Para restaurar EC2 los recursos de Amazon mediante la AWS Backup consola

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, selecciona Recursos protegidos y, a continuación, elige el ID del EC2 recurso de Amazon para abrir la página de detalles del recurso.
3. En el panel Puntos de recuperación, active el botón de opción situado junto al ID del punto de recuperación que va a restaurar. En la esquina superior derecha del panel, elija Restaurar.
4. En el panel Configuración de red, utilizamos la configuración de la instancia protegida para seleccionar los valores predeterminados del tipo de instancia, la VPC, la subred, el grupo de seguridad y el rol de IAM de la instancia. Puede utilizar estos valores predeterminados o cambiarlos como sea necesario.
5. En el panel Restaurar funciones, utilice la función predeterminada o elija una función de IAM para especificar una función de IAM que conceda AWS Backup permiso para restaurar la copia de seguridad.
6. En el panel Etiquetas de recursos protegidos, seleccionamos Copiar etiquetas del recurso protegido al recurso restaurado de forma predeterminada. Si no desea copiar estas etiquetas, desactive la casilla de verificación.
7. En el panel Configuración avanzada, acepte los valores predeterminados de la configuración de la instancia o cámbielos según sea necesario. Para obtener información sobre estos ajustes, seleccione Información para que el ajuste abra su panel de ayuda.
8. Cuando termine de configurar la instancia, seleccione Restaurar copia de seguridad.

Restaure Amazon EC2 con AWS CLI

En la interfaz de línea de comandos, [start-restore-job](#) permite restaurar con hasta 32 parámetros (incluidos algunos parámetros que no se pueden personalizar a través de la AWS Backup consola).

La siguiente lista contiene los metadatos aceptados que puedes transferir para restaurar un punto de EC2 recuperación de Amazon.

```
InstanceType
KeyName
SubnetId
Architecture
EnaSupport
SecurityGroupIds
IamInstanceProfileName
CpuOptions
InstanceInitiatedShutdownBehavior
HibernationOptions
DisableApiTermination
CreditSpecification
Placement
RootDeviceType
RamdiskId
KernelId
UserData
Monitoring
NetworkInterfaces
ElasticGpuSpecification
CapacityReservationSpecification
InstanceMarketOptions
LicenseSpecifications
EbsOptimized
VirtualizationType
Platform
RequireIMDSv2
BlockDeviceMappings
aws:backup:request-id
```

AWS Backup acepta los siguientes atributos únicamente informativos. -Sin embargo, su inclusión no afectará a la restauración:

```
vpcId
```

[BlockDeviceMappings](#) es un parámetro opcional que puede incluir. AWS Backup admite los siguientes `BlockDeviceMappings` atributos.

 Note

SnapshotId y OutpostArn no son compatibles.

```
{
  "BlockDeviceMappings": [
    {
      "DeviceName" : string,
      "NoDevice" : string,
      "VirtualName" : string,
      "Ebs": {
        "DeleteOnTermination": boolean,
        "Iops": number,
        "VolumeSize": number,
        "VolumeType": string,
        "Throughput": number,
        "Encrypted": boolean,
        "KmsKeyId": string
      }
    }
  ]
}
```

Por ejemplo:

```
{
  "BlockDeviceMappings": [
    {
      "DeviceName": "/def/tuvw",
      "Ebs": {
        "DeleteOnTermination": true,
        "Iops": 3000,
        "VolumeSize": 16,
        "VolumeType": "gp3",
        "Throughput": 125,
        "Encrypted": true,
        "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/ab3cde45-67f8-9g01-
hi2j-3456klmno7p8"
      }
    },
    {
      "DeviceName": "/abc/xyz",
```

```
"Ebs": {  
  "DeleteOnTermination": false,  
  "Iops": 3000,  
  "VolumeSize": 16,  
  "VolumeType": "gp3",  
  "Throughput": 125,  
  "Encrypted": false  
}  
}  
]  
}
```

También puedes restaurar una EC2 instancia de Amazon sin incluir ningún parámetro almacenado. Esta opción está disponible en la pestaña Recursos protegidos de la AWS Backup consola.

Important

Si no anula la AWS KMS clave del BlockDeviceMappings al restaurar a partir de copias de seguridad entre cuentas o regiones, la restauración podría fallar. Para obtener más información, consulte [Solucionar problemas de restauración de EC2 instancias de Amazon](#).

Solucionar problemas de restauración de EC2 instancias de Amazon

Solución de problemas de incidencias

- [Errores en la restauración entre cuentas](#)
- [Errores en la restauración entre regiones](#)

Errores en la restauración entre cuentas

Descripción: La restauración de EC2 instancias de Amazon produce un error al intentar restaurarla desde una copia de seguridad compartida con tu cuenta.

Posibles problemas: es posible que tu cuenta no tenga acceso a las AWS KMS claves utilizadas para cifrar los volúmenes de origen de la cuenta compartida. Es posible que las claves de KMS no se compartan con su cuenta.

O bien, los volúmenes asociados a la instancia de origen no están cifrados.

Solución: para resolver este problema, establezca el atributo `encrypted` en `true` y siga uno de estos pasos:

- Anule las claves de KMS en `BlockDeviceMappings` y especifique una clave de KMS que sea de su propiedad en su cuenta.
- Solicite a la cuenta propietaria que le conceda acceso a las claves de KMS utilizadas para cifrar los volúmenes mediante la actualización de la política de claves de KMS. Para obtener más información, consulte [Permiso para que los usuarios de otras cuentas utilicen una clave de KMS](#).

Errores en la restauración entre regiones

Descripción: La restauración de EC2 instancias de Amazon produce un error al intentar restaurarla desde una copia de seguridad entre regiones.

Problema: es posible que los volúmenes de la copia de seguridad estén cifrados con AWS KMS claves de una sola región que no estén disponibles en la región de destino. O bien, los volúmenes asociados a la instancia de origen no están cifrados.

Solución: para resolver este problema, defina el atributo `encrypted` en `true` y sustituya la clave de KMS en `BlockDeviceMappings` por una clave de KMS en la región de destino.

Restauración de un sistema de archivos de Amazon EFS

Si va a restaurar una instancia de Amazon Elastic File System (Amazon EFS), puede realizar una restauración completa o una restauración a nivel de elemento.

Restauración completa

Cuando se realiza una restauración completa, se restaura todo el sistema de archivos.

AWS Backup no admite restauraciones destructivas con Amazon EFS. Una restauración destructiva se produce cuando un sistema de archivos restaurado elimina o sobrescribe el sistema de archivos de origen o existente. En cambio, AWS Backup restaura el sistema de archivos en un directorio de recuperación fuera del directorio raíz.

Restauración a nivel de elemento

Al realizar una restauración a nivel de elemento, AWS Backup restaura un archivo o directorio específico. Debe especificar la ruta relativa a la raíz del sistema de archivos. Por ejemplo, si el

sistema de archivos está montado en `/user/home/myname/efs` y la ruta de archivo es `user/home/myname/efs/file1`, escriba **`/file1`**. Las etiquetas distinguen entre mayúsculas y minúsculas. No se admiten caracteres comodín ni cadenas de expresiones regulares. La ruta puede ser diferente de la del host si el sistema de archivos se monta mediante un punto de acceso.

Puede seleccionar hasta 10 elementos si utiliza la consola para realizar una restauración de EFS. No hay límite de elementos cuando se utiliza la CLI para realizar restauraciones; sin embargo, hay un límite de 200 KB en la longitud de los metadatos de restauración que se pueden transferir.

Puede restaurar esos elementos en un sistema de archivos nuevo o existente. En cualquier caso, AWS Backup crea un nuevo directorio de Amazon EFS (`aws-backup-restore_datetime`) a partir del directorio raíz para contener los elementos. La jerarquía completa de los elementos especificados se conserva en el directorio de recuperación. Por ejemplo, si el directorio A contiene los subdirectorios B, C y D, AWS Backup mantiene la misma estructura jerárquica cuando se recuperan A, B, C y D. Independientemente de si realiza una restauración de nivel de elemento de Amazon EFS en un sistema de archivos existente o en un sistema de archivos nuevo, cada intento de restauración creará un nuevo directorio de recuperación fuera del directorio raíz que contendrá los archivos restaurados. Si intenta realizar varias restauraciones de la misma ruta, es posible que existan varios directorios que contengan los elementos restaurados.

Note

Si solo mantiene una copia de seguridad semanal, solo podrá restaurar el estado del sistema de archivos al momento en que realizó la copia de seguridad. No podrá restaurar copias de seguridad incrementales anteriores.

Utilice la AWS Backup consola para restaurar un punto de recuperación de Amazon EFS

Para restaurar un sistema de archivos de Amazon EFS

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. Su almacén de copias de seguridad de EFS recibe la política de acceso Deny `backup:StartRestoreJob` al crearse. Si es la primera vez que va a restaurar el almacén de copias de seguridad, debe cambiar la política de acceso como se indica a continuación.
 - a. Elija Almacenes de Backup.

- b. Elija el almacén de copias de seguridad que contenga el punto de recuperación que desea restaurar.
 - c. Elija la Política de acceso al almacén.
 - d. Si está presente, elimine `backup:StartRestoreJob` de `Statement`. Para ello, elija Editar, elimine `backup:StartRestoreJob` y, a continuación, elija Guardar política.
3. En el panel de navegación, elija Recursos protegidos y el ID del sistema de archivos de EFS que desee restaurar.
4. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID del sistema de archivos seleccionado. Para restaurar un sistema de archivos, en el panel Copias de seguridad, active el botón de opción situado junto al ID del punto de recuperación del sistema de archivos. En la esquina superior derecha del panel, elija Restaurar.
5. Especifique los parámetros de restauración del sistema de archivos. Los parámetros de restauración establecidos son específicos del tipo de recurso seleccionado.

Puede realizar una restauración completa, que restaura todo el sistema de archivos. También puede restaurar archivos y directorios específicos mediante una restauración de nivel de elemento.

- Elija la opción Restauración completa para restaurar el sistema de archivos en su totalidad, incluidas todas las carpetas y archivos del nivel raíz.
- Elija la opción Restaurar a nivel de elemento para restaurar un archivo o directorio específico. Puede seleccionar y restaurar hasta cinco elementos en su Amazon EFS.

Para restaurar un archivo o directorio concretos, debe especificar la ruta relativa relacionada con el punto de montaje. Por ejemplo, si el sistema de archivos está montado en `/user/home/myname/efs` y la ruta de archivo es `user/home/myname/efs/file1`, escriba **/file1**. Las rutas distinguen entre mayúsculas y minúsculas y no pueden contener caracteres especiales, caracteres comodín ni cadenas de expresiones regulares.

1. En el cuadro de texto Ruta de elemento, escriba la ruta de acceso del archivo o la carpeta.
 2. Elija Agregar elemento para agregar otros archivos o directorios. Puede seleccionar y restaurar hasta cinco elementos en su sistema de archivos de EFS.
6. En Restore location (Ubicación de la restauración)
 - Elija Restaurar a un directorio del sistema de archivos de origen si desea restaurar al sistema de archivos de origen.
 - Elija Restaurar a un sistema de archivos nuevo si desea restaurar a otro sistema de archivos.

7. El Tipo de sistema de archivos.

- (Recomendado) Elija Regional si desea restaurar el sistema de archivos en varias zonas de AWS disponibilidad.
- Elija Una zona si desea restaurar el sistema de archivos en una única zona de disponibilidad. A continuación, en el menú desplegable de Zona de disponibilidad, elija el destino de la restauración.

Para obtener más información, consulte [Managing Amazon EFS storage classes](#) en la Guía del usuario de Amazon EFS.

8. Para el Rendimiento

- Si opta por realizar una restauración Regional, elija entre Uso general (recomendado) o Máximo de E/S.
- Si opta por realizar una restauración de Una zona, tiene que elegir Uso general (recomendado). Las restauraciones de Una zona no admiten Máximo de E/S.

9. Para Habilitar el cifrado

- Elija Habilitar el cifrado si desea cifrar el sistema de archivos. La clave IDs y los alias de KMS aparecen en la lista una vez creados con la consola AWS Key Management Service (AWS KMS).
- En el cuadro de texto Clave de KMS, elija la clave que desee utilizar de la lista.

10. En la función de restauración, elija la función de IAM que AWS Backup asumirá para esta restauración.

Note

Si la función AWS Backup predeterminada no está presente en su cuenta, se creará una función predeterminada para usted con los permisos correctos. Puede eliminar este rol predeterminado o inutilizarlo.

11. Seleccione Restaurar copia de seguridad.

Aparecerá el panel Trabajos de restauración. En la parte superior de la página, aparecerá un mensaje con información sobre el trabajo de restauración.

 Note

Si solo mantiene una copia de seguridad semanal, solo podrá restaurar el estado del sistema de archivos al momento en que realizó la copia de seguridad. No podrá restaurar copias de seguridad incrementales anteriores.

Utilice la AWS Backup API, la CLI o el SDK para restaurar los puntos de recuperación de Amazon EFS

Utilice [StartRestoreJob](#). Cuando restaure una instancia de Amazon EFS, puede restaurar un sistema de archivos completo o archivos y directorios específicos. Para restaurar recursos de Amazon EFS, necesita la siguiente información:

- **file-system-id**— El ID del sistema de archivos Amazon EFS del que se hace la copia de seguridad AWS Backup. Devuelta por `GetRecoveryPointRestoreMetadata`. Esto no es necesario cuando se restaura un nuevo sistema de archivos (este valor se ignora si el parámetro `newFileSystem` es `True`).
- **Encrypted**: un valor booleano que, si es verdadero, especifica que el sistema de archivos está cifrado. Si se especifica `KmsKeyId`, `Encrypted` se debe configurar en `true`.
- **KmsKeyId**— Especifica la AWS KMS clave que se utiliza para cifrar el sistema de archivos restaurado.
- **PerformanceMode**: especifica el modo de rendimiento del sistema de archivos. Los valores válidos son `generalPurpose` (predeterminado) y `maxIO`. El modo `generalPurpose` proporciona la latencia más baja por operación y puede realizar hasta 7000 operaciones de archivos por segundo. El modo `maxIO` puede escalar a niveles superiores de operaciones y rendimiento agregado por segundo con una latencia un poco mayor en las operaciones con archivos.
- **CreationToken**: un valor proporcionado por el usuario que garantiza la exclusividad (idempotencia) de la solicitud.
- **newFileSystem**: un valor booleano que, si es verdadero, especifica que el punto de recuperación se restaura en un nuevo sistema de archivos de Amazon EFS.
- **ItemsToRestore** : una matriz de hasta cinco cadenas en la que cada cadena es una ruta de archivo. Utilice `ItemsToRestore` para restaurar archivos o directorios específicos en lugar de restaurar todo el sistema de archivos. Este parámetro es opcional.

También puede incluir `aws:backup:request-id`.

Las restauraciones de One Zone se pueden realizar incluyendo los siguientes parámetros:

```
"singleAzFilesystem": "true"  
"availabilityZoneName": "ap-northeast-3"
```

Para obtener más información sobre los valores de configuración de Amazon EFS, consulte [create-file-system](#).

Deshabilitación de las copias de seguridad automáticas en Amazon EFS

De forma predeterminada, [Amazon EFS crea copias de seguridad de los datos automáticamente](#). Estas copias de seguridad se representan como puntos de recuperación en AWS Backup. Si se intenta eliminar el punto de recuperación, aparecerá un mensaje de error que indica que no hay suficientes privilegios para realizar la acción.

Se recomienda mantener activa esta opción de copia de seguridad automática. Especialmente en el caso de una eliminación accidental de datos, la copia de seguridad permite restaurar el contenido del sistema de archivos a la fecha del último punto de recuperación creado.

En el improbable caso de que desee desactivarlas, la política de acceso debe cambiarse de `"Effect": "Deny"` a `"Effect": "Allow"`. Consulte la Guía del usuario de Amazon EFS para obtener más información sobre cómo activar o desactivar las [copias de seguridad automáticas](#).

Restaurar un clúster de Amazon EKS

Puede restaurar las copias de seguridad del clúster de EKS mediante la AWS Backup consola o la CLI. Las copias de seguridad de EKS son puntos de recuperación compuestos que incluyen tanto las copias de seguridad del estado del clúster de EKS como las de los volúmenes persistentes.

AWS Backup admite múltiples experiencias de restauración, incluidas las restauraciones granulares a nivel de espacio de nombres. Las restauraciones no son destructivas y no sobrescribirán ningún objeto de Kubernetes existente en el clúster de EKS de destino. Las restauraciones tampoco sobrescribirán las versiones de Kubernetes del clúster de EKS de destino.

Las copias de seguridad de EKS deben restaurarse en un clúster de EKS de destino, es decir, en un clúster de Amazon EKS que se haya aprovisionado previamente. Como parte del flujo de trabajo de restauración, puede optar por crear un nuevo clúster de EKS que AWS Backup se creará en su nombre.

Note

AWS Backup proporcionará un conjunto limitado de opciones para crear un nuevo clúster de EKS como parte de una restauración. Para todas las funciones de creación de clústeres de EKS, los clientes pueden crear un nuevo clúster de [EKS mediante la consola](#) de EKS o APIs seleccionarlo como su objetivo de restauración.

Capacidades de restauración para Amazon EKS

Tipo de restauración	Restaurar el destino	Restaurar el comportamiento
Restauración de clústeres existentes	Restaura al clúster EKS de origen o al clúster EKS existente	Restaura todos los recursos y volúmenes persistentes de Kubernetes en los clústeres de EKS existentes. Todas las restauraciones no son destructivas y los objetos existentes no se sobrescriben. En el caso de los objetos que se omiten, puede suscribirse a las notificaciones de SNS
Restauración de un nuevo clúster	Crea un nuevo clúster de Amazon EKS como parte de la restauración de EKS	La restauración crea un nuevo clúster de EKS y restaura todos los recursos y volúmenes persistentes de Kubernetes en un clúster recién creado
Restauración del espacio de nombres	Clúster Amazon EKS existente	Restaura solo los espacios de nombres específicos; sus recursos de Kubernetes y las correspondientes restauraciones de almacenamiento persistente no son destructivas y los objetos existente

Tipo de restauración	Restaurar el destino	Restaurar el comportamiento
		s no se sobrescriben. En el caso de los objetos que se omiten, puedes suscribirte a las notificaciones de SNS
Restauración de almacenamiento persistente	Depende del almacenamiento persistente	Restablezca el almacenamiento persistente individual como restauraciones independientes. Consulte Restaurar el comportamiento de Amazon EBS , Amazon S3 y Amazon EFS .

Permisos

Los permisos necesarios dependen del tipo de restauración y del destino de destino.

- AWS Backup La política gestionada [AWSBackupServiceRolePolicyForRestores](#) contiene los permisos necesarios para restaurar el clúster de Amazon EKS y el almacenamiento persistente de EBS y EFS.
- Si su clúster EKS contiene un bucket de S3 o si va a restaurar el punto de recuperación de S3 secundario por sí solo, tendrá que asegurarse de que las siguientes políticas o permisos estén asignados a su función [AWSBackupServiceRolePolicyForS3Restore](#).

Consideraciones antes de la restauración

Antes de comenzar un trabajo de restauración de EKS, revise lo siguiente. Si va a restaurar una copia de seguridad de EKS que se ha copiado en una cuenta o región, asegúrese de tener en cuenta estas consideraciones antes de realizar la restauración para evitar errores de restauración.

1. Funciones de IAM: al restaurar en un clúster diferente, las funciones de IAM utilizadas en el clúster de origen (como Pod identity o IRSA). El OIDC (configuraciones de proveedor, etc.) debe estar presente en la cuenta o región como clúster de destino.
2. Compruebe la versión y la compatibilidad de EKS: las versiones de API de los objetos que desee restaurar deben ser de la misma versión (o lo más parecidas posible) y ser compatibles con el

- nuevo clúster. AWS Backup hará todo lo posible por restaurar entre versiones de EKS, aunque pueden surgir problemas de compatibilidad al restaurar entre versiones muy diferentes.
3. Clases de almacenamiento coincidentes: para realizar restauraciones en un clúster EKS existente, asegúrese de instalar los complementos del controlador de almacenamiento CSI adecuados antes de la restauración
 4. Depósitos de S3: al restaurar un clúster de EKS con cubos de S3, asegúrese de que el depósito de S3 esté versionado y sea accesible en la cuenta o región de destino.
 5. Repositorio de imágenes: al restaurar un clúster de EKS, asegúrese de que la cuenta o región del clúster de EKS de destino tenga acceso a las imágenes a las que se hace referencia como parte de la restauración. Compruebe que su registro tenga los permisos necesarios para la política entre regiones y cuentas.
 6. Grupos de seguridad: los grupos de seguridad deben crearse previamente para ALB, Pod Identities, grupos de nodos EKS, etc. en la cuenta y región de destino si va a crear un nuevo clúster de EKS como parte de la restauración
 7. Nodos y zonas de disponibilidad de EBS: las zonas de disponibilidad en las que se recuperan los volúmenes de EBS deben asignarse a la zona de disponibilidad de un nodo de EKS existente
 8. Restauraciones no destructivas: todas las restauraciones de EKS no serán destructivas y no sobrescribirán los objetos de Kubernetes de la restauración de destino.
 9. Habilite los registros de auditoría de EKS: habilite los registros de auditoría de EKS para realizar más registros y solucionar problemas antes de la restauración. También puede suscribirse a [las notificaciones de SNS](#) para notificar los objetos omitidos o defectuosos durante la restauración.

Configuraciones de EKS

Cuando restauras el Amazon compuesto AWS Backup, eliges el tipo de restauración y el destino de destino. Puede optar por restaurar en el clúster de EKS de origen, en un clúster de EKS existente o crear un nuevo clúster de EKS como destino de la restauración. Para los nuevos clústeres de EKS, puede optar por utilizar los mismos ajustes de infraestructura existentes (por ejemplo, VPC, subredes) que el clúster del que se hizo la copia de seguridad o configurar otros nuevos. AWS Backup siempre realizará una restauración no destructiva que no sobrescriba los recursos existentes.

Para las restauraciones de espacios de nombres, puedes especificar hasta 5 espacios de nombres para restaurarlos de forma selectiva. Solo se restauran los recursos del ámbito del espacio de nombres, mientras que los recursos del ámbito del clúster se excluyen, excepto los volúmenes persistentes relacionados.

Como configuración avanzada, puedes optar por cambiar el orden de restauración de los objetos de Kubernetes. De forma predeterminada, AWS Backup restaurará todos los objetos de Kubernetes en el siguiente orden:

Recursos de Kubernetes con alcance de clúster

1. Definiciones de recursos personalizadas
2. Espacios de nombres (el espacio de nombres en sí, no los recursos dentro de ese espacio de nombres)
3. StorageClasses
4. PersistentVolumes

Recursos de Kubernetes con ámbito de espacio de nombres

1. PersistentVolumeClaims
2. Secretos
3. ConfigMaps
4. ServiceAccounts
5. LimitRanges
6. Pods
7. ReplicaSets

Configuraciones de almacenamiento persistente

Como parte de la restauración de la copia de seguridad compuesta de Amazon EKS, el segundo paso consistirá en configurar las configuraciones de almacenamiento persistente. Esto variará en función del almacenamiento persistente del que se haga una copia de seguridad como parte del clúster de EKS.

Para las instantáneas de Amazon EBS, debe proporcionar una zona de disponibilidad en la que se restaurará y creará el volumen de Amazon EBS. AWS Backup A continuación, intentará crear el pod de EKS en la misma zona de disponibilidad que la seleccionada para poder volver a montar el volumen en el clúster de EKS como parte de la restauración.

Como parte de la restauración, AWS Backup volverá a montar los volúmenes de Amazon EBS y los buckets de Amazon S3 en el clúster de EKS restaurado. Los sistemas de archivos Amazon EFS se restauran con prefijos aleatorios y requieren la creación manual de puntos de acceso después de la

restauración para volver a montarlos en el clúster de EKS. AWS Backup [no crea puntos de acceso ni monta objetivos en su nombre; consulte esta guía para obtener información sobre los puntos de acceso y los objetivos de montaje.](#)

Procedimiento de restauración de Amazon EKS

Siga estos pasos para restaurar las copias de seguridad de Amazon EKS mediante la AWS Backup consola o AWS CLI:

Console

Para restaurar el clúster de Amazon EKS

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, elija Backup vaults (Almacenes de copia de seguridad).
3. Elija el almacén de copias de seguridad que contiene la copia de seguridad de Amazon EKS y, a continuación, seleccione el punto de recuperación de la copia de seguridad de Amazon EKS.
4. Elija Restore (Restaurar).
5. En el panel de opciones de restauración, elija el tipo de restauración:
 - Restaurar el clúster de EKS completo: restaura todo el punto de recuperación compuesto de Amazon EKS
 - Seleccione los espacios de nombres que desee restaurar: restaura hasta cinco espacios de nombres específicos
6. Configure el destino de destino:
 - Para la restauración del clúster, elija crear un clúster nuevo o utilizar uno existente
 - Para los clústeres nuevos, especifique el nombre del clúster, la versión de Kubernetes, la configuración de la VPC, las funciones de IAM, las subredes, los grupos de seguridad adicionales, la configuración de los grupos de nodos, los perfiles de Fargate y las funciones de IAM de identidad del pod
 - Para los clústeres existentes, selecciona el clúster de destino en el menú desplegable
 - Para la restauración del espacio de nombres, especifique el clúster de destino y los nombres del espacio de nombres
7. Si lo desea, configure los ajustes avanzados para personalizar el orden de restauración de los recursos de Kubernetes.

8. Elija el rol de restauración de IAM para el trabajo. Si no usa el rol predeterminado, asegúrese de que el rol seleccionado incluya el permiso `iam::PassRole`
9. Seleccione Restaurar copia de seguridad.

AWS CLI

Utilice el `aws backup start-restore-job` comando con metadatos específicos de Amazon EKS.

Los metadatos necesarios dependen del tipo de restauración. Todas las operaciones de restauración requieren el `clusterName` parámetro.

Restaura los puntos de recuperación de Amazon EKS mediante AWS CLI

Uso `StartRestoreJob`. Puede especificar los siguientes metadatos durante las restauraciones de Amazon EKS:

Metadatos obligatorios:

- `clusterName`- Nombre del clúster en el que se va a restaurar

Metadatos opcionales:

- `newCluster`- (verdadero/falso) Si debemos crear un nuevo clúster de EKS durante la restauración
 - Si `newCluster` es «verdadero», se aplican los siguientes campos de metadatos:
 - `eksClusterVersion`- Se recomienda la versión K8 del clúster si se desea aumentar la versión del clúster durante la restauración
 - `clusterRole`- El ARN del rol de IAM que se debe adjuntar al clúster EKS creado
 - `clusterVpcConfig`- VPC/Networking configuración del clúster EKS creado. Este campo tiene los siguientes campos anidados:
 - `vpcId`- La VPC asociada a su clúster
 - `subnetIds`- Las subredes asociadas a su clúster
 - `securityGroupIds`- Los grupos de seguridad adicionales asociados a su clúster
 - `nodeGroups`- Los grupos de nodos gestionados que se crearán en el clúster EKS. El objeto `NodeGroups` de la restauración debe tener todos los mismos grupos de nodos de la época de la copia de seguridad y ser coincidentes `nodeGroupId`.

- `nodeGroupId`- El ID del grupo de nodos
- `subnetIds`- Las subredes que se especificaron para el grupo de Auto Scaling que está asociado a su grupo de nodos
- `instanceTypes`- Si el grupo de nodos no se implementó con una plantilla de lanzamiento, este es el tipo de instancia que está asociado al grupo de nodos
- `nodeRole`- El rol de IAM asociado a tu grupo de nodos
- `securityGroupIds`- El grupo de seguridad al IDs que se le permite el acceso SSH a los nodos
- `remoteAccessEc2SshKey`- El nombre de la clave Amazon EC2 SSH que proporciona acceso a la comunicación SSH con los nodos del grupo de nodos gestionado
- `fargateProfiles`- Los perfiles de Fargate que se crearán en el clúster EKS. Los perfiles de Fargate para la restauración deben tener todos los mismos perfiles de Fargate de la época de la copia de seguridad y tener un nombre coincidente.
 - `name`- El nombre del perfil de Fargate
 - `subnetIds`- El número IDs de subredes en las que lanzar un pod
 - `podExecutionRoleArn`- El ARN del rol de IAM del rol de ejecución del pod que se utilizará en un pod que coincida con los selectores del perfil de Fargate
- `podIdentityAssociations`- Las asociaciones de identidad de los pods que se crearán en el clúster EKS
 - `associationId`- El ID de la asociación de identidad del Pod
 - `roleArn`- El ARN del rol de IAM para la Pod Identity Association
- `kubernetesRestoreOrder`- Anule el orden en que se restauran los manifiestos de Kubernetes. Este orden tendrá prioridad sobre el orden de restauración del servicio predeterminado. Esto sigue el formato: `group/version/kind` or `version/kind`

[`"v1/persistentvolumes"`], `«v1/pods»`,» `«] customresource/v2/custom`

- `namespaceLevelRestore`- (verdadero/falso) Si desea realizar una restauración a nivel de espacio de nombres
- `namespaces`- Una lista de espacios de nombres para restaurar si es `«verdadera»`. `namespaceLevelRestore` Puede proporcionar hasta 5 espacios de nombres para restaurar
- `restoreKubernetesManifestsOnly`- (verdadero/falso) Si desea restaurar únicamente los archivos de manifiesto de Kubernetes y no los sistemas de almacenamiento persistente (EBS, S3, EFS, etc.)

- **nestedRestoreJobs**- Restaure la configuración de metadatos de todos los puntos de recuperación anidados de los sistemas de PersistentVolume almacenamiento en el punto de recuperación compuesto. Este es un mapa de **RecoveryPointArn**: de ese **RestoreMetadata** punto de recuperación

Restaure a un clúster existente

```
aws backup start-restore-job \
    --recovery-point-arn "arn:aws:backup:us-
west-2:123456789012:recovery-point:composite:eks/my-cluster-20240115" \
    --iam-role-arn "arn:aws:iam::123456789012:role/
AWSBackupServiceRolePolicyForEKSRestore" \
    --metadata '{"clusterName":"existing-
cluster","newCluster":false}' \
    --resource-type "EKS"
```

Restaurar a un clúster nuevo

```
aws backup start-restore-job \
    --recovery-point-arn "arn:aws:backup:us-
west-2:123456789012:recovery-point:composite:eks/my-cluster-20240115" \
    --iam-role-arn "arn:aws:iam::123456789012:role/
AWSBackupServiceRolePolicyForEKSRestore" \
    --metadata '{"clusterName":"new-
cluster","newCluster":true,"clusterRole":"arn:aws:iam::123456789012:role/
EKSClusterRole","eksClusterVersion":"1.33","clusterVpcConfig":{"vpcId
\":"vpc-1234\","\subnetIds\":[\subnet-1\","\subnet-2\","\subnet-3\"],
\securityGroupIds\":[\sg-123\]}","nodeGroups":[{"nodeGroupId":
\nodegroup-1\","\subnetIds\":[\subnet-1\","\subnet-2\","\subnet-3\"],
\nodeRole\":"arn:aws:iam::123456789012:role/EKSNodeGroupRole\","\instanceTypes
\":[\t3.small\]}]","fargateProfiles":[{"name\":"fargate-profile-1\",
\subnetIds\":[\subnet-1\","\subnet-2\","\subnet-3\"],"podExecutionRoleArn\":"
arn:aws:iam::123456789012:role/EKSFargateProfileRole\}]}"' \
    --resource-type "EKS"
```

Tras iniciar el trabajo de restauración, úselo `describe-restore-job` para supervisar el progreso:

```
aws backup describe-restore-job --restore-job-id restore-job-id
```

Puede suscribirse a los eventos de notificación de los objetos omitidos o fallidos para restaurarlos. Para obtener más información, consulte [Opciones de notificación con AWS Backup](#).

Restablece un sistema FSx de archivos

Las opciones de restauración que están disponibles cuando se restauran AWS Backup los sistemas de FSx archivos de Amazon son las mismas que cuando se utiliza la FSx copia de seguridad nativa de Amazon. Puede utilizar el punto de recuperación de una copia de seguridad para crear un nuevo sistema de archivos y restaurar una point-in-time instantánea de otro sistema de archivos.

AWS Backup admite la restauración de sistemas de archivos que utilizan almacenamiento por niveles inteligente tanto para los sistemas de archivos Lustre como FSx para los sistemas de archivos OpenZFS. FSx Los sistemas de archivos de organización inteligente por niveles tienen requisitos de configuración específicos durante las operaciones de restauración.

Al restaurar los sistemas de FSx archivos de Amazon, AWS Backup crea un nuevo sistema de archivos y lo rellena con los datos (Amazon FSx for NetApp ONTAP permite restaurar un volumen en un sistema de archivos existente). Esto es similar a la forma en que Amazon nativo hace FSx copias de seguridad y restaura los sistemas de archivos. La restauración de una copia de seguridad en un nuevo sistema de archivos lleva el mismo tiempo que la creación de un nuevo sistema de archivos. Los datos restaurados a partir de la copia de seguridad se cargan de forma diferida en el sistema de archivos. Por lo tanto, es posible que observe una latencia ligeramente mayor durante el proceso.

Note

No puedes restaurar a un sistema de FSx archivos de Amazon existente, ni puedes restaurar archivos o carpetas individuales.

FSx porque ONTAP no admite la creación de copias de seguridad de determinados tipos de volúmenes, incluidos los volúmenes DP (protección de datos), los volúmenes LS (carga compartida), los volúmenes completos o los volúmenes de sistemas de archivos que están llenos. Para obtener más información, consulte [ONTAP Cómo trabajar con copias FSx de seguridad](#).

AWS Backup Las bóvedas que contienen puntos de recuperación de los sistemas de FSx archivos de Amazon están visibles fuera de. AWS Backup Puedes restaurar los puntos de recuperación con Amazon FSx , pero no puedes eliminarlos.

Puede ver las copias de seguridad creadas por la función de copia de seguridad FSx automática integrada de Amazon desde la AWS Backup consola. También puede recuperar estas copias de

seguridad utilizando AWS Backup. Sin embargo, no puede eliminar estas copias de seguridad ni cambiar los programas de copias de seguridad automáticas de sus sistemas de FSx archivos de Amazon mediante AWS Backup.

Usa la AWS Backup consola para restaurar los puntos de FSx recuperación de Amazon

Puedes restaurar la mayoría de las FSx copias de seguridad de Amazon creadas AWS Backup mediante la AWS Backup consola, la API o AWS CLI.

En esta sección se muestra cómo utilizar la AWS Backup consola para restaurar los sistemas de FSx archivos de Amazon.

Restauración de un sistema de archivos FSx para Windows File Server

Para restaurar un sistema FSx de archivos del servidor de archivos de Windows

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, selecciona Recursos protegidos y, a continuación, elige el ID de FSx recurso de Amazon que deseas restaurar.
3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID de recurso seleccionado. Elija el ID del punto de recuperación del recurso.
4. En la esquina superior derecha del panel, elija Restaurar para abrir la página Restaurar copia de seguridad.
5. En la sección Detalles del sistema de archivos, el ID de la copia de seguridad se muestra en ID de copia de seguridad y el tipo de sistema de archivos se muestra en Tipo de sistema de archivos. Puede restaurar tanto FSx para el servidor de archivos de Windows como FSx para los sistemas de archivos Lustre.
6. Acepte el valor predeterminado para Tipo de implementación. No puede cambiar el tipo de implementación de un sistema de archivos durante la restauración.
7. Elija el Tipo de almacenamiento que va a usar. Si la capacidad de almacenamiento del sistema de archivos es inferior a 2000 GiB, no puede utilizar el tipo de almacenamiento HDD.
8. En cuanto a la capacidad de rendimiento, seleccione Capacidad de rendimiento recomendada para utilizar la velocidad recomendada de 16 MB por segundo (MBps) o seleccione Especificar la capacidad de rendimiento e introduzca una nueva velocidad.
9. En la sección Red y seguridad, proporcione la información requerida.

10. Si va a restaurar un sistema de archivos FSx para Windows File Server, proporcione la información de autenticación de Windows utilizada para acceder al sistema de archivos o puede crear uno nuevo.

 Note

Al restaurar una copia de seguridad, no puede cambiar el tipo de Active Directory del sistema de archivos.

Para obtener más información acerca de Microsoft Active Directory, consulte [Trabajar con Active Directory en Amazon FSx for Windows File Server](#) en la Guía del usuario de Amazon FSx for Windows File Server.

11. De forma opcional, en la sección Copia de seguridad y mantenimiento, proporcione la información para configurar sus preferencias de copia de seguridad.
12. En la sección Rol de restauración, elija el rol de IAM que AWS Backup utilizará para crear y administrar las copias de seguridad en su nombre. Se recomienda elegir el Rol predeterminado. Si no hay un rol predeterminado, se creará uno automáticamente con los permisos adecuados. También puede proporcionar su propio rol de IAM.
13. Compruebe todas las entradas y elija Restaurar copia de seguridad.

Restauración de un sistema FSx de archivos Amazon for Lustre

AWS Backup es compatible con los sistemas de archivos Amazon FSx for Lustre que tienen un tipo de implementación de almacenamiento persistente y no están vinculados a un repositorio de datos como Amazon S3.

 Note

Solo puede restaurar la copia de seguridad en un sistema de archivos del mismo tipo de implementación, clase de almacenamiento, capacidad de rendimiento, capacidad de almacenamiento, tipo de compresión de datos y AWS región que el original. Puede aumentar la capacidad de almacenamiento del sistema de archivos restaurado una vez que esté disponible.

Para restaurar un sistema de archivos FSx de Amazon for Lustre

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, selecciona Recursos protegidos y, a continuación, elige el ID de FSx recurso de Amazon que deseas restaurar.
3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID de recurso seleccionado. Elija el ID del punto de recuperación del recurso.
4. En la esquina superior derecha del panel, elija Restaurar para abrir la página Restaurar copia de seguridad al nuevo sistema de archivos.
5. En la sección Configuración, el ID de la copia de seguridad se muestra en ID de copia de seguridad y el tipo de sistema de archivos se muestra en Tipo de sistema de archivos. El Tipo de sistema de archivos debe ser Lustre.
6. Elija un tipo de implementación. AWS Backup solo admite el tipo de despliegue persistente. No puede cambiar el tipo de implementación de un sistema de archivos durante la restauración.

El tipo de implementación persistente es para el almacenamiento a largo plazo. Para obtener información detallada sobre FSx las opciones de despliegue de Lustre, consulte [Uso de las opciones de despliegue disponibles para Amazon FSx for Lustre File Systems](#) en la Guía del usuario de Amazon FSx for Lustre.

7. Elija el Rendimiento por unidad de almacenamiento que desee utilizar.

Note

El rendimiento por unidad de almacenamiento no se puede configurar para los sistemas de archivos que utilizan la clase de almacenamiento Intelligent-Tiering.

8. (Opcional) Para los sistemas de archivos que utilizan la clase de almacenamiento Intelligent-Tiering, elija el modo de dimensionamiento y la capacidad de la caché de lectura SSD. Para obtener más información, consulte la FSx documentación sobre la [administración de la caché de lectura de la SSD aprovisionada](#).
9. (Optional) For file systems using Intelligent-Tiering storage class, choose whether to enable EFA (Elastic Fabric Adapter). To enable EFA, make sure that your security group allows all inbound and outbound traffic within the security group.
10. Especifique la Capacidad de almacenamiento que se va a utilizar. Introduzca una capacidad entre 32 GiB y 64 436 GiB.

 Note

En el caso de los sistemas de archivos de organización inteligente por niveles, la capacidad de almacenamiento es elástica y no se puede especificar durante la restauración. La capacidad se ampliará automáticamente en función del uso de datos.

11. En la sección Red y seguridad, proporcione la información requerida.
12. De forma opcional, en la sección Copia de seguridad y mantenimiento, proporcione la información para configurar sus preferencias de copia de seguridad.
13. En la sección Rol de restauración, elija el rol de IAM que AWS Backup utilizará para crear y administrar las copias de seguridad en su nombre. Se recomienda elegir el Rol predeterminado. Si no hay un rol predeterminado, se creará uno automáticamente con los permisos adecuados. También puede proporcionar su rol de IAM.
14. Compruebe todas las entradas y elija Restaurar copia de seguridad.

Restauración de volúmenes FSx de Amazon para NetApp ONTAP

Para restaurar los volúmenes de Amazon FSx for NetApp ONTAP:

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, selecciona Recursos protegidos y, a continuación, elige el ID de FSx recurso de Amazon que deseas restaurar.
3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID de recurso seleccionado. Elija el ID del punto de recuperación del recurso.
4. En la esquina superior derecha del panel, elija Restaurar para abrir la página Restaurar.

La primera sección, Detalles del sistema de archivos, muestra el ID del punto de recuperación, el ID del sistema de archivos y el tipo de sistema de archivos.

5. En Opciones de restauración, hay varias posibilidades. En primer lugar, elija el Sistema de archivos del menú desplegable.
6. A continuación, elija la Máquina virtual de almacenamiento preferida del menú desplegable.
7. Escriba un nombre para su volumen.
8. Especifique la Ruta de unión, que es la ubicación dentro del sistema de archivos donde se montará el volumen.

9. Especifique en megabytes (MB) el Tamaño del volumen que va a crear.
10. De forma opcional, puede marcar la casilla para Habilitar la eficiencia de almacenamiento. Esto permitirá la deduplicación, la compresión y la compactación.
11. En el menú desplegable Política de clasificación por niveles de los grupos de capacidad, seleccione la preferencia de nivel.
12. En los Permisos de restauración, elija el rol de IAM que AWS Backup utilizará para restaurar las copias de seguridad.
13. Compruebe todas las entradas y elija Restaurar copia de seguridad.

Restauración de un sistema FSx de archivos Amazon for OpenZFS

Note

No se admite la restauración desde una copia de seguridad con una clase de almacenamiento determinada a un sistema de archivos con una clase de almacenamiento diferente.

Para restaurar un sistema FSx de archivos OpenZFS

1. [Abra la AWS Backup consola en /backup. https://console.aws.amazon.com](https://console.aws.amazon.com/backup)
2. En el panel de navegación, selecciona Recursos protegidos y, a continuación, elige el ID de FSx recurso de Amazon que desees restaurar.
3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID de recurso seleccionado. Elija el ID del punto de recuperación del recurso.
4. En la esquina superior derecha del panel, elija Restaurar para abrir la página Restaurar copia de seguridad.

En la sección Detalles del sistema de archivos, el ID de la copia de seguridad se muestra en ID de copia de seguridad y el tipo de sistema de archivos se muestra en Tipo de sistema de archivos. El tipo de sistema de archivos debe ser FSx para OpenZFS.

5. En Opciones de restauración, puede seleccionar Restauración rápida o Restauración estándar. La restauración rápida utilizará la configuración predeterminada del sistema de archivos de origen. Si realiza una restauración rápida, vaya al paso 7.

Si elige la restauración estándar, especifique las siguientes configuraciones adicionales:

- a. IOPS de SSD aprovisionadas: puede elegir el botón de opción Automático o puede elegir la opción Aprovisionado por el usuario, si está disponible.

 Note

Las IOPS de SSD no se pueden configurar para sistemas de archivos que utilicen la clase de almacenamiento Intelling-Tiering

- b. Capacidad de rendimiento: puede elegir la capacidad de rendimiento recomendada de 64 MB/sec (para la clase de almacenamiento SSD) y 160 MB/sec (para la clase de almacenamiento Intelligent-Tiering), o puede elegir especificar la capacidad de rendimiento.
 - c. (Opcional) Grupos de seguridad de VPC: puede especificar grupos de seguridad de VPC para asociarlos a la interfaz de red del sistema de archivos.
 - d. Clave de cifrado: especifique la AWS Key Management Service clave para proteger los datos en reposo del sistema de archivos restaurados.
 - e. (Opcional) Configuración del volumen raíz: esta configuración está comprimida de forma predeterminada. Para ampliarla, haga clic en el quilate (flecha) que apunta hacia abajo. Al crear un sistema de archivos a partir de una copia de seguridad, se creará un nuevo sistema de archivos; los volúmenes y las instantáneas retendrán sus configuraciones de origen.
 - f. (Opcional) Copia de seguridad y mantenimiento: para configurar una copia de seguridad programada, haga clic en el quilate (flecha) que apunta hacia abajo para ampliar la sección. Puede elegir el intervalo de copia de seguridad, la hora y el minuto, el periodo de retención y el intervalo de mantenimiento semanal.
6. La Capacidad de almacenamiento de SSD mostrará la capacidad de almacenamiento del sistema de archivos.

 Note

En los sistemas de archivos de organización inteligente por niveles, la capacidad de almacenamiento es elástica y no se puede especificar durante la restauración. La capacidad se ampliará automáticamente en función del uso de datos.

7. (Opcional) Para los sistemas de archivos que utilizan la clase de almacenamiento por niveles inteligentes, elija el modo de dimensionamiento y la capacidad de la caché de lectura de la SSD.

Para obtener más información, consulte la FSx documentación sobre la [administración de la caché de lectura de la SSD aprovisionada](#).

8. Elija la Nube privada virtual (VPC) desde la que se puede acceder a su sistema de archivos.
9. En el menú desplegable Subred, elija la subred en la que reside la interfaz de red del sistema de archivos.
10. En la sección Rol de restauración, elija el rol de IAM que AWS Backup utilizará para crear y administrar las copias de seguridad en su nombre. Se recomienda elegir el Rol predeterminado. Si no hay un rol predeterminado, se creará uno automáticamente con los permisos adecuados. También puede elegir un rol de IAM.
11. Compruebe todas las entradas y elija Restaurar copia de seguridad.

Utilice la AWS Backup API, la CLI o el SDK para restaurar los puntos de FSx recuperación de Amazon

Para restaurar Amazon FSx mediante la API o la CLI, utilice [StartRestoreJob](#). Puedes especificar los siguientes metadatos durante una FSx restauración de Amazon:

```
StorageCapacity
StorageType
VpcId
KmsKeyId
SecurityGroupIds
SubnetIds
DeploymentType
WeeklyMaintenanceStartTime
DailyAutomaticBackupStartTime
AutomaticBackupRetentionDays
CopyTagsToBackups
WindowsConfiguration
LustreConfiguration
OntapConfiguration
OpenZFSConfiguration
aws:backup:request-id
```

 Note

La capacidad de almacenamiento no se puede especificar para los sistemas de archivos de organización inteligente por niveles, ya que utilizan un almacenamiento elástico que se escala automáticamente en función del uso de los datos.

FSx para Windows File Server, restaure los metadatos

Puede especificar los siguientes metadatos durante una restauración FSx para un servidor de archivos de Windows:

- `ThroughputCapacity`
- `PreferredSubnetId`
- `ActiveDirectoryId`

FSx para Lustre, restaure los metadatos

Puede especificar los siguientes subcampos `LustreConfiguration` en los metadatos durante una restauración de FSx for Lustre:

- `PerUnitStorageThroughput`- Especifica la capacidad de rendimiento por unidad de almacenamiento aprovisionada, medida por MB/s TiB de almacenamiento.
- `DriveCacheType`- El tipo de memoria caché de la unidad que utilizan los sistemas de `PERSISTENT_1` archivos que se aprovisionan con dispositivos de almacenamiento en disco duro. Este parámetro es necesario cuando `StorageType` se establece en `HDD`.
- `DataReadCacheConfiguration`- Especifica la caché de lectura SSD aprovisionada para los sistemas de archivos de organización inteligente por niveles. Necesario cuando `StorageType` se establece en `INTELLIGENT_TIERING`. Consulte [LustreReadCacheConfiguration](#) para obtener más información.
- `EfaEnabled`- Especifica si la compatibilidad con Elastic Fabric Adapter (EFA) y GPUDirect Storage (GDS) está habilitada para el FSx sistema de archivos for Lustre.

Para obtener información completa sobre todos los parámetros disponibles en `LustreConfiguration`, consulta [CreateFileSystemLustreConfiguration](#) la referencia de la FSx API de Amazon.

FSx para ONTAP, restaure los metadatos

Puede especificar los siguientes metadatos durante una restauración FSx para ONTAP:

- Name #nombre del volumen que se va a crear
- OntapConfiguration: # configuración ontap
- junctionPath
- sizeInMegabytes
- storageEfficiencyEnabled
- storageVirtualMachineId
- tieringPolicy

FSx para OpenZFS, restaure los metadatos

Puede especificar los siguientes subcampos OpenZFSConfiguration en los metadatos durante una restauración FSx para OpenZFS:

- ThroughputCapacity- Especifica la capacidad de rendimiento del sistema de archivos restaurado, medida en MB/s.
- DiskIopsConfiguration- Al especificar las IOPS para la clase de almacenamiento SSD, utilice un valor entre 0 y 160 000. No incluya el modo cuando se especifiquen las IOPS.
- ReadCacheConfiguration- Especifica la caché de lectura SSD aprovisionada para los sistemas de archivos de organización inteligente por niveles. Necesario cuando StorageType se establece en INTELLIGENT_TIERING. Consulte [Abrir ZFSRead CacheConfiguration](#) para obtener más información.

Para obtener información completa sobre todos los parámetros disponibles enOpenZFSConfiguration, consulta [CreateFileSystemOpenZFSConfiguration](#) la referencia de la FSx API de Amazon.

Ejemplo de comando de restauración de la CLI:

```
aws backup start-restore-job --recovery-point-arn "arn:aws:fsx:us-west-2:1234:backup/backup-1234" --iam-role-arn "arn:aws:iam::1234:role/Role" --resource-type "FSx" --region us-west-2 --metadata 'SubnetIds=["subnet-1234", "subnet-5678"]',StorageType=HDD,SecurityGroupIds=["sg-bb5efdc4",
```



```
\ "sg-0faa52\""],WindowsConfiguration="{\"DeploymentType\": \"MULTI_AZ_1\",
\"PreferredSubnetId\": \"subnet-1234\", \"ThroughputCapacity\": \"32\"}"'
```

Ejemplo de restauración de metadatos:

```
"restoreMetadata": "{ \"StorageType\": \"SSD\", \"KmsKeyId\": \"arn:aws:kms:us-
east-1:123456789012:key/123456a-123b-123c-defg-1h2i2345678\", \"StorageCapacity
\": \"1200\", \"VpcId\": \"vpc-0ab0979fa431ad326\", \"FileSystemType\": \"LUSTRE\",
\"LustreConfiguration\": \"{\\\"WeeklyMaintenanceStartTime\\\": \\\"4:10:30\\\", \\
\"DeploymentType\\\": \\\"PERSISTENT_1\\\", \\\"PerUnitStorageThroughput\\\": 50, \\
\"CopyTagsToBackups\\\": true}\"\", \"FileSystemId\": \"fs-0ca11fb3d218a35c2\", \"SubnetIds
\": \"[\\\"subnet-0e66e94eb43235351\\\"]\"}"
```

Restauración de un clúster de Neptune

Utilice la AWS Backup consola para restaurar los puntos de recuperación de Amazon Neptune

Para restaurar una base de datos de Amazon Neptune, se han de especificar varias opciones de restauración. Para obtener información sobre estas opciones, consulte [Restoring from a DB Cluster Snapshot](#) en la Guía del usuario de Neptune.

Para restaurar una base de datos de Neptune

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, elija Recursos protegidos y el ID del recurso de Neptune que desee restaurar.
3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID de recurso seleccionado. Para restaurar un recurso, en el panel Copias de seguridad, active el botón de opción situado junto al ID del punto de recuperación del recurso. En la esquina superior derecha del panel, elija Restaurar.
4. En el panel Especificaciones de instancias, acepte los valores predeterminados o especifique el Motor de base de datos y la Versión.
5. En el panel de configuración, especifique un nombre que sea exclusivo para todas las instancias de clústeres de bases de datos que le pertenezcan Cuenta de AWS en la región actual. El identificador de clúster de bases de datos no distingue entre mayúsculas y minúsculas, pero se almacena con todas las letras en minúsculas (como en "mydbclusterinstance"). Este campo es obligatorio.

6. En el panel Opciones de base de datos, acepte los valores predeterminados o especifique las opciones de configuración de Puerto de base de datos, Grupo de parámetros de clúster de bases de datos y Autenticación de bases de datos de IAM habilitada.
7. En el panel Encryption (Cifrado), acepte el valor predeterminado o especifique las opciones de configuración de Enable encryption (Habilitar cifrado) o Disable encryption (Deshabilitar cifrado).
8. En el panel Exportaciones de registros, elija los tipos de registro que desee publicar en Amazon CloudWatch Logs. El rol de IAM ya se ha definido.
9. En el panel Restore role (Restaurar rol), elija el rol de IAM que AWS Backup asumirá para esta restauración.
10. Después de especificar todos los ajustes, elija Restore backup (Restaurar copia de seguridad).

Aparecerá el panel Trabajos de restauración. En la parte superior de la página, aparecerá un mensaje con información sobre el trabajo de restauración.

11. Una vez finalizada la restauración, asocie el clúster de Neptune restaurado a una instancia de Amazon RDS.

Utilice la AWS Backup API, la CLI o el SDK para restaurar los puntos de recuperación de Neptune

En primer lugar, restaure el clúster. Utilice [StartRestoreJob](#). Puede especificar los siguientes metadatos durante las restauraciones de Amazon DocumentDB:

```
availabilityZones
backtrackWindow
copyTagsToSnapshot // Boolean
databaseName // string
dbClusterIdentifier // string
dbClusterParameterGroupName // string
dbSubnetGroupName // string
enableCloudwatchLogsExports // string
enableIAMDatabaseAuthentication // Boolean
engine // string
engineMode // string
engineVersion // string
kmsKeyId // string
port // integer
optionGroupName // string
scalingConfiguration
```

```
vpcSecurityGroupIds // string
```

A continuación, asocie el clúster de Neptune restaurado a una instancia de Amazon RDS mediante `create-db-instance`.

- Para Linux, macOS o Unix:

```
aws neptune create-db-instance --db-instance-identifier sample-instance \  
                                --db-instance-class db.r5.large --engine neptune --engine-  
version 1.0.5.0 --db-cluster-identifier sample-cluster --region us-east-1
```

- Para Windows:

```
aws neptune create-db-instance --db-instance-identifier sample-instance ^  
                                --db-instance-class db.r5.large --engine neptune --engine-  
version 1.0.5.0 --db-cluster-identifier sample-cluster --region us-east-1
```

Para obtener más información, consulte [RestoreDBClusterFromSnapshot](#) en la Referencia de la API de administración de Neptune y [restore-db-cluster-from-snapshot](#) en la Guía de la CLI de Neptune.

Restauración de una base de datos de RDS

Para restaurar una base de datos de Amazon RDS, se han de especificar varias opciones de restauración. Para obtener más información acerca de estas opciones, consulte [Copia de seguridad y restauración de una instancia de base de datos de Amazon RDS](#) en la Guía del usuario de Amazon RDS.

Utilice la AWS Backup consola para restaurar los puntos de recuperación de Amazon RDS

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, elija Recursos protegidos y el ID del recurso de Amazon RDS que desee restaurar.
3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID de recurso seleccionado. Para restaurar un recurso, en el panel Copias de seguridad, active el botón de opción situado junto al ID del punto de recuperación del recurso. En la esquina superior derecha del panel, elija Restaurar.

4. En el panel Especificaciones de instancias, acepte los valores predeterminados o especifique las opciones que necesite.
5. En el panel de configuración, especifique un nombre que sea único para todas las instancias de base de datos y los clústeres de su propiedad Cuenta de AWS en la región actual. El identificador de instancias de bases de datos no distingue entre mayúsculas y minúsculas, pero se almacena con todas las letras en minúsculas (como en "mydbinstance"). Este campo es obligatorio.
6. En el panel Red y seguridad acepte los valores predeterminados o especifique las opciones que necesite.
7. En el panel Opciones de bases de datos acepte los valores predeterminados o especifique las opciones que necesite.
8. En Cifrado, use la configuración predeterminada. Si la instancia de base de datos de origen de la instantánea se cifró, la instancia de base de datos restaurada también se cifrará. Este cifrado no se puede eliminar.
9. En el panel Exportaciones de registros, elija los tipos de registro que desee publicar en Amazon CloudWatch Logs. El rol de IAM ya se ha definido.
10. En el panel Maintenance (Mantenimiento), acepte el valor predeterminado o especifique la opción de Auto minor version upgrade (Actualización automática de versiones secundarias).
11. En el panel Restore role (Restaurar rol), elija el rol de IAM que AWS Backup asumirá para esta restauración.
12. Seleccione Restaurar copia de seguridad.

Aparecerá el panel Trabajos de restauración. En la parte superior de la página, aparecerá un mensaje con información sobre el trabajo de restauración.

Utilice la AWS Backup API, la CLI o el SDK para restaurar los puntos de recuperación de Amazon RDS

Utilice [StartRestoreJob](#). Para obtener información sobre los metadatos y los valores aceptados, consulte [RestoreDBInstanceFromDBSnapshot](#) y [RestoreDBInstanceToPointInTime](#) en la Referencia de la API de Amazon RDS. Además, AWS Backup acepta los siguientes atributos únicamente informativos. -Sin embargo, su inclusión no afectará a la restauración:

```
EngineVersion
KmsKeyId
Encrypted
```

`vpcId`

Restauración de un clúster de Amazon Redshift

Puede restaurar instantáneas automáticas y manuales en la AWS Backup consola o mediante CLI.

Al restaurar un clúster de Amazon Redshift, la configuración original del clúster se introduce en la consola de forma predeterminada. Puede especificar diferentes ajustes para las siguientes configuraciones. Cuando restaure una tabla, tiene que especificar las bases de datos de origen y destino. Para obtener más información sobre estas configuraciones, consulte [Restauración de un clúster desde una instantánea](#) en la Guía de administración de Amazon Redshift.

- Una sola tabla o clúster: puede elegir entre restaurar un clúster completo o una sola tabla. Si decide restaurar una sola tabla, necesitará la base de datos de origen, el esquema de origen y el nombre de la tabla de origen, así como el clúster de destino, el esquema y el nombre de la nueva tabla.
- Tipo de nodo: cada clúster de Amazon Redshift consta de un nodo principal y al menos un nodo de computación. Al restaurar un clúster, tiene que especificar el tipo de nodo que cumpla con sus requisitos de CPU, RAM, capacidad de almacenamiento y tipo de unidad.
- Número de nodos: al restaurar un clúster, tiene que especificar el número de nodos necesarios.
- Resumen de la configuración
- Permisos de clúster

Para restaurar un clúster o una tabla de Amazon Redshift mediante la consola AWS Backup

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, elija Recursos protegidos y el ID del recurso de Amazon Redshift que desee restaurar.
3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID de recurso seleccionado. Para restaurar un recurso, en el panel Puntos de recuperación, active el botón de opción situado junto al ID del punto de recuperación del recurso. En la esquina superior derecha del panel, elija Restaurar.
4. Opciones de restauración
 - a. Restaure el clúster de una instantánea, o

- b. Restaure una sola tabla de una instantánea en un nuevo clúster. Si elige estas opciones, tiene que configurar lo siguiente:
 - i. Activar o desactivar los nombres que distinguen entre mayúsculas y minúsculas.
 - ii. Introducir los valores de la tabla de origen, incluida la base de datos, el esquema y la tabla. La información de la tabla de origen se encuentra en la consola de [Amazon Redshift](#).
 - iii. Introducir los valores de la tabla de destino, incluida la base de datos, el esquema y el nombre de la nueva tabla.
5. Especifique los ajustes de configuración del nuevo clúster.
 - a. Para restaurar el clúster: elija el identificador del clúster, el tipo de nodo y el número de nodos.
 - b. Especifique la zona de disponibilidad y los intervalos de mantenimiento.
 - c. Para asociar roles adicionales, haga clic en Asociar roles de IAM.
6. Opcional: configuraciones adicionales:
 - a. La opción Usar valores predeterminados está activada de forma predeterminada.
 - b. Use los menús desplegables para seleccionar la configuración de redes y seguridad, grupos de seguridad de VPC, grupo de subredes del clúster y zona de disponibilidad.
 - c. Active o desactive el Enrutamiento de VPC mejorado.
 - d. Determine si quiere que el punto de conexión de su clúster sea accesible públicamente. Si es así, las instancias y los dispositivos fuera de la VPC pueden conectarse a la base de datos a través del punto de conexión del clúster. Si está activado, introduzca la dirección IP elástica.
7. Opcional: configuración de la base de datos. Puede optar por introducir lo siguiente
 - a. Puerto de la base de datos (escriba en el campo de texto)
 - b. Grupos de parámetros
8. Mantenimiento: puede elegir lo siguiente
 - a. período de mantenimiento
 - b. Pista de mantenimiento, entre actual, de seguimiento o vista previa. Esto controla qué versión del clúster se aplica durante un intervalo de mantenimiento.
9. La instantánea automática está configurada de forma predeterminada.

- a. Periodo de retención de instantáneas automatizadas. El periodo de retención debe ser de 0 a 35 días. Elija 0 para no crear instantáneas automatizadas.
 - b. El periodo de retención manual de las instantáneas es de 1 a 3653 días.
 - c. Existe una casilla de verificación opcional para la reubicar el clúster. Si está marcada, permite reubicar el clúster en otra zona de disponibilidad. Una vez que haya habilitado la reubicación, puede usar el punto de conexión de VPC.
10. Supervisión: después de restaurar un clúster, puede configurar la supervisión a través CloudWatch de Amazon Redshift.
 11. Elija el rol de IAM que desee transferir para realizar las restauraciones. Puede usar el rol predeterminado o especificar uno diferente.

Los trabajos de restauración serán visibles en Trabajos. Para ver el estado actual de su trabajo de restauración, haga clic en el botón de actualización o en CTRL-R.

Restaurar un clúster de Amazon Redshift mediante la API, la CLI o el SDK

Utilice [StartRestoreJob](#) para restaurar un clúster de Amazon Redshift.

Para restaurar un Amazon Redshift mediante el AWS CLI, utilice el comando `start-restore-job` y especifique los siguientes metadatos:

```
ClusterIdentifier // required string
AdditionalInfo // optional string
AllowVersionUpgrade // optional Boolean
AquaConfigurationStatus // optional string
AutomatedSnapshotRetentionPeriod // optional integer 0 to 35
AvailabilityZone // optional string
AvailabilityZoneRelocation // optional Boolean
ClusterParameterGroupName // optional string
ClusterSecurityGroups // optional array of strings
ClusterSubnetGroupName // optional strings
DefaultIamRoleArn // optional string
ElasticIp // optional string
Encrypted // Optional TRUE or FALSE
EnhancedVpcRouting // optional Boolean
HsmClientCertificateIdentifier // optional string
HsmConfigurationIdentifier // optional string
IamRoles // optional array of strings
KmsKeyId // optional string
```

```

MaintenanceTrackName // optional string
ManageMasterPassword // optional Boolean
ManualSnapshotRetentionPeriod // optional integer
MasterPasswordSecretKmsKeyId // optional string
NodeType // optional string
NumberOfNodes // optional integer
OwnerAccount // optional string
Port // optional integer
PreferredMaintenanceWindow // optional string
PubliclyAccessible // optional Boolean
ReservedNodeId // optional string
SnapshotClusterIdentifier // optional string
SnapshotScheduleIdentifier // optional string
TargetReservedNodeOfferingId // optional string
VpcSecurityGroupIds // optional array of strings
RestoreType // CLUSTER_RESTORE or TABLE_RESTORE or NAMESPACE_RESTORE

```

Para obtener más información, consulte [RestoreFromClusterSnapshot](#) en la Referencia de la API de Amazon Redshift y [restore-from-cluster-snapshot](#) en la Guía de AWS CLI .

A continuación, se muestra una plantilla de ejemplo:

```

aws backup start-restore-job \
-\-recovery-point-arn "arn:aws:backup:region:account:snapshot:name" \
-\-iam-role-arn "arn:aws:iam:account:role/role-name" \
-\-metadata
-\-resource-type Redshift \
-\-region Región de AWS
-\-endpoint-url URL

```

A continuación se muestra un ejemplo:

```

aws backup start-restore-job \
-\-recovery-point-arn "arn:aws:redshift:us-west-2:123456789012:snapshot:redshift-
cluster-1/awsbackup:job-c40dda3c-fdcc-b1ba-fa56-234d23209a40" \
-\-iam-role-arn "arn:aws:iam::974288443796:role/Backup-Redshift-Role" \
-\-metadata 'RestoreType=CLUSTER_RESTORE,ClusterIdentifier=redshift-cluster-
restore-78,Encrypted=true,KmsKeyId=45e261e4-075a-46c7-9261-dfb91e1c739c' \
-\-resource-type Redshift \
-\-region us-west-2 \

```

También puede utilizar [DescribeRestoreJob](#) para obtener información de la restauración.

En AWS CLI, utilice la operación `describe-restore-job` y utilice los siguientes metadatos:

```
Region
```

A continuación, se muestra una plantilla de ejemplo:

```
aws backup describe-restore-job --restore-job-id restore job ID
-\-region Región de AWS
```

A continuación se muestra un ejemplo:

```
aws backup describe-restore-job --restore-job-id BEA3B353-576C-22C0-9E99-09632F262620
\
-\-region us-west-2 \
```

Restauración de Amazon Redshift sin servidor

Puede restaurar instantáneas manuales de bases de datos o tablas mediante la AWS Backup consola o AWS CLI.

Redshift Serverless y AWS Backup admiten restauración intercambiable para instantáneas de almacenes de datos. Esto significa que puede restaurar las copias de seguridad de Redshift sin servidor en los [clústeres aprovisionados de Amazon Redshift](#) o restaurar las copias de seguridad aprovisionadas en los espacios de nombres de Redshift sin servidor. Esto solo se aplica a la restauración completa de la base de datos, no a la restauración de una sola tabla.

Capacidades de restauración de Redshift sin servidor

Capacidades de restauración	Namespace	Una única tabla
Tipo de instantánea	Manual	Manual
Información necesaria	- Instantánea de origen - Espacio de nombres de destino - Grupo de trabajo	- Instantánea de origen - Base de datos de origen - Nombre de la tabla de origen - Bases de datos de destino - Nombre de la nueva tabla

Capacidades de restauración	Namespace	Una única tabla
Restaura el efecto de destino	Restaura un espacio de nombres existente mediante una restauración destructiva que sobrescribe los datos existentes.	Restauración en una tabla nueva
¿Restauración intercambiable?	Sí. - Las copias de seguridad de Redshift sin servidor se pueden restaurar en clústeres aprovisionados por Amazon Redshift. - Las copias de seguridad aprovisionadas por Amazon Redshift se pueden restaurar en clústeres aprovisionados por Redshift sin servidor.	No admitido.

Para obtener más información sobre las configuraciones, consulte [Instantáneas y puntos de recuperación](#) en la Guía de administración de Amazon Redshift.

Consideraciones previas a la restauración

Antes de comenzar un trabajo de restauración, revise lo siguiente:

Configuraciones

Al restaurar una instantánea de Redshift sin servidor, debe elegir el espacio de nombres de destino en el que desea restaurar todas las bases de datos o una sola tabla.

La restauración de bases de datos de una instantánea en un espacio de nombres sin servidor es una restauración destructiva. Esto significa que todos los datos existentes previamente en el espacio de nombres de restauración de destino se sobrescriben al restaurar en ese espacio de nombres.

La restauración en una única tabla no es destructiva. Para restaurar una tabla, especifique el grupo de trabajo, la instantánea, la base de datos de origen, la tabla de origen, el espacio de nombres de restauración de destino y el nombre de la nueva tabla.

Permisos

Los permisos necesarios los determina el almacén de datos de destino (es decir, el espacio de nombres o el clúster aprovisionado en el que se restaurarán las bases de datos o la tabla). La siguiente tabla puede ayudarle a determinar los permisos, el rol y la política que debe utilizar. Para obtener más información acerca de la administración de políticas de IAM, consulte [Administración de identidades y accesos en Amazon Redshift](#).

Permisos y roles necesarios para las operaciones de restauración

Restaurar el destino	Se necesitan permisos	Política y rol de IAM
Clúster aprovisionado de Amazon Redshift	<code>redshift:RestoreFromClusterSnapshot</code>	<code>AWSBackupServiceRolePolicyForRestores</code> contiene este permiso; se puede usar para <code>aws backup start-restore-job</code> .
Espacio de nombres de Redshift sin servidor	<code>redshift-serverless:RestoreFromSnapshot</code>	Debe añadir este permiso al rol y la política que utilizará para llamar a <code>aws backup start-restore-job</code> . Como se trata de un trabajo de restauración destructivo, no se puede utilizar la política de rol de servicio para las restauraciones.

Procedimiento de restauración de Redshift sin servidor

Siga estos pasos para restaurar las copias de seguridad de Redshift Serverless mediante la AWS Backup consola o: AWS CLI

Console

1. [Abra la AWS Backup consola en /backup. https://console.aws.amazon.com](https://console.aws.amazon.com/backup)

2. En el panel de navegación, elija Configuración y el ID del recurso de Redshift sin servidor que desee restaurar.
3. En la página Detalles del recurso, seleccione el ID del punto de recuperación en el panel Puntos de recuperación y, a continuación, seleccione Restaurar.
4. En el panel Opciones de restauración, elija restaurar todo el almacén de datos o una sola tabla.
5. Seleccione el destino en el panel Configuración del almacén de datos de destino.
 - Para restaurar un almacén de datos completo, elija entre el clúster aprovisionado de Amazon Redshift o el espacio de nombres de Redshift sin servidor.
 - Para restaurar una sola tabla, especifique la instantánea de origen, la base de datos, el esquema, el nombre de la tabla y los detalles de destino.
6. Elija el rol de restauración de IAM para el trabajo. Si no va a utilizar el rol predeterminado, asegúrese de que el rol seleccionado incluya el permiso `iam:PassRole`.

AWS CLI

Utilice el comando `aws backup start-restore-job`.

AWS Backup trabaja con Redshift Serverless para organizar el trabajo de restauración. El comando de la CLI irá precedido de `aws backup`, pero también incluirá metadatos relevantes para Redshift sin servidor o Amazon Redshift.

Los metadatos obligatorios y opcionales dependen de si va a restaurar un almacén de datos completo o una sola tabla.

- Para la restauración de una sola tabla, consulte la AWS CLI Referencia de [restore-table-from-snapshot](#) comandos.
- Para la restauración del espacio de nombres, consulte la [restore-from-snapshot](#) Referencia de AWS CLI comandos.
- Para restaurar en un clúster aprovisionado por Amazon Redshift, consulte la AWS CLI Referencia de [restore-from-cluster-snapshot](#) comandos.

Example Plantilla para **start-restore-job** para restaurar en un espacio de nombres sin servidor:

```
aws backup start-restore-job \
```

```
--recovery-point-arn "arn:aws:backup:region:account:snapshot:name--iam-role-arn  
"arn:aws:iam:account:role/role-name" \  
--metadata \  
--resource-type Redshift Serverless \  
--region Region \  
--endpoint-url URL
```

Example Ejemplo para **start-restore-job** para restaurar en un espacio de nombres sin servidor:

```
aws backup start-restore-job \  
--recovery-point-arn "arn:aws:redshift-serverless:us-east-1:123456789012:snapshot/  
a12bc34d-567e-890f-123g-h4ijk56l78m9" \  
--iam-role-arn "arn:aws:iam::974288443796:role/Backup-Redshift-Role" \  
--metadata 'RestoreType=NAMESPACE_RESTORE,NamespaceIdentifier=redshift-namespace-1-  
restore' \  
--resource-type "RedshiftServerless" \  
--region us-west-2
```

Tras iniciar el trabajo de restauración, use `describe-restore-job` para supervisar el progreso.

Restaurar una base de datos SAP HANA en una EC2 instancia de Amazon

Las bases de datos de SAP HANA en las EC2 instancias se pueden restaurar mediante la AWS Backup consola, la API o mediante AWS CLI.

Temas

- [Restaure una base de datos de SAP HANA con la AWS Backup consola](#)
- [StartRestoreJob API para SAP HANA en EC2](#)
- [CLI para SAP HANA en EC2](#)
- [Restauración de alta disponibilidad \(HA\) de SAP HANA](#)
- [Resolución de problemas](#)

Restaure una base de datos de SAP HANA con la AWS Backup consola

Tenga en cuenta que los trabajos de copia de seguridad y restauración que involucren la misma base de datos no pueden realizarse simultáneamente. Cuando se realiza un trabajo de restauración

de una base de datos de SAP HANA, es probable que al intentar hacer una copia de seguridad de la misma base de datos se produzca un error: "Database cannot be backed up while it is stopped".

1. Acceda a la AWS Backup consola con las credenciales de los requisitos previos.
2. En el menú desplegable Ubicación de restauración de destino, elija una base de datos para sobrescribirla con el punto de recuperación que va a utilizar para la restauración (tenga en cuenta que la instancia que aloja la base de datos de destino de la restauración también debe tener los permisos establecidos en los requisitos previos).

 Important

Las restauraciones de bases de datos de SAP HANA son destructivas. La restauración de una base de datos sobrescribirá la base de datos en la ubicación de restauración de destino especificada.

3. Complete este paso solo si va a realizar una restauración de copia del sistema; de lo contrario, vaya al paso 4.

Las restauraciones de copia del sistema son trabajos de restauración que restauran en una base de datos de destino diferente de la base de datos de origen que generó el punto de recuperación. Para las restauraciones de copia del sistema, observe el comando `aws ssm-sap put-resource-permission` que aparece en la consola. Este comando debe copiarse, pegarse y ejecutarse en la máquina que haya cumplido los requisitos previos. Al ejecutar el comando, utilice las credenciales del rol en el requisito previo en el que se configuran los permisos necesarios para registrar aplicaciones.

```
// Example command
aws ssm-sap put-resource-permission \
--region us-east-1 \
--action-type RESTORE \
--source-resource-arn arn:aws:ssm-sap-east-1:112233445566:HANA/Foo/DB/HDB \
--resource-arn arn:aws:ssm-sap:us-east-1:112233445566:HANA/Bar/DB/HDB
```

4. Una vez que elija la ubicación de restauración, podrá ver el ID de recurso de la base de datos de destino, el nombre de la aplicación, el tipo de base de datos y la EC2 instancia.
5. Si lo desea, puede ampliar la Configuración avanzada de restauración para cambiar la opción de restauración del catálogo. Las opciones disponibles varían en función de la configuración de restauración seleccionada.

6. Haga clic en Restaurar copia de seguridad.
7. La ubicación de destino se sobrescribirá durante la restauración (“restauración destructiva”), por lo que debe confirmar que lo permite en el siguiente cuadro de diálogo emergente.
 - a. Para continuar, debe comprender que la base de datos existente se sobrescribirá con la que está restaurando.
 - b. Una vez entendido esto, debe reconocer que los datos existentes se sobrescribirán. Para confirmarlo y continuar, escriba `overwrite` en el campo de entrada de texto.
8. Haga clic en Restaurar copia de seguridad.

Si el procedimiento tiene éxito, aparecerá un banner azul en la parte superior de la consola. Esto significa que el trabajo de restauración está en curso. Se le redirigirá automáticamente a la página de trabajos, donde su trabajo de restauración aparecerá en la lista de trabajos de restauración. Este trabajo más reciente tendrá un estado `Pending`. Puede buscar el ID del trabajo de restauración y, a continuación, hacer clic en él para ver los detalles de cada trabajo de restauración. Para actualizar la lista de trabajos de restauración, haga clic en el botón de actualización para ver los cambios en el estado del trabajo de restauración.

[StartRestoreJob API](#) para SAP HANA en EC2

Esta acción recupera el recurso guardado identificado por un nombre de recurso de Amazon (ARN).

Sintaxis de la solicitud

```
PUT /restore-jobs HTTP/1.1
Content-type: application/json
{
  "IdempotencyToken": "string",
  "Metadata": {
    "string" : "string"
  },
  "RecoveryPointArn": "string",
  "ResourceType": "string"
}
```

Parámetros de solicitud de URI: la solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud: la solicitud admite los siguientes datos en formato JSON:

IdempotencyToken Una cadena elegida por el cliente que puede utilizar para distinguir entre llamadas a las que, de otro modo, serían idénticas. **StartRestoreJob** Si se vuelve a intentar una solicitud correcta con el mismo token de idempotencia, aparece un mensaje de confirmación y no se realiza ninguna acción.

Tipo: cadena

Requerido: no

Metadatos

Un conjunto de pares clave-valor de metadatos. Contiene información, como el nombre del recurso, necesaria para restaurar un punto de recuperación. Para obtener los metadatos de configuración de un recurso en el momento en que se realizó la copia de seguridad, solo tiene que llamar a `GetRecoveryPointRestoreMetadata`. Sin embargo, es posible que para restaurar un recurso se necesiten valores adicionales a los proporcionados por el recurso `GetRecoveryPointRestoreMetadata`. Por ejemplo, puede que tenga que proporcionar un nombre de recurso nuevo si el original ya existe.

Debe incluir metadatos específicos para restaurar una EC2 instancia de SAP HANA en Amazon. Consulte [StartRestoreJob los metadatos](#) de los elementos específicos de SAP HANA.

Para recuperar los metadatos pertinentes, puede utilizar la llamada [GetRecoveryPointRestoreMetadata](#).

Ejemplo de un punto de recuperación estándar de base de datos SAP HANA:

```
"RestoreMetadata": {
  "BackupSize": "1660948480",
  "DatabaseName": "DATABASENAME",
  "DatabaseType": "SYSTEM",
  "HanaBackupEndTime": "1674838362",
  "HanaBackupId": "1234567890123",
  "HanaBackupPrefix": "1234567890123_SYSTEMDB_FULL",
  "HanaBackupStartTime": "1674838349",
  "HanaVersion": "2.00.040.00.1553674765",
  "IsCompressedBySap": "FALSE",
  "IsEncryptedBySap": "FALSE",
  "SourceDatabaseArn": "arn:aws:ssm-sap:region:accountID:HANA/applicationID/DB/DATABASENAME",
  "SystemDatabaseSid": "HDB",
  "aws:backup:request-id": "46bbtt4q-7unr-2897-m486-yn378k2mrw9c"
```



```
}
```

Ejemplo de un punto de recuperación continuo de base de datos SAP HANA:

```
"RestoreMetadata": {
  "AvailableRestoreBases":
    "[1234567890123,9876543210987,1472583691472,7418529637418,1678942598761]",
  "BackupSize": "1711284224",
  "DatabaseName": "DATABASENAME",
  "DatabaseType": "TENANT",
  "EarliestRestorablePitrTimestamp": "1674764799789",
  "HanaBackupEndTime": "1668032687",
  "HanaBackupId": "1234567890123",
  "HanaBackupPrefix": "1234567890123_HDB_FULL",
  "HanaBackupStartTime": "1668032667",
  "HanaVersion": "2.00.040.00.1553674765",
  "IsCompressedBySap": "FALSE",
  "IsEncryptedBySap": "FALSE",
  "LatestRestorablePitrTimestamp": "1674850299789",
  "SourceDatabaseArn": "arn:aws:ssm-sap:region:accountID:HANA/applicationID/
DB/SystemDatabaseSid",
  "SystemDatabaseSid": "HDB",
  "aws:backup:request-id": "46bbtt4q-7unr-2897-m486-yn378k2mrw9d"
}
```

CLI para SAP HANA en EC2

El comando `start-restore-job` recupera el recurso guardado identificado con un nombre de recurso de Amazon (ARN). La CLI seguirá la directriz de API anterior.

Sinopsis:

```
start-restore-job
--recovery-point-arn value
--metadata value
--aws:backup:request-id value
[--idempotency-token value]
[--resource-type value]
[--cli-input-json value]
[--generate-cli-skeleton value]
[--debug]
[--endpoint-url value]
[--no-verify-ssl]
```

```
[--no-paginate]
[--output value]
[--query value]
[--profile value]
[--region value]
[--version value]
[--color value]
[--no-sign-request]
[--ca-bundle value]
[--cli-read-timeout value]
[--cli-connect-timeout value]
```

Opciones

`--recovery-point-arn` (cadena) es una cadena en forma de número de recurso de Amazon (ARN) que identifica de forma exclusiva un punto de recuperación; por ejemplo `arn:aws:backup:region:123456789012:recovery-point:46bbtt4q-7unr-2897-m486-yn378k2mrw9d`.

`--metadata` (mapa): un conjunto de pares clave-valor de metadatos. Contiene información, como el nombre del recurso, necesaria para restaurar un punto de recuperación. Para obtener los metadatos de configuración de un recurso en el momento en que se realizó la copia de seguridad, solo tiene que llamar a `GetRecoveryPointRestoreMetadata`. Sin embargo, es posible que para restaurar un recurso se necesiten valores adicionales a los proporcionados por el recurso `GetRecoveryPointRestoreMetadata`. Debe especificar metadatos específicos para restaurar una EC2 instancia de SAP HANA en Amazon:

- `aws:backup:request-id`: se trata de cualquier cadena de UUID utilizada para la idempotencia. No altera en modo alguno su experiencia de restauración.
- `aws:backup:TargetDatabaseArn`: especifique la base de datos en la que desee restaurar. Este es el ARN de la EC2 base de datos de SAP HANA en Amazon.
- `CatalogRestoreOption`: especifique dónde restaurar el catálogo. Uno de `NO_CATALOG`, `LATEST_CATALOG_FROM_AWS_BACKUP`, `CATALOG_FROM_LOCAL_PATH`.
- `LocalCatalogPath`: Si el valor de `CatalogRestoreOption` los metadatos es `CATALOG_FROM_LOCAL_PATH`, especifique la ruta al catálogo local de la EC2 instancia. Debe ser una ruta de archivo válida en la EC2 instancia.
- `RecoveryType`: actualmente se admiten los tipos de recuperación, `FULL_DATA_BACKUP_RECOVERY`, `POINT_IN_TIME_RECOVERY` y `MOST_RECENT_TIME_RECOVERY`.

clave = (cadena); valor = (cadena). Sintaxis abreviada:

```
KeyName1=string,KeyName2=string
```

Sintaxis de JSON:

```
{"string": "string"  
...}
```

--idempotency-token es una cadena elegida por el usuario que puede utilizar para distinguir entre llamadas a `StartRestoreJob` que, de otro modo, serían idénticas. Si se vuelve a intentar una solicitud correcta con el mismo token de idempotencia, aparece un mensaje de confirmación y no se realiza ninguna acción.

--resource-types es una cadena que inicia un trabajo para restaurar un punto de recuperación para uno de los siguientes recursos: SAP HANA on Amazon EC2 para SAP HANA en Amazon EC2. Opcionalmente, los recursos de SAP HANA se pueden etiquetar mediante el comando `aws ssm-sap tag-resource`.

Resultado: `RestoreJobId` es una cadena que identifica de forma exclusiva el trabajo que restaura un punto de recuperación.

Restauración de alta disponibilidad (HA) de SAP HANA

Hay consideraciones importantes y pasos adicionales que se deben tener en cuenta al restaurar un sistema de alta disponibilidad (HA) de SAP HANA. Amplíe la sección que mejor se adapte a su caso de uso.

Escenario de restauración:

Base de datos del sistema a un destino de HA de SAP HANA

Antes de restaurar el sistema de HA de SAP HANA de destino,

1. Si hay un clúster instalado, ponga todas las notas del clúster en modo Mantenimiento.
2. Detenga la base de datos de SAP HANA en todos los nodos, incluidos el principal y el secundario.
3. (Recomendado) Desactive cualquier plan de copia de seguridad para asegurarse de que no interfiera con la operación de restauración.

Una vez finalizado el trabajo de restauración, vaya al sistema de HA de SAP HANA restaurado y, a continuación:

1. Inicie la base de datos de SAP HANA en el modo principal.
2. Inicie manualmente cualquier base de datos de inquilinos en la que se haya restaurado la base de datos del sistema pero no se hayan restaurado sus inquilinos.
3. Restablezca la replicación del sistema (HSR) de SAP HANA entre los nodos principal y secundario.
4. Inicie la base de datos SAP HANA en el nodo secundario.
5. Si hay un clúster instalado, asegúrese de que todos los nodos del clúster estén en línea.
6. Habilite cualquier plan de copia de seguridad que haya desactivado antes de la operación de restauración.

(Opcional) Puede mantener la aplicación sincronizada en [AWS Systems Manager for SAP](#) llamando [StartApplicationRefresh](#) o puede esperar a la actualización programada de la aplicación que incluirá los metadatos de SAP más recientes.

Base de datos del sistema a un destino de nodo único de SAP HANA

Antes de comenzar un trabajo de restauración, vaya al sistema SAP HANA de nodo único de destino y, a continuación:

1. Detenga la base de datos de SAP HANA en el sistema SAP HANA de destino.
2. (Recomendado) Desactive cualquier plan de copia de seguridad para asegurarse de que no interfiera con la operación de restauración.

Una vez finalizado el trabajo de restauración, vaya al sistema de SAP HANA de nodo único de destino y, a continuación:

1. Inicie SAP HANA en el sistema SAP HANA de destino.
2. Inicie manualmente cada base de datos de inquilinos en el nodo de destino.
3. Habilite cualquier plan de copia de seguridad que haya desactivado antes de la operación de restauración.

(Opcional) Puede mantener la aplicación sincronizada en [AWS Systems Manager for SAP](#) llamando [StartApplicationRefresh](#) o puede esperar a la actualización programada de la aplicación que incluirá los metadatos de SAP más recientes.

Base de datos de inquilinos (instalada o copia del sistema)

Antes de comenzar un trabajo de restauración, vaya al sistema SAP HANA de destino y, a continuación:

1. (Opcional, pero recomendado) Coloque los clústeres instalados en modo de mantenimiento para evitar una toma de control inesperada durante la operación de restauración.
2. Asegúrese de que la base de datos del sistema se ejecute en el sistema SAP HANA de destino.
3. (Recomendado) Desactive cualquier plan de copia de seguridad para asegurarse de que no interfiera con la operación de restauración.

Una vez finalizado el trabajo de restauración:

- Habilite cualquier plan de copia de seguridad que haya desactivado antes de la operación de restauración.

Resolución de problemas

Si se produce alguno de los siguientes errores al intentar realizar una operación de copia de seguridad, consulte la resolución correspondiente.

- Error: error en el registro de copias de seguridad continuas

Para mantener los puntos de recuperación para las copias de seguridad continuas, SAP HANA crea registros de todos los cambios. Si los registros no están disponibles, el estado de cada uno de estos puntos de recuperación continua es STOPPED. El último punto de recuperación viable que se puede utilizar para restaurar es uno que tenga el estado AVAILABLE. Si faltan datos de registro durante el tiempo transcurrido entre los puntos de recuperación con un estado STOPPED y los puntos con un estado AVAILABLE, no se puede garantizar que la restauración se realice correctamente en esos momentos. Si introduce una fecha y una hora dentro de este intervalo, AWS Backup intentará realizar la copia de seguridad, pero utilizará la hora de restauración más cercana disponible. Este error se muestra en el mensaje "Encountered an issue with log backups. Please check SAP HANA for details."

Solución: en la consola, se muestra la hora de restauración más reciente, con base en los registros. Puede introducir una hora más reciente que la que se muestra. Sin embargo, si los datos de este momento no están disponibles en los registros, AWS Backup utilizará la hora de restauración más reciente.

- Error: Internal error

Solución: crea un caso de soporte desde la consola o ponte en contacto Soporte con ellos con los detalles de la restauración, como el identificador del trabajo de restauración.

- Error: The provided role arn:aws:iam::ACCOUNT_ID:role/ServiceLinkedRole cannot be assumed by AWS Backup

Solución: asegúrese de que el rol asumido al realizar la restauración tenga los permisos necesarios para crear roles vinculados a servicios.

- Error: User: arn:aws:sts::ACCOUNT_ID:assumed-role/ServiceLinkedRole/AWSBackup-ServiceLinkedRole is not authorized to perform: ssm-sap:GetOperation on resource: arn:aws:ssm-sap:us-east-1:ACCOUNT_ID:...

Solución: asegúrese de introducir correctamente el rol que se asume al solicitar los permisos de restauración descritos en los requisitos previos.

- Error: b* 449: recovery strategy could not be determined: [111014] The backup with backup id '1660627536506' cannot be used for recovery
SQLSTATE: HY000\n

Solución: asegúrese de que el agente BackInt esté instalado correctamente. Compruebe todos los requisitos previos, especialmente el de [instalar el AWS BackInt agente y el AWS Systems Manager de SAP](#) en su servidor de aplicaciones SAP y, a continuación, vuelva a intentar instalar el BackInt agente.

- Error: IllegalArgumentException: Restore job provided is not ready to return chunks, current restore job status is: CANCELLED

Solución: el flujo de trabajo del servicio canceló el trabajo de restauración. Vuelva a intentar el trabajo de restauración.

- Error: se produjo un problema al restaurar una base de datos de inquilinos en un sistema de alta disponibilidad de SAP HANA: b* -10709: Connection failed (RTE:[89006] System call 'connect' failed, rc=111:Connection refused (:::1):40404 # localhost:30013))\n

Solución: compruebe SAP HANA para asegurarse de que SYSTEMDB esté en funcionamiento.

- Error: b'* 448: recovery could not be completed: [301102] exception 301153: Sending root key to secondary failed: connection refused. This may be caused by a stopped system replication secondary. Please keep the secondary online to receive the restored root key. Alternatively you could unregister the secondary site in case of an urgent recovery.\n SQLSTATE: HY000\n'

Solución: en un sistema de alta disponibilidad de SAP HANA, es posible que SAP HANA no se ejecute en el nodo secundario mientras se esté ejecutando una operación de restauración activa. Inicie SAP HANA en el nodo secundario y, a continuación, vuelva a intentar el trabajo de restauración.

- Error: RequestError: send request failed\ncaused by: read tcp 10.0.131.4:40482->35.84.99.47:443: read: connection timed out"

Solución: se está produciendo una inestabilidad de red transitoria en la instancia. Vuelva a intentar la restauración. Si este problema se produce de forma constante, intente agregar ForceRetry: "true" al archivo de configuración del agente en /hana/shared/aws-backint-agent/aws-backint-agent-config.yaml.

Para cualquier otro problema relacionado con el agente de AWS Backint, consulte [Solución de problemas del AWS agente de Backint para SAP HANA](#).

Restauración de los datos de S3 mediante AWS Backup

Puede restaurar los datos de S3 de los que realizó una copia de AWS Backup seguridad en la clase de almacenamiento S3 Standard. Puede restaurar todos los objetos de un bucket u objetos específicos. Puede restaurarlos en un bucket existente o nuevo.

Permisos de restauración de Amazon S3

Antes de empezar a restaurar los recursos, asegúrese de que el rol que está utilizando tenga permisos suficientes.

Para obtener más información, consulte los siguientes temas sobre políticas:

1. [AWSBackupServiceRolePolicyForS3Restore](#)
2. [AWSBackupServiceRolePolicyForRestores](#)

3. [Políticas administradas para AWS Backup](#)

Consideraciones sobre la restauración de Amazon S3

- Si ACLs se activó durante la copia de seguridad, el depósito de destino de la restauración debe estar ACLs activado; de lo contrario, se producirá un error en la tarea de restauración.
- Si la opción Bloquear el acceso público está habilitada en el depósito de destino, el trabajo de restauración se completa correctamente, pero los objetos con acceso público no ACLs se restauran.
- Las restauraciones de objetos se omiten si el bucket de origen tiene un objeto con el mismo nombre o ID de versión.
- Al restaurar el bucket de S3 original,
 - AWS Backup no realiza una restauración destructiva, lo que significa que no AWS Backup colocará un objeto en un depósito en lugar de un objeto que ya existe, independientemente de la versión.
 - En la versión actual, un marcador de borrado se considera que el objeto no existe, por lo que se puede realizar una restauración.
 - AWS Backup no elimina objetos (sin eliminar marcadores) de un depósito durante una restauración (por ejemplo: las claves que se encuentran actualmente en el depósito y que no estaban presentes durante la copia de seguridad permanecerán).
- Restauración de copias entre regiones
 - Si bien las copias de seguridad de S3 se pueden copiar entre regiones, los trabajos de restauración solo se realizan en la misma región en la que se encuentra la copia de seguridad o copia original.

Example

Ejemplo: un bucket de S3 creado en la región Este de EE. UU. (Norte de Virginia) se puede copiar en la región Canadá (centro). El trabajo de restauración puede iniciarse mediante el bucket original de la región Este de EE. UU. (Norte de Virginia) y restaurarse a esa región, o bien puede iniciarse con la copia en la región de Canadá (centro) y restaurarse en esa región.

- El método de cifrado original no se puede utilizar para restaurar un punto de recuperación (copia de seguridad) copiado de otra región. El AWS KMS cifrado de copias entre regiones no está disponible para los recursos de Amazon S3; en su lugar, utilice un tipo de cifrado diferente para un trabajo de restauración.

Etiquetas de objetos ACLs y de restauración

Al restaurar los datos de Amazon S3, usted decide si ACLs forman parte de la restauración.

Si ACLs están disponibles en el punto de recuperación, puede elegir entre restaurarlos o excluirlos ACLs mediante la ACLs configuración de restauración; si ACLs no están en la copia de seguridad, no se pueden restaurar independientemente de la configuración. Si intenta crear un trabajo de restauración con la ACLs opción habilitada pero no formaba parte de la copia de seguridad, es posible que aparezca un error como el siguiente `Unable to restore Access Control Lists (ACLs) for bucket because backup was created with the 'BackupACLs' option disabled. Please proceed with restoring without ACLs.`

Las etiquetas de objetos se restauran automáticamente si se incluyeron en la copia de seguridad original.

Note

Restaurar puntos de recuperación sin ACLs

AWS CLI Si intenta restaurar a ACLs partir de una copia de seguridad excluida ACLs, la operación de restauración fallará y aparecerá un mensaje de error que indicará que los parámetros de restauración no son válidos.

Restauración de varias versiones

De forma predeterminada, AWS Backup restaura solo la versión más reciente de los objetos. Tiene la opción de restaurar versiones adicionales o todas las versiones de los objetos.

Consulte el paso 6 de la siguiente sección para saber cómo restaurar las 10 versiones más recientes o todas las versiones mediante la AWS Backup consola.

Consulte [???](#) más adelante en esta página para ver los detalles de los metadatos que se deben incluir al restaurar mediante programación.

Restaure a través de la AWS Backup consola

Para restaurar los datos de Amazon S3 mediante la AWS Backup consola:

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.

2. En el panel de navegación, elija Recursos protegidos y seleccione el ID del recurso de Amazon S3 que desee restaurar.
3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID del recurso seleccionado. Para restaurar un recurso:
 - a. En el panel Copias de seguridad, elija el ID del punto de recuperación del recurso.
 - b. En la esquina superior derecha del panel, elija Restaurar.

(También puede ir al almacén de copias de seguridad, buscar el punto de recuperación, hacer clic en Acciones y, a continuación, hacer clic en Restaurar).

4. Si va a restaurar una copia de seguridad continua, en el panel Tiempo de restauración, seleccione una de las siguientes opciones:
 - a. Acepte el valor predeterminado para restaurar a la Última hora restaurable.
 - b. Especifique la fecha y la hora de la restauración.
5. En el panel Configuración, especifique si desea Restaurar todo el bucket o realizar una Restauración a nivel de elemento.
 - a. Si elige la Restauración a nivel de elemento, restaurará hasta 5 elementos (objetos o carpetas en un bucket) por trabajo de restauración especificando el [URI de S3](#) de cada elemento que identifica de forma única ese objeto.

(Para obtener más información sobre el depósito de S3 URIs, consulte [Métodos para acceder a un depósito](#) en la Guía del usuario de Amazon Simple Storage Service).

- b. Elija Agregar elemento para especificar otro elemento para restaurarlo.
6. De forma predeterminada, solo restaura la versión más reciente de un objeto. Puede restaurar hasta las diez versiones más recientes o todas las versiones de los objetos. Seleccione sus preferencias en el menú desplegable.
7. Elige el Destino de restauración. Puede Restaurar al bucket fuente, Usar bucket existente o Crear nuevo bucket.

 Note

El bucket de destino de la restauración debe tener activado el control de versiones. AWS Backup le notifica si el depósito que ha seleccionado no cumple este requisito.

- a. Si elige Usar bucket existente, seleccione el bucket de S3 de destino en el menú, que muestra todos los buckets existentes en su región de AWS actual.
 - b. Si elige Crear nuevo bucket, escriba el Nuevo nombre de bucket. Una vez creado el bucket, puede modificar los ajustes predeterminados de control de versiones de BPA (bloqueo de acceso público) y S3.
8. Para el cifrado de los objetos de su bucket de S3, puede elegir el cifrado de objeto restaurado. Utilice las claves de cifrado originales (de forma predeterminada), una clave de Amazon S3 (SSE-S3) o una clave de AWS Key Management Service (SSE-KMS).

Esta configuración solo se aplica al cifrado de los objetos del bucket de S3. Esto no afecta al cifrado del propio bucket.

- a. Utilizar claves de cifrado originales (opción predeterminada) restaura los objetos con las mismas claves de cifrado utilizadas por el objeto de origen. Si un objeto de origen no estaba cifrado, este método restaura el objeto sin cifrar.

Esta opción de restauración le permite elegir opcionalmente una clave de cifrado sustituta para cifrar los objetos de restauración si la clave original no está disponible.

- b. Si elige la clave de Amazon S3 (SSE-S3), no es necesario que especifique ninguna otra opción.
 - c. Si elige la AWS Key Management Service clave (SSE-KMS), puede realizar las siguientes elecciones: Clave administrada de AWS (aws/s3), elegir una de AWS KMS las claves o introducir el ARN de la clave. AWS KMS
 - i. Si elige la Clave administrada de AWS (aws/s3), no es necesario que especifique ninguna otra opción.
 - ii. Si eliges una de tus AWS KMS claves, selecciona una AWS KMS clave en el menú desplegable. Como alternativa, elija Crear clave.
 - iii. Si introduce un AWS KMS ARN clave, escriba el ARN en el cuadro de texto. Como alternativa, elija Crear clave.
9. En el panel Restore role (Restaurar rol), elija el rol de IAM que AWS Backup asumirá para esta restauración.
10. Seleccione Restaurar copia de seguridad. Aparecerá el panel Trabajos de restauración. En la parte superior de la página, aparecerá un mensaje con información sobre el trabajo de restauración.

Restaura los puntos de recuperación de Amazon S3 mediante AWS CLI

Utilice [StartRestoreJob](#). Puede especificar los siguientes metadatos durante las restauraciones de Amazon S3:

```
// Mandatory metadata:
DestinationBucketName // The destination bucket for your restore.

// Optional metadata:
RestoreACLs // Boolean. If ACLs were part of the backup, include and set to TRUE. If
the backup
does not include ACLs and this parameter is included, set to FALSE.
EncryptionType // The type of encryption to encrypt your restored objects. Options
are original (same encryption as the original object), SSE-S3, or SSE-KMS).
ItemsToRestore // A list of up to five paths of individual objects to restore. Only
required for item-level restore.
KMSKey // Specifies the SSE-KMS key to use. Only needed if encryption is SSE-KMS.
RestoreLatestVersionsUpTo // Include this optional parameter to multiple versions.
RestoreTime // The restore time (only valid for continuous recovery points where it is
required, in format 2021-11-27T03:30:27Z).
```

`RestoreLatestVersionsUpTo` es un par clave-valor de metadatos opcional. De forma predeterminada, o si se omite, se restaura la versión más reciente. Incluya estos metadatos para restaurar versiones adicionales de sus objetos. Los valores aceptados son:

- 1 (para restaurar la versión más reciente)
- *n*, donde *n* es cualquier número entero positivo mayor que 1. Se restaurarán las *n* versiones más recientes de sus objetos. Si el número real de versiones de un objeto es inferior a *n*, se restaurará ese número de versiones para ese objeto.
- all (para restaurar todas las versiones)

Estado del punto de recuperación

Los puntos de recuperación tendrán un estado que indica su estado.

EXPIRED El estado indica que el punto de recuperación ha superado su período de retención, pero AWS Backup carece de permiso o no puede eliminarlo por algún motivo. Para eliminar estos puntos de recuperación manualmente, consulte el [Paso 3: elimine los puntos de recuperación](#) en la sección Depuración de recursos de la Introducción.

El estado STOPPED se produce en una copia de seguridad continua cuando un usuario ha realizado alguna acción que provoca la desactivación de la copia de seguridad continua. Esto puede deberse a la eliminación de permisos, la desactivación del control de versiones, la desactivación de los eventos que se envían a Amazon EventBridge o la desactivación de EventBridge las reglas establecidas por AWS Backup.

Para resolver el estado STOPPED, asegúrese de que todos los permisos solicitados estén en vigor y de que el control de versiones esté activado en el bucket de S3. Una vez que se cumplan estas condiciones, la siguiente instancia de una regla de copia de seguridad que se ejecute provocará la creación de un nuevo punto de recuperación continuo. No es necesario eliminar los puntos de recuperación con el estado STOPPED.

Mensajes de restauración de S3

Si un trabajo de restauración se completa o genera un error, puede aparecer el siguiente mensaje. La siguiente tabla puede ayudarlo a determinar la posible causa del mensaje de estado.

Escenario	Estado del trabajo	Mensaje	Ejemplo
No se ha podido restaurar ningún objeto.	FAILED	«No se restauró ningún objeto de a <i>RecoveryPoint</i> <i>arn:aws:s3:::bucket</i> . To get notified of these failures, enable SNS event notifications”.	El rol utilizado para iniciar el trabajo de restauración no tiene permiso para colocar objetos en el bucket de destino. El rol de restauración no tiene permiso para comprobar si existe una versión del objeto en el bucket de destino.
No se han podido restaurar uno o más objetos (no todos).	COMPLETED	«No se pudieron restaurar uno o más objetos desde <i>RecoveryPoint</i> <i>arn:aws:s3:::bucket</i> ».	El rol utilizado para iniciar el trabajo de restauración no tiene acceso a la clave de KMS utilizada por uno

Escenario	Estado del trabajo	Mensaje	Ejemplo
		hasta bucket . To get notified of these failures, enable SNS event notifications”.	o varios de los objetos originales.
No hay objetos para restaurar.	COMPLETED	«No hay ningún objeto que coincida con la solicitud de restauración» RecoveryPointARN .	El punto de recuperación (copia de seguridad) del bucket de origen que se va a restaurar no tiene ningún objeto. El prefijo utilizado para el trabajo de restauración no se corresponde con ningún objeto.

Restauración de un volumen de Storage Gateway

Si va a restaurar una instantánea de AWS Storage Gateway volumen, puede elegir restaurarla como un volumen de Storage Gateway o como un volumen de Amazon EBS. Esto se debe a que AWS Backup se integra con ambos servicios y cualquier instantánea de Storage Gateway se puede restaurar en un volumen de Storage Gateway o en un volumen de Amazon EBS.

Restaurar Storage Gateway a través de la AWS Backup consola

Para restaurar un volumen de Storage Gateway

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, elija Recursos protegidos y el ID del recurso de Storage Gateway que desee restaurar.
3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID de recurso seleccionado. Para restaurar un recurso, en el panel Copias de seguridad, active el

botón de opción situado junto al ID del punto de recuperación del recurso. En la esquina superior derecha del panel, elija Restaurar.

4. Especifique los parámetros de restauración del recurso. Los parámetros de restauración establecidos son específicos del tipo de recurso seleccionado.

En Tipo de recurso, elija el AWS recurso que se va a crear al restaurar esta copia de seguridad.

5. Si elige Volumen de Storage Gateway, elija una Puerta de enlace en un estado accesible. Elija también el Nombre de destino iSCSI.
 1. Para las puertas de enlace del “Volumen almacenado”, elija un ID de disco.
 2. Para las puertas de enlace del “Volumen en caché”, elija una capacidad que sea al menos tan grande como el recurso protegido.

Si elige EBS volume (Volumen de EBS), proporcione los valores de Volume type (Tipo de volumen) y Size (GiB) (Tamaño [GiB]) y seleccione una zona de disponibilidad.

6. En la función de restauración, elija la función de IAM que AWS Backup asumirá para esta restauración.

Note

Si la función AWS Backup predeterminada no está presente en su cuenta, se creará una función predeterminada para usted con los permisos correctos. Puede eliminar este rol predeterminado o inutilizarlo.

7. Seleccione Restaurar copia de seguridad.

Aparecerá el panel Trabajos de restauración. En la parte superior de la página, aparecerá un mensaje con información sobre el trabajo de restauración.

Restauración de Storage Gateway con AWS CLI

En la interfaz de línea de comandos, [start-restore-job](#) permite restaurar un volumen de Storage Gateway.

La siguiente lista contiene los metadatos aceptados.

```
gatewayArn // The Amazon Resource Name (ARN) of the gateway. Use the ListGateways
operation to return a list of gateways for your account and Región de AWS.
```

```
gatewayType // The type of created gateway. Valid value is BACKUP_VM
targetName
kmsKey
volumeSize
volumeSizeInBytes
diskId
```

Restauración de una tabla de Amazon Timestream

Al restaurar una tabla de Amazon Timestream, hay varias opciones que configurar, como el nombre de la nueva tabla, la base de datos de destino, las preferencias de asignación de almacenamiento (memoria y almacenamiento magnético) y el rol que utilizará para completar el trabajo de restauración. También puede elegir un bucket de Amazon S3 para almacenar los registros de errores. Las escrituras en el almacenamiento magnético son asíncronas, por lo que se recomienda registrar los errores.

El almacenamiento de datos de Timestream tiene dos niveles: un almacén en memoria y un almacén magnético. Se requiere un almacén en memoria, pero tiene la opción de transferir la tabla restaurada a un almacenamiento magnético una vez transcurrido el tiempo de memoria especificado. El almacén de memoria está optimizado para escrituras de datos de alto rendimiento y point-in-time consultas rápidas. El almacén magnético está optimizado para permitir escrituras de datos tardías con menor rendimiento, almacenamiento de datos a largo plazo y consultas analíticas rápidas.

Cuando restaura una tabla de Timestream, determina cuánto tiempo desea que la tabla permanezca en cada nivel de almacenamiento. Con la consola o la API, puede configurar el tiempo de almacenamiento de ambos. Tenga en cuenta que el almacenamiento es lineal y secuencial. Timestream almacenará primero la tabla restaurada en el almacenamiento en memoria y, a continuación, la transferirá automáticamente al almacenamiento magnético cuando se alcance el tiempo de almacenamiento en memoria.

Note

El periodo de retención del almacenamiento magnético debe ser igual o superior al periodo de retención original (que se muestra en la parte superior derecha de la consola) o se perderán datos.

Ejemplo: configura la asignación del almacén en memoria para que almacene los datos durante una semana y configura la asignación del almacenamiento magnético para que almacene los mismos

datos durante un año. Cuando los datos del almacén en memoria cumplen una semana, se mueven automáticamente al almacén magnético. A continuación, se conservan en el almacén magnético durante un año. Al final de ese plazo, se eliminan de Timestream y de AWS Backup.

Para restaurar una tabla de Amazon Timestream mediante la consola AWS Backup

Puede restaurar las tablas Timestream en la AWS Backup consola que fueron creadas por AWS Backup

1. [Abra la AWS Backup consola en /backup. https://console.aws.amazon.com](https://console.aws.amazon.com/backup)
2. En el panel de navegación, elija Recursos protegidos y el ID del recurso de Amazon Timestream que desee restaurar.
3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID de recurso seleccionado. Para restaurar un recurso, en el panel Copias de seguridad, active el botón de opción situado junto al ID del punto de recuperación del recurso. En la esquina superior derecha del panel, elija Restaurar.
4. Especifique los ajustes de configuración de la nueva tabla, que incluyen:
 - a. Nombre de tabla nueva, compuesto de 2 a 256 caracteres (letras, números, guiones, puntos y guiones bajos).
 - b. Base de datos de destino, elegida en el menú desplegable.
5. Asignación de almacenamiento: establezca la cantidad de tiempo que la tabla restaurada residirá primero en el [almacenamiento en memoria](#) y, a continuación, la cantidad de tiempo que la tabla restaurada permanecerá en el [almacenamiento magnético](#). El almacenamiento en memoria puede establecerse en horas, días, semanas o meses. El almacenamiento magnético puede establecerse en días, semanas, meses o años.
6. (Opcional) Habilitar escrituras de almacenamiento magnético: tiene la opción de permitir las escrituras en el almacenamiento magnético. Si esta opción está marcada, los datos que lleguen tarde, es decir, los datos con una marca temporal fuera del periodo de retención de memoria, se escribirán directamente en el almacén magnético.
7. (Opcional) Ubicación de los registros de errores de Amazon S3: puede especificar una ubicación de S3 en la que se almacenarán los registros de errores. Examine sus archivos de S3 o copie y pegue la ruta del archivo de S3.

Note

Si decide especificar una ubicación para el registro de errores de S3, el rol que utilice para esta restauración debe tener permiso para escribir en un bucket de S3 o debe contener una política con ese permiso.

8. Elija el rol de IAM que desee transferir para realizar las restauraciones. Puede usar el rol de IAM predeterminado o especificar uno diferente.
9. Haga clic en Restaurar copia de seguridad.

Sus trabajos de restauración serán visibles en Recursos protegidos. Para ver el estado actual de su trabajo de restauración, haga clic en el botón de actualización o en CTRL-R.

Para restaurar una tabla de Amazon Timestream mediante la API, la CLI o el SDK

Utilice [StartRestoreJob](#) para restaurar una tabla de Timestream mediante la API.

Para restaurar un Timestream mediante AWS CLI, utilice la operación `start-restore-job`. y especifique los siguientes metadatos:

```
TableName: string;
DestinationDatabase: string;
MemoryStoreRetentionPeriodInHours: value: number unit: 'hours' | 'days' | 'weeks' |
'months'
MagneticStoreRetentionPeriodInDays: value: number unit: 'days' | 'weeks' | 'months' |
'years'
EnableMagneticStoreWrites?: boolean;
aws:backup:request-id
```

A continuación, se muestra una plantilla de ejemplo:

```
aws backup start-restore-job \
--recovery-point-arn "arn:aws:backup:us-west-2:accountnumber:recovery-point:1a2b3cde-
f405-6789-012g-3456hi789012_beta" \
--iam-role-arn "arn:aws:iam::accountnumber:role/rolename" \
--metadata
'TableName=tablename,DatabaseName=databasename,MagneticStoreRetentionPeriodInDays=1,MemoryStoreWrites=
\":true,\"MagneticStoreRejectedDataLocation\":{\"S3Configuration\":{\"BucketName\":
\"bucketname\",\"EncryptionOption\":\"SSE_S3\"}}}' \
```

```
--region us-west-2 \  
--endpoint-url url
```

También puede utilizar [DescribeRestoreJob](#) para obtener información de la restauración.

En AWS CLI, utilice la operación `describe-restore-job` y utilice los siguientes metadatos:

```
TableName: string;  
DestinationDatabase: string;  
MemoryStoreRetentionPeriodInHours: value: number unit: 'hours' | 'days' | 'weeks' |  
  'months'  
MagneticStoreRetentionPeriodInDays: value: number unit: 'days' | 'weeks' | 'months' |  
  'years'  
EnableMagneticStoreWrites?: boolean;
```

A continuación, se muestra una plantilla de ejemplo:

```
aws backup describe-restore-job \  
--restore-job-id restore job ID \  
--region awsregion \  
--endpoint-url url
```

Restaure una máquina virtual mediante AWS Backup

Puede restaurar una máquina virtual en Cloud on VMware, VMware Cloud on AWS, VMware en AWS Outposts un volumen de Amazon EBS o en [una EC2 instancia de Amazon](#). Para restaurar (o migrar) una máquina virtual se EC2 requiere una licencia. De forma predeterminada, AWS incluirá una licencia (de pago). Para obtener más información, consulte [las opciones de licencia](#) en la Guía del Import/Export usuario de máquinas virtuales.

Puede restaurar una máquina VMware virtual mediante la AWS Backup consola o mediante el AWS CLI. Cuando se restaura una máquina virtual, la carpeta VMware Herramientas no se incluye. Consulte VMware la documentación para volver a instalar VMware las herramientas.

AWS Backup las restauraciones de máquinas virtuales no son destructivas, es decir, AWS Backup no sobrescriben las máquinas virtuales existentes durante una restauración. En cambio, el trabajo de restauración implementa una nueva máquina virtual.

Tareas

- [Consideraciones a la hora de restaurar una máquina virtual en una EC2 instancia de Amazon](#)

- [Use la AWS Backup consola para restaurar los puntos de recuperación de máquinas virtuales](#)
- [Se utiliza AWS CLI para restaurar los puntos de recuperación de máquinas virtuales](#)

Consideraciones a la hora de restaurar una máquina virtual en una EC2 instancia de Amazon

- Para restaurar (o migrar) una máquina virtual se EC2 requiere una licencia. De forma predeterminada, una AWS incluirá una licencia (de pago). Para obtener más información, consulte [las opciones de licencia](#) en la Guía del Import/Export usuario de máquinas virtuales.
- Hay un límite máximo de 5 TB (terabytes) para cada disco de máquina virtual.
- No puede especificar un par de claves al restaurar la máquina virtual en una instancia. Puedes añadir un key pair `authorized_keys` durante el lanzamiento (a través de los datos de usuario de la instancia) o después del lanzamiento (tal y como se describe en [esta sección de solución de problemas](#) de la Guía del EC2 usuario de Amazon).
- Confirma que tu [sistema operativo es compatible con](#) la importación y exportación desde Amazon EC2 en la Guía del Import/Export usuario de máquinas virtuales.
- Consulta las limitaciones relacionadas con la [importación VMs a Amazon EC2](#) en la Guía del Import/Export usuario de máquinas virtuales.
- Cuando restaure a una EC2 instancia de Amazon mediante AWS CLI, debe especificar `"RestoreTo": "EC2Instance"`. Todos los demás atributos tienen valores predeterminados.
- [EC2 Se permiten EC2](#) ofertas de Amazon AMIs. Si esta configuración está habilitada en su cuenta, añada el alias `aws-backup-vault` a su lista de permitidos. De lo contrario, las operaciones de restauración de los puntos de recuperación de máquinas virtuales en EC2 las instancias fallarán y aparecerá un mensaje de error, como «La AMI de origen no se encuentra en la región».

Use la AWS Backup consola para restaurar los puntos de recuperación de máquinas virtuales

Puede restaurar una máquina virtual desde varias ubicaciones en el panel de navegación izquierdo de la AWS Backup consola:

- Elija Hipervisores para ver los puntos de recuperación de las máquinas virtuales administradas por un hipervisor que esté conectado a AWS Backup.

- Elija Máquinas virtuales para ver los puntos de recuperación de las máquinas virtuales en todos los hipervisores que estén conectados a AWS Backup.
- Seleccione Backup Vaults para ver los puntos de recuperación almacenados en un almacén específico AWS Backup .
- Elija Recursos protegidos para ver los puntos de recuperación de todos sus recursos AWS Backup protegidos.

Si tiene que restaurar una máquina virtual que ya no tiene conexión con la puerta de enlace de copia de seguridad, elija Almacenes de copia de seguridad o Recursos protegidos para localizar el punto de recuperación.

Opciones

- [Restaure a VMware](#)
- [Restauración en un volumen de Amazon EBS](#)
- [Restaurar en una EC2 instancia de Amazon](#)

Para restaurar una máquina virtual en VMware Cloud on AWS y VMware Cloud on VMware AWS Outposts

1. En las vistas Hipervisores o Máquinas virtuales, elija el Nombre de máquina virtual que desea restaurar. En la vista Recursos protegidos, elija el ID de recurso de la máquina virtual que desea restaurar.
2. Elija el botón de opción situado junto al ID de punto de recuperación que se va a restaurar.
3. Elija Restore (Restaurar).
4. Elija el Tipo de restauración.
 - a. La Restauración completa restaura todos los discos de la máquina virtual.
 - b. La Restauración a nivel de disco restaura una selección de uno o más discos definida por el usuario. Utilice el menú desplegable para seleccionar los discos que desea restaurar.
5. Elija la Ubicación de la restauración. Las opciones son VMwareVMware Cloud on AWS y VMware Cloud on AWS Outposts.
6. Si va a realizar una restauración en su totalidad, vaya al paso siguiente. Si va a realizar una restauración a nivel de disco, aparecerá un menú desplegable en Discos de máquina virtual. Elija uno o más volúmenes de arranque para restaurarlos.

7. Seleccione un Hipervisor en el menú desplegable para administrar la máquina virtual restaurada
8. Para la máquina virtual restaurada, utilice las prácticas recomendadas de su organización para especificar:
 - a. Nombre
 - b. Ruta (como /datacenter/vm)
 - c. Nombre del recurso de cómputo (por ejemplo, VMHost o clúster)

Si un host forma parte de un clúster, no puede restaurarlo en el host, sino solo en el clúster en cuestión.
 - d. Almacén de datos
9. En Rol de restauración, seleccione el Rol predeterminado (recomendado) o Elegir un rol de IAM en el menú desplegable.
10. Seleccione Restaurar copia de seguridad.
11. Opcional: compruebe si su trabajo de restauración tiene el estado Completed. En el panel de navegación izquierdo, elija Trabajos.

Para restaurar una máquina virtual en un volumen de Amazon EBS

1. En las vistas Hipervisores o Máquinas virtuales, elija el Nombre de máquina virtual que desea restaurar. En la vista Recursos protegidos, elija el ID de recurso de la máquina virtual que desea restaurar.
2. Elija el botón de opción situado junto al ID de punto de recuperación que se va a restaurar.
3. Elija Restore (Restaurar).
4. Elija el Tipo de restauración.
 - La Restauración de disco restaura una selección de uno o más discos definida por el usuario. Utilice el menú desplegable para seleccionar el disco que desea restaurar.
5. Elija la Ubicación de la restauración como Amazon EBS.
6. En el menú desplegable Disco de máquina virtual, elija el volumen de arranque que desea restaurar.
7. En Tipo de volumen de EBS, elija el tipo de volumen.
8. Elige la zona de disponibilidad.
9. Cifrado (opcional). Marque la casilla si elige cifrar el volumen de EBS.

10. Seleccione su clave de KMS en el menú.
11. En Rol de restauración, seleccione el Rol predeterminado (recomendado) o Elegir un rol de IAM.
12. Seleccione Restaurar copia de seguridad.
13. Opcional: compruebe si su trabajo de restauración tiene el estado `Completed`. En el panel de navegación izquierdo, elija Trabajos.
14. Opcional: visite [How do I use LVM to create a logical volume on an Amazon EBS volume's partition?](#) para obtener más información sobre cómo montar volúmenes administrados y acceder a los datos del volumen de Amazon EBS restaurado.

Para restaurar una máquina virtual en una EC2 instancia de Amazon

1. En las vistas Hipervisores o Máquinas virtuales, elija el Nombre de máquina virtual que desea restaurar. En la vista Recursos protegidos, elija el ID de recurso de la máquina virtual que desea restaurar.
2. Elija el botón de opción situado junto al ID de punto de recuperación que se va a restaurar.
3. Elija Restore (Restaurar).
4. Elija el Tipo de restauración.
 - La Restauración completa restaura el sistema de archivos por completo, incluida la carpeta y los archivos del nivel raíz.
5. Elige la ubicación de restauración como Amazon EC2.
6. En Tipo de instancia, elija la combinación de computación y memoria necesaria para ejecutar la aplicación en la nueva instancia.

 Tip

Elija un tipo de instancia que coincida o supere las especificaciones de la máquina virtual original. Para obtener más información, consulte la [Guía de tipos de EC2 instancias de Amazon](#).

7. En Virtual Private Cloud (VPC), elija una nube privada virtual (VPC), que define el entorno de red de la instancia.
8. En Subred, seleccione una de las subredes en la VPC. Su instancia recibe una dirección IP privada del intervalo de direcciones de la subred.

9. En el caso de los grupos de seguridad, elija un grupo de seguridad que actúe como un firewall para el tráfico de la instancia.
10. En Rol de restauración, seleccione el Rol predeterminado (recomendado) o Elegir un rol de IAM.
11. Opcional: para ejecutar un script en la instancia en el momento del lanzamiento, expanda Configuración avanzada e introduzca el script en Datos de usuario.
12. Seleccione Restaurar copia de seguridad.
13. Opcional: compruebe si su trabajo de restauración tiene el estado `Completed`. En el panel de navegación izquierdo, elija Trabajos.

Se utiliza AWS CLI para restaurar los puntos de recuperación de máquinas virtuales

Utilice [StartRestoreJob](#).

Puede especificar los siguientes metadatos para la restauración de una máquina virtual en Amazon EC2 y Amazon EBS:

```
RestoreTo
InstanceType
VpcId
SubnetId
SecurityGroupIds
IamInstanceProfileName
InstanceInitiatedShutdownBehavior
HibernationOptions
DisableApiTermination
Placement
CreditSpecification
RamdiskId
KernelId
UserData
EbsOptimized
LicenseSpecifications
KmsKeyId
AvailabilityZone
EbsVolumeType
IsEncrypted
ItemsToRestore
RequireIMDSv2
NetworkInterfaces
```


Puede especificar los siguientes metadatos para la restauración de una máquina virtual en VMware Cloud on AWS y en la VMware nube en AWS Outpost: VMware

```
RestoreTo
HypervisorArn
VMName
VMPath
ComputeResourceName
VMDatastore
DisksToRestore
ItemsToRestore
```

En este ejemplo, se muestra cómo realizar una restauración completa en: VMware

```
'{"RestoreTo":"VMware","HypervisorArn":"arn:aws:backup-gateway:us-east-1:209870788375:hypervisor/hype-9B1AB1F1","VMName":"name","VMPath":"/Labster/vm","ComputeResourceName":"Cluster","VMDatastore":"vsanDatastore","DisksToRestore":[{"DiskId":"2000","Label":"Hard disk 1"}],"vmId":"vm-101"}'
```

Pruebas de restauración

Las pruebas de restauración, una función ofrecida por AWS Backup, proporcionan una evaluación automática y periódica de la viabilidad de la restauración, así como la capacidad de monitorear los tiempos de duración de las tareas de restauración.

Contenido

- [Descripción general de](#)
- [Pruebas de restauración comparadas con el proceso de restauración](#)
- [Restaurar la gestión de pruebas](#)
- [Creación de un plan de prueba de restauración](#)
- [Actualizar un plan de prueba de restauración](#)
- [Visualización de planes de prueba de restauración existentes](#)
- [Visualización de los trabajos de prueba de restauración](#)
- [Eliminación de un plan de prueba de restauración](#)
- [Auditoría de pruebas de restauración](#)
- [Restauración de cuotas y parámetros de prueba](#)

- [Solución de error de pruebas de restauración](#)
- [Restauración de metadatos inferidos de las pruebas](#)
- [Restaurar la validación de las pruebas](#)

Descripción general de

En primer lugar se crea un plan de prueba de restauración en el que se indica un nombre para el plan, la frecuencia de las pruebas de restauración y la hora de inicio objetivo. A continuación, asigne los recursos que desea incluir en el plan. Luego, elige incluir puntos de recuperación específicos o aleatorios en la prueba. AWS Backup la copia de seguridad [deduce de forma inteligente los metadatos](#) que se necesitarán para que el trabajo de restauración se realice correctamente.

Cuando llegue la hora programada de su plan, AWS Backup inicia las tareas de restauración según su plan y supervisa el tiempo que se tarda en completar la restauración.

Cuando el plan de prueba de restauración termina de ejecutarse, puede utilizar los resultados para demostrar conformidad con los requisitos de la organización o de gobernanza, por ejemplo, la ejecución correcta de escenarios de prueba de restauración o la hora de finalización del trabajo de restauración.

Si lo desea, puede utilizar [Restaurar la validación de las pruebas](#) para confirmar los resultados de la prueba de restauración.

Una vez que se complete la validación opcional o se cierre el período de validación, AWS Backup elimina los recursos involucrados en la prueba de restauración y los recursos se eliminarán de acuerdo con el servicio SLAs.

Al final del proceso de prueba puede ver los resultados y la hora de finalización de las pruebas.

Pruebas de restauración comparadas con el proceso de restauración

Las pruebas de restauración ejecutan las tareas de restauración del mismo modo que las restauraciones bajo demanda y utilizan los mismos puntos de recuperación (copias de seguridad) que la restauración bajo demanda. Verá las llamadas para `StartRestoreJob` participar CloudTrail (si ha optado por participar) para cada trabajo iniciado mediante las pruebas de restauración

Sin embargo, hay algunas diferencias entre la operación de una prueba de restauración programada y una operación de restauración bajo demanda:

	Pruebas de restauración	Restaurar
Cuenta	La práctica recomendada es designar una cuenta para utilizarla en las pruebas de restauración	Puede restaurar los recursos desde una cuenta
AWS Backup Audit Manager	Puede activar un control para confirmar si una prueba de restauración cumple los objetivos de restauración especificados	
Cadencia	Periódicamente como parte de un plan programado.	Bajo demanda
Recursos	Los tipos de recursos que puede asignar a su plan de pruebas incluyen: Aurora, Amazon DocumentDB, Amazon DynamoDB, Amazon EBS, Amazon, Amazon EFS, EC2 Amazon (Lustre, ONTAP, FSx OpenZFS, Windows), Amazon Neptune, Amazon RDS y Amazon S3.	Pueden restaurarse todos los recursos.
Resultados	Cuando se completa el trabajo de prueba de restauración, el recurso restaurado se elimina cuando termina el periodo de Restaurar la validación de las pruebas .	Cuando finaliza el trabajo de restauración permanece la versión restaurada del recurso.
Etiquetas	En el caso de los tipos de recursos que admiten etiquetas en la restauración,	Las etiquetas son opcionales para los recursos compatibles.

	Pruebas de restauración	Restaurar
	las pruebas aplican etiquetas en la restauración.	

Restaurar la gestión de pruebas

Puede crear, ver, actualizar o eliminar un plan de prueba de restauración en la [consola de AWS Backup](#).

Puede utilizar [AWS CLI](#) para realizar operaciones mediante programación en planes de prueba de restauración. Cada CLI es específica del AWS servicio en el que se origina. Los comandos deben ir precedidos de `aws backup`.

Eliminación de datos

Cuando finaliza una prueba de restauración, AWS Backup comienza a eliminar los recursos involucrados en la prueba. Esta eliminación no se realiza al instante. Cada recurso tiene una configuración subyacente que determina cómo se almacenan y administra el ciclo de vida esos recursos. Por ejemplo, si los buckets de Amazon S3 forman parte de la prueba de restauración, [se agregan al bucket reglas del ciclo de vida](#). La ejecución de las reglas y la eliminación completa del bucket y sus objetos pueden tardar varios días, pero solo se cobrará por estos recursos hasta el día en que se inicie la regla de ciclo de vida (de forma predeterminada, es 1 día). La velocidad de eliminación dependerá del tipo de recurso.

Los recursos que forman parte de un plan de prueba de restauración contienen una etiqueta llamada `awsbackup-restore-test`. Si un usuario elimina esta etiqueta, AWS Backup no podrá eliminar el recurso al final del período de prueba y, en su lugar, tendrá que eliminarlo manualmente.

Para comprobar por qué es posible que los recursos no se hayan eliminado como se esperaba, puede buscar en la consola los trabajos con error o utilizar la interfaz de línea de comandos para llamar a la solicitud de la API `DescribeRestoreJob` para recuperar los mensajes de estado de eliminación.

Los planes de copia de seguridad (planes de pruebas que no son de restauración) ignoran los recursos creados por las pruebas de restauración (aquellos con la etiqueta `awsbackup-restore-test` o cuyo nombre comience por `awsbackup-restore-test`).

Control de costos

Las pruebas de restauración tienen un costo por prueba. Según los recursos incluidos en el plan de prueba de restauración, los trabajos de restauración que forman parte del plan también pueden tener un costo. Para obtener más información, consulte [Precios de AWS Backup](#).

Al configurar un plan de prueba de restauración por primera vez, puede resultarle beneficioso incluir un número mínimo de tipos de recursos y recursos protegidos para familiarizarse con la característica, el proceso y los costos medios involucrados. Puede actualizar un plan después de su creación para añadir más tipos de recursos y recursos protegidos.

Creación de un plan de prueba de restauración

Un plan de prueba de restauración consta de dos partes: creación del plan y asignación de recursos.

Cuando se utiliza la consola, estas partes son secuenciales. En la primera parte se establecen el nombre, la frecuencia y las horas de inicio. En la segunda parte se asignan recursos al plan de prueba.

Cuando utilices AWS CLI una API, utilízala primero [create-restore-testing-plan](#). Una vez que reciba una respuesta correcta y se haya creado el plan, utilice [create-restore-testing-selection](#) para cada tipo de recurso que incluir en el plan.

Cuando crea pruebas de restauración, creamos un rol vinculado a servicios para usted. Para obtener más información, consulte [Uso de roles para pruebas de restauración](#).

Console

Parte I: Crear un plan de prueba de restauración mediante la consola

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el menú de navegación de la izquierda, seleccione Prueba de restauración.
3. Elija Crear un plan de prueba de restauración.
4. General
 - a. Nombre: escriba un nombre para el nuevo plan de prueba de restauración. El nombre no se puede cambiar después de crear el plan. El nombre consta de únicamente de caracteres alfanuméricos y guiones bajos.
 - b. Frecuencia de prueba: elija la frecuencia con la que se ejecutarán las pruebas de restauración.

- c. Hora de inicio: establezca la hora (en horas y minutos) a la que desea que comience la prueba. También puede configurar la zona horaria local en la que desea que se desarrolle el plan de prueba de restauración.
 - d. Comenzar dentro: este valor (en horas) es el período de tiempo en el que está previsto que comience la prueba de restauración. AWS Backup hace todo lo posible por iniciar todas las tareas de restauración designadas durante el inicio dentro de un plazo determinado y distribuye aleatoriamente las horas de inicio dentro de este período.
5. Selección de puntos de recuperación: aquí puede configurar los almacenes de origen, el rango de puntos de recuperación y los criterios de selección para los puntos de recuperación (copias de seguridad) que desea incluir en el plan.
- a. Almacenes de origen: elija si desea incluir todos los almacenes disponibles o solo almacenes específicos para ayudar a filtrar los puntos de recuperación que pueden incluirse en el plan. Si elige almacenes específicos, seleccione en el menú desplegable los almacenes que desea incluir.
 - b. Puntos de recuperación aptos: especifique el periodo de tiempo del que se seleccionarán puntos de recuperación. Puede seleccionar de 1 a 365 días, de 1 a 52 semanas, de 1 a 12 meses o 1 año.
 - c. Criterios de selección: una vez especificado el rango de fechas de los puntos de recuperación, puede elegir si desea incluir el último o uno aleatorio en el plan. Puede resultar conveniente elegir uno aleatorio para evaluar el estado general de los puntos de recuperación con mayor frecuencia en el caso de que en algún momento esté justificado restaurar a una versión anterior.
 - d. Point-in-time puntos de recuperación: si su plan incluye recursos con puntos de respaldo continuo (point-in-time-restore/PITR), puede marcar esta casilla para que su plan de pruebas incluya copias de seguridad continuas como puntos de recuperación elegibles (consulte [Disponibilidad de funciones por recurso para ver qué tipos de recursos tienen esta función](#)).
6. (opcional) Etiquetas agregada al plan de prueba de restauración: puede agregar hasta 50 etiquetas al plan de prueba de restauración. Cada etiqueta debe agregarse por separado. Para agregar una etiqueta, elija Agregar nueva etiqueta.

Parte II: Asignar recursos al plan mediante la consola

En esta sección, elija los recursos de los que ha hecho una copia de seguridad para incluirlos en el plan de prueba de restauración. Elija el nombre de la asignación de recursos, el rol utilizado

para la prueba de restauración y el periodo de retención antes de la limpieza. A continuación, seleccione el tipo de recurso, seleccione el ámbito y, si lo desea, ajuste la selección con etiquetas.

 Tip

Para volver al plan de prueba de restauración al que desea agregar recursos, puede ir a la [consola de AWS Backup](#), seleccionar Prueba de restauración y, a continuación, buscar el plan de prueba que prefiera y seleccionarlo.

1. General

- a. Nombre de asignación de recursos: introduzca un nombre para esta asignación de recursos mediante una cadena de caracteres alfanuméricos y guiones bajos, sin espacios en blanco.
- b. Restaurar el rol de IAM: la prueba debe utilizar el rol de IAM (Identity and Access Management) que designe. Puede elegir el rol AWS Backup predeterminado o uno diferente. Si el AWS Backup predeterminado aún no existe al finalizar este proceso, lo AWS Backup creará automáticamente con los permisos necesarios. El rol de IAM que elija para las pruebas de restauración debe contener los permisos que se encuentran en [AWSBackupServiceRolePolicyForRestores](#).
- c. Periodo de retención antes de la limpieza: durante una prueba de restauración, los datos de copia de seguridad se restauran temporalmente. De forma predeterminada, estos datos se eliminan una vez finalizada la prueba. Tiene la opción de demorar la eliminación de estos datos si desea ejecutar la validación de la restauración.

Si planea ejecutar la validación, seleccione Retener durante un número específico de horas e introduzca un valor de 1 a 168 horas, ambos incluidos. Tenga en cuenta que la validación se puede ejecutar mediante programación, pero no desde la consola de AWS Backup .

2. Recursos protegidos:

- a. Seleccionar el tipo de recurso: seleccione los tipos de recursos y el ámbito de las copias de seguridad de esos tipos que desea incluir en el plan de prueba de recursos. Cada plan puede contener varios tipos de recursos, pero cada tipo de recurso debe asignarse al plan de forma individual.

- b. Alcance de la selección de recursos: una vez elegido el tipo, seleccione si desea incluir todos los recursos protegidos disponibles de ese tipo o si desea incluir únicamente recursos protegidos específicos.
- c. (opcional) Refinar selección de recursos mediante etiquetas: si sus copias de seguridad tienen etiquetas, puedes filtrarlas por etiquetas para seleccionar recursos protegidos específicos. Introduzca la clave de la etiqueta, la condición para que esta clave se incluya o no y el valor de la clave. A continuación, seleccione el botón Añadir etiquetas.

Las etiquetas de los recursos protegidos se evalúan comprobando las etiquetas del último punto de recuperación del almacén de copia de seguridad que contiene el recurso protegido.

3. Parámetros de restauración: algunos recursos requieren la especificación de parámetros para preparar un trabajo de restauración. En la mayoría de los casos, AWS Backup deducirá los valores en función de la copia de seguridad almacenada.

En la mayoría de los casos, se recomienda mantener estos parámetros; sin embargo, puede cambiar los valores realizando una selección diferente en el menú desplegable. Algunos ejemplos en los que cambiar los valores puede ser óptimo son la anulación de las claves de cifrado, la FSx configuración de Amazon en la que no se pueden deducir datos y la creación de subredes.

Por ejemplo, si una base de datos de RDS es uno de los tipos de recursos que asigna a su plan de prueba de restauración, parámetros como zona de disponibilidad, nombre de la base de datos, clase de instancia de base de datos y grupo de seguridad de VPC aparecerán con valores inferidos que puede cambiar si lo desea.

AWS CLI

El comando de la CLI `CreateRestoreTestingPlan` sirve para crear un plan de prueba de restauración.

El plan de prueba debe contener:

- `RestoreTestingPlan`, que debe contener un `RestoreTestingPlanName` único
- Expresión cron [ScheduleExpression](#)
- [RecoveryPointSelection](#)

Aunque se llama de forma similar, NO es lo mismo que `RestoreTestingSelection`.

[RecoveryPointSelection](#) tiene cinco parámetros (tres obligatorios y dos opcionales). Los valores que especifique determinan qué punto de recuperación se incluye en la prueba de restauración. Debe indicar `Algorithm` si desea incluir el último punto de recuperación dentro del suyo `SelectionWindowDays` o si desea un punto de recuperación aleatorio, y debe indicar a través de `IncludeVaults` de qué bóvedas se pueden elegir los puntos de recuperación.

Una selección puede tener uno o más recursos protegidos ARNs o puede tener una o más condiciones, pero no puede tener ambas.

También puede incluir:

- [ScheduleExpressionTimezone](#)
- [Tags](#)
- [CreatorRequestId](#)
- [StartWindowHours](#)

Utilice el comando de la CLI [create-restore-testing-plan](#).

Una vez que el plan se haya creado correctamente, debe asignarle recursos utilizando [create-restore-testing-selection](#).

Consta de `RestoreTestingSelectionName`, `ProtectedResourceType` y uno de los siguientes elementos:

 Note

`RestoreTestingSelectionName` requisitos de denominación:

- Debe tener entre 1 y 256 caracteres de longitud
- Puede contener letras (a-z, A-Z), números (0-9), guiones (-) y guiones bajos (_)
- Deben comenzar por un número o una letra
- No puede terminar con un guion o un guion bajo
- Debe ser exclusivo dentro del plan de restauración de prueba

- ProtectedResourceArns
- ProtectedResourceConditions

Cada tipo de recurso protegido puede tener un único valor. Una selección de pruebas de restauración puede incluir un valor comodín ("*") como ProtectedResourceArns junto con ProtectedResourceConditions. Como alternativa, puede incluir hasta 30 recursos protegidos específicos ARNs en ProtectedResourceArns.

Determinación del punto de recuperación

Cada vez que se ejecuta un plan de pruebas (según la frecuencia y la hora de inicio especificadas), la prueba de restauración restaura un punto de recuperación elegible por cada recurso protegido seleccionado. Si ningún punto de recuperación de un recurso cumple los criterios de selección de puntos de recuperación, ese recurso no se incluirá en la prueba.

Un punto de recuperación para un recurso protegido seleccionado en una prueba es elegible si cumple los criterios del período de tiempo especificado e incluye almacenes en el plan de pruebas de restauración.

Se selecciona un recurso protegido si la selección de recursos para la prueba incluye el tipo de recurso y si se cumple alguna de las siguientes condiciones:

- El ARN del recurso se especifica en esa selección; o,
- Las condiciones de etiqueta de esa selección coinciden con las etiquetas del último punto de recuperación del recurso

Actualizar un plan de prueba de restauración

Puede actualizar partes de su plan de prueba de restauración y las selecciones de recursos que contiene a través de la consola o de AWS CLI.

Console

Actualizar planes y selecciones de prueba de restauración en la consola

Cuando ve la página de detalles del plan de prueba de restauración en la consola, puede editar (actualizar) muchos de los ajustes del plan. Para ello,

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el menú de navegación de la izquierda, seleccione Prueba de restauración.
3. Seleccione el botón Editar.
4. Ajuste la frecuencia, la hora de inicio y la hora en que comenzará la prueba después de la hora de inicio elegida.
5. Guarde los cambios.

AWS CLI

Actualice, restaure, los planes de pruebas y las selecciones mediante AWS CLI

Solicita [UpdateRestoreTestingPlan](#)y se [UpdateRestoreTestingSelection](#)puede utilizar para enviar actualizaciones parciales a un plan o selección específicos. Los nombres no se pueden cambiar, pero puede actualizar otros parámetros. Incluya solo los parámetros que desee cambiar en cada solicitud.

Antes de enviar una solicitud de actualización, utilice [GetRestoreTestingPlan](#) y [GetRestoreTestingSelection](#) para determinar si RestoreTestingSelection contiene condiciones específicas ARNs o si utiliza el comodín y las condiciones.

Si la selección de las pruebas de restauración se ha especificado ARNs (en lugar de un comodín) y desea cambiarla por un comodín con condiciones, la solicitud de actualización debe incluir tanto el comodín del ARN como las condiciones. Una selección puede tener un recurso protegido ARNs o usar el comodín con condiciones, pero no puede tener ambos.

- [get-restore-testing-plan](#)
- [get-restore-testing-selection](#)
- [update-restore-testing-plan](#)
- [update-restore-testing-selection](#)

Visualización de planes de prueba de restauración existentes

Console

Vea los detalles sobre un plan de prueba de restauración existente y los recursos asignados en la consola

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el menú de navegación de la izquierda, seleccione Prueba de restauración. La pantalla muestra sus planes de prueba de restauración. Los planes se muestran de forma predeterminada por último tiempo de ejecución.
3. Seleccione el enlace de un plan para ver sus detalles, incluido un resumen del plan, su nombre, frecuencia, hora de inicio y valor de inicio.

También puede ver los recursos protegidos de este plan, los trabajos de pruebas de restauración de los últimos 30 días incluidos en este plan y cualquier etiqueta que haya creado para formar parte de este plan de prueba.

AWS CLI

Obtenga detalles sobre un plan de prueba de restauración existente y la selección de pruebas mediante la línea de comandos

- [list-restore-testing-plan](#)
- [list-restore-testing-selections](#)
- [get-restore-testing-plan](#)
- [get-restore-testing-selection](#)

Visualización de los trabajos de prueba de restauración

Console

Visualización de trabajos de prueba de restauración existentes en la consola

Los trabajos de prueba de restauración se incluyen en la página de trabajos de restauración.

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. Navegue a la página Trabajos.

Como alternativa, puede seleccionar Prueba de restauración y, a continuación, seleccionar un plan de prueba de restauración para ver sus detalles y los trabajos asociados al plan.

3. Seleccione la pestaña Trabajos de restauración.

En esta página puede ver el estado, la hora de restauración, el tipo de restauración, el identificador del recurso, el tipo de recurso, el plan de prueba de restauración al que pertenece el trabajo, la hora de creación y el identificador del punto de recuperación del trabajo de restauración.

Los trabajos incluidos en un plan de prueba de restauración tienen el tipo de restauración Prueba.

Los trabajos de prueba de restauración tienen varias categorías de estado:

- El tipo de estado que requiere atención aparece subrayado; pase el ratón sobre el estado para ver detalles adicionales, si están disponibles.
- Se mostrará un estado de validación si se han iniciado [Restaurar la validación de las pruebas](#) en la prueba (no disponible en la consola).
- El estado de eliminación indica el estado de los datos generados por la prueba de restauración. Hay tres estados de eliminación posibles: Correcto, Eliminando y Error.

Si se produce un error al eliminar un trabajo de prueba de restauración, tendrá que eliminar el recurso manualmente, ya que el flujo de la prueba de restauración no ha podido completarlo automáticamente. A menudo, si se quita la etiqueta `awsbackup-restore-test` del recurso, se desencadena un error de eliminación.

AWS CLI

Visualización de trabajos de prueba de restauración existentes en la línea de comandos

- [list-restore-jobs-by-protected-resource](#)

Eliminación de un plan de prueba de restauración

Console

Eliminación del plan de prueba de restauración en la consola

1. Vaya a [Visualización de planes de prueba de restauración existentes](#) para ver sus planes de prueba de restauración actuales.
2. En la página de detalles del plan de prueba de restauración, elimine un plan seleccionando Eliminar.
3. Después de seleccionar Eliminar, aparecerá una pantalla emergente para confirmar de que desea eliminar el plan. En esta pantalla, el nombre del plan de prueba de restauración específico aparecerá en negrita. Para continuar, escriba el nombre exacto del plan de prueba, distinguiendo mayúsculas y minúsculas, incluidos guiones bajos, guiones y puntos.

Si no se puede seleccionar la opción Eliminar el plan de prueba de restauración, vuelva a introducir el nombre hasta que coincida con el nombre mostrado. Cuando coincida exactamente, se podrá seleccionar la opción de eliminar el plan de prueba de restauración.

AWS CLI

Eliminación del plan de prueba de restauración mediante la línea de comandos

El comando CLI se [DeleteRestoreTestingSelection](#) puede usar para eliminar una selección de pruebas de restauración. Incluya `RestoreTestingPlanName` y `RestoreTestingSelectionName` en la solicitud.

Todas las selecciones de pruebas asociadas a un plan de prueba deben eliminarse antes de eliminar el plan de prueba. Una vez eliminadas todas las selecciones de prueba, puedes usar la solicitud de API [DeleteRestoreTestingPlan](#) para eliminar un plan de pruebas de restauración. Debe incluir `RestoreTestingPlanName`.

- [delete-restore-testing-selection](#)
- [delete-restore-testing-plan](#)

Auditoría de pruebas de restauración

Restaura las integraciones de las pruebas con AWS Backup Audit Manager para ayudarlo a evaluar si un recurso restaurado se completó dentro del tiempo de restauración previsto.

Para obtener más información, consulte el control [Tiempo de restauración para que los recursos cumplan el objetivo](#) en [Controles y corrección de AWS Backup Audit Manager](#).

Restauración de cuotas y parámetros de prueba

- 100 planes de prueba de restauración
- Se pueden agregar 50 etiquetas a cada plan de prueba de restauración
- 30 selecciones por plan
- 30 recursos protegidos ARNs por selección
- 30 condiciones de recursos protegidos por selección (incluidas las que se encuentran en `StringEquals` y `StringNotEquals`)
- 30 selectores de almacén por selección
- Días del periodo máximo de selección: 365 días
- Horas del periodo de inicio: mínimo: 1 hora; máximo: 168 horas (7 días)
- Longitud máxima del nombre del plan: 50 caracteres
- Longitud máxima del nombre de la selección: 50 caracteres

Puede consultar información adicional sobre los límites en [AWS Backup cuotas](#).

Solución de error de pruebas de restauración

Si tiene trabajos de pruebas de restauración con un estado de restauración de `Failed`, los siguientes motivos pueden ayudarle a determinar la causa y la solución.

Los mensajes de error [se pueden ver](#) en la AWS Backup consola, en la página de detalles del estado del trabajo o mediante los comandos CLI `list-restore-jobs-by-protected-resource` o `list-restore-jobs`.

1. Error: *No default VPC for this user. GroupName is only supported for EC2-Classic and default VPC.*

Solución 1: actualice la selección de pruebas de restauración y [anule](#) el parámetro `SubnetId`. La AWS Backup consola muestra este parámetro como «Subred».

Solución 2: vuelva a crear la [VPC predeterminada](#).

Tipos de recursos afectados: Amazon EC2

2. Error: *No subnets found for the default VPC [vpc]. Please specify a subnet.*

Solución 1: actualice la selección de pruebas de restauración y [anule](#) el parámetro de restauración SubnetId. La AWS Backup consola muestra este parámetro como «Subred».

Solución 2: [cree una subred predeterminada](#) en la VPC predeterminada.

Tipos de recursos afectados: Amazon EC2

3. Error: *No default subnet detected in VPC. Please contact AWS Support to recreate default Subnets.*

Solución 1: actualice la selección de pruebas de restauración y [anule](#) el parámetro de restauración DBSubnetGroupName. La consola de AWS Backup muestra este parámetro como el grupo Subred.

Solución 2: [cree una subred predeterminada](#) en la VPC predeterminada.

Tipos de recursos afectados: Amazon Aurora, Amazon DocumentDB, Amazon RDS, Neptune

4. Error: *IAM Role cannot be assumed by AWS Backup.*

Solución: la función de restauración debe ser asumible por AWS Backup. Actualice la política de confianza del rol en IAM para permitir que lo asuma "backup.amazonaws.com" o actualice su selección de pruebas de restauración para utilizar un rol que pueda asumir AWS Backup.

Tipos de recursos afectados: todos

5. Error: *Access denied to KMS key. o The specified AWS KMS key ARN does not exist, is not enabled or you do not have permissions to access it.*

Solución: verifique lo siguiente:

- La función de restauración tiene acceso a la AWS KMS clave utilizada para cifrar las copias de seguridad y, si corresponde, a la clave de KMS utilizada para cifrar el recurso restaurado.
- Las políticas de recursos de las claves de KMS anteriores permiten que el rol de restauración acceda a ellas.

Si aún no se cumplen las condiciones anteriores, configure el rol de restauración y las políticas de recursos para el acceso adecuado. A continuación, vuelva a ejecutar el trabajo de prueba de restauración.

Tipos de recursos afectados: todos

6. Errors: *User **ARN** is not authorized to perform **action** on **resource** because no identity based policy allows the **action**.* o *Access denied performing **s3:CreateBucket** on **awsbackup-restore-test-xxxxxx**.*

Solución: el rol de restauración no tiene los permisos adecuados. Actualice los permisos en IAM para el rol de restauración.

Tipos de recursos afectados: todos

7. Errores: *User **ARN** is not authorized to perform **action** on **resource** because no resource-based policy allows the **action**.* o *User **ARN** is not authorized to perform **action** on **resource** with an explicit deny in a resource based policy.*

Solución: el rol de restauración no tiene un acceso adecuado al recurso especificado en el mensaje. Actualice la política de recursos del recurso mencionado.

Tipos de recursos afectados: todos

Restauración de metadatos inferidos de las pruebas

La restauración de un punto de recuperación requiere la restauración de los metadatos. Para realizar pruebas de restauración, AWS Backup infiere automáticamente metadatos que pueden permitir una restauración satisfactoria. El comando `get-restore-testing-inferred-metadata` puede utilizar para obtener una vista previa de lo que AWS Backup se deduce. El comando `get-restore-job-metadata` devuelve el conjunto de metadatos inferido por. AWS Backup Tenga en cuenta que, para algunos tipos de recursos (Amazon FSx), AWS Backup no puede inferir un conjunto completo de metadatos.

Los metadatos de restauración inferidos se determinan durante el proceso de prueba de restauración. Puede anular determinadas claves de metadatos de restauración incluyendo el

parámetro `RestoreMetadataOverrides` en el cuerpo de `RestoreTestingSelection`. Algunas anulaciones de metadatos no están disponibles en la AWS Backup consola.

Cada recurso compatible tiene claves y valores de metadatos de restauración inferidos y claves de metadatos de restauración anulables. Solo `RestoreMetadataOverrides` es necesario incluir los pares de valores clave o los pares de valores clave anidados marcados con *required for successful restore* (los demás son opcionales). Tenga en cuenta que los valores de clave no distinguen entre mayúsculas y minúsculas.

Important

AWS Backup puede deducir que un recurso debe restaurarse a la configuración predeterminada, como una EC2 instancia de Amazon o un clúster de Amazon RDS que se restaure a la VPC predeterminada. Sin embargo, si el valor predeterminado no está presente (por ejemplo, se ha eliminado la VPC o la subred predeterminada y no se ha introducido ninguna anulación de metadatos), la restauración no se realizará correctamente.

Tipo de recurso	Claves y valores de metadatos de restauración inferidos	Metadatos anulables
DynamoDB	<code>deletionProtection</code> , donde el valor se establece en <code>false</code> <code>encryptionType</code> toma el valor <code>Default</code> <code>targetTableName</code> , donde el valor se establece en un valor aleatorio que empieza por <code>awsbackup-restore-test-</code>	<code>encryptionType</code> <code>kmsMasterKeyArn</code>
Amazon EBS	<code>availabilityZone</code> , cuyo valor se establece en una zona de disponibilidad aleatoria	<code>availabilityZone</code> <code>iops</code> <code>kmsKeyId</code>

Tipo de recurso	Claves y valores de metadatos de restauración inferidos	Metadatos anulables
	encrypted , cuyo valor se establece en true	throughput volumesize volumetype
Amazon EC2	El valor de disableApiTermination se establece en false El valor de instanceType se establece en el instanceType del punto de recuperación que se está restaurando El valor de requireImdsV2 se establece en true	iamInstanceProfileName (nulo o UseBackedUpValue) instanceType requireImdsV2 securityGroupIds subnetId
Amazon EFS	El valor de encrypted se establece en true El valor de file-system-id se establece en el ID del sistema de archivos del punto de recuperación que se está restaurando kmsKeyId value toma el valor alias/aws/elasticfilesystem El valor de newFileSystem se establece en true El valor de performanceMode se establece en generalPurpose	kmsKeyId performanceMode

Tipo de recurso	Claves y valores de metadatos de restauración inferidos	Metadatos anulables
Amazon FSx para Lustre	lustreConfiguration tiene claves anidadas. Una clave anidada es automaticBackupRetentionDays , cuyo valor se establece en 0	kmsKeyId lustreConfiguration tiene la clave anidada logConfiguration securityGroupIds subnetIds , <i>required for successful restore</i>
Amazon FSx para NetApp ONTAP	name se establece en un valor aleatorio que empieza por awsbackup_restore_test_ ontapConfiguration tiene claves anidadas, incluidas: • junctionPath donde /name es el nombre del volumen que se está restaurando • sizeInMegabytes , cuyo valor se establece en el tamaño en megabytes del punto de recuperación que se está restaurando • snapshotPolicy cuyo se establece en none	ontapConfiguration tiene claves anidadas anulables específicas, incluidas: • junctionPath • ontapVolumeType • securityStyle • sizeInMegabytes • storageEfficiencyEnabled • storageVirtualMachineId , <i>required for successful restore</i> • tieringPolicy

Tipo de recurso	Claves y valores de metadatos de restauración inferidos	Metadatos anulables
Amazon FSx para OpenZFS	<code>openZfsConfiguration</code> , que tiene claves anidadas, incluidas: • <code>automaticBackupRetentionDays</code> con valor establecido en 0 • <code>deploymentType</code> con un valor establecido en el tipo de implementación del punto de recuperación que se está restaurando • <code>throughputCapacity</code> , cuyo valor se basa en el <code>deploymentType</code> . Si <code>deploymentType</code> es <code>SINGLE_AZ_1</code> , el valor se establece en 64; si <code>deploymentType</code> es <code>SINGLE_AZ_2</code> or <code>MULTI_AZ_1</code> , el valor se establece en 160	<code>kmsKeyId</code> <code>openZfsConfiguration</code> tiene claves anidadas anulables específicas, incluidas: • <code>deploymentType</code> • <code>throughputCapacity</code> • <code>diskIopsConfiguration</code> <code>securityGroupIds</code> <code>subnetIds</code>

Tipo de recurso	Claves y valores de metadatos de restauración inferidos	Metadatos anulables
Servidor FSx de archivos Amazon para Windows	<code>windowsConfiguration</code> , que tiene claves anidadas, incluidas: • <code>automaticBackupRetentionDays</code> con valor establecido en 0 • <code>deploymentType</code> con un valor establecido en el tipo de implementación del punto de recuperación que se está restaurando • <code>throughputCapacity</code> con valor establecido en 8	<code>kmsKeyId</code> <code>securityGroupIds</code> <code>subnetIds</code> <i>required for successful restore</i> <code>windowsConfiguration</code> , con claves anidadas anulables específicas • <code>throughputCapacity</code> • <code>activeDirectoryId</code> <i>required for successful restore</i> • <code>preferredSubnetId</code>

Tipo de recurso	Claves y valores de metadatos de restauración inferidos	Metadatos anulables
Clústeres de Amazon RDS, Aurora, Amazon DocumentDB y Amazon Neptune	<code>availabilityZones</code> con un valor establecido en una lista de hasta tres zonas de disponibilidad aleatorias <code>dbClusterIdentifier</code> con un valor aleatorio que empieza por <code>awsbackup-restore-test</code> <code>engine</code> con un valor establecido en el motor del punto de recuperación que se está restaurando	<code>availabilityZones</code> <code>databaseName</code> <code>dbClusterParameterGroupName</code> <code>dbSubnetGroupName</code> <code>enableCloudwatchLogsExports</code> <code>enableIamDatabaseAuthentication</code> <code>engine</code> <code>engineMode</code> <code>engineVersion</code> <code>kmskeyId</code> <code>port</code> <code>optionGroupName</code> <code>scalingConfiguration</code> <code>vpcSecurityGroupIds</code>

Tipo de recurso	Claves y valores de metadatos de restauración inferidos	Metadatos anulables
Instancias de Amazon RDS	<code>dbInstanceIdentifier</code> con un valor aleatorio que empieza por <code>awsbackup-restore-test-</code> <code>deletionProtection</code> con valor establecido en <code>false</code> <code>multiAz</code> con valor establecido en <code>false</code> <code>publiclyAccessible</code> con un valor establecido en <code>false</code>	<code>allocatedStorage</code> <code>availabilityZones</code> <code>dbInstanceClass</code> <code>dbName</code> <code>dbParameterGroupName</code> <code>dbSubnetGroupName</code> <code>domain</code> <code>domainIamRoleName</code> <code>enableCloudwatchLogsExports</code> <code>enableIamDatabaseAuthentication</code> <code>iops</code> <code>licensemodel</code> <code>multiAz</code> <code>optionGroupName</code> <code>port</code> <code>processorFeatures</code> <code>publiclyAccessible</code> <code>storageType</code> <code>vpcSecurityGroupIds</code>

Tipo de recurso	Claves y valores de metadatos de restauración inferidos	Metadatos anulables
Amazon Simple Storage Service (Amazon S3)	<code>destinationBucketName</code> con un valor aleatorio que empieza por <code>awsbackup-</code> <code>-restore-test-</code> <code>encrypted</code> con valor establecido en <code>true</code> <code>encryptionType</code> con valor establecido en <code>SSE-S3</code> <code>newBucket</code> con valor establecido en <code>true</code>	<code>encryptionType</code> <code>kmsKey</code>

Restaurar la validación de las pruebas

Tiene la opción de crear una validación basada en eventos que se ejecute cuando se complete un trabajo de prueba de restauración.

En primer lugar, crea un flujo de trabajo de validación con cualquier objetivo compatible con Amazon EventBridge, como AWS Lambda. En segundo lugar, añade una EventBridge regla que se encargue de que el trabajo de restauración alcance el estado `COMPLETED`. En tercer lugar, cree un plan de pruebas de restauración (o deje que uno existente se ejecute según lo programado). Por último, una vez finalizada la prueba de restauración, supervise los registros del flujo de trabajo de validación para asegurarse de que se ha ejecutado según lo esperado (una vez ejecutada la validación, aparecerá el estado de la validación en la [consola de AWS Backup](#)).

1. Configuración del flujo de trabajo de validación

Puede configurar un flujo de trabajo de validación mediante Lambda o cualquier otro objetivo compatible con EventBridge. Por ejemplo, si estás validando una prueba de restauración que contiene una EC2 instancia de Amazon, puedes incluir un código que haga ping a un punto final de comprobación de estado.

Puede usar los detalles del evento para determinar qué recursos validar.

Puede usar [capas de Lambda](#) para usar el SDK más reciente (ya que no `PutRestoreValidationResult` está disponible en el SDK de Lambda).

Este es un ejemplo:

```
import { Backup } from "@aws-sdk/client-backup";

export const handler = async (event) => {
  console.log("Handling event: ", event);

  const restoreTestingPlanArn = event.detail.restoreTestingPlanArn;
  const resourceType = event.detail.resourceType;
  const createdResourceArn = event.detail.createdResourceArn;

  // TODO: Validate the resource

  const backup = new Backup();
  const response = await backup.putRestoreValidationResult({
    RestoreJobId: event.detail.restoreJobId,
    ValidationStatus: "SUCCESSFUL", // TODO
    ValidationStatusMessage: "" // TODO
  });

  console.log("PutRestoreValidationResult: ", response);
  console.log("Finished");
};
```

2. Agrega una regla EventBridge

[Cree una EventBridge regla](#) que escuche el [COMPLETEDevento](#) de restauración del trabajo.

Si lo desea, puede filtrar los eventos por tipo de recurso o restaurar el ARN del plan de pruebas. Establezca el objetivo de esta regla para invocar el flujo de trabajo de validación que definió en el Paso 1. A continuación se muestra un ejemplo:

```
{
  "source": [
    "aws.backup"
  ],
  "detail-type": [
    "Restore Job State Change"
  ],
```

```
"detail":{
  "resourceType":[
    "...",
  ],
  "restoreTestingPlanArn":[
    "...",
  ],
  "status":[
    "COMPLETED"
  ]
}
```

3. Dejar que el plan de restauración se ejecute y complete

El plan de pruebas de restauración se ejecutará de acuerdo con la programación que haya configurado.

Consulte [Create a restore testing plan](#) si aún no tiene uno o [Update a restore testing plan](#) si desea cambiar la configuración.

4. Monitorear los resultados

Una vez que el plan de pruebas de restauración se haya ejecutado según lo programado, puede comprobar los registros de su flujo de trabajo de validación para asegurarse de que se ha ejecutado correctamente.

Puede llamar a la API `PutRestoreValidationResult` para publicar los resultados, que luego se podrán ver en la [AWS Backup consola](#) y mediante llamadas a la AWS Backup API que describen y enumeran los trabajos de restauración, como `DescribeRestoreJob` o `ListRestoreJob`.

Una vez establecido un estado de validación, no se puede cambiar.

Detener un trabajo de copia de seguridad

Puede detener un trabajo de copia de seguridad una AWS Backup vez iniciado. Al hacerlo, la copia de seguridad no se crea y el registro del trabajo de copia de seguridad se conserva con el estado `aborted` (anulado).

Para detener un trabajo de copia de seguridad mediante la AWS Backup consola

1. Inicie sesión en y abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
[Consola de administración de AWS](#)
2. En el panel de navegación de la izquierda, elija Jobs (Trabajos).
3. Elija el trabajo de copia de seguridad que desea detener.
4. En el panel de detalles del trabajo de copia de seguridad, elija Stop (Detener).

Visualizar copias de seguridad existentes

Puede ver una lista de sus copias de seguridad mediante la [consola de AWS Backup](#) o mediante programación.

Temas

- [Listado de copias de seguridad por recurso protegido en la consola](#)
- [Listado de copias de seguridad por almacén de copias de seguridad en la consola](#)
- [Listado de copias de seguridad mediante programación](#)

Listado de copias de seguridad por recurso protegido en la consola

Siga estos pasos para ver una lista de las copias de seguridad de un recurso concreto en la consola de AWS Backup .

1. Inicie sesión en y abra la Consola de administración de AWS AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, elija Protected resources (Recursos protegidos).
3. Elija un recurso protegido en la lista para ver la lista de copias de seguridad. Solo los recursos de los que se ha realizado una copia de seguridad AWS Backup se muestran en Recursos protegidos.

Puede ver las copias de seguridad para el recurso. Desde esta vista, también puede elegir una copia de seguridad y restaurarla.

Listado de copias de seguridad por almacén de copias de seguridad en la consola

Siga estos pasos para ver una lista de copias de seguridad organizadas en un almacén de copias de seguridad.

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, elija Backup vaults (Almacenes de copia de seguridad).
3. En la sección Backups (Copias de seguridad), vea la lista de todas las copias de seguridad organizadas en este almacén de copias de seguridad. En esta vista, puede ordenar las copias de seguridad por cualquiera de los encabezados de las columnas (incluido el estado), así como seleccionar una copia de seguridad para restaurarla, editarla o eliminarla.

Listado de copias de seguridad mediante programación

Puede enumerar las copias de seguridad mediante programación mediante las operaciones de la API `ListRecoveryPoint`:

- [ListRecoveryPointsByBackupVault](#)
- [ListRecoveryPointsByResource](#)

Por ejemplo, el siguiente comando AWS Command Line Interface (AWS CLI) muestra todas las copias de seguridad con el EXPIRED estado:

```
aws backup list-recovery-points-by-backup-vault \  
  --backup-vault-name sample-vault \  
  --query 'RecoveryPoints[?Status == `EXPIRED`]'
```

AWS Backup Audit Manager

Puede usar AWS Backup Audit Manager para auditar el cumplimiento de sus AWS Backup políticas con respecto a los controles que defina. Un control es un procedimiento diseñado para auditar la conformidad de un requisito de copia de seguridad, como la frecuencia de la copia de seguridad o el periodo de retención de la copia de seguridad.

AWS Backup Audit Manager le ayuda a responder preguntas como:

- “¿Estoy haciendo copias de seguridad de todos mis recursos?”
- “¿Están cifradas todas mis copias de seguridad?”
- “¿Mis copias de seguridad se realizan a diario?”

Puede utilizar AWS Backup Audit Manager para encontrar la actividad y los recursos de respaldo que aún no cumplen con los controles que ha definido. Tenga en cuenta que solo se incluirán los recursos activos cuando los controles evalúen la conformidad de los recursos. Por ejemplo, se evaluará una EC2 instancia de Amazon en estado de ejecución. Una EC2 instancia detenida no se incluirá en la evaluación de conformidad.

También puede usarlo para generar automáticamente un seguimiento de auditoría de informes diarios y bajo demanda para fines de control de copia de seguridad.

Los siguientes pasos proporcionan una descripción general de cómo utilizar AWS Backup Audit Manager. Para ver tutoriales detallados, elija uno de los temas al final de esta página.

1. Cree marcos que contengan una o más plantillas de control de gobernanza. Las preguntas anteriores son ejemplos de tres plantillas de control de gobernanza. Puede personalizar los parámetros de algunas plantillas de control de gobernanza. Por ejemplo, puede personalizar el último control para que pregunte: “¿Mis copias de seguridad se realizan semanalmente?” en lugar de a diario.
2. Consulte su marco para ver cuántos de sus recursos cumplen (o no) con los controles que definió en ese marco.
3. Cree informes sobre su estado de copia de seguridad y conformidad. Guarde estos informes como evidencia fehaciente de sus prácticas de conformidad o para identificar las actividades y los recursos de copia de seguridad individuales que aún no cumplen con las normas.

AWS Backup Audit Manager genera automáticamente un nuevo informe cada 24 horas y lo publica en Amazon S3. También puede generar informes bajo demanda.

Note

Antes de crear su primer marco relacionado con la conformidad, debe activar el seguimiento de los recursos. De este modo, podrá AWS Config realizar un seguimiento de sus AWS Backup recursos. Para obtener documentación técnica sobre cómo gestionar el seguimiento de los recursos, consulte [Configuración AWS Config con la consola](#) en la Guía para AWS Config desarrolladores.

Al activar el seguimiento de los recursos, se aplican cargos. Para obtener información sobre el seguimiento de los recursos, los precios y la facturación de AWS Backup Audit Manager, consulte [Medición, costes y facturación](#).

Temas

- [Uso de marcos de auditoría](#)
- [Uso de informes de auditoría](#)
- [Uso de AWS Backup Audit Manager con CloudFormation](#)
- [Uso de AWS Backup Audit Manager con AWS Audit Manager](#)
- [Controles y corrección](#)

Uso de marcos de auditoría

Un marco es un conjunto de controles que le ayuda a evaluar sus prácticas de copia de seguridad. Puede utilizar controles personalizables y prediseñados para definir sus políticas y evaluar si sus prácticas de copia de seguridad cumplen con sus políticas. También puede configurar informes diarios automáticos para obtener información sobre el estado de conformidad de sus marcos.

Cada marco se aplica a una sola cuenta y Región de AWS. Puede implementar un máximo de 15 marcos por cuenta y región. No puede implementar marcos duplicados (marcos que contengan los mismos controles y parámetros).

Hay dos tipos diferentes de marcos:

- El marco de AWS Backup (recomendado): utilice el marco de AWS Backup para implementar todos los controles disponibles a fin de monitorizar la actividad, la cobertura y los recursos de copia de seguridad según las prácticas recomendadas.
- Un marco personalizado que usted defina: utilice un marco personalizado para elegir uno o más controles específicos y personalizar los parámetros de control.

Temas

- [Elección de controles](#)
- [Activación del seguimiento de recursos](#)
- [Creación de marcos mediante la consola de AWS Backup](#)
- [Creación de marcos mediante la AWS Backup API](#)
- [Visualización del estado de conformidad del marco](#)
- [Búsqueda de recursos no conformes](#)
- [Actualización de los marcos de auditoría](#)
- [Eliminación de los marcos de auditoría](#)

Elección de controles

En la siguiente tabla se enumeran los controles de AWS Backup Audit Manager, sus parámetros personalizables y sus tipos de recursos de AWS Config registro.

Controles disponibles

Nombre del control	Descripción del control	Parámetros personalizables	AWS Config tipo de recurso de registro
Los recursos de copia de seguridad están incluidos en al menos un plan de copia de seguridad	Evalúa si los recursos de copia de seguridad están incluidos en al menos un plan de copia de seguridad.	Ninguno	AWS Backup: backup selection
El plan de copia de seguridad tiene	Evalúa si la frecuencia de las copias de seguridad es de al	Frecuencia de copia de seguridad; periodo de retención	AWS Backup: backup plans

Nombre del control	Descripción del control	Parámetros personalizables	AWS Config tipo de recurso de registro
frecuencia mínima y retención	menos [1 día] y el periodo de retención es de al menos [35 días].		
Los almacenes impiden la eliminación manual de los puntos de recuperación	Evalúa si las bóvedas de respaldo no permiten la eliminación manual de los puntos de recuperación, excepto para determinadas funciones AWS Identity and Access Management (IAM). De forma predeterminada, no hay excepciones a los roles de IAM. Tampoco hay excepciones a las funciones de IAM cuando se implementa este control con el marco. AWS Backup	Hasta 5 roles de IAM que permiten la eliminación manual de los puntos de recuperación	AWS Backup: backup vaults
Los puntos de recuperación están cifrados	Evalúa si los puntos de recuperación están cifrados.	Ninguno	AWS Backup: recovery points
Se ha establecido una retención mínima para el punto de recuperación	Evalúa si el periodo de retención del punto de recuperación es de al menos [35 días].	Periodo de retención del punto de recuperación	AWS Backup: recovery points

Nombre del control	Descripción del control	Parámetros personalizables	AWS Config tipo de recurso de registro
Se ha programado una copia de la copia de seguridad entre regiones	Evalúa si un recurso está configurado para crear copias de sus copias de seguridad en otra Región de AWS.	Región de AWS	AWS Backup: backup selection
Se ha programado una copia de la copia de seguridad entre cuentas	Evalúa si un recurso tiene configurada una copia de la copia de la copia de seguridad entre cuentas.	AWS ID de cuenta	AWS Backup: backup selection
Los recursos están en un plan de respaldo con un AWS Backup Vault Lock	Evalúa si un recurso tiene un plan de copias de seguridad configurado para que se almacenen copias de seguridad en un almacén de copias de seguridad bloqueado.	Días de retención mínimos; días de retención máximos	AWS Backup: backup selection
Se creó el último punto de recuperación	Evalúa si se creó un punto de recuperación dentro del periodo de tiempo especificado.	Valor en horas [1 a 744] o días [1 a 31].	AWS Backup recovery points
El tiempo de restauración de los recursos cumple el objetivo	Evalúa si el trabajo de pruebas de restauración se completó dentro del tiempo de restauración objetivo	Valor en minutos	Ninguno

Nombre del control	Descripción del control	Parámetros personalizables	AWS Config tipo de recurso de registro
Los recursos están en un almacén aislado lógicamente	Evalúa si los recursos tienen al menos un punto de recuperación copiado en un almacén aislado lógicamente dentro del valor y el plazo especificados.	Valor en minutos, horas o días	AWS Backup: recovery points

Para obtener información detallada sobre estos controles, consulte [Controles y corrección](#).

Para obtener una lista AWS Backup de los recursos compatibles que no admiten todos los controles, consulte la sección AWS Backup Audit Manager de la [Disponibilidad de características por recurso](#) tabla.

Note

Si no desea utilizar ninguno de los controles anteriores, puede seguir utilizando AWS Backup Audit Manager para crear informes diarios de sus trabajos de copia de seguridad, copia y restauración. Consulte [Uso de informes de auditoría](#).

Activación del seguimiento de recursos

Antes de crear su primer marco relacionado con la conformidad, debe activar el seguimiento de los recursos. De este modo, podrá AWS Config realizar un seguimiento de sus AWS Backup recursos. Para obtener documentación técnica sobre cómo gestionar el seguimiento de los recursos, consulte [Configuración AWS Config con la consola](#) en la Guía para AWS Config desarrolladores.

Al activar el seguimiento de los recursos, se aplican cargos. Para obtener información sobre el seguimiento de los recursos, los precios y la facturación de AWS Backup Audit Manager, consulte [Medición, costes y facturación](#).

Temas

- [Activación del seguimiento de recursos mediante la consola](#)

- [Activación del seguimiento de recursos mediante la AWS Command Line Interface \(AWS CLI\)](#)
- [Activación del seguimiento de recursos mediante una plantilla de CloudFormation](#)

Activación del seguimiento de recursos mediante la consola

Active el seguimiento de recursos mediante la consola:

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación izquierdo, en Audit Manager, elija Marcos.
3. Para activar el seguimiento de recursos, seleccione Administrar el seguimiento de recursos.
4. Seleccione Ir a la AWS Config configuración.
5. Elija Habilitar o deshabilitar el registro.
6. Elija Habilitar el registro para todos los tipos de recursos siguientes o elija habilitar el registro para algunos tipos de recursos. Consulte [Controles y correcciones de AWS Backup Audit Manager](#) para ver qué tipos de recursos se requieren para sus controles.
 - AWS Backup: backup plans
 - AWS Backup: backup vaults
 - AWS Backup: recovery points
 - AWS Backup: backup selection
7. Seleccione Cerrar.
8. Espere a que el banner azul con el texto Activando el seguimiento de recursos pase al banner verde con el texto El seguimiento de recursos está activado.

Puedes comprobar si has activado el seguimiento de recursos y, de ser así, qué tipos de recursos estás grabando, en dos lugares de la AWS Backup consola. En el panel de navegación izquierdo:

- Elija Marcos y, a continuación, elija el texto en estado de registro de AWS Config .
- Elija Configuración y, a continuación, elija el texto en estado de registro de AWS Config .

Activación del seguimiento de recursos mediante la AWS Command Line Interface (AWS CLI)

Si aún no lo has incorporado AWS Config, puede que sea más rápido hacerlo con el. AWS CLI

Para activar el seguimiento de recursos mediante la AWS CLI:

1. Escriba el siguiente comando para determinar si ya ha habilitado el registro de AWS Config .

```
$ aws configservice describe-configuration-records
```

- a. Si la lista `ConfigurationRecorders` está vacía de esta manera:

```
{
  "ConfigurationRecorders": []
}
```

El registro no está habilitado. Continúe con el paso 2 para crear el registro.

- b. Si ya ha habilitado el registro para todos los recursos, el resultado `ConfigurationRecorders` tendrá el siguiente aspecto:

```
{
  "ConfigurationRecorders": [
    {
      "recordingGroup": {
        "allSupported": true,
        "resourceTypes": [

        ],
        "includeGlobalResourceTypes": true
      },
      "roleARN": "arn:aws:iam::[account]:role/[roleName]",
      "name": "default"
    }
  ]
}
```

Dado que ha habilitado todos los recursos, ya ha activado el seguimiento de recursos. No necesita completar el resto de este procedimiento para utilizar AWS Backup Audit Manager.

2. Cree una AWS Config grabadora con los tipos de recursos de AWS Backup Audit Manager

```
$ aws configservice put-configuration-recorder --configuration-recorder
name=default, \
roleARN=arn:aws:iam::accountId:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig \
```

```
--recording-group
resourceTypes=["AWS::Backup::BackupPlan','AWS::Backup::BackupSelection', \
'AWS::Backup::BackupVault','AWS::Backup::RecoveryPoint']"
```

3. Describa su AWS Config grabadora.

```
$ aws configservice describe-configuration-recorders
```

Compruebe que tiene los tipos de recursos de AWS Backup Audit Manager comparando el resultado con el siguiente resultado esperado.

```
{
  "ConfigurationRecorders":[
    {
      "name":"default",
      "roleARN":"arn:aws:iam::accountId:role/AWSServiceRoleForConfig",
      "recordingGroup":{
        "allSupported":false,
        "includeGlobalResourceTypes":false,
        "resourceTypes":[
          "AWS::Backup::BackupPlan",
          "AWS::Backup::BackupSelection",
          "AWS::Backup::BackupVault",
          "AWS::Backup::RecoveryPoint"
        ]
      }
    }
  ]
}
```

4. Cree un bucket de Amazon S3 como destino para almacenar los archivos AWS Config de configuración.

```
$ aws s3api create-bucket --bucket amzn-s3-demo-bucket --region us-east-1
```

5. *policy.json* Utilícelo para conceder AWS Config permiso de acceso a su bucket. Consulte el siguiente ejemplo *policy.json*.

```
$ aws s3api put-bucket-policy --bucket amzn-s3-demo-bucket --policy file://
policy.json
```

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
    },
    {
      "Sid": "AWSConfigBucketExistenceCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
    },
    {
      "Sid": "AWSConfigBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    }
  ]
}
```

6. Configure su depósito como canal AWS Config de entrega

```
$ aws configservice put-delivery-channel --delivery-channel
name=default,s3BucketName=amzn-s3-demo-bucket
```

7. Habilita la AWS Config grabación

```
$ aws configservice start-configuration-recorder --configuration-recorder-name default
```

8. Verifique que "FrameworkStatus":"ACTIVE" en la última línea de su resultado de DescribeFramework es como sigue.

```
$ aws backup describe-framework --framework-name test --region us-east-1
```

```
{
  "FrameworkName":"test",
  "FrameworkArn":"arn:aws:backup:us-east-1:accountId:framework:test-f0001b0a-0000-1111-ad3d-4444f5cc6666",
  "FrameworkDescription":"",
  "FrameworkControls":[
    {
      "ControlName":"BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK",
      "ControlInputParameters":[
        {
          "ParameterName":"requiredRetentionDays",
          "ParameterValue":"1"
        }
      ],
      "ControlScope":{
      }
    },
    {
      "ControlName":"BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK",
      "ControlInputParameters":[
        {
          "ParameterName":"requiredFrequencyUnit",
          "ParameterValue":"hours"
        },
        {
          "ParameterName":"requiredRetentionDays",
          "ParameterValue":"35"
        },
        {
          "ParameterName":"requiredFrequencyValue",
          "ParameterValue":"1"
        }
      ]
    }
  ]
}
```



```
    ],
    "ControlScope":{

    }
  },
  {
    "ControlName":"BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN",
    "ControlInputParameters":[

    ],
    "ControlScope":{

    }
  },
  {
    "ControlName":"BACKUP_RECOVERY_POINT_ENCRYPTED",
    "ControlInputParameters":[

    ],
    "ControlScope":{

    }
  },
  {
    "ControlName":"BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED",
    "ControlInputParameters":[

    ],
    "ControlScope":{

    }
  }
],
"CreationTime":1633463605.233,
"DeploymentStatus":"COMPLETED",
"FrameworkStatus":"ACTIVE"
}
```

Activación del seguimiento de recursos mediante una plantilla de CloudFormation

Para ver una CloudFormation plantilla que active el seguimiento de recursos, consulte [Uso de AWS Backup Audit Manager con CloudFormation](#).

Creación de marcos mediante la consola de AWS Backup

Tras activar el seguimiento de recursos, cree un marco mediante los siguientes pasos.

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación izquierdo, elija Marcos.
3. Elija Crear marco.
4. En Nombre del marco, introduzca un nombre exclusivo. El nombre del marco debe contener entre 1 y 256 caracteres, comenzando por una letra, y contar con letras (a-z, A-Z), números (0-9) y guiones bajos (_).
5. De forma opcional, puede introducir una Descripción del marco.
6. En Controles, se mostrarán los controles activos. De forma predeterminada, se muestran todos los controles aptos para un recurso.

Para cambiar los controles que están activos, haga clic en Editar controles.

- a. La primera casilla de verificación indica si el control está activado. Para desactivar un control, quite la marca de la casilla.
- b. En Elegir recursos para evaluar, puede seleccionar cómo elegir los recursos, ya sea por tipo, por etiquetas o por un único recurso.

La lista de [controles de AWS Backup Audit Manager](#) describe las opciones de personalización de cada control.

7. De forma opcional, puede agregar el marco seleccionando Añadir nueva etiqueta. Puede utilizar etiquetas para buscar y filtrar los marcos o hacer un seguimiento de los costos.
8. Elija Crear marco.

AWS Backup Audit Manager puede tardar varios minutos en crear el marco.

Si se produce el error `AlreadyExists`, ya existe un marco con los mismos controles y parámetros. Para crear correctamente un nuevo marco, al menos un control o parámetro debe ser diferente de los marcos existentes.

Creación de marcos mediante la AWS Backup API

La siguiente tabla contiene ejemplos de solicitudes de API [CreateFramework](#) para cada control, junto con ejemplos de respuestas de API a las solicitudes [DescribeFramework](#) correspondientes. Para trabajar con AWS Backup Audit Manager mediante programación, puede consultar estos fragmentos de código.

Controlar	Solicitud de CreateFramework	Respuesta de DescribeFramework
Backup resources are included in at least one backup plan	<pre>{ "FrameworkName": "Control1", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN", "ControlInputParameters": [], "ControlScope": { "ComplianceResourceTypes": ["RDS"] // Evaluate only RDS instances } }], "IdempotencyToken": "Control1", "FrameworkTags": { "key1": "foo" } }</pre>	<pre>{ "FrameworkName": "Control1", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control1-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN", "ControlInputParameters": [], "ControlScope": { "ComplianceResourceTypes": ["RDS"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", }</pre>

Controlar	Solicitud de CreateFramework	Respuesta de DescribeFramework
		<pre>"FrameworkStatus": "Completed", "IdempotencyToken": "Control1", "FrameworkTags": {"key1": "foo"} }</pre>

Controlar	Solicitud de CreateFramework	Respuesta de DescribeFramework
Backup plan minimum frequency and minimum retention	<pre> {"FrameworkName": "Control2", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_PLAN_MIN_F REQUENCY_AND_MIN_R ETENTION_CHECK", "ControlInputParam eters": [{"Paramet erName": "required RetentionDays", "Paramete rValue": "35"}, {"Paramet erName": "required FrequencyUnit", "Paramete rValue": "hours"}, {"Paramet erName": "required FrequencyValue", "Paramete rValue": "24"}], "ControlScope": { "Tags": {"key1": "prod"} // Evaluate backup plans that tagged with "key1": "prod". } }], </pre>	<pre> {"FrameworkName": "Control2", "FrameworkArn": "arn:aws:backup:us -east-1:1234567890 12:framework/Contr ol2-de7655ae-1e31- 45cb-96a0-4f43d8c1 969d", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_PLAN_MIN_F REQUENCY_AND_MIN_R ETENTION_CHECK", "ControlInputParam eters": [{"Paramet erName": "required RetentionDays", "Paramete rValue": "35"}, {"Paramet erName": "required FrequencyUnit", "Paramete rValue": "hours"}, {"Paramet erName": "required FrequencyValue", "Paramete rValue": "24"}], "ControlScope": { </pre>

Controlar	Solicitud de CreateFramework	Respuesta de DescribeFramework
	<pre>"IdempotencyToken": "Control2", "FrameworkTags": {"key1": "foo"} }</pre>	<pre> "Tags": {"key1": "prod"} }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control2", "FrameworkTags": {"key1": "foo"} }</pre>

Controlar	Solicitud de CreateFramework	Respuesta de DescribeFramework
Vaults prevent manual deletion of recovery points	<pre>{ "FrameworkName": "Control3", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED", "ControlInputParameters": [{ "ParameterName": "principalArnList", "ParameterValue": "arn:aws:iam::123456789012:role/application_abc/component_xyz/RDSEAccess", "arn:aws:iam::123456789012:role/aws-service-role/access-analyzer.amazonaws.com/AWSServiceRoleForAccessAnalyzer", "arn:aws:iam::123456789012:role/service-role/QuickSightAction" }], "ControlScope": { "ComplianceResourceIds": ["default"] } }] }</pre>	<pre>{ "FrameworkName": "Control3", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control2-de7655ae-1e31-45cb-96a0-4f43d8c1969d", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED", "ControlInputParameters": [{ "ParameterName": "principalArnList", "ParameterValue": "arn:aws:iam::123456789012:role/application_abc/component_xyz/RDSEAccess", "arn:aws:iam::123456789012:role/aws-service-role/access-analyzer.amazonaws.com/AWSServiceRoleForAccessAnalyzer", "arn:aws:iam::123456789012:role/service-role/QuickSightAction" }] }] }</pre>

Controlar	Solicitud de CreateFramework	Respuesta de DescribeFramework
	<pre>"ComplianceResourceTypes": ["AWS::Backup::BackupVault"] }], "IdempotencyToken": "Control3", "FrameworkTags": {"key1": "foo"} }</pre>	<pre>role/service-role/QuickSightAction"}], "ControlScope": {"ComplianceResourceIds":["default"], "ComplianceResourceTypes": ["AWS::Backup::BackupVault"] }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control3", "FrameworkTags": {"key1": "foo"} }</pre>

Controlar	Solicitud de CreateFramework	Respuesta de DescribeFramework
Minimum retention established for recovery point	<pre>{ "FrameworkName": "Control4", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK", "ControlInputParameters": [{ "ParameterName": "requiredRetentionDays", "ParameterValue": "35" }], "ControlScope": {} // Default scope (no scope input) sets scope to all recovery points. }], "IdempotencyToken": "Control4", "FrameworkTags": { "key1": "foo" } }</pre>	<pre>{ "FrameworkName": "Control4", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control6-6e7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK", "ControlInputParameters": [{ "ParameterName": "requiredRetentionDays", "ParameterValue": "35" }], "ControlScope": {} }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control4", "FrameworkTags": {} }</pre>

Controlar	Solicitud de CreateFramework	Respuesta de DescribeFramework
		<pre>{ "key1": "foo" }</pre>

Backup recovery points are encrypted

```
{
  "FrameworkName": "Control5",
  "FrameworkDescription": "This is a test framework",
  "FrameworkControls": [
    {
      "ControlName": "BACKUP_RECOVERY_POINT_ENCRYPTED",
      "ControlInputParameters": [],
      "ControlScope": {} // Default scope (no scope input) is all recovery points
    }
  ],
  "IdempotencyToken": "Control5",
  "FrameworkTags": {
    "key1": "foo"
  }
}
```

```
{
  "FrameworkName": "Control5",
  "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control7-7e7655ae-1e31-45cb-96a0-4f43d8c19642",
  "FrameworkDescription": "This is a test framework",
  "FrameworkControls": [
    {
      "ControlName": "BACKUP_RECOVERY_POINT_ENCRYPTED",
      "ControlInputParameters": [],
      "ControlScope": {}
    }
  ],
  "CreationTime": 1516925490,
  "DeploymentStatus": "Active",
  "FrameworkStatus": "Completed",
  "IdempotencyToken": "Control5",
  "FrameworkTags": {
    "key1": "foo"
  }
}
```

Controlar	Solicitud de CreateFramework	Respuesta de DescribeFramework
Cross-Region backup copy is scheduled	<pre>{ "FrameworkName": "Control6", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_REGION", "ControlInputParameters": [], "ControlScope": { "ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control6", "FrameworkTags": { "key1": "foo" } }</pre>	<pre>{ "FrameworkName": "Control6", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control6-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_REGION", "ControlInputParameters": [], "ControlScope": { "ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control6", "FrameworkTags": { "key1": "foo" } }</pre>

Controlar	Solicitud de CreateFramework	Respuesta de DescribeFramework
Cross-account backup copy is scheduled	<pre>{ "FrameworkName": "Control7", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_ACCOUNT", "ControlInputParameters": [], "ControlScope": { "ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control7", "FrameworkTags": { "key1": "foo" } }</pre>	<pre>{ "FrameworkName": "Control7", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control7-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_ACCOUNT", "ControlInputParameters": [], "ControlScope": { "ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control7", "FrameworkTags": { "key1": "foo" } }</pre>

Controlar	Solicitud de CreateFramework	Respuesta de DescribeFramework
Resources are in a backup plan with an AWS Backup Vault Lock	<pre>{ "FrameworkName": "Control8", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_VAULT_LOCK", "ControlInputParameters": [], "ControlScope": { "ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control8", "FrameworkTags": { "key1": "foo" } }</pre>	<pre>{ "FrameworkName": "Control8", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control8-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_VAULT_LOCK", "ControlInputParameters": [], "ControlScope": { "ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control8", "FrameworkTags": { "key1": "foo" } }</pre>

Controlar	Solicitud de CreateFramework	Respuesta de DescribeFramework
Last recovery point was created	<pre>{ "FrameworkName": "Control9", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_LAST_RECOVERY_POINT_CREATED", "ControlInputParameters": [], "ControlScope": { "ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control9", "FrameworkTags": { "key1": "foo" } }</pre>	<pre>{ "FrameworkName": "Control9", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control9-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_LAST_RECOVERY_POINT_CREATED", "ControlInputParameters": [], "ControlScope": { "ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control9", "FrameworkTags": { "key1": "foo" } }</pre>

Controlar	Solicitud de CreateFramework	Respuesta de DescribeFramework
Restore time for resources meet target	<pre>{ "FrameworkName": "Control10", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "RESTORE_TIME_FOR_RESOURCES_MEET_TARGET", "ControlInputParameters": [{ "ParameterName": "maxRestoreTime", "ParameterValue": "720" }], "ControlScope": { "ComplianceResourceIds": ["ComplianceResourceTypes": ["DynamoDB"] }], "IdempotencyToken": "Control10", "FrameworkTags": { "key1": "foo" } }] }</pre>	<pre>{ "FrameworkName": "Control10", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control10-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "RESTORE_TIME_FOR_RESOURCES_MEET_TARGET", "ControlInputParameters": [], "ControlScope": { "ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control10", "FrameworkTags": { "key1": "foo" } }</pre>

Controlar	Solicitud de CreateFramework	Respuesta de DescribeFramework
	}	

Controlar	Solicitud de CreateFramework	Respuesta de DescribeFramework
RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT	<pre>{ "FrameworkName": "Control11", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT", "ControlInputParameters": [{ "ParameterName": "recoveryPointAgeValue", "ParameterValue": "10" }, { "ParameterName": "recoveryPointAgeUnit", "ParameterValue": "days" }], "ControlScope": { "ComplianceResourceTypes": ["EC2"] } }], "IdempotencyToken": "Control11", "FrameworkTags": {</pre>	<pre>{ "FrameworkName": "Control11", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control11-ab1234cd-5e67-89fg-06a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "", "ControlInputParameters": [], "ControlScope": { "ComplianceResourceTypes": ["EC2", "EBS"] } }], "CreationTime": 1726087776.316, "DeploymentStatus": "COMPLETED", "FrameworkStatus": "ACTIVE", "IdempotencyToken": "Control11", "FrameworkTags": { "key1": "foo" } }</pre>

Controlar	Solicitud de CreateFramework	Respuesta de DescribeFramework
	<pre> { "key1": "foo" } </pre>	

Visualización del estado de conformidad del marco

Una vez que haya creado un marco de auditoría, aparecerá en la tabla Marcos. Para ver esta tabla, seleccione Frameworks en el panel de navegación izquierdo de la AWS Backup consola. Para ver los resultados de la auditoría de su marco, elija el Nombre del marco. Al hacerlo, accederá a la página de Detalles del marco, que tiene dos secciones: Resumen y Controles.

La sección Resumen muestra los siguientes estados de izquierda a derecha:

- El estado de conformidad es el estado de conformidad general de su marco de auditoría, determinado por el estado de conformidad de cada uno de sus controles. El estado de conformidad de cada control viene determinado por el estado de conformidad de cada recurso que evalúa.

El estado de conformidad del marco es **Compliant** únicamente si todos los recursos incluidos en el ámbito de sus evaluaciones de control han superado dichas evaluaciones. Si uno o más recursos no superaron una evaluación de control, el estado de conformidad será **Non-Compliant**. Para obtener información sobre cómo encontrar los recursos no conformes, consulte [Búsqueda de recursos no conformes](#). Para obtener información sobre cómo conseguir la conformidad de sus recursos, consulte la sección de corrección de [Controles y correcciones de AWS Backup Audit Manager](#).

- El estado del marco se refiere a si ha activado el seguimiento de recursos para todos sus recursos. Los posibles estados son:
 - **Active** cuando el registro está activado para todos los recursos que el marco evalúa.
 - **Partially active** cuando el registro está desactivado para al menos un recurso que el marco evalúa.
 - **Inactive** cuando el registro está desactivado para todos los recursos que el marco evalúa.
 - **Unavailable** cuando AWS Backup Audit Manager no puede validar el estado de la grabación en este momento.

Para corregir un estado **Inactive** o **Partially active**

1. En el panel de navegación izquierdo, elija Marcos.
2. Elija Administrar el seguimiento de recursos.
3. Siga las instrucciones de la ventana emergente para habilitar el registro que antes no estaba habilitado para sus tipos de recursos.

Para obtener más información sobre los tipos de recursos que requieren un seguimiento de los recursos en función de los controles que haya incluido en sus marcos, consulte el componente de recursos de [Controles y correcciones de AWS Backup Audit Manager](#).

- El estado de implementación hace referencia al estado de implementación de su marco. Este estado suele ser Completed, pero también puede ser Create in progress Update in progress, Delete in progress y Failed.
 - Un estado Failed significa que el marco no se implementó correctamente. [Elimine el marco](#) y, a continuación, vuelva a crearlo mediante la [consola de AWS Backup](#) o la [API de AWS Backup](#).
- Los controles conformes muestran un recuento de los controles del marco con todas las evaluaciones aprobadas.
- Los controles no conformes muestran un recuento de los controles del marco con al menos una evaluación no aprobada.

La sección Controles muestra la siguiente información:

- El estado de control se refiere al estado de conformidad de cada control. Un control puede ser Compliant, lo que significa que todos los recursos superan esa evaluación; Non-compliant, lo que significa que al menos un recurso no supera esa evaluación, o Insufficient data, lo que significa que el control no ha encontrado ningún recurso que evaluar dentro del ámbito de la evaluación.
- El ámbito de la evaluación puede limitar cada control a uno o más Tipos de recursos, un ID de recurso o una Clave de etiqueta y un Valor de etiqueta, en función de la forma en que haya personalizado el control al crear el marco de auditoría. Si todos los campos están vacíos (lo que se muestra mediante un guion, "-"), el control evalúa todos los recursos aplicables.

Búsqueda de recursos no conformes

AWS Backup Audit Manager le ayuda a encontrar los recursos que no cumplen con las normas de dos maneras.

- En [Visualización del estado de conformidad del marco](#), elija el nombre del control en la Sección de detalles. Al hacerlo, accederá a la AWS Config consola, donde podrá ver una lista de sus Non-Compliant recursos.
- Después de [Crear un plan de informes con la plantilla de conformidad del recurso](#) que incluye el marco, puede [Ver el informe](#) para identificar todos los recursos Non-Compliant en todos los controles.

Además, Resource compliance report muestra la última vez que AWS Backup Audit Manager evaluó cada uno de sus controles por última vez.

Actualización de los marcos de auditoría

Puede actualizar la descripción, los controles y los parámetros de un marco de auditoría existente.

Para actualizar un marco existente

1. En el panel de navegación izquierdo de la AWS Backup consola, elija Frameworks.
2. Elija el marco que desee editar por el Nombre del marco.
3. Seleccione Editar.

Eliminación de los marcos de auditoría

Para eliminar un marco existente

1. En el panel de navegación izquierdo de la AWS Backup consola, elija Frameworks.
2. Elija el marco que desee eliminar por el Nombre del marco.
3. Elija Eliminar.
4. Escriba el nombre del marco y elija Eliminar el marco.

Uso de informes de auditoría

AWS Backup Los informes de Audit Manager se generan automáticamente como evidencia de su AWS Backup actividad, como:

- Qué trabajos de copia de seguridad finalizaron y cuándo
- De qué recursos hizo una copia de seguridad

Existen dos tipos de informes. Al crear un informe, elige el tipo que se va a crear.

Uno de ellos es el informe de trabajos, que muestra los trabajos finalizados en las últimas 24 horas y todos los trabajos activos con un contexto completo sobre las propiedades del almacén, las configuraciones del plan de copia de seguridad y los ajustes del ciclo de vida. Los informes de trabajos no muestran un estado de `completed with issues`. Para encontrar este estado, puede filtrar los `Completed` trabajos con uno o más mensajes de estado. AWS Backup solo incluirá un mensaje de estado como parte del estado de un `Completed` trabajo si el mensaje requiere atención o acción.

El segundo tipo de informe es un informe de conformidad. Los informes de conformidad pueden monitorizar los niveles de recursos o los diferentes controles vigentes.

AWS Backup Audit Manager envía un informe diario a su bucket de Amazon S3. Si el informe es para la región actual y la cuenta actual, puede elegir recibirlo en formato CSV o JSON. De lo contrario, el informe está disponible en formato CSV. La duración del informe diario puede fluctuar durante varias horas porque AWS Backup Audit Manager realiza una aleatorización para mantener su rendimiento. También puede ejecutar un informe bajo demanda en cualquier momento.

Todos los titulares de cuentas pueden crear informes entre regiones; los titulares de cuentas de administración y de [administrador delegado](#) también pueden crear informes entre cuentas.

Tip

Para garantizar que los informes generados por las cuentas de administrador delegado muestren todos los datos de las cuentas de miembro, [cree marcos](#) en cada una de esas cuentas de miembros.

Contexto del informe de trabajo mejorado

AWS Backup Los informes de trabajo de Audit Manager ahora incluyen un contexto ampliado para ayudar a los clientes a comprender mejor las operaciones de respaldo, especialmente para la supervisión de las cuentas de administradores delegados en todas las organizaciones.

Los informes mejorados ahora incluyen:

- Información del almacén: tipo de almacén, estado de bloqueo y detalles de cifrado
- Contexto del plan de copia de seguridad: nombres de planes, nombres de reglas, programaciones y zonas horarias
- Configuración del ciclo de vida: períodos de retención y configuración de la transferencia al almacenamiento en frío
- Detalles del recurso: nombres de los recursos y metadatos de trabajo mejorados

Este contexto ampliado elimina la necesidad de realizar más llamadas a la API y `DescribeBackupVault`, `DescribeBackupPlan`, además `DescribeRecoveryPoint`, proporciona información completa sobre el trabajo en un solo informe.

Note

El contexto ampliado proporciona información que anteriormente requería llamadas a la API independientes con permisos adicionales. Asegúrese de que los usuarios con acceso a estos informes tengan los permisos adecuados para la información mejorada que se proporciona.

Puede tener un máximo de 20 planes de informes por cada uno Cuenta de AWS.

Note

Los recursos como RDS que no tienen la capacidad de mostrar los bytes incrementales de datos de una copia de seguridad específica mostrarán el valor `backupSizeInBytes` como 0.

Para permitir que AWS Backup Audit Manager cree informes diarios o bajo demanda, primero debe crear un plan de informes a partir de una plantilla de informe.

Temas

- [Elección de la plantilla de informe](#)
- [Creación de planes de informes mediante la consola de AWS Backup](#)
- [Crear planes de informes mediante la API AWS Backup](#)
- [Creación de informes bajo demanda](#)
- [Visualización de los informes de auditoría](#)
- [Actualización de los planes de informes](#)
- [Eliminación de los planes de informes](#)

Elección de la plantilla de informe

Una plantilla de informe define la información que su plan de informes incluye en el informe. Cuando automatiza sus informes mediante un plan de informes, AWS Backup Audit Manager le proporciona los informes de las 24 horas anteriores. AWS Backup Audit Manager crea estos informes entre la 1 y las 5 a.m. UTC. Ofrece las siguientes plantillas de informes.

Plantillas de informes de copia de seguridad

Plantillas de informes de copia de seguridad. Estas plantillas le proporcionan actualizaciones diarias sobre sus trabajos de copia de seguridad, restauración o copia con un contexto mejorado, que incluye propiedades del almacén, detalles del plan de copia de seguridad y configuración del ciclo de vida. Puede utilizar estos informes para supervisar su estado operativo, comprender las configuraciones de copia de seguridad e identificar cualquier error que pueda requerir la adopción de medidas adicionales. La tabla siguiente enumera el nombre de cada plantilla de informe de copia de seguridad y su resultado de muestra.

Plantilla de informe de copia de seguridad	Informe de muestra en formato JSON
BACKUP_JOB_REPORT	<pre>{ "reportItems": [{ "reportTimePeriodStart": "2021-07-14T00:00:00Z", "reportTimePeriodEnd": "2021-07-15T00:00:00Z", "accountId": "112233445566", "region": "us-west-2",</pre>

Plantilla de informe de copia de seguridad	Informe de muestra en formato JSON
	<pre> "backupJobId": "FCCB040A -9426-2A49-2EA9-5EAFFAC656AC", "jobStatus": "COMPLETED", "resourceType": "EC2", "resourceArn": "arn:aws:ec2:us- west-2:112233445566:instance/ i-0bc877aee7782ba75", "resourceName": "MyEC2Ins tance", "backupPlanArn": "arn:aws: backup:us-west-2:1122334455 66:backup-plan:349f2247-b48 9-4301-83ac-4b7dd724db9a", "backupRuleId": "ab88bbf8- ff4e-4f1b-92e7-e13d3e65dcfb", "initiationDate": "2021-07- 14T23:53:47.229Z", "backupPlanName": "MyBackup Plan", "backupRuleName": "DailyBac kups", "backupRuleSchedule": "cron(0 5 ? * * *)", "backupRuleTimezone": "UTC", "startWindowEnd": "2021-07- 14T23:53:47.229Z", "backupOptions": {}, "isParentJob": false, "parentJobId": null, "creationDate": "2021-07- 14T23:53:47.229Z", "completionDate": "2021-07- 15T00:16:07.282Z", "recoveryPointArn": "arn:aws: ec2:us-west-2::image/ami-03 0cafb98e5a6dcdf", "jobRunTime": "00:22:20", "backupSizeInBytes": 858993459 2, "backupVaultName": "Default", </pre>

Plantilla de informe de copia de seguridad	Informe de muestra en formato JSON
	<pre data-bbox="849 212 1422 957">{ "backupVaultArn": "arn:aws: backup:us-west-2:1122334455 66:backup-vault:Default", "vaultType": "BACKUP_VAULT", "vaultLockStatus": "UNLOCKED", "isEncrypted": true, "encryptionKeyArn": "arn:aws: kms:us-west-2:112233445566: key/12345678-1234-1234-1234 -123456789012", "deleteAfterDays": 30, "moveToColdAfterDays": 7, "enableArchive": false, "iamRoleArn": "arn:aws: iam::112233445566:role/service- role/AWSBackupDefaultServiceRole" }</pre>

Plantilla de informe de copia de seguridad	Informe de muestra en formato JSON
COPY_JOB_REPORT	<pre> { "reportItems": [{ "reportTimePeriodStart": "2021-07-14T15:48:31Z", "reportTimePeriodEnd": "2021-07-15T15:48:31Z", "accountId": "112233445566", "region": "us-west-2", "copyJobId": "E0AD48A9-0560-B66 8-3EF0-941FDC0AD6B1", "jobStatus": "RUNNING", "jobRunTime": "2021-07- 16T00:00:00.010Z", "resourceType": "EC2", "resourceArn": "arn:aws:ec2:us- west-2:112233445566:instance/ i-0bc877aee7782ba75", "resourceName": "string", "initiationDate": "2021-07- 14T15:48:31Z", "backupPlanName": "string", "backupRuleName": "string", "backupRuleSchedule": "string", "backupRuleTimezone": "string", "startWindowEnd": "2021-07- 14T15:48:31Z", "backupOptions": {}, "isParentJob": false, "parentJobId": null, "creationDate": "2021-07- 15T15:42:04.771Z", "completionDate": "2021-07- 16T00:16:07.282Z", "backupSizeInBytes": 858993459 2, "sourceRecoveryPointArn": "arn:aws:ec2:us-west-2::image/ ami-007b3819f25697299", </pre>

Plantilla de informe de copia de seguridad	Informe de muestra en formato JSON
	<pre>"sourceBackupVaultArn": "arn:aws:backup:us-west-2:1 12233445566:backup-vault:Default", "destinationRecoveryPointAr n": "arn:aws:ec2:us-east-2::image/ ami-0eba2199a0bcece3c", "destinationBackupVaultArn" : "arn:aws:backup:us-east-2:1 12233445566:backup-vault:Default", "vaultType": "BACKUP_VAULT", "vaultLockStatus": "string", "isEncrypted": true, "encryptionKeyArn": "arn:aws: kms:us-west-2:112233445566: key/...", "deleteAfterDays": 30, "moveToColdAfterDays": 7, "enableArchive": false, "iamRoleArn": "arn:aws: iam::112233445566:role/service- role/AWSBackupDefaultServiceRole" }] }</pre>

Plantilla de informe de copia de seguridad

Informe de muestra en formato JSON

RESTORE_JOB_REPORT

```
{
  "reportItems": [
    {
      "reportTimePeriod": "2021-07-14T15:53:30Z - 2021-07-15T15:53:30Z",
      "accountId": "112233445566",
      "region": "us-west-2",
      "restoreJobId": "4CACA67D-4E12-DC05-6C2B-0E97D01FA41E",
      "jobStatus": "RUNNING",
      "recoveryPointArn": "arn:aws:ec2:us-west-2::image/ami-00201ecb57a5271ae",
      "resourceName": "string",
      "initiationDate": "2021-07-14T15:53:30Z",
      "backupPlanName": "string",
      "backupRuleName": "string",
      "backupRuleSchedule": "string",
      "backupRuleTimezone": "string",
      "startWindowEnd": "2021-07-14T15:53:30Z",
      "backupOptions": {},
      "isParentJob": false,
      "parentJobId": null,
      "vaultType": "BACKUP_VAULT",
      "vaultLockStatus": "string",
      "isEncrypted": true,
      "encryptionKeyArn": "arn:aws:kms:us-west-2:112233445566:key/...",
      "deleteAfterDays": 30,
      "moveToColdAfterDays": 7,
      "enableArchive": false,
      "sourceResourceArn": "arn:aws:ec2:us-west-2:112233445566:instance/i-0bc877aee7782ba75",
    }
  ]
}
```

Plantilla de informe de copia de seguridad	Informe de muestra en formato JSON
	<pre> "backupVaultArn": "arn:aws: backup:us-west-2:1122334455 66:backup-vault:Default", "creationDate": "2021-07- 15T15:52:49.797Z", "backupSizeInBytes": 858993459 2, "percentDone": "0.00%", "iamRoleArn": "arn:aws: iam::112233445566:role/service- role/AWSBackupDefaultServiceRole" }] }</pre>

Plantillas de informes de conformidad

Las plantillas de informes de conformidad le proporcionan informes diarios sobre la conformidad de su actividad y sus recursos de copia de seguridad con respecto a los controles que haya definido en uno o más marcos. Si el estado de conformidad de uno de sus marcos es Non-compliant, revise un informe de conformidad para identificar los recursos no conformes.

Tipos de Plantillas de informes de conformidad

- `Control compliance report` le ayuda a realizar un seguimiento del estado de conformidad de los controles que ha definido en sus marcos.
- `Resource compliance report` le ayuda a realizar un seguimiento del estado de conformidad de sus recursos con respecto a los controles que ha definido en sus marcos. Estos informes incluyen resultados de evaluación detallados, incluida información de identificación sobre los recursos no conformes que puede utilizar para identificar y corregir esos recursos.

La siguiente tabla muestra resultados de ejemplo de un informe de conformidad.

Plantilla de informe de conformidad	Informe de muestra en formato JSON
CONTROL_COMPLIANCE_REPORT	<pre>{</pre>

Plantilla de informe de conformidad	Informe de muestra en formato JSON
	<pre> "reportItems": [{ "accountId": "112233445566", "region": "me-south-1", "frameworkName": "TestFramework7", "frameworkDescription": "A test framework", "controlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN", "controlComplianceStatus": "NON_COMPLIANT", "lastEvaluationTime": "2021-08-17T03:21:56.002Z", "numResourcesCompliant": 91, "numResourcesNonCompliant": 205, "controlFrequency": "Twelve_Hours", "controlScope": "", "controlParameters": "" }, { "accountId": "112233445566", "region": "me-south-1", "frameworkName": "TestFramework7", "frameworkDescription": "A test framework", "controlName": "BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK", "controlComplianceStatus": "NON_COMPLIANT", "lastEvaluationTime": "2021-08-17T03:21:19.995Z", "numResourcesCompliant": 0, "numResourcesNonCompliant": 25, "controlScope": "{ComplianceResourceTypes: [],}", "controlParameters": "{\\requiredFrequencyValue\\":\\\"1\\\",\\ </pre>

Plantilla de informe de conformidad	Informe de muestra en formato JSON
	<pre>"requiredRetentionDays\":"35", "requiredFrequencyUnit\":"hours" }</pre>

Plantilla de informe de conformidad	Informe de muestra en formato JSON
RESOURCE_COMPLIANCE_REPORT	<pre> { "reportItems": [{ "accountId": "112233445566", "region": "us-west-2", "frameworkName": "MyTestFramework", "frameworkDescription": "", "controlName": "BACKUP_L AST_RECOVERY_POINT_CREATED", "resourceId": "AWS::EFS ::FileSystem/fs-63c74e66", "resourceType": "AWS::EFS ::FileSystem", "resourceComplianceStatus": "NON_COMPLIANT", "lastEvaluationTime": "2021-07- 07T18:55:40.963Z" }, { "accountId": "112233445566", "region": "us-west-2", "frameworkName": "MyTestFramework", "frameworkDescription": "", "controlName": "BACKUP_L AST_RECOVERY_POINT_CREATED", "resourceId": "AWS::EFS ::FileSystem/fs-b3d7c218", "resourceType": "AWS::EFS ::FileSystem", "resourceComplianceStatus": "NON_COMPLIANT", "lastEvaluationTime": "2021-07- 07T18:55:40.961Z" }] } </pre>

Escaneando plantillas de informes

Escaneo de plantillas de informes. Estas plantillas le proporcionan actualizaciones diarias sobre sus trabajos de digitalización con un contexto más amplio, que incluye las propiedades del almacén y los detalles del plan de respaldo. Puede utilizar estos informes para supervisar el estado y los informes de sus trabajos de digitalización e identificar cualquier fallo que pueda requerir la adopción de medidas adicionales. En la siguiente tabla se muestra el nombre de una plantilla de informe de digitalización y su resultado de muestra.

Plantilla de informe de digitalización	Informe de muestra en formato JSON
MALWARE_JOB_REPORT	<pre>{ "reportTimePeriodStart": "2025-11-09T00:00:00Z", "reportTimePeriodEnd": "2025-11-10T00:00:00Z", "accountId": "025066259999", "region": "us-east-1", "scanJobId": "489abba3-0a57-4207-93ff-d3947d85a8d3", "scanId": "9ddd3144f68ea3ee6e388c66a0b55467", "malwareScanner": "GUARDDUTY", "jobStatus": "RUNNING", "scanResultStatus": "", "statusMessage": "", "resourceType": "EBS", "resourceArn": "arn:aws:ec2:us-east-1:025066259999:volume/vol-0f1c480a6a9b33cb7", "backupPlanArn": "arn:aws:backup:us-east-1:025066259999:backup-plan:orgs/4232272a-ed54-3a88-b1d0-ace894b6c24c", "creationDate": "2025-10-28T17:30:50.820Z", "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-03fef858bad24c7a6", "backupVaultName": "Default",</pre>

Plantilla de informe de digitalización	Informe de muestra en formato JSON
	<pre> "backupVaultArn": "arn:aws: backup:us-east-1:0250662599 99:backup-vault:Default", "iamRoleArn": "arn:aws:iam::0250 66259999:role/service-role/ AWSBackupDefaultServiceRole", "scannerRoleArn": "arn:aws: iam::025066259999:role/AWSB ackupGuardDutyRolePolicyForScans" } </pre>

Creación de planes de informes mediante la consola de AWS Backup

Existen dos tipos de informes. Uno de ellos es el informe de trabajos, que muestra los trabajos finalizados en las últimas 24 horas y todos los trabajos activos. El segundo tipo de informe es un informe de conformidad. Los informes de conformidad pueden monitorizar los niveles de recursos o los diferentes controles vigentes. Al crear un informe, elige el tipo de informe que se va a crear.

Según el tipo de cuenta, la pantalla de la consola puede variar. Solo las cuentas de administración tendrán la funcionalidad de varias cuentas.

Al igual que en un plan de copia de seguridad, usted crea un plan de informes para automatizar la creación de sus informes y definir su bucket de Amazon S3 de destino. Un plan de informes requiere tener un bucket de S3 que reciba los informes. No puede usar un bucket de otra cuenta. Para obtener instrucciones sobre cómo configurar un nuevo bucket de S3, consulte el [Paso 1: Crear su primer bucket de S3](#) en la Guía del usuario de Amazon Simple Storage Service.

Para crear su plan de informes en la AWS Backup consola

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación izquierdo, elija Informes.
3. Elija Crear plan de informe.
4. Elija una de las plantillas de informes de la lista.

5. Introduzca un Nombre del plan de informe único. El nombre debe contener entre 1 y 256 caracteres, comenzando por una letra, y contar con letras (a-z, A-Z), números (0-9) y guiones bajos (_).
6. De forma opcional, puede introducir una Descripción del plan de informe.
7. Plantillas de informes de conformidad para una sola cuenta. Elija uno o más marcos sobre los que informar. Puede agregar un máximo de 1000 marcos a un plan de informes.
 1. Elige tu AWS región.
 2. Elija un marco de esa región.
 3. Elija Agregar marco.
8. De forma opcional, para agregar etiquetas a su plan de informes, elija Agregar etiquetas al plan de informe.
9. Si utiliza una cuenta de administración, puede especificar qué cuentas desea incluir en este plan de informes. Puede seleccionar Solo mi cuenta, que generará informes solo sobre la cuenta en la que ha iniciado sesión actualmente. O bien, puede seleccionar Una o varias cuentas de mi organización (solo disponible para las cuentas de administración).
10. (Si va a crear un informe de conformidad para una sola región, omita este paso). Puede elegir las regiones que desea incluir en el informe. Haga clic en el menú desplegable para ver las regiones a su disposición. Seleccione Todas las regiones disponibles o las regiones que prefiera.
 - La casilla Incluir regiones nuevas cuando se incorporen a Backup Audit Manager activará la inclusión de nuevas regiones en sus informes cuando estén disponibles.
11. Elija el Formato del archivo de su informe. Todos los informes se pueden exportar en formato CSV. Además, los informes para una sola región se pueden exportar en formato JSON.
12. En Nombre del bucket de S3, elija un bucket de su cuenta.
13. De forma opcional, puede introducir un prefijo del bucket.

AWS Backup entrega su cuenta corriente, a la que informa la región actual `s3://amzn-s3-demo-bucket/prefix/Backup/accountID/Region/year/month/day/report-name`.

AWS Backup entrega sus informes multicuentas a `s3://amzn-s3-demo-bucket/prefix/Backup/crossaccount/Region/year/month/day/report-name`

AWS Backup entrega sus informes interregionales a `s3://amzn-s3-demo-bucket/prefix/Backup/accountID/crossregion/year/month/day/report-name`

14. Elija Crear plan de informe.

A continuación, debe permitir que su bucket de S3 reciba informes desde AWS Backup. Tras crear un plan de informes, AWS Backup Audit Manager genera automáticamente una política de acceso al bucket de S3 para que la aplique.

Si cifra su bucket con una clave de KMS administrada por el cliente, la política de claves de KMS debe cumplir los siguientes requisitos:

- El atributo `Principal` debe incluir el ARN [AWSServiceRolePolicyForBackupReports](#) del rol vinculado al servicio Backup Audit Manager.
- El atributo `Action` debe incluir `kms:GenerateDataKey` y `kms:Decrypt` como mínimo.

La política [AWSServiceRolePolicyForBackupReports](#) tiene estos permisos.

Para ver y aplicar esta política de acceso a su bucket de S3

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación izquierdo, elija Informes.
3. En Nombre del plan de informe, elija el nombre de un plan para seleccionarlo.
4. Seleccione Editar.
5. Elija Ver política de acceso para el bucket de S3. Puede usar también la política al final de este procedimiento.
6. Elija Copiar permisos.
7. Elija Editar política del bucket. Tenga en cuenta que, hasta que no se cree el informe de copia de seguridad por primera vez, el rol vinculado al servicio al que se hace referencia en la política de bucket de S3 aún no existirá, lo que generará el error "Entidad principal no válida".
8. Copie los permisos a la Política.

Ejemplo de política de bucket

JSON

```
{
```

```

"Version":"2012-10-17",
"Statement":[
  {
    "Effect":"Allow",
    "Principal":{"
      "AWS":"arn:aws:iam::123456789012:role/aws-service-role/
reports.backup.amazonaws.com/AWSServiceRoleForBackupReports"
    },
    "Action":"s3:PutObject",
    "Resource":[
      "arn:aws:s3:::BucketName/*"
    ],
    "Condition":{"
      "StringEquals":{"
        "s3:x-amz-acl":"bucket-owner-full-control"
      }
    }
  }
]
}

```

Si utiliza una opción personalizada AWS Key Management Service para cifrar el bucket de S3 de destino que almacena los informes, incluya las siguientes acciones en su política:

```

"Action":[
  "kms:GenerateDataKey",
  "kms:Encrypt"
],
"Resource":[
  "*"
],

```

Crear planes de informes mediante la API AWS Backup

También puede trabajar con los planes de informes mediante programación.

Existen dos tipos de informes. Uno de ellos es el informe de trabajos, que muestra los trabajos finalizados en las últimas 24 horas y todos los trabajos activos. El segundo tipo de informe es un informe de conformidad. Los informes de conformidad pueden monitorizar los niveles de recursos o los diferentes controles vigentes. Al crear un informe, elige el tipo de informe que se va a crear.

Al igual que en un plan de copia de seguridad, usted crea un plan de informes para automatizar la creación de sus informes y definir su bucket de Amazon S3 de destino. Un plan de informes requiere tener un bucket de S3 que reciba los informes. Para obtener instrucciones sobre cómo configurar un nuevo bucket de S3, consulte el [Paso 1: Crear su primer bucket de S3](#) en la Guía del usuario de Amazon Simple Storage Service.

Si cifra su bucket con una clave de KMS personalizada, la política de claves de KMS debe cumplir los siguientes requisitos:

- El atributo `Principal` debe incluir el ARN [AWSServiceRolePolicyForBackupReports](#) del rol vinculado al servicio Backup Audit Manager.
- El atributo `Action` debe incluir `kms:GenerateDataKey` y `kms:Decrypt` como mínimo.

La política [AWSServiceRolePolicyForBackupReports](#) tiene estos permisos.

Para los informes de una sola cuenta y una sola región, utilice la siguiente sintaxis para llamar a [CreateReportPlan](#).

```
{
  "ReportPlanName": "string",
  "ReportPlanDescription": "string",
  "ReportSetting": {
    "ReportTemplate": enum, // Can be RESOURCE_COMPLIANCE_REPORT,
CONTROL_COMPLIANCE_REPORT, BACKUP_JOB_REPORT, COPY_JOB_REPORT, or RESTORE_JOB_REPORT.
Only include "ReportCoverageList" if your report is a COMPLIANCE_REPORT.
    "ReportDeliveryChannel": {
      "S3BucketName": "string",
      "S3KeyPrefix": "string",
      "Formats": [ enum ] // Optional. Can be either CSV, JSON, or both. Default is
CSV if left blank.
    },
    "ReportPlanTags": {
      "string" : "string" // Optional.
    },
    "IdempotencyToken": "string"
  }
}
```

Cuando llame a [DescribeReportPlan](#) con el nombre exclusivo de un plan de informes, la API de AWS Backup responde con la siguiente información.

```
{
  "ReportPlanArn": "string",
  "ReportPlanName": "string",
  "ReportPlanDescription": "string",
  "ReportSetting": {
    "ReportTemplate": enum,
  },
  "ReportDeliveryChannel": {
    "S3BucketName": "string",
    "S3KeyPrefix": "string",
    "Formats": [ enum ]
  },
  "DeploymentStatus": enum
  "CreationTime": timestamp,
  "LastAttemptExecutionTime": timestamp,
  "LastSuccessfulExecutionTime": timestamp
}
```

Para los informes de varias cuentas y varias regiones, utilice la siguiente sintaxis para llamar a [CreateReportPlan](#).

```
{
  "IdempotencyToken": "string",
  "ReportDeliveryChannel": {
    "Formats": [ "string" ], *//Organization report only support CSV file*
    "S3BucketName": "string",
    "S3KeyPrefix": "string"
  },
  "ReportPlanDescription": "string",
  "ReportPlanName": "string",
  "ReportPlanTags": {
    "string" : "string"
  },
  "ReportSetting": {
    "Accounts": [ "string" ], // Use string value of "R00T" to include all
organizational units
    "OrganizationUnits": [ "string" ],
    "Regions": [ "string" ], // Use wildcard value in string to include all Regions
    "FrameworkArns": [ "string" ],
    "NumberOfFrameworks": number,
    "ReportTemplate": "string"
  }
}
```

```
}
```

Cuando llame a [DescribeReportPlan](#) con el nombre exclusivo de un plan de informes, la API de AWS Backup responde con la siguiente información para varias cuentas y varias regiones:

```
{
  "ReportPlan": {
    "CreationTime": number,
    "DeploymentStatus": "string",
    "LastAttemptedExecutionTime": number,
    "LastSuccessfulExecutionTime": number,
    "ReportDeliveryChannel": {
      "Formats": [ "string" ],
      "S3BucketName": "string",
      "S3KeyPrefix": "string"
    },
    "ReportPlanArn": "string",
    "ReportPlanDescription": "string",
    "ReportPlanName": "string",
    "ReportSetting": {
      "Accounts": [ "string" ],
      "OrganizationUnits": [ "string" ],
      "Regions": [ "string" ],
      "FrameworkArns": [ "string" ],
      "NumberOfFrameworks": number,
      "ReportTemplate": "string"
    }
  }
}
```

Creación de informes bajo demanda

Puede generar nuevos informes cuando lo desee creando un informe bajo demanda siguiendo los siguientes pasos. AWS Backup Audit Manager envía su informe bajo demanda al bucket de Amazon S3 que especificó en su plan de informes.

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación izquierdo, elija Informes.
3. En Nombre del plan de informe, elija el nombre de un plan para seleccionarlo.
4. Elija Crear informe en diferido.

Puede generar un informe bajo demanda para un plan de informes existente.

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación izquierdo, elija Informes.
3. En Planes de informes, haga clic en el botón de opción situado junto al nombre del plan para seleccionarlo.
4. Haga clic en Acciones y, a continuación, en Crear informe en diferido.

Puede hacer esto para varios informes, incluso mientras se generan los informes.

Visualización de los informes de auditoría

Puede abrir, ver y analizar los informes de AWS Backup Audit Manager mediante los programas que suele utilizar para trabajar con archivos CSV o JSON. Tenga en cuenta que los informes de varias regiones o cuentas solo están disponibles en formato CSV.

Los archivos grandes se dividen en varios informes si el tamaño total del archivo supera los 50 MB. Si los archivos resultantes pesan más de 50 MB, AWS Backup Audit Manager creará archivos CSV adicionales con el resto del informe.

Para ver un informe

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación izquierdo, elija Informes.
3. En Nombre del plan de informe, elija el nombre de un plan para seleccionarlo.
4. En Trabajos de informe, haga clic en el enlace del informe para verlo.
5. Si el Estado del informe tiene un subrayado punteado, selecciónelo para obtener información sobre el informe.
6. Elija qué informe desea ver según su Hora de finalización.
7. Elija el enlace de S3. Esto abre el bucket de S3 de destino.
8. En Nombre, elija el nombre del informe que desea ver.
9. Puede guardar el informe en su equipo, elija Descargar.

Actualización de los planes de informes

Puede actualizar la descripción, el destino de entrega y el formato de un plan de informes existente. Si procede, también puede agregar o eliminar marcos del plan de informes.

Para actualizar un plan de informes existente

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación izquierdo, elija Informes.
3. En Nombre del plan de informe, elija el nombre de un plan para seleccionarlo.
4. Seleccione Editar.
5. Puede editar los detalles del plan del informe, incluidos el nombre y la descripción del informe, así como las cuentas y regiones que se incluyen en el informe.

Eliminación de los planes de informes

Puede eliminar un plan de informes existente. Cuando elimine un plan de informes, todos los informes que ya haya creado dicho plan permanecerán en su bucket de Amazon S3 de destino.

Para eliminar un plan de informes existente

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación izquierdo, elija Informes.
3. En Nombre del plan de informe, elija el nombre de un plan para seleccionarlo.
4. Elija Eliminar.
5. Introduzca el nombre del plan de informes y, a continuación, elija Eliminar el plan de informe.

Uso de AWS Backup Audit Manager con CloudFormation

Proporcionamos las siguientes CloudFormation plantillas de muestra para su consulta:

Temas

- [Activación del seguimiento de recursos](#)
- [Implementación de controles predeterminados](#)
- [Exención de roles de IAM de la evaluación de control](#)

- [Creación de un plan de informes](#)

Activación del seguimiento de recursos

La siguiente plantilla activa el seguimiento de recursos, tal y como se describe en [Activación del seguimiento de recursos](#).

```
AWSTemplateFormatVersion: 2010-09-09
Description: Enable AWS Config

Metadata:
  AWS::CloudFormation::Interface:
    ParameterGroups:
      - Label:
          default: Recorder Configuration
        Parameters:
          - AllSupported
          - IncludeGlobalResourceTypes
          - ResourceTypes
      - Label:
          default: Delivery Channel Configuration
        Parameters:
          - DeliveryChannelName
          - Frequency
      - Label:
          default: Delivery Notifications
        Parameters:
          - TopicArn
          - NotificationEmail
    ParameterLabels:
      AllSupported:
        default: Support all resource types
      IncludeGlobalResourceTypes:
        default: Include global resource types
      ResourceTypes:
        default: List of resource types if not all supported
      DeliveryChannelName:
        default: Configuration delivery channel name
      Frequency:
        default: Snapshot delivery frequency
      TopicArn:
        default: SNS topic name
```

NotificationEmail:

default: Notification Email (optional)

Parameters:

AllSupported:

Type: String

Default: True

Description: Indicates whether to record all supported resource types.

AllowedValues:

- True
- False

IncludeGlobalResourceTypes:

Type: String

Default: True

Description: Indicates whether AWS Config records all supported global resource types.

AllowedValues:

- True
- False

ResourceTypes:

Type: List<String>

Description: A list of valid AWS resource types to include in this recording group, such as AWS::EC2::Instance or AWS::CloudTrail::Trail.

Default: <All>

DeliveryChannelName:

Type: String

Default: <Generated>

Description: The name of the delivery channel.

Frequency:

Type: String

Default: 24hours

Description: The frequency with which AWS Config delivers configuration snapshots.

AllowedValues:

- 1hour
- 3hours
- 6hours
- 12hours
- 24hours

TopicArn:

Type: String

Default: <New Topic>

Description: The Amazon Resource Name (ARN) of the Amazon Simple Notification Service (Amazon SNS) topic that AWS Config delivers notifications to.

NotificationEmail:

Type: String

Default: <None>

Description: Email address for AWS Config notifications (for new topics).

Conditions:

IsAllSupported: !Equals

- !Ref AllSupported
- True

IsGeneratedDeliveryChannelName: !Equals

- !Ref DeliveryChannelName
- <Generated>

CreateTopic: !Equals

- !Ref TopicArn
- <New Topic>

CreateSubscription: !And

- !Condition CreateTopic
- !Not
 - !Equals
 - !Ref NotificationEmail
 - <None>

Mappings:

Settings:

FrequencyMap:

1hour : One_Hour
3hours : Three_Hours
6hours : Six_Hours
12hours : Twelve_Hours
24hours : TwentyFour_Hours

Resources:

ConfigBucket:

DeletionPolicy: Retain

Type: AWS::S3::Bucket

Properties:

BucketEncryption:

ServerSideEncryptionConfiguration:

- ServerSideEncryptionByDefault:
 - SSEAlgorithm: AES256

ConfigBucketPolicy:

Type: AWS::S3::BucketPolicy

Properties:

Bucket: !Ref ConfigBucket

PolicyDocument:

Version: 2012-10-17

Statement:

- Sid: AWSConfigBucketPermissionsCheck
 - Effect: Allow
 - Principal:
 - Service:
 - config.amazonaws.com
 - Action: s3:GetBucketAcl
 - Resource:
 - !Sub "arn:\${AWS::Partition}:s3:::\${ConfigBucket}"
- Sid: AWSConfigBucketDelivery
 - Effect: Allow
 - Principal:
 - Service:
 - config.amazonaws.com
 - Action: s3:PutObject
 - Resource:
 - !Sub "arn:\${AWS::Partition}:s3:::\${ConfigBucket}/AWSLogs/\${AWS::AccountId}/*"
- Sid: AWSConfigBucketSecureTransport
 - Action:
 - s3:*
 - Effect: Deny
 - Resource:
 - !Sub "arn:\${AWS::Partition}:s3:::\${ConfigBucket}"
 - !Sub "arn:\${AWS::Partition}:s3:::\${ConfigBucket}/*"
 - Principal: "*"
 - Condition:
 - Bool:
 - aws:SecureTransport:
 - false

ConfigTopic:

Condition: CreateTopic

Type: AWS::SNS::Topic

Properties:

```
TopicName: !Sub "config-topic-${AWS::AccountId}"
DisplayName: AWS Config Notification Topic
KmsMasterKeyId: "alias/aws/sns"
```

ConfigTopicPolicy:

```
Condition: CreateTopic
Type: AWS::SNS::TopicPolicy
Properties:
  Topics:
    - !Ref ConfigTopic
  PolicyDocument:
    Statement:
      - Sid: AWSConfigSNSPolicy
        Action:
          - sns:Publish
        Effect: Allow
        Resource: !Ref ConfigTopic
        Principal:
          Service:
            - config.amazonaws.com
```

EmailNotification:

```
Condition: CreateSubscription
Type: AWS::SNS::Subscription
Properties:
  Endpoint: !Ref NotificationEmail
  Protocol: email
  TopicArn: !Ref ConfigTopic
```

ConfigRecorderServiceRole:

```
Type: AWS::IAM::ServiceLinkedRole
Properties:
  AWSServiceName: config.amazonaws.com
  Description: Service Role for AWS Config
```

ConfigRecorder:

```
Type: AWS::Config::ConfigurationRecorder
DependsOn:
  - ConfigBucketPolicy
  - ConfigRecorderServiceRole
Properties:
  RoleARN: !Sub arn:${AWS::Partition}:iam::${AWS::AccountId}:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig
RecordingGroup:
```

```

    AllSupported: !Ref AllSupported
    IncludeGlobalResourceTypes: !Ref IncludeGlobalResourceTypes
    ResourceTypes: !If
      - IsAllSupported
      - !Ref AWS::NoValue
      - !Ref ResourceTypes

ConfigDeliveryChannel:
  Type: AWS::Config::DeliveryChannel
  DependsOn:
    - ConfigBucketPolicy
  Properties:
    Name: !If
      - IsGeneratedDeliveryChannelName
      - !Ref AWS::NoValue
      - !Ref DeliveryChannelName
    ConfigSnapshotDeliveryProperties:
      DeliveryFrequency: !FindInMap
        - Settings
        - FrequencyMap
        - !Ref Frequency
    S3BucketName: !Ref ConfigBucket
    SnsTopicARN: !If
      - CreateTopic
      - !Ref ConfigTopic
      - !Ref TopicArn

```

Implementación de controles predeterminados

La siguiente plantilla crea un marco con los controles predeterminados descritos en [Controles y correcciones de AWS Backup](#).

```

AWSTemplateFormatVersion: '2010-09-09'
Resources:
  TestFramework:
    Type: AWS::Backup::Framework
    Properties:
      FrameworkControls:
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN
        - ControlName: BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK
      ControlInputParameters:
        - ParameterName: requiredRetentionDays
          ParameterValue: '35'

```



```

- ControlName: BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
- ControlName: BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK
ControlInputParameters:
  - ParameterName: requiredRetentionDays
    ParameterValue: '35'
  - ParameterName: requiredFrequencyUnit
    ParameterValue: 'hours'
  - ParameterName: requiredFrequencyValue
    ParameterValue: '24'
ControlScope:
  Tags:
    - Key: customizedKey
      Value: customizedValue
- ControlName: BACKUP_RECOVERY_POINT_ENCRYPTED
- ControlName: BACKUP_RESOURCES_PROTECTED_BY_CROSS_REGION
ControlInputParameters:
  - ParameterName: crossRegionList
    ParameterValue: 'eu-west-2'
- ControlName: BACKUP_RESOURCES_PROTECTED_BY_CROSS_ACCOUNT
ControlInputParameters:
  - ParameterName: crossAccountList
    ParameterValue: '111122223333'
- ControlName: BACKUP_RESOURCES_PROTECTED_BY_BACKUP_VAULT_LOCK
- ControlName: BACKUP_LAST_RECOVERY_POINT_CREATED
- ControlName: RESTORE_TIME_FOR_RESOURCES_MEET_TARGET
ControlInputParameters:
  - ParameterName: maxRestoreTime
    ParameterValue: '720'

```

Outputs:

```

FrameworkArn:
  Value: !GetAtt TestFramework.FrameworkArn

```

Exención de roles de IAM de la evaluación de control

El control `BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED` permite eximir hasta cinco roles de IAM que aún pueden eliminar manualmente puntos de recuperación. La siguiente plantilla implementa este control y también exime dos roles de IAM.

```

AWSTemplateFormatVersion: '2010-09-09'
Resources:
  TestFramework:
    Type: AWS::Backup::Framework

```

```

Properties:
  FrameworkControls:
    - ControlName: BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
      ControlInputParameters:
        - ParameterName: "principalArnList"
          ParameterValue: !Sub
            "arn:aws:iam::${AWS::AccountId}:role/AccAdminRole,arn:aws:iam::${AWS::AccountId}:role/
ConfigRole"

Outputs:
  FrameworkArn:
    Value: !GetAtt TestFramework.FrameworkArn

```

Creación de un plan de informes

La siguiente plantilla crea un plan de informes.

```

Description: "Basic AWS::Backup::ReportPlan template"

Parameters:
  ReportPlanDescription:
    Type: String
    Default: "SomeReportPlanDescription"
  S3BucketName:
    Type: String
    Default: "some-s3-bucket-name"
  S3KeyPrefix:
    Type: String
    Default: "some-s3-key-prefix"
  ReportTemplate:
    Type: String
    Default: "BACKUP_JOB_REPORT"

Resources:
  TestReportPlan:
    Type: "AWS::Backup::ReportPlan"
    Properties:
      ReportPlanDescription: !Ref ReportPlanDescription
      ReportDeliveryChannel:
        Formats:
          - "CSV"
      S3BucketName: !Ref S3BucketName
      S3KeyPrefix: !Ref S3KeyPrefix

```

```
ReportSetting:
  ReportTemplate: !Ref ReportTemplate
  Regions: ['us-west-2', 'eu-west-1', 'us-east-1']
  Accounts: ['123456789098']
  OrganizationUnits: ['ou-abcd-1234wxyz']
ReportPlanTags:
  - Key: "a"
    Value: "1"
  - Key: "b"
    Value: "2"
```

Outputs:

```
ReportPlanArn:
  Value: !GetAtt TestReportPlan.ReportPlanArn
```

Uso de AWS Backup Audit Manager con AWS Audit Manager

AWS Backup Los controles de Audit Manager se corresponden con controles estándar prediseñados AWS Audit Manager, lo que le permite importar las conclusiones de conformidad de AWS Backup Audit Manager a sus AWS Audit Manager informes. Puede que desee hacerlo para ayudar a un responsable de conformidad, director de auditoría u otro compañero que informe sobre las actividades de copia de seguridad como parte de la postura de conformidad general de su organización.

Puede importar los resultados de conformidad de sus controles de AWS Backup Audit Manager a sus AWS Audit Manager marcos. AWS Audit Manager Para permitir la recopilación automática de datos de los controles de AWS Backup Audit Manager, cree un control personalizado AWS Audit Manager siguiendo las instrucciones para [personalizar un control existente](#) de la Guía del AWS Audit Manager usuario. Al seguir estas instrucciones, tenga en cuenta que la fuente de datos de los AWS Backup controles es AWS Config.

Para obtener una lista de AWS Backup los controles, [consulte Elegir los controles](#).

Controles y corrección

En esta página se enumeran los controles disponibles para AWS Backup Audit Manager. Puede elegir el panel de información derecho para ver una lista de controles y pasar a un control específico. Para comparar rápidamente los controles, consulta la tabla en [Elección de controles](#). Para definir los controles mediante programación, consulte los fragmentos de código en [Creación de marcos mediante la API de AWS Backup](#).

Puede usar hasta 50 controles por cuenta y región. Usar el mismo control en dos marcos diferentes cuenta como usar dos controles del límite de 50 controles.

En esta página se muestra cada control con la siguiente información:

- Descripción. Los valores entre corchetes (“[]”) son los valores de los parámetros predeterminados.
- Los recursos que evalúa el control.
- Los parámetros del control.
- Ocasión en la que se produce la ejecución del control.
- El ámbito del control, como sigue:
 - Puede especificar Recursos por tipo. Para ello, elija uno o más servicios compatibles con AWS Backup.
 - Puede especificar un ámbito de Recursos etiquetados con una única clave de etiqueta y un valor opcional.
 - Puede especificar un único recurso mediante la lista desplegable Recurso único.
- Medidas correctivas para que los recursos aplicables logren la conformidad.

Tenga en cuenta que solo se incluirán los recursos activos cuando los controles evalúen la conformidad de los recursos. Por ejemplo, una EC2 instancia de Amazon en estado de ejecución será evaluada por el control Se [creó el último punto de recuperación](#). Una EC2 instancia detenida no se incluirá en la evaluación de conformidad.

Los recursos de copia de seguridad están incluidos en al menos un plan de copia de seguridad

Descripción: evalúa si los recursos de copia de seguridad están incluidos en al menos un plan de copia de seguridad.

Recurso: AWS Backup: backup selection

Parámetros: ninguno

Se produce: automáticamente cada 24 horas

Ámbito:

- Recursos etiquetados
- Recursos por tipo (predeterminado)

- Recurso único

Corrección: asigne los recursos a un plan de copia de seguridad. AWS Backup protege automáticamente sus recursos después de que los asigne a un plan de copia de seguridad. Para obtener más información, consulte [Asignación de recursos a un plan de copia de seguridad](#).

Frecuencia mínima y retención mínima del plan de copia de seguridad

Descripción: evalúa si los planes de copia de seguridad contienen al menos una regla de copia de seguridad según la cual la frecuencia de copia de seguridad sea de al menos [1 día] y el periodo de retención sea de al menos [35 días].

Recurso: AWS Backup: backup plans

Parámetros:

- Frecuencia de copia de seguridad requerida en número de horas o días.
- Periodo de retención obligatorio en días, semanas, meses o años. Recomendamos conservar el almacenamiento en caliente durante un período de al menos una semana AWS Backup para poder realizar copias de seguridad incrementales siempre que sea posible y así evitar cargos adicionales.

Se produce: cambios de configuración

Ámbito:

- Recursos etiquetados
- Recurso único

Corrección: [actualice un plan de copia de seguridad](#) para cambiar su frecuencia de copia de seguridad, su periodo de retención o ambos. La actualización del plan de copia de seguridad cambia el periodo de retención de los puntos de recuperación que el plan crea después de la actualización.

Los almacenes impiden la eliminación manual de los puntos de recuperación

Descripción: evalúa si los almacenes de copias de seguridad no permiten la eliminación manual de los puntos de recuperación, excepto mediante determinados roles de IAM.

Recurso: AWS Backup: `backup vaults`

Parámetros: Los nombres de recursos de Amazon (ARNs) de hasta cinco funciones de IAM permitían eliminar manualmente los puntos de recuperación.

Se produce: cambios de configuración

Ámbito:

- Recursos etiquetados
- Recurso único

Corrección: cree o modifique una política de acceso basada en recursos en un almacén de copias de seguridad. Para ver un ejemplo de la política e instrucciones sobre cómo establecer una política de acceso en un almacén de copias de seguridad, consulte [Denegación del acceso para eliminar puntos de recuperación en un almacén de copias de seguridad](#).

Los puntos de recuperación están cifrados

Descripción: evalúa si los puntos de recuperación están cifrados.

Recurso: AWS Backup: `recovery points`

Parámetros: ninguno

Se produce: cambios de configuración

Ámbito:

- Recursos etiquetados

Corrección: configure el cifrado de los puntos de recuperación. La forma de configurar el cifrado de los puntos de AWS Backup recuperación varía según el tipo de recurso.

Puede configurar el cifrado para los tipos de recursos que admitan una AWS Backup administración completa de su uso AWS Backup. Si el tipo de recurso no admite la AWS Backup administración completa, debe configurar su cifrado de respaldo siguiendo las instrucciones de ese servicio, como el [cifrado de Amazon EBS](#) en la Guía del usuario de Amazon Elastic Compute Cloud. Para ver la lista de tipos de recursos que admiten la AWS Backup administración completa, consulte la sección «AWS Backup Administración completa» de la [Disponibilidad de características por recurso](#) tabla.

Se ha establecido una retención mínima para el punto de recuperación

Descripción: evalúa si el periodo de retención del punto de recuperación es de al menos [35 días].

Recurso: AWS Backup: `recovery points`

Parámetros: periodo de retención obligatorio en días, semanas, meses o años. Recomendamos conservar el almacenamiento en caliente durante un período de al menos una semana para poder AWS Backup realizar copias de seguridad incrementales siempre que sea posible y evitar cargos adicionales.

Se produce: cambios de configuración

Ámbito:

- Recursos etiquetados

Corrección: cambie los periodos de retención de sus puntos de recuperación. Para obtener más información, consulte [Edición de una copia de seguridad](#).

Se ha programado una copia de la copia de seguridad entre regiones

Descripción: Evalúa si un recurso está configurado para crear copias de sus copias de seguridad en otra AWS región.

Recurso: AWS Backup: `backup selection`

Parámetros:

- Seleccione los Región de AWS lugares donde debe estar la copia de seguridad (opcional)
- Region

Se produce: automáticamente cada 24 horas

Ámbito:

- Recursos etiquetados
- Recursos por tipo
- Recurso único

Solución: actualice [un plan de respaldo](#) para cambiar el Región de AWS lugar donde debe estar la copia de seguridad.

Se ha programado una copia de la copia de seguridad entre cuentas

Descripción: evalúa si un recurso está configurado para crear copias de sus copias de seguridad en otra cuenta. Puede añadir hasta 5 cuentas para que el control las evalúe. La cuenta de destino debe estar en la misma organización que la cuenta de origen en AWS Organizations.

Recurso: AWS Backup: backup selection

Parámetros:

- Seleccione los ID de AWS cuenta en los que debe estar la copia de seguridad (opcional)
- ID de cuenta

Se produce: automáticamente cada 24 horas

Ámbito:

- Recursos etiquetados
- Recursos por tipo
- Recurso único

Solución: [actualice un plan de respaldo](#) para cambiar o agregar los ID de AWS cuenta en los que debería estar la copia.

Los recursos están en un plan de respaldo con un AWS Backup Vault Lock

Descripción: evalúa si un recurso tiene copias de seguridad inmutables almacenadas en un almacén de copias de seguridad bloqueado.

Recurso: AWS Backup: backup selection

Parámetros:

- Introduzca los días de retención mínimos y máximos de AWS Backup Vault Lock (opcional)
- Días de retención mínimos
- Días de retención máximos

Se produce: automáticamente cada 24 horas

Ámbito:

- Recursos etiquetados
- Recursos por tipo
- Recurso único

Corrección: [bloquee un almacén de copias de seguridad](#) para establecer su nombre, cambiar sus días de retención mínimos o máximos, o ambos. También puede incluir `ChangeableForDays` para un bloqueo del almacén en modo de cumplimiento.

Se creó el último punto de recuperación

Descripción: este control evalúa si se ha creado un punto de recuperación dentro del periodo de tiempo especificado (en días u horas).

El control es conforme si se ha creado un punto de recuperación del recurso dentro del periodo de tiempo especificado. El control no es conforme si no se ha creado un punto de recuperación dentro del número de días u horas especificado.

Recurso: AWS Backup: `recovery points`

Parámetros:

- Introduzca el periodo de tiempo especificado en números enteros, ya sea en horas o en días.
- Los valores de `hours` pueden oscilar entre 1 y 744.
- El valor de `days` puede oscilar entre 1 y 31.

Se produce: automáticamente cada 24 horas

Ámbito:

- Recursos etiquetados
- Recursos por tipo
- Recurso único

Corrección:

- [Actualice un plan de copia de seguridad](#) para cambiar el periodo de tiempo especificado para la creación del punto de recuperación.
- Además, puede crear una copia de seguridad bajo demanda.

El tiempo de restauración de los recursos cumple el objetivo

Descripción: evalúa si la restauración de los recursos protegidos se completó dentro del tiempo de restauración objetivo.

Este control comprueba si el tiempo de restauración de un recurso concreto cumple la duración objetivo. La regla es `NON_COMPLIANT` si `LatestRestoreExecutionTimeMinutes` de un tipo de recurso es mayor que `maxRestoreTime` en minutos.

Parámetros:

- `maxRestoreTime` (en minutos)

Se produce: automáticamente cada 24 horas

Ámbito:

- Recursos etiquetados
- Recursos por tipo
- Recurso único

Note

AWS Backup no proporciona ningún acuerdo de nivel de servicio (SLAs) para el tiempo de restauración. Los tiempos de restauración pueden variar en función de la carga y la capacidad del sistema, incluso en el caso de restauraciones que contengan los mismos recursos.

Recursos en un almacén aislado lógicamente

Descripción: este control evalúa si los recursos tienen al menos un punto de recuperación copiado en almacén aislado lógicamente dentro del valor y el plazo especificados. Este control es

NON_COMPLIANT si un punto de recuperación no se ha copiado en un almacén aislado lógicamente en el período de tiempo configurado para el control.

Recurso: AWS Backup: `recovery points`

Parámetros:

- `recoveryPointAgeValue`
- `recoveryPointAgeUnit`

Introduzca el período de tiempo. Especifique la unidad en `days` o `hours`. Especifique un valor para esa unidad. Los valores de las horas pueden estar comprendidos entre 24 y 2184 ambos inclusive. Los valores de los días pueden estar comprendidos entre 1 y 91 ambos inclusive.

Se recomienda un valor mínimo de 7 días o 168 horas. El valor de control no debe ser más frecuente que la frecuencia de creación de copias de su plan de copias de seguridad; de lo contrario, es posible que aparezca un estado NON_COMPLIANT inesperado hasta que la siguiente copia de seguridad se copie en un almacén aislado lógicamente y se ejecute este control.

Se produce: automáticamente cada 24 horas

Ámbito:

- Recursos por tipo
- Recurso único

Administrar AWS Backup recursos en múltiples Cuentas de AWS

Note

Antes de administrar los recursos Cuentas de AWS en varios AWS Backup ingresos, sus cuentas deben pertenecer a la misma organización del AWS Organizations servicio.

Descripción general de la administración entre cuentas

Puede utilizar la función de administración multicuenta AWS Backup para gestionar y supervisar los trabajos de copia de seguridad, restauración y copia con AWS Organizations los Cuentas de AWS que haya configurado. [AWS Organizations](#) es un servicio que ofrece una administración basada en políticas para múltiples cuentas de administración Cuentas de AWS desde una única cuenta de administración. Le permite estandarizar la forma en que implementa las políticas de copia de seguridad, minimizando los errores manuales y el esfuerzo simultáneamente. Desde una vista central, puede identificar fácilmente los recursos en todas las cuentas que cumplan los criterios que le interesan.

Si lo configuras AWS Organizations, puedes configurarlo AWS Backup para monitorear las actividades de todas tus cuentas en un solo lugar. También puede crear una política de copias de seguridad y aplicarla a determinadas cuentas que formen parte de su organización y ver las actividades agregadas de las tareas de copia de seguridad directamente desde la AWS Backup consola. Esta funcionalidad permite a los administradores de copias de seguridad monitorizar eficazmente el estado del trabajo de copia de seguridad en cientos de cuentas de toda la empresa desde una sola cuenta maestra. Se aplican las [Cuotas para AWS Organizations](#).

Por ejemplo, se define una política de copia de seguridad A que toma copias de seguridad diarias de recursos específicos y las mantiene durante 7 días. Puede aplicar la política de copia de seguridad A a toda la organización. (Esto significa que cada cuenta de la organización obtiene esa política de copia de seguridad, lo que crea un plan de copia de seguridad correspondiente que está visible en esa cuenta). A continuación, crea una unidad organizativa denominada Finance y decide mantener sus copias de seguridad durante solo 30 días. En este caso, se define una política de copia de seguridad B, que anula el valor del ciclo de vida y se adjunta a esa unidad organizativa Finance. Esto significa que todas las cuentas bajo la unidad organizativa Finance obtienen un nuevo plan de copia

de seguridad efectivo que toma copias de seguridad diarias de todos los recursos especificados y las mantiene durante 30 días.

En este ejemplo, la política de copia de seguridad A y la política de copia de seguridad B se fusionaron en una única política de copia de seguridad, que define la estrategia de protección para todas las cuentas de la unidad organizativa denominada Finance. Todas las demás cuentas de la organización permanecen protegidas por la política de copia de seguridad A. La combinación se realiza solo para las políticas de copia de seguridad que comparten el mismo nombre de plan de copia de seguridad. También puede hacer que la política A y la política B coexistan en esa cuenta sin ninguna combinación. Solo puede utilizar operadores avanzados de fusión en la vista JSON de la consola. Para obtener más información sobre la combinación de políticas, consulte [Definición de políticas, sintaxis de políticas y herencia de políticas](#) en la Guía del usuario de AWS Organizations. Para obtener referencias y casos de uso adicionales, consulte el blog [Cómo administrar copias de seguridad a gran escala AWS Organizations con su uso AWS Backup y el tutorial en vídeo](#) [Cómo gestionar las copias de seguridad a escala AWS Organizations con su uso AWS Backup](#).

La administración entre cuentas consiste en la supervisión entre cuentas, las copias de seguridad entre cuentas, las políticas de copias de seguridad y las cuentas de administrador delegado. No todos estos elementos están disponibles en todas las regiones. Para obtener información sobre dónde está disponible la administración multicuenta, consulte [Disponibilidad de funciones por AWS región](#).

Cómo usar la administración entre cuentas

1. Cree una cuenta de administración AWS Organizations y añada cuentas a la cuenta de administración.
2. Habilite la función de administración multicuenta en AWS Backup.
3. Cree una política de respaldo para aplicarla a todos los usuarios Cuentas de AWS de su cuenta de administración.

Note

Para los planes de copia de seguridad administrados por Organizations, la configuración de suscripción del recurso en la cuenta de administración anula la configuración de la cuenta de un miembro, aunque estén configuradas una o varias cuentas de administrador delegado. Las cuentas de administrador delegado son cuentas de miembros con

características mejoradas y no pueden anular la configuración como una cuenta de administración.

4. Gestione los trabajos de copia de seguridad, restauración y copia en todos sus archivos Cuentas de AWS.

Creación de una cuenta de administración en Organizations

En primer lugar, debe [crear su organización](#) y configurarla con las cuentas de AWS los miembros integradas AWS Organizations. Para obtener instrucciones, consulte [Tutorial: Creación y configuración de una organización](#) en la Guía del usuario de AWS Organizations .

Al añadir cuentas de miembro a su organización, asegúrese de que cada cuenta tenga:

- Al menos una bóveda de respaldo and/or cerrada de forma lógica
- un rol de IAM.

Las políticas de copia de seguridad que cree tendrán un plan de copia de seguridad, pero también identificarán las Regiones de AWS bóvedas utilizadas en el plan de copia de seguridad, los recursos de los que se realizará la copia de seguridad y la función de IAM que se utilizará para crear la copia de seguridad. Las políticas de copias de seguridad que hacen referencia a cuentas que carecen de la información requerida no funcionarán según se espera.

Para obtener más información, consulte [Sintaxis de las políticas de copia de seguridad](#) en la Guía del usuario de AWS Organizations .

Habilitación de la administración entre cuentas

Para poder utilizar la administración multicuenta AWS Backup, la cuenta de administración debe habilitar la función (es decir, habilitarla). Una vez que la cuenta de administración habilite la administración entre cuentas, puede crear políticas de copia de seguridad que administren los recursos de varias cuentas.

Para habilitar la administración entre cuentas

1. Abra la barra Consola de AWS Backup . <https://console.aws.amazon.com/backup/> Debe iniciar sesión con las credenciales de la cuenta de administración.

2. En el panel de navegación izquierdo, elija Settings (Configuración) para abrir la página de administración entre cuentas.
3. En la sección Backup policies (Políticas de copia de seguridad), elija Enable (Habilitar).

Esto le da acceso a todas las cuentas y le permite crear políticas que automatizan la administración de varias cuentas en su organización simultáneamente.

4. En la sección Supervisión entre cuentas elija Enable (Habilitar).

Esto le permite monitorizar las actividades de copia de seguridad, copia y restauración de todas las cuentas de su organización desde su cuenta de administración.

Políticas de copia de seguridad

Puede combinar los planes de copia de seguridad con la escalabilidad de [las políticas de AWS Organizations](#) para crear [políticas de respaldo](#) que simplifiquen la administración en toda su organización.

Consulte la Guía del usuario de AWS Organizations para obtener información sobre cómo habilitar las políticas de copia de seguridad para su organización, de modo que pueda:

- [Crear una política de copias de seguridad](#).
- [Actualizar una política de copias de seguridad](#); o,
- [Eliminar una política de copias de seguridad](#)
- [Sintaxis y ejemplos de políticas de Backup](#)

Consulte [AWS Backup cuotas](#) para obtener información sobre las cuotas específicas de AWS Backup de los elementos incluidos en una política.

Administrador delegado

La administración delegada proporciona una forma cómoda para que los usuarios asignados a una cuenta de miembro registrado realicen la mayoría de las tareas AWS Backup administrativas. Puede optar por delegar la administración de AWS Backup una cuenta de miembro en AWS Organizations, lo que amplía la capacidad AWS Backup de administrar desde fuera de la cuenta de administración y en toda la organización.

Una cuenta de administración, de forma predeterminada, es la cuenta que se usa para editar y administrar las políticas. Con la característica de administrador delegado, puede delegar estas funciones de administración a las cuentas miembro que designe. A su vez, esas cuentas pueden administrar políticas, además de la cuenta de administración.

Una vez que la cuenta miembro se haya registrado correctamente para la administración delegada, se convierte en una cuenta de administrador delegado. Tenga en cuenta que las cuentas, no los usuarios, se designan como administradores delegados.

La habilitación de cuentas de administrador delegado permite administrar las políticas de copia de seguridad, minimiza la cantidad de usuarios con acceso a la cuenta de administración y facilita la monitorización de los trabajos entre cuentas.

A continuación, se muestra una tabla que muestra las funciones de la cuenta de administración, las cuentas delegadas como administradores de Backup y las cuentas que son miembros de la AWS organización.

 Note

Las cuentas de administrador delegado son cuentas de miembros con características mejoradas, pero no pueden anular la configuración de suscripción al servicio de otras cuentas de miembros como una cuenta de administración.

PRIVILEGIOS	CUENTA DE ADMINISTRACIÓN	ADMINISTRADOR DELEGADO	CUENTA MIEMBRO
Registrar o anular el registro de cuentas de administrador delegado	Sí	No	No
Activar la administración entre cuentas	Sí	No	No
Administre las políticas de respaldo en todas las cuentas	Sí	Sí	No

PRIVILEGIOS	CUENTA DE ADMINISTRACIÓN	ADMINISTRADOR DELEGADO	CUENTA MIEMBRO
en AWS Organizations			
Monitorizar los trabajos entre cuentas	Sí	Sí	No

Requisitos previos

Para poder delegar la administración de las copias de seguridad, primero debe registrar al menos una cuenta de miembro en su AWS organización como administrador delegado. Antes de poder registrar una cuenta como administrador delegado, primero debe configurar lo siguiente:

- [AWS Organizations debe estar habilitada y configurada](#) con al menos una cuenta de miembro además de la cuenta de administración predeterminada.
- Se recomienda que la cuenta de administración de la organización tenga presente la función AWS Backup Backup Service-Linked Role (AWS Backup ServiceRoleForBackup) para sincronizar automáticamente los permisos de administrador delegado con las organizaciones. Esto garantiza que los administradores delegados tengan el acceso adecuado cuando se habilitan las regiones opcionales o se cambia la asignación de administrador. Si el rol vinculado a Backup Service no está presente o se ha eliminado, los clientes tienen varias opciones para crearlo:
 - Enabling the Delegated Administrator feature.
 - Access the Backup Vaults Console page.
 - Manually create it following the documentation in [Crear el rol de servicio predeterminado](#).
- En la AWS Backup consola, asegúrate de que las políticas de respaldo, la supervisión multicuenta, la copia de seguridad multicuenta y las funciones de administrador delegado estén activadas. Se encuentran debajo del panel de administradores delegados de la consola. AWS Backup
 - La [monitorización entre cuentas](#) le permite monitorizar la actividad de copia de seguridad en todas las cuentas de su organización, tanto desde la cuenta de administración como desde las cuentas de administrador delegado.
 - Opcional: copia de seguridad entre cuentas, que permite a las cuentas de su organización replicar copias de seguridad en otras cuentas (para los recursos entre cuentas compatibles con Backup).

- Opcional: administrador delegado, que permite a AWS Backup crear automáticamente la función Backup Service-Linked para sincronizar los permisos de administrador delegado con Organizations.
- [Habilite el acceso al servicio con.](#) AWS Backup

La configuración de la administración delegada consta de dos pasos. El primer paso es delegar la monitorización de los trabajos entre cuentas. El segundo paso es delegar la administración de las políticas de copia de seguridad.

Registro de una cuenta miembro como cuenta del administrador delegado

Esta es la primera sección: Uso de la AWS Backup consola para registrar una cuenta de administrador delegado a fin de supervisar los trabajos entre cuentas. Para delegar AWS Backup políticas, utilizará la consola Organizations en la siguiente sección.

Para registrar una cuenta de miembro mediante la AWS Backup consola:

1. Abra el Consola de AWS Backup chat <https://console.aws.amazon.com/backup/>. Debe iniciar sesión con las credenciales de la cuenta de administración.
2. En Mi cuenta, en el panel de navegación izquierdo de la consola, elija Configuración.
3. En el panel Administradores delegados, haga clic en Registrar administrador delegado o Agregar administrador delegado.
4. En la página Registrar administrador delegado, seleccione la cuenta que desee registrar y, a continuación, elija Registrar cuenta.

Esta cuenta designada ahora se registrará como un administrador delegado, con privilegios administrativos para monitorizar los trabajos en todas las cuentas de la organización. Además, podrá ver y editar las políticas (delegación de políticas). Esta cuenta miembro no puede registrar ni anular el registro de otras cuentas de administrador delegado. Puede usar la consola para registrar un máximo de 5 cuentas como administradores delegados.

Asegúrese de que el administrador delegado tenga los permisos otorgados por [the section called "AWSBackupOrganizationAdminAccess"](#).

Para registrar una cuenta miembro mediante programación:

Utilice el comando CLI `register-delegated-administrator`. Puede especificar los siguientes parámetros en su solicitud de CLI:

- `service-principal`
- `account-id`

A continuación se muestra un ejemplo de una solicitud de CLI para registrar una cuenta miembro mediante programación:

```
aws organizations register-delegated-administrator \  
--account-id 012345678912 \  
--service-principal "backup.amazonaws.com"
```

Anulación del registro de una cuenta miembro

Utilice el siguiente procedimiento para eliminar el acceso administrativo AWS Backup anulando el registro de una cuenta de miembro de su AWS organización que anteriormente había sido designada como administrador delegado.

Para anular el registro de una cuenta miembro con la consola

1. Abra el arte. Consola de AWS Backup <https://console.aws.amazon.com/backup/> Debe iniciar sesión con las credenciales de la cuenta de administración.
2. En Mi cuenta, en el panel de navegación izquierdo de la consola, elija Configuración.
3. En la sección Administrador delegado, elija Anular el registro de cuenta.
4. Elige la cuenta o cuentas para las que desea anular el registro.
5. En el cuadro de diálogo Anular el registro de cuenta, revise las implicaciones de seguridad y, a continuación, escriba `confirm` para completar la anulación del registro.
6. Elija `Deregister account`.

Para anular el registro de una cuenta miembro mediante programación:

Utilice el comando de la CLI `deregister-delegated-administrator` para anular el registro de una cuenta de administrador delegado. Puede especificar los siguientes parámetros en su solicitud de API:

- `service-principal`
- `account-id`

A continuación se muestra un ejemplo de una solicitud de CLI para anular el registro de una cuenta miembro mediante programación:

```
aws organizations deregister-delegated-administrator \  
--account-id 012345678912 \  
--service-principal "backup.amazonaws.com"
```

Delega AWS Backup políticas a través de AWS Organizations

Dentro de la AWS Organizations consola, puede delegar la administración de varias políticas, incluidas las políticas de Backup.

Desde la cuenta de administración que ha iniciado sesión en la [consola de AWS Organizations](#), puede crear, ver o eliminar una política de delegación basada en recursos para su organización. Para ver los pasos para delegar políticas, consulte [Crear una política de delegación basada en recursos](#) en la Guía del usuario de AWS Organizations .

Monitorización de actividades en varias Cuentas de AWS

Para supervisar los trabajos de copia de seguridad, copia y restauración en todas las cuentas, debe habilitar la supervisión entre cuentas. Esto le permite monitorizar las actividades de copia de seguridad en todas las cuentas desde la cuenta de administración de la organización. Después de participar, todos los trabajos de la organización que se crearon después de la suscripción están visibles. Cuando se desactiva, AWS Backup mantiene los trabajos en la vista conjunta durante 30 días (desde que se llega a un estado de finalización). Los trabajos creados después de la exclusión no son visibles y no muestran los trabajos de copia de seguridad recién creados. Para obtener instrucciones de aceptación, consulte [Habilitación de la administración entre cuentas](#).

Para supervisar varias cuentas

1. Abre el Consola de AWS Backup anuncio <https://console.aws.amazon.com/backup/>. Debe iniciar sesión con las credenciales de la cuenta de administración.
2. En el panel de navegación izquierdo, elija Settings (Configuración) para abrir la página de administración entre cuentas.
3. En la sección Supervisión entre cuentas elija Enable (Habilitar).

Esto le permite monitorizar las actividades de copia de seguridad y restauración de todas las cuentas de su organización desde su cuenta de administración.

4. En el panel de navegación izquierdo, elija Cross-account monitoring (Supervisión entre cuentas).
5. En la página Supervisión entre cuentas, elija la pestaña Trabajos de copia de seguridad, Trabajos de restauración o Trabajos de copia para ver todos los trabajos creados en todas sus cuentas. Puede ver cada uno de estos trabajos por Cuenta de AWS ID y puede ver todos los trabajos de una cuenta en particular.
6. En el cuadro de búsqueda, puede filtrar los trabajos por Account ID (ID de cuenta), Status (Estado), o Job ID (ID de trabajo).

Por ejemplo, puede elegir la pestaña Backup jobs (Trabajos de copia de seguridad) y ver todos los trabajos de copia de seguridad creados en todas sus cuentas. Puede filtrar la lista por Account ID (ID de cuenta) y ver todos los trabajos de copia de seguridad creados en esa cuenta.

Reglas de suscripción de recursos

Si el plan de copia de seguridad de una cuenta miembro se creó mediante una política de copia de seguridad a nivel de organización, la configuración de suscripción de AWS Backup de la cuenta de administración de Organizations anulará la configuración de suscripción de esa cuenta miembro, pero solo para ese plan de copia de seguridad.

Si la cuenta miembro también tiene planes de copia de seguridad a nivel local creados por los usuarios, dichos planes de copia de seguridad seguirán la configuración de suscripción de la cuenta miembro, sin referencia a la configuración de suscripción de la cuenta de administración de Organizations.

Definición de políticas, sintaxis de políticas y herencia de políticas

Los siguientes temas están documentados en la Guía AWS Organizations del usuario.

- Políticas de copia de seguridad: consulte [Políticas de copia de seguridad](#).
- Sintaxis de políticas: consulte [Ejemplos y sintaxis de políticas de copia de seguridad](#).
- Herencia para tipos de políticas de administración: consulte [Herencia para tipos de políticas de administración](#).

AWS Backup y CloudFormation

En general

Con CloudFormation, puede aprovisionar y administrar sus recursos de AWS de forma segura y repetible mediante las plantillas que cree. Puede utilizar plantillas de CloudFormation y conjuntos de pilas para administrar sus planes de copia de seguridad, selecciones de recursos de copia de seguridad y almacenes de copias de seguridad. Para obtener información sobre el uso de CloudFormation, consulte [¿Cómo funciona CloudFormation?](#) en la Guía del usuario de AWS CloudFormation.

Antes de crear su plantilla de CloudFormation o conjunto de pilas, debe tener en cuenta lo siguiente:

- Cree plantillas independientes para sus planes de copia de seguridad y sus almacenes de copias de seguridad. Solo puede eliminar los almacenes de copias de seguridad que estén vacíos. No puede eliminar una pila que tenga almacenes de copias de seguridad si contienen puntos de recuperación.
- Verifique que tiene disponible un rol de servicio antes de crear la pila. El rol de servicio predeterminado de AWS Backup se crea automáticamente la primera vez que asigna recursos a un plan de copia de seguridad. Si no ha asignado recursos al plan de copia de seguridad, hágalo antes de crear la pila. También puede especificar un rol personalizado que haya creado. Para obtener más información acerca de los roles, consulte [Roles de servicio de IAM](#).

Implementación de un almacén de copias de seguridad, un plan de copia de seguridad y una asignación de recursos mediante CloudFormation

Para ver una plantilla de CloudFormation de ejemplo que implementa un almacén de copias de seguridad, planes de copia de seguridad y asignación de recursos, consulte [Asigne AWS Backup recursos mediante CloudFormation](#).

Implementación de planes de copia de seguridad mediante CloudFormation

Para ver plantillas de CloudFormation de ejemplo que implementan planes de copia de seguridad, consulte [the section called “CloudFormation plantillas para planes de respaldo”](#).

Implementación de marcos y planes de informes de AWS Backup Audit Manager mediante CloudFormation

Para ver plantillas de CloudFormation de ejemplo que implementan marcos y planes de informes del administrador de auditoría de AWS Backup, consulte [the section called “Uso CloudFormation para implementar los recursos AWS Backup de Audit Manager”](#).

Implementación de planes de copia de seguridad en todas las cuentas mediante CloudFormation

Puede [utilizar conjuntos de pilas de AWS CloudFormation en varias cuentas en una AWS Organization](#). Hay plantillas de muestra disponibles en la [Guía del usuario de CloudFormation](#).

Un excelente punto de partida y referencia es la publicación [Automate centralized backup at scale across AWS services using AWS Backup](#). Por Ibukun Oyewumi y Sabith Venkitachalapathy (julio de 2021).

Más información sobre CloudFormation

Para obtener información sobre el uso de CloudFormation con AWS Backup, consulte la [AWS Backup Resource Type Reference](#) en la Guía del usuario de AWS CloudFormation.

Para obtener más información sobre el control de acceso a los recursos del servicio de AWS cuando utiliza CloudFormation, consulte [Controlar el acceso con AWS Identity and Access Management](#) en la Guía del usuario de AWS CloudFormation.

AWS Backup red

AWS Backup puntos finales

AWS Backup ofrece puntos finales públicos y privados para sus necesidades de conectividad. Para estos puntos finales, AWS Backup es compatible con los protocolos de Internet, versión 4 (IPv4) y versión 6 (IPv6), para los tipos de recursos compatibles. IPv6

El dispositivo de punto final público más reciente `backup.[Region].api.aws` tiene capacidades de doble pila y puede resolver uno o ambos IPv4 puntos de enlace o ambos. IPv6 Al realizar una solicitud a un punto final de AWS Backup API de doble pila, el punto final se resolverá en la dirección determinada por la configuración del protocolo utilizado por la red y el cliente.

El punto final anterior solo IPv4 se `backup.[Region].amazonaws.com` puede usar para llamadas de referencia.

Puede ver los [puntos de conexión del servicio público para AWS Backup](#) en Referencia general de Amazon Web Services. Puede ver los pasos para configurar puntos de conexión privados en [AWS Backup a través de la VPC](#).

AWS Backup a través de puntos finales de VPC

Puede establecer una conexión privada entre su nube privada virtual (VPC) y AWS Backup creando un punto de conexión de VPC de tipo interfaz. Los puntos finales de la interfaz funcionan con una tecnología que le permite acceder a la AWS Backup API sin utilizar una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o Direct Connect una conexión. [AWS PrivateLink](#) Las instancias de su VPC no necesitan direcciones IP públicas para comunicarse con los puntos de enlace de la AWS Backup API. Sus instancias tampoco necesitan direcciones IP públicas para usar ninguna de las operaciones de AWS Backup API y API de Backup Gateway disponibles.

Para obtener más información, consulte [Acceder a AWS los servicios AWS PrivateLink](#) en la AWS PrivateLink Guía.

Consideraciones sobre los puntos de conexión de Amazon VPC

Todas AWS Backup las operaciones relevantes para la administración de sus recursos están disponibles en su VPC mediante. AWS PrivateLink

Las políticas de los puntos de conexión de VPC son compatibles con los puntos de conexión de Backup. De forma predeterminada, se permite el acceso completo a las operaciones de Backup a través del punto de conexión. Como alternativa, puede asociar un grupo de seguridad a las interfaces de red del punto de conexión para controlar el tráfico a AWS Backup a través del punto de conexión de interfaz.

Puede seleccionar IPv4 una pila doble o doble al crear un punto final. IPv6 Recibirá los mismos nombres de DNS (que tendrán ambos nombres IPv4 y IPv6 direcciones si selecciona la pila doble).

AWS Backup para SAP HANA no es compatible AWS PrivateLink. Las copias de seguridad de SAP HANA las habilita el Agente de AWS Backint, que no es compatible con los puntos finales de VPC; envía los datos de respaldo al punto final de almacenamiento para. AWS Backup

Crear un punto final AWS Backup de VPC

Puede crear un punto de conexión de VPC para AWS Backup usar la consola de Amazon VPC o la (AWS Command Line Interface CLI).AWS Para obtener más información, consulte [Creación de un punto de conexión de interfaz](#) en la Guía de AWS PrivateLink .

PrivateLink Los puntos de enlace utilizan la misma estructura de nombres IPv4, aunque cada punto de enlace puede configurarse para una pila IPv4 doble o IPv6 doble.

Cree un punto final de VPC para AWS Backup usar el nombre del servicio.
`com.amazonaws.region.backup`

En la región de China (Pekín) y la región de China (Ningxia), el nombre del servicio debe ser
`cn.com.amazonaws.region.backup`.

Para los puntos de conexión de la puerta de enlace de copia de seguridad, utilice
`com.amazonaws.region.backup-gateway`.

Los siguientes puertos TCP deben estar permitidos en el grupo de seguridad al crear un punto de conexión de VPC para la puerta de enlace de copia de seguridad:

- TCP 443
- TCP 1026
- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

Protocolo	Puerto	Dirección	Origen	Destino	De uso
TCP	443 (HTTPS)	Salida	Puerta de enlace de copia de seguridad	AWS	Para la comunicación entre Backup Gateway y el punto final del AWS servicio

Uso de un punto de conexión de VPC

Si habilitas el DNS privado para el punto final, puedes realizar solicitudes de API al AWS Backup punto final de la VPC utilizando su nombre de DNS predeterminado para la AWS región, por ejemplo, `backup.us-east-1.api.aws`

Sin embargo, para la región de China (Pekín) y la región de China (Ningxia) Regiones de AWS, las solicitudes de API deben realizarse con el punto final de la VPC `backup.cn-north-1.amazonaws.com.cn` utilizando `backup.cn-northwest-1.amazonaws.com.cn` y, respectivamente.

Creación de una política de punto de conexión de VPC

Puede asociar una política de punto de conexión al punto de conexión de VPC que controla el acceso a la API de Amazon Backup. La política especifica:

- La entidad de seguridad que puede realizar acciones.
- Las acciones que se pueden realizar.
- Los recursos en los que se pueden llevar a cabo las acciones.

Important

Cuando se aplica una política no predeterminada a un punto final AWS Backup de la VPC de la interfaz, es posible que determinadas solicitudes de API con errores, como las que no llegan `RequestLimitExceeded`, no se registren en Amazon AWS CloudTrail . CloudWatch

Para obtener más información, consulte [Control del acceso a los servicios con políticas de punto de conexión](#) en la Guía del usuario de AWS PrivateLink .

Ejemplo: política de puntos finales de VPC para acciones AWS Backup

El siguiente es un ejemplo de una política de puntos finales para AWS Backup. Cuando se adjunta a un punto final, esta política otorga acceso a las AWS Backup acciones enumeradas para todos los principios de todos los recursos.

```
{
  "Statement": [
    {
      "Action": "backup:*",
      "Effect": "Allow",
      "Principal": "*",
      "Resource": "*"
    }
  ]
}
```

Ejemplo: Política de punto de conexión de VPC que deniega todo el acceso desde una cuenta de AWS especificada

La siguiente política de punto final de VPC deniega a la AWS cuenta 123456789012 todo acceso a los recursos que utilizan el punto final. La política permite todas las acciones de otras cuentas.

JSON

```
{
  "Id": "Policy1645236617225",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1645236612384",
      "Action": "backup:*",
      "Effect": "Deny",
      "Resource": "*",
      "Principal": {
        "AWS": [
          "123456789012"
        ]
      }
    }
  ]
}
```

```
}  
}  
]  
}
```

Para obtener más información sobre las respuestas de API disponibles, consulte la [Guía de API](#).

Seguridad en AWS Backup

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 Nube de AWS. 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 aplicables AWS Backup, consulte los [AWS servicios incluidos en el ámbito de aplicación por programa de conformidad](#).
- Seguridad en la nube: su responsabilidad con respecto a AWS Backup incluye, pero no se limita a, lo siguiente. Usted también es responsable de otros factores incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.
 - Responder a las comunicaciones que reciba de AWS.
 - Administrar las credenciales que usted y su equipo utilizan. Para obtener más información, consulte [Administración de identidad y acceso en AWS Backup](#).
 - Configurar los planes de copia de seguridad y las asignaciones de recursos para que reflejen las políticas de protección de datos de su organización. Para obtener más información, consulte [Administración de planes de copia de seguridad](#).
 - Probar periódicamente la capacidad de encontrar determinados puntos de recuperación y restaurarlos. Para obtener más información, consulte [Trabajar con copias de seguridad](#).
 - Incorporar AWS Backup los procedimientos en los procedimientos escritos de recuperación ante desastres y continuidad empresarial de su organización. Para empezar, consulte [Introducción a AWS Backup](#).
 - Asegúrese de que sus empleados estén familiarizados con los procedimientos organizativos y hayan practicado utilizarlos AWS Backup junto con ellos en caso de una emergencia. Para obtener más información, consulte [AWS Well-Architected Framework](#).

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza AWS Backup. Los siguientes temas muestran cómo configurarlo AWS Backup para

cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus AWS Backup recursos.

Temas

- [Validación de conformidad para AWS Backup](#)
- [Protección de datos en AWS Backup](#)
- [Gestión de identidad y acceso en AWS Backup](#)
- [Seguridad de la infraestructura en AWS Backup](#)
- [Integridad de los datos en AWS Backup](#)
- [Obligaciones legales y AWS Backup](#)
- [Protección contra malware en AWS Backup](#)
- [Resiliencia en AWS Backup](#)

Validación de conformidad para AWS Backup

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte [Servicios de AWS Alcance por programa de cumplimiento](#) [Servicios de AWS](#) de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de [AWS cumplimiento > Programas AWS](#) .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte [Descarga de informes en AWS Artifact](#) .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. Para obtener más información sobre su responsabilidad de conformidad al utilizarlos Servicios de AWS, consulte [AWS la documentación de seguridad](#).

Protección de datos en AWS Backup

AWS Backup se ajusta al [modelo de responsabilidad AWS compartida](#), que incluye normas y directrices para la protección de datos. AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los AWS servicios. AWS mantiene el control de los datos alojados en esta infraestructura, incluidos los controles de configuración de seguridad para gestionar el contenido y

los datos personales de los clientes. AWS los clientes y los socios de AWS Partner Network (APN), que actúan como controladores o procesadores de datos, son responsables de cualquier dato personal que introduzcan en la Nube de AWS.

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure cuentas de usuario individuales con AWS Identity and Access Management (IAM). Esto ayuda a garantizar que a cada usuario solo se le otorguen 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.
- Utilice una capa de conexión segura (SSL)/seguridad de la capa de transporte (TLS) para comunicarse con los recursos de AWS .
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados de los AWS servicios.

Le recomendamos encarecidamente que nunca introduzca información de identificación confidencial, como, por ejemplo, números de cuenta de sus clientes, en los campos de formato libre, como el campo Nombre. Esto incluye cuando trabaja con AWS Backup u otros AWS servicios mediante la consola, la API o AWS SDKs. AWS CLI Es posible que cualquier dato que ingrese en AWS Backup o en otros servicios se incluya en los registros de diagnóstico. Cuando proporcione una URL a un servidor externo, no incluya información de credenciales en la URL para validar la solicitud para ese servidor.

Para obtener más información sobre la protección de datos, consulte la entrada de blog relativa al [modelo de responsabilidad compartida de AWS y GDPR](#) en el blog de seguridad de AWS .

Cifrado de copias de seguridad en AWS Backup

Cifrado de independiente

AWS Backup ofrece un cifrado independiente para los [tipos de recursos que permiten una AWS Backup administración completa](#). El cifrado independiente significa que los puntos de recuperación (copias de seguridad) que se crean AWS Backup pueden tener un método de cifrado distinto del determinado por el cifrado del recurso de origen. Por ejemplo, la copia de seguridad de un bucket de Amazon S3 puede tener un método de cifrado diferente al del bucket de origen que cifró con el cifrado de Amazon S3. Este cifrado se controla mediante la configuración de AWS KMS claves en la bóveda de copias de seguridad donde se almacena la copia de seguridad.

Las copias de seguridad de los tipos de recursos que no se gestionan por completo AWS Backup suelen heredar la configuración de cifrado de su recurso de origen. Puede configurar estos ajustes de cifrado según las instrucciones de ese servicio, como [Cifrado de Amazon EBS](#) en la Guía del usuario de Amazon EBS.

Su rol de IAM debe tener acceso a la Clave de KMS que se utiliza para hacer copias de seguridad del objeto y restaurarlo. De lo contrario, el trabajo se realizará correctamente, pero no se realizará una copia de seguridad de los objetos ni se restaurará. Los permisos de la política de IAM y la política de claves de KMS deben ser coherentes. Para obtener más información, consulte [Specifying KMS keys in IAM policy statements](#) en la Guía para desarrolladores de AWS Key Management Service .

En la siguiente tabla se muestra cada tipo de recurso admitido, cómo está configurado el cifrado para las copias de seguridad y si se admite el cifrado independiente para las copias de seguridad. Cuando AWS Backup cifra de forma independiente una copia de seguridad, utiliza el algoritmo de cifrado AES-256 estándar del sector. Para obtener más información sobre el cifrado AWS Backup, consulte Copias de seguridad [entre regiones](#) y [entre cuentas](#).

Tipo de recurso	Cómo configurar el cifrado	Cifrado independiente AWS Backup
Amazon Simple Storage Service (Amazon S3)	Las copias de seguridad de Amazon S3 se cifran mediante una clave AWS KMS (AWS Key Management Service) asociada a la bóveda de copias de seguridad. La clave AWS KMS puede ser una clave administrada por el cliente o una clave AWS administrada asociada al servicio. AWS Backup AWS Backup cifra todas las copias de seguridad incluso si los buckets de Amazon S3 de origen no están cifrados.	compatible

Tipo de recurso	Cómo configurar el cifrado	Cifrado independiente AWS Backup
VMware máquinas virtuales	Las copias de seguridad de VM están siempre cifradas. La clave de AWS KMS cifrado para las copias de seguridad de las máquinas virtuales se configura en el AWS Backup almacén en el que se almacenan las copias de seguridad de las máquinas virtuales.	compatible
Amazon DynamoDB después de habilitar Copia de seguridad avanzada de DynamoDB	Las copias de seguridad de DynamoDB siempre están cifradas. La clave de AWS KMS cifrado de las copias de seguridad de DynamoDB se configura en AWS Backup el almacén en el que se almacenan las copias de seguridad de DynamoDB.	compatible

Tipo de recurso	Cómo configurar el cifrado	Cifrado independiente AWS Backup
Amazon DynamoDB sin habilitar Copia de seguridad avanzada de DynamoDB	Las copias de seguridad de DynamoDB se cifran automáticamente con la misma clave de cifrado que se utilizó para cifrar la tabla de DynamoDB de origen. Las instantáneas de tablas de DynamoDB sin cifrar también están sin cifrar. AWS Backup Para crear una copia de seguridad de una tabla de DynamoDB cifrada, debe añadir los kms:Decrypt permisos kms:GenerateDataKey y la función de IAM utilizada para la copia de seguridad. Como alternativa, puede utilizar el rol de servicio predeterminado. AWS Backup	No compatible
Amazon Elastic File System (Amazon EFS)	Las copias de seguridad de Amazon EFS siempre están cifradas. La clave de AWS KMS cifrado de las copias de seguridad de Amazon EFS se configura en el AWS Backup almacén en el que se almacenan las copias de seguridad de Amazon EFS.	compatible

Tipo de recurso	Cómo configurar el cifrado	Cifrado independiente AWS Backup
Amazon Elastic Block Store (Amazon EBS)	De forma predeterminada, las copias de seguridad de Amazon EBS se cifran con la clave que se utilizó para cifrar el volumen de origen, o no se cifran. Durante la restauración, puede especificar una clave de KMS para anular el método de cifrado predeterminado.	No compatible
Amazon Elastic Compute Cloud (Amazon EC2) AMIs	AMIs no están cifrados. Las instantáneas de EBS se cifran según las reglas de cifrado predeterminadas para las copias de seguridad de EBS (consulte la entrada correspondiente a EBS). Las instantáneas de EBS de datos y volúmenes raíz se pueden cifrar y adjuntar a una AMI.	No compatible
Amazon Relational Database Service (Amazon RDS)	Las instantáneas de Amazon RDS se cifran automáticamente con la misma clave de cifrado que se utilizó para cifrar la base de datos de Amazon RDS de origen. Las instantáneas de bases de datos de Amazon RDS sin cifrar también están sin cifrar.	No compatible

Tipo de recurso	Cómo configurar el cifrado	Cifrado independiente AWS Backup
Amazon Aurora	Las instantáneas de clúster de Aurora se cifran automáticamente con la misma clave de cifrado que se utilizó para cifrar el clúster de Amazon Aurora de origen. Las instantáneas de clústeres de Aurora sin cifrar también están sin cifrar.	No compatible
AWS Storage Gateway	Las instantáneas de Storage Gateway se cifran automáticamente con la misma clave de cifrado que se utilizó para cifrar el volumen de Storage Gateway de origen. Las instantáneas de volúmenes de Storage Gateway sin cifrar también están sin cifrar. No es necesario utilizar una clave administrada por el cliente en todos los servicios para habilitar Storage Gateway. Basta con replicar la copia de seguridad de Storage Gateway en un almacén donde se haya configurado una clave de KMS. Esto se debe a que Storage Gateway no tiene una clave AWS KMS administrada específica del servicio.	No compatible

Tipo de recurso	Cómo configurar el cifrado	Cifrado independiente AWS Backup
Amazon FSx	Las funciones de cifrado de los sistemas de FSx archivos de Amazon varían según el sistema de archivos subyacente. Para obtener más información sobre tu sistema de FSx archivos de Amazon en particular, consulta la Guía FSx del usuario correspondiente.	No compatible
Amazon DocumentDB	Las instantáneas de clúster de Amazon DocumentDB se cifran automáticamente con la misma clave de cifrado que se utilizó para cifrar el clúster de Amazon DocumentDB de origen. Las instantáneas de clústeres de Amazon DocumentDB sin cifrar también están sin cifrar.	No compatible
Amazon Neptune	Las instantáneas de clúster de Neptune se cifran automáticamente con la misma clave de cifrado que se utilizó para cifrar el clúster de Neptune de origen. Las instantáneas de clústeres de Neptune sin cifrar también están sin cifrar.	No compatible

Tipo de recurso	Cómo configurar el cifrado	Cifrado independiente AWS Backup
Amazon Timestream	Las copias de seguridad de las instantáneas de la tabla de Timestream siempre están cifradas. La clave de AWS KMS cifrado de las copias de seguridad de Timestream se configura en la bóveda de copias de seguridad en la que se almacenan las copias de seguridad de Timestream.	compatible
Amazon Redshift	Las instantáneas de clúster de Amazon Redshift se cifran automáticamente con la misma clave de cifrado que se utilizó para cifrar el clúster de Amazon Redshift de origen. Las instantáneas de clústeres de Amazon Redshift sin cifrar también están sin cifrar.	No compatible
Amazon Redshift sin servidor	Las instantáneas de Redshift sin servidor se cifran automáticamente con la misma clave de cifrado que se utilizó para cifrar el origen.	No compatible

Tipo de recurso	Cómo configurar el cifrado	Cifrado independiente AWS Backup
CloudFormation	CloudFormation las copias de seguridad siempre están cifradas. La clave de CloudFormation cifrado de las CloudFormation copias de seguridad se configura en el CloudFormation almacén en el que se almacenan las CloudFormation copias de seguridad.	compatible
Bases de datos SAP HANA en EC2 instancias de Amazon	Las copias de seguridad de las bases de datos de SAP HANA siempre están cifradas. La clave de AWS KMS cifrado para las copias de seguridad de las bases de datos de SAP HANA se configura en el AWS Backup almacén en el que se almacenan las copias de seguridad de las bases de datos.	compatible

 Tip

[AWS Backup Audit Manager](#) le ayuda a detectar automáticamente las copias de seguridad no cifradas.

Cifrado para copias de una copia de seguridad en una cuenta diferente o Región de AWS

Al copiar las copias de seguridad entre cuentas o regiones, las cifra AWS Backup automáticamente para la mayoría de los tipos de recursos, incluso si la copia de seguridad original no está cifrada. AWS Backup cifra la copia con la clave KMS del almacén de destino.

Antes de copiar una copia de seguridad de una cuenta a otra (tarea de copia entre cuentas) o de copiar una copia de seguridad de una región a otra (tarea de copia entre regiones), tenga en cuenta las siguientes condiciones, muchas de las cuales dependen de si el tipo de recurso de la copia de seguridad (punto de recuperación) está [completamente administrado AWS Backup o no](#).

- La copia de una copia de seguridad a otra Región de AWS se cifra con la clave del almacén de destino.
- Si se trata de una copia de un punto de recuperación (copia de seguridad) de un recurso gestionado en su totalidad AWS Backup, puede optar por cifrarla con una [clave gestionada por el cliente \(CMK\)](#) o una clave AWS Backup gestionada (aws/backup).

Para obtener una copia de un punto de recuperación de un recurso que no esté completamente gestionado AWS Backup, la clave asociada al almacén de destino debe ser una CMK o la clave gestionada del servicio propietario del recurso subyacente. Por ejemplo, si está copiando una EC2 instancia, no se puede usar una clave gestionada por Backup. En su lugar, se debe usar una clave de CMK o Amazon EBS KMS (aws/ebs) para evitar errores en el trabajo de copia.

- No se admite la copia multicuenta con claves AWS administradas en el caso de recursos que no estén totalmente gestionados por AWS Backup ellos. La [política de claves](#) de una clave administrada de AWS es inmutable, lo que impide que se copie la clave entre cuentas. Si tus recursos están cifrados con claves AWS administradas y deseas realizar una copia multicuenta, puedes [cambiarlas por una clave gestionada por el cliente](#), que se puede utilizar para copiar entre cuentas. O bien, puede seguir las instrucciones de [Protección de instancias de Amazon RDS cifradas con copias de seguridad entre cuentas y regiones para](#) seguir utilizando AWS las claves gestionadas.
- Las copias de los clústeres de Amazon Aurora, Amazon DocumentDB y Amazon Neptune sin cifrar también están sin cifrar.

AWS Backup declaraciones de permisos, concesiones y denegaciones

Para evitar errores en los trabajos, puede examinar la política AWS KMS clave para asegurarse de que cuenta con los permisos necesarios y que no contiene ninguna declaración de denegación que impida que las operaciones se realicen correctamente.

Los errores en los trabajos pueden producirse debido a la aplicación de una o más instrucciones de rechazo a la clave de KMS o a la revocación de la [concesión](#) de la clave.

En una política de acceso AWS gestionado, por ejemplo [AWSBackupFullAccess](#), se incluyen acciones de permiso que AWS Backup permiten interactuar con AWS KMS la creación de una concesión de una clave KMS en nombre de un cliente como parte de las operaciones de copia de seguridad, copia y almacenamiento.

La política de claves requiere, como mínimo, los siguientes permisos:

- kms:createGrant
- kms:generateDataKey
- kms:decrypt

Si las políticas de rechazo son necesarias, tendrá que incluir en una lista los roles necesarios para las operaciones de copia de seguridad y de restauración.

Estos elementos pueden tener el siguiente aspecto:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "KmsPermissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/root"
      },
      "Action": [
        "kms:ListKeys",
        "kms:DescribeKey",
        "kms:GenerateDataKey",
```

```

        "kms:ListAliases"
    ],
    "Resource": "*"
},
{
    "Sid": "KmsCreateGrantPermissions",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/root"
    },
    "Action": [
        "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "kms:EncryptionContextKeys": "aws:backup:backup-vault"
        },
        "Bool": {
            "kms:GrantIsForAWSResource": true
        },
        "StringLike": {
            "kms:ViaService": "backup.*.amazonaws.com"
        }
    }
}
]
}

```

Estos permisos deben formar parte de la clave, ya sea que esté AWS gestionada o gestionada por el cliente.

1. Asegúrese de que los permisos necesarios formen parte de la política de claves de KMS.
 - a. Ejecute el comando `get-key-policy` ([kms:GetKeyPolicy](#)) de la CLI de KMS para ver la política de claves asociada a la clave de KMS especificada.
 - b. Revise los permisos devueltos.
2. Asegúrese de que no haya instrucciones de rechazo que afecten a las operaciones.
 - a. Ejecute (o vuelva a ejecutar) el comando `get-key-policy` ([kms:GetKeyPolicy](#)) de la CLI para ver la política de claves asociada a la clave de KMS especificada.

- b. Revise la política.
 - c. Elimine las instrucciones de rechazo pertinentes de la política de claves de KMS.
3. Si es necesario, ejecute [kms:put-key-policy](#) para reemplazar o actualizar la política de claves con los permisos revisados y las instrucciones de rechazo eliminadas.

Además, la clave asociada al rol que inicia un trabajo de copia entre regiones debe tener "kms:ResourcesAliases": "alias/aws/backup" en el permiso DescribeKey.

Cifrado de credenciales del hipervisor de máquinas virtuales

Las máquinas virtuales [administradas por un hipervisor](#) utilizan una [AWS Backup Gateway](#) para conectar los sistemas en las instalaciones a AWS Backup. Es importante que los hipervisores cuenten con la misma seguridad sólida y fiable. Esta seguridad se puede lograr cifrando el hipervisor, ya sea mediante claves AWS propias o administradas por el cliente.

AWS claves propias y administradas por el cliente

AWS Backup proporciona cifrado para las credenciales del hipervisor a fin de proteger la información confidencial de inicio de sesión de los clientes mediante claves AWS de cifrado propias. En su lugar, tiene la opción de utilizar claves administradas por el cliente.

De forma predeterminada, las claves que se utilizan para cifrar las credenciales en el hipervisor son AWS claves propias. AWS Backup utiliza estas claves para cifrar automáticamente las credenciales del hipervisor. No puede ver, administrar ni usar las claves AWS propias, ni puede auditar su uso. Sin embargo, no tiene que realizar ninguna acción ni cambiar ningún programa para proteger las claves que cifran sus datos. Para obtener más información, consulta las claves AWS propias en la [Guía para AWS KMS desarrolladores](#).

Como alternativa, las credenciales se pueden cifrar mediante claves administradas por el cliente. AWS Backup admite el uso de claves simétricas administradas por el cliente que usted crea, posee y administra para realizar el cifrado. Como usted tiene el control total de este cifrado, puede realizar tareas como las siguientes:

- Establecer y mantener políticas de claves
- Establecer y mantener concesiones y políticas de IAM
- Habilitar y deshabilitar políticas de claves
- Rotar el material criptográfico

- Adición de etiquetas
- Crear alias de clave
- Programar la eliminación de claves

Cuando utilizas una clave gestionada por el cliente, AWS Backup valida si tu rol tiene permiso para descifrar con esta clave (antes de ejecutar una tarea de copia de seguridad o restauración). Debe agregar la acción `kms:Decrypt` al rol utilizado para iniciar un trabajo de copia de seguridad o restauración.

Como la acción `kms:Decrypt` no se puede agregar al rol de copia de seguridad predeterminado, debe usar un rol distinto del rol de copia de seguridad predeterminado para usar las claves administradas por el cliente.

Para obtener más información, consulte las [claves administradas por el cliente](#) en la Guía para desarrolladores de AWS Key Management Service .

Concesión necesaria cuando se utilizan claves administradas por el cliente

AWS KMS requiere una [concesión](#) para utilizar la clave gestionada por el cliente. Al importar una [configuración de hipervisor](#) cifrada con una clave gestionada por el cliente, AWS Backup crea una concesión en tu nombre enviando una [CreateGrant](#) solicitud a AWS KMS. AWS Backup utiliza las concesiones para acceder a una clave de KMS en una cuenta de cliente.

Puede revocar el acceso a la concesión o eliminar el acceso a AWS Backup la clave gestionada por el cliente en cualquier momento. Si lo hace, todas las puertas de enlace asociadas al hipervisor ya no podrán acceder al nombre de usuario y la contraseña del hipervisor cifrados por la clave administrada por el cliente, lo que afectará a sus trabajos de copia de seguridad y restauración. En concreto, los trabajos de copia de seguridad y restauración que realice en las máquinas virtuales de este hipervisor darán como resultado un error.

La puerta de enlace de la copia de seguridad utiliza la operación `RetireGrant` para eliminar una concesión cuando se elimina un hipervisor.

Monitorización de claves de cifrado

Cuando utilizas una clave gestionada por el AWS KMS cliente con tus AWS Backup recursos, puedes utilizar [AWS CloudTrailAmazon CloudWatch Logs](#) para realizar un seguimiento de las solicitudes que se AWS Backup envían a AWS KMS.

Busca AWS CloudTrail eventos con los siguientes "eventName" campos para supervisar AWS KMS las operaciones solicitadas para acceder AWS Backup a los datos cifrados por tu clave gestionada por el cliente:

- "eventName": "CreateGrant"
- "eventName": "Decrypt"
- "eventName": "Encrypt"
- "eventName": "DescribeKey"

Gestión de identidad y acceso en AWS Backup

El acceso a AWS Backup requiere credenciales. Estas credenciales deben tener permisos para acceder a los recursos de AWS como, por ejemplo, una base de datos de Amazon DynamoDB o un sistema de archivos de Amazon EFS. Además, los puntos de recuperación creados AWS Backup por algunos servicios AWS Backup compatibles no se pueden eliminar mediante el servicio de origen (como Amazon EFS). Puede eliminar esos puntos de recuperación utilizando AWS Backup.

En las siguientes secciones se proporcionan detalles sobre cómo utilizar [AWS Identity and Access Management \(IAM\)](#) y cómo ayudar AWS Backup a proteger el acceso a los recursos.

Warning

AWS Backup utiliza la misma función de IAM que eligió al asignar recursos para administrar el ciclo de vida de sus puntos de recuperación. Si elimina o modifica esa función, AWS Backup no podrá administrar el ciclo de vida de los puntos de recuperación. Cuando esto ocurra, intentará utilizar un rol vinculado al servicio para administrar su ciclo de vida. En un pequeño porcentaje de casos, es posible que esto tampoco funcione y deje puntos de recuperación EXPIRED en el almacenamiento, lo que podría generar costos no deseados. Para eliminar los puntos de recuperación EXPIRED, elimínelos manualmente mediante el procedimiento descrito en [Eliminación de copias de seguridad](#).

Temas

- [Autenticación](#)
- [Control de acceso](#)
- [Roles de servicio de IAM](#)

- [Políticas administradas para AWS Backup](#)
- [Cómo utilizar roles vinculados a servicios de AWS Backup](#)
- [Prevención de la sustitución confusa entre servicios](#)

Autenticación

El acceso a AWS Backup los AWS servicios de los que está realizando una copia de seguridad requieren credenciales que AWS pueda utilizar para autenticar sus solicitudes. Puede acceder AWS con cualquiera de los siguientes tipos de identidades:

- Cuenta de AWS usuario root: cuando te registras AWS, proporcionas una dirección de correo electrónico y una contraseña asociadas a tu AWS cuenta. Se trata de su usuario raíz de la Cuenta de AWS . Sus credenciales proporcionan acceso completo a todos tus AWS recursos.

Important

Por razones de seguridad, recomendamos que utilice el usuario raíz solo para crear un administrador. El administrador es un usuario de IAM con permisos completos en su Cuenta de AWS. Entonces, podrá utilizar este usuario administrador para crear otros roles y usuarios de IAM con permisos limitados. Para obtener más información, consulte [Prácticas recomendadas de IAM](#) y [Creación del primer grupo y usuario de administrador de IAM](#) en la Guía del usuario de IAM.

- Usuario de IAM: un [usuario de IAM](#) es una identidad dentro de su Cuenta de AWS que tiene permisos personalizados específicos (por ejemplo, permisos para crear un almacén de copias de seguridad para almacenar sus copias de seguridad). [Puede utilizar un nombre de usuario y una contraseña de IAM para iniciar sesión en AWS páginas web seguras Consola de administración de AWS, como los foros de AWS debate o el AWS Support Centro.](#)

Además de un nombre de usuario y una contraseña, también puede generar [claves de acceso](#) para cada usuario. Puede utilizar estas teclas al acceder a AWS los servicios mediante programación, ya sea mediante [una de las varias opciones SDKs](#) o mediante la ([AWS Command Line InterfaceAWS CLI](#)). El SDK y las herramientas de la AWS CLI usan claves de acceso para firmar criptográficamente la solicitud. Si no utiliza las herramientas de AWS , debe firmar usted mismo la solicitud. Para obtener más información acerca de la autenticación de solicitudes, consulte [Proceso de firma Signature Version 4](#) en la Referencia general de AWS.

- Rol de IAM: un [rol de IAM](#) es otra identidad de IAM que puede crear en la cuenta y que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una persona determinada. Una función de IAM le permite obtener claves de acceso temporales que se pueden utilizar para acceder a los AWS servicios y recursos. Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:
 - Acceso de usuario federado: en lugar de crear un usuario de IAM, puede utilizar identidades de usuario preexistentes Directory Service, del directorio de usuarios de su empresa o de un proveedor de identidades web. A estas identidades se les llama usuarios federados. AWS asigna una función a un usuario federado cuando se solicita acceso a través de un [proveedor de identidad](#). Para obtener más información acerca de los usuarios federados, consulte [Usuarios federados y roles](#) en la Guía del usuario de IAM.
 - Administración multicuenta: puedes usar un rol de IAM en tu cuenta para conceder otros Cuenta de AWS permisos a fin de administrar los recursos de tu cuenta. Para ver un ejemplo, consulte el [tutorial: Delegar el acceso a todos los roles de Cuentas de AWS IAM](#) en la Guía del usuario de IAM.
 - AWS acceso al servicio: puede utilizar un rol de IAM en su cuenta para conceder a un AWS servicio permisos de acceso a los recursos de su cuenta. Para obtener más información, consulte [Creación de un rol para delegar permisos a un AWS servicio](#) en la Guía del usuario de IAM.
 - Aplicaciones que se ejecutan en Amazon Elastic Compute Cloud (Amazon EC2): puedes usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia de Amazon y que realizan solicitudes de AWS API. Es preferible hacerlo de este modo a almacenar claves de acceso dentro de la instancia EC2. Para asignar un AWS rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se encuentran en ejecución en la instancia EC2 obtener credenciales temporales. Para obtener más información, consulte [Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en EC2 instancias de Amazon](#) en la Guía del usuario de IAM.

Control de acceso

Puedes tener credenciales válidas para autenticar tus solicitudes, pero a menos que tengas los permisos adecuados, no podrás acceder a AWS Backup recursos como las bóvedas de respaldo. Tampoco puedes hacer copias de seguridad de AWS recursos como los volúmenes de Amazon Elastic Block Store (Amazon EBS).

Cada AWS recurso es propiedad de un Cuenta de AWS, y los permisos para crear o acceder a un recurso se rigen por las políticas de permisos. Un administrador de cuentas puede adjuntar políticas de permisos a las identidades AWS Identity and Access Management (IAM) (es decir, usuarios, grupos y roles). Y algunos servicios también permiten asociar políticas de permisos a recursos.

Un administrador de la cuenta (o usuario administrador) es un usuario con permisos de administrador. Para obtener más información, consulte [Prácticas recomendadas de IAM](#) en la Guía del usuario de IAM.

Cuando concede permisos, decide quién debe obtener los permisos, para qué recursos se obtienen permisos y qué acciones específicas desea permitir en esos recursos.

En las secciones siguientes se explica cómo funcionan las políticas de acceso y como puede utilizarlas para proteger sus copias de seguridad.

Temas

- [Recursos y operaciones](#)
- [Propiedad del recurso](#)
- [Especificación de los elementos de las políticas: acciones, efectos y entidades principales](#)
- [Especificación de las condiciones de una política](#)
- [Permisos de la API: referencia de acciones, recursos y condiciones](#)
- [Permisos de copia de etiquetas](#)
- [Políticas de acceso](#)

Recursos y operaciones

Un recurso es un objeto que existe dentro de un servicio. AWS Backup los recursos incluyen planes de respaldo, bóvedas de respaldo y copias de seguridad. Backup es un término general que se refiere a los distintos tipos de recursos de respaldo que existen en AWS. Por ejemplo, las instantáneas de Amazon EBS, las instantáneas de Amazon Relational Database Service (Amazon RDS) y las copias de seguridad de Amazon DynamoDB son todos tipos de recursos de copia de seguridad.

En AWS Backup, las copias de seguridad también se denominan puntos de recuperación. Cuando lo usa AWS Backup, también trabaja con los recursos de otros AWS servicios que intenta proteger, como los volúmenes de Amazon EBS o las tablas de DynamoDB. Estos recursos tienen nombres de recursos de Amazon (ARNs) exclusivos asociados a ellos. ARNs identifique los AWS recursos de

forma exclusiva. Debe tener un ARN cuando sea preciso especificar un recurso de forma inequívoca para todo AWS, como en las políticas de IAM o las llamadas a la API.

En la siguiente tabla se muestran recursos, subrecursos, formato de ARN y un ID único de ejemplo.

AWS Backup recurso ARNs

Tipo de recurso	Formato de ARN	ID único de ejemplo
Plan de copias de seguridad	arn:aws:backup: <i>region</i> : <i>account-id</i> :backup-plan:*	
Almacén de copias de seguridad	arn:aws:backup: <i>region</i> : <i>account-id</i> :backup-vault:*	
Punto de recuperación para Amazon EBS	arn:aws:ec2: <i>region</i> :::snapshot/*	snapshot/snap-05f426fd8kdjb4224
Punto de recuperación para EC2 imágenes de Amazon	arn:aws:ec2: <i>region</i> :::image/ami-*	image/ami-1a2b3e4f5e6f7g890
Punto de recuperación para Amazon RDS	arn:aws:rds: <i>region</i> : <i>account-id</i> :snapshot:awsbackup:*	awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453
Punto de recuperación para Aurora	arn:aws:rds: <i>region</i> : <i>account-id</i> :cluster-snapshot:awsbackup:*	awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453
Punto de recuperación para Aurora DSQL	arn:aws-partition:backup: <i>region</i> : <i>account-id</i> :recovery-	arn:aws:backup:us-east-1:012345678901:recovery-point:8

Tipo de recurso	Formato de ARN	ID único de ejemplo
	point: <i>recovery-point-id</i>	a92c3f1-b475-4d9e-95e6-7c138f2d4b0a
Punto de recuperación para Storage Gateway	arn:aws:e c2: <i>region</i> ::snapshot/ *	snapshot/snap-0d40 e49137e31d9e0
Punto de recuperación para DynamoDB sin Copia de seguridad avanzada de DynamoDB	arn:aws:d ynamodb: <i>region:account-id</i> :table/*/backup/*	table/MyDynamoDBTa ble/backup/0154708 7347000-c8b6kdk3
Punto de recuperación para DynamoDB con Copia de seguridad avanzada de DynamoDB habilitado	arn:aws:b ackup: <i>region:account-id</i> :recovery-point:*	12a34a56-7bb8-901c- cd23-4567d8e9ef01
Punto de recuperación para Amazon EFS	arn:aws:b ackup: <i>region:account-id</i> :recovery-point:*	d99699e7-e183-477e- bfcd-ccb1c6e5455e
Punto de recuperación para Amazon FSx	arn:aws:f sx: <i>region:account-id</i> :backup/backup-*	backup/backup-1a20 e49137e31d9e0
Punto de recuperación para máquina virtual	arn:aws:b ackup: <i>region:account-id</i> :recovery-point:*	1801234a-5b6b-7dc8 -8032-836f7ffc623b
Punto de recuperación para la copia de seguridad continua de Amazon S3	arn:aws:b ackup: <i>region:account-id</i> :recovery-point:*	<i>amzn-s3-demo-bucke</i> <i>t</i> -5ec207d0
Punto de recuperación para la copia de seguridad periódica de S3	arn:aws:b ackup: <i>region:account-id</i> :recovery-point:*	<i>amzn-s3-demo-bucke</i> <i>t</i> -20211231900000-5e c207d0

Tipo de recurso	Formato de ARN	ID único de ejemplo
Punto de recuperación para Amazon DocumentDB	arn:aws:rds: <i>region</i> : <i>account-id</i> :cluster-snapshot:awsbackup:*	awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012
Punto de recuperación para Neptune	arn:aws:rds: <i>region</i> : <i>account-id</i> :cluster-snapshot:awsbackup:*	awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012
Punto de recuperación para Amazon Redshift	arn:aws:redshift: <i>region</i> : <i>account-id</i> :snapshot: <i>resource</i> /awsbackup:*	awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012
Punto de recuperación para Amazon Redshift sin servidor	arn:aws:redshift-serverless: <i>region</i> : <i>account-id</i> :snapshot: <i>resource</i> /awsbackup:*	awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012
Punto de recuperación para Amazon Timestream	arn:aws:backup: <i>region</i> : <i>account-id</i> :recovery-point:*	recovery-point:1a2b3cde-f405-6789-012g-3456hi789012_beta
Punto de recuperación para la AWS CloudFormation plantilla	arn:aws:backup: <i>region</i> : <i>account-id</i> :recovery-point:*	recovery-point:1a2b3cde-f405-6789-012g-3456hi789012
Punto de recuperación para la base de datos SAP HANA en la EC2 instancia de Amazon	arn:aws:backup: <i>region</i> : <i>account-id</i> :recovery-point:*	recovery-point:1a2b3cde-f405-6789-012g-3456hi789012

Todos los recursos que permiten una AWS Backup gestión completa tienen puntos de recuperación en ese formato `arn:aws:backup:region:account-id::recovery-point:*`, lo que facilita la aplicación de políticas de permisos para proteger esos puntos de recuperación. Para ver qué recursos admiten la AWS Backup administración completa, consulte esa sección de la [Disponibilidad de características por recurso](#) tabla.

AWS Backup proporciona un conjunto de operaciones para trabajar con AWS Backup los recursos. Para ver la lista de las operaciones disponibles, consulte AWS Backup [Acciones](#).

Propiedad del recurso

Cuenta de AWS Es propietario de los recursos que se crean en la cuenta, independientemente de quién los haya creado. En concreto, el propietario del recurso es el Cuenta de AWS de la [entidad principal](#) (es decir, el usuario Cuenta de AWS raíz, un usuario de IAM o un rol de IAM) que autentica la solicitud de creación de recursos. Los siguientes ejemplos ilustran cómo funciona:

- Si utiliza sus credenciales de usuario Cuenta de AWS raíz Cuenta de AWS para crear un almacén de respaldo, será el Cuenta de AWS propietario del almacén.
- Si crea un usuario de IAM en su cuenta Cuenta de AWS y le concede permisos para crear una bóveda de copias de seguridad, el usuario podrá crear una bóveda de copias de seguridad. Sin embargo, la cuenta de AWS a la que pertenece el usuario será la propietaria del recurso del almacén de copias de seguridad.
- Si crea una función de IAM Cuenta de AWS con permisos para crear una bóveda de copias de seguridad, cualquier persona que pueda asumir esa función podrá crear una bóveda. Usted Cuenta de AWS, al que pertenece el rol, es propietario del recurso de la bóveda de respaldo.

Especificación de los elementos de las políticas: acciones, efectos y entidades principales

Para cada AWS Backup recurso (consulte [Recursos y operaciones](#)), el servicio define un conjunto de operaciones de API (consulte [Acciones](#)). Para conceder permisos para estas operaciones de la API, AWS Backup define un conjunto de acciones que puede especificar en una política. Para realizar una operación API pueden ser necesarios permisos para más de una acción.

A continuación se indican los elementos más básicos de la política:

- **Recurso:** en una política, se usa un nombre de recurso de Amazon (ARN) para identificar el recurso al que se aplica la política. Para obtener más información, consulte [Recursos y operaciones](#).
- **Acción:** utilice palabras clave de acción para identificar las operaciones del recurso que desea permitir o denegar.
- **Efecto:** especifique el efecto que se producirá cuando el usuario solicite la acción específica; puede ser permitir o denegar. Si no concede acceso de forma explícita (permitir) a un recurso, 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).

Para obtener más información sobre la sintaxis y descripciones de las políticas de IAM, consulte [IAM JSON Policy Reference](#) (Referencia de la política JSON de IAM) en la Guía del usuario de IAM.

Para ver una tabla que muestra todas las acciones de la AWS Backup API, consulte [Permisos de la API: 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 la 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 sobre cómo especificar condiciones en un lenguaje de política, consulte [Condición](#) en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición globales, consulte [Claves de contexto de condición globales de AWS](#) en la Guía del usuario de IAM.

AWS Backup define su propio conjunto de claves de condición. Para ver una lista de claves de AWS Backup condición, consulte las [claves de condición AWS Backup](#) en la Referencia de autorización de servicio.

Permisos de la API: referencia de acciones, recursos y condiciones

Cuando configure [Control de acceso](#) y escriba una política de permisos que se pueda asociar a una identidad de IAM (políticas basadas en identidad), puede utilizar la siguiente lista como referencia. La incluye cada operación de la AWS Backup API, las acciones correspondientes para las que puedes conceder permisos para realizar la acción y el AWS recurso para el que puedes conceder los permisos. 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. Si el campo `Resource` está en blanco, puede usar el comodín (*) para incluir todos los recursos.

Puedes usar claves AWS de condición generales en tus AWS Backup políticas 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.

¹ Utiliza la política de acceso a almacenes existentes.

² Consulte el [AWS Backup recurso ARNs](#) punto de recuperación específico del recurso. ARNs

³ `StartRestoreJob` también debe tener el par clave-valor en los metadatos del recurso. Para obtener los metadatos del recurso, llame a la API `GetRecoveryPointRestoreMetadata`.

Para obtener más información, consulte [Acciones, recursos y claves de condición de AWS Backup](#) en la Referencia de autorizaciones de servicio.

Permisos de copia de etiquetas

Cuando AWS Backup realiza un trabajo de copia de seguridad o copia, intenta copiar las etiquetas del recurso de origen (o del punto de recuperación en el caso de una copia) al punto de recuperación.

Note

AWS Backup no copia las etiquetas de forma nativa durante los trabajos de restauración. Para ver una arquitectura basada en eventos que copie las etiquetas durante los trabajos de restauración, consulte [Cómo conservar las etiquetas de recursos en AWS Backup](#) los trabajos de restauración.

Durante un trabajo de copia de seguridad o copia, AWS Backup agrega las etiquetas que especifique en su plan de copia de seguridad (o plan de copia o copia de seguridad bajo demanda) con las

etiquetas del recurso de origen. Sin embargo, AWS impone un límite de 50 etiquetas por recurso, que AWS Backup no se puede superar. Cuando un trabajo de copia de seguridad o copia agrega etiquetas del plan y del recurso de origen, podría detectar más de 50 etiquetas en total, no podrá completar el trabajo y dará como resultado un error. Esto es coherente con las mejores AWS prácticas de etiquetado en general.

- Su recurso tiene más de 50 etiquetas después de agregar las etiquetas de los trabajos de respaldo con las etiquetas de los recursos de origen. AWS admite hasta 50 etiquetas por recurso.
- La función de IAM que le proporciona AWS Backup carece de permisos para leer las etiquetas de origen o establecer las etiquetas de destino. Para obtener más información y un ejemplo de las políticas del rol de IAM, consulte [Políticas administradas](#).

Puede utilizar su plan de copia de seguridad (se han añadido etiquetas a los puntos de recuperación) para crear etiquetas que contradigan a las etiquetas del recurso de origen. Cuando ambas estén en conflicto, prevalecerán las etiquetas del plan de copia de seguridad. Utilice esta técnica si prefiere no copiar el valor de una etiqueta del recurso de origen. Especifique la misma clave de etiqueta, pero con un valor diferente o vacío, utilizando su plan de copia de seguridad.

Permisos necesarios para asignar etiquetas a copias de seguridad

Tipo de recurso	Permiso necesario
Sistema de archivos de Amazon EFS	<code>elasticfilesystem:DescribeTags</code>
Sistema de FSx archivos Amazon	<code>fsx:ListTagsForResource</code>
Base de datos de Amazon RDS y clúster de Amazon Aurora	<code>rds:AddTagsToResource</code> <code>rds:ListTagsForResource</code>
Volumen de Storage Gateway	<code>storagegateway:ListTagsForResource</code>
EC2 Instancia de Amazon y volumen de Amazon EBS	<code>EC2:CreateTags</code> <code>EC2:DescribeTags</code>

DynamoDB no admite la asignación de etiquetas a las copias de seguridad a menos que habilite primero la [Copia de seguridad avanzada de DynamoDB](#).

Cuando una EC2 copia de seguridad de Amazon crea un punto de recuperación de imágenes y un conjunto de instantáneas, AWS Backup copia las etiquetas en la AMI resultante. AWS Backup también copia las etiquetas de los volúmenes asociados a la EC2 instancia de Amazon en las instantáneas resultantes.

Políticas de acceso

Una política de permisos describe quién tiene acceso a qué. Las políticas que se asocian a una identidad de IAM se denominan políticas basadas en identidades (o políticas de IAM). Las políticas adjuntas a un recurso se denominan políticas basadas en recursos. AWS Backup admite tanto las políticas basadas en la identidad como las políticas basadas en los recursos.

Note

En esta sección se analiza el uso de la IAM en el contexto de. AWS Backup No se proporciona información detallada sobre el servicio de IAM. Para ver la documentación completa de IAM, consulte [¿Qué es IAM?](#) en la Guía del usuario de IAM. Para obtener más información acerca de la sintaxis y las descripciones de las políticas de IAM, consulte [Referencia de políticas JSON de IAM](#) en la Guía del usuario de IAM.

Políticas basadas en identidades (políticas de IAM)

Las políticas basadas en identidad son políticas que puede asociar a identidades de IAM, como usuarios o roles. Por ejemplo, puede definir una política que permita a un usuario ver los AWS recursos y realizar copias de seguridad, pero que le impida restaurar las copias de seguridad.

Para obtener más información sobre usuarios, grupos, roles y permisos, consulte [Identidades \(usuarios, grupos y roles\)](#) en la Guía del usuario de IAM.

Para obtener más información acerca de cómo utilizar políticas de IAM para controlar el acceso a las copias de seguridad, consulte [Políticas administradas para AWS Backup](#).

Políticas basadas en recursos

AWS Backup admite políticas de acceso basadas en recursos para las bóvedas de respaldo. De este modo, puede definir una política de acceso que puede controlar qué usuarios tienen qué tipo de acceso a cualquiera de las copias de seguridad organizadas en un almacén de copias de seguridad. Las políticas de acceso basadas en recursos para almacenes de copia de seguridad ofrecen una manera fácil de controlar el acceso a sus copias de seguridad.

Las políticas de acceso a la bóveda de Backup controlan el acceso de los usuarios cuando usted lo usa AWS Backup APIs. También se puede acceder a algunos tipos de copias de seguridad, como las instantáneas de Amazon Elastic Block Store (Amazon EBS) y Amazon Relational Database Service (Amazon RDS), mediante esos servicios». APIs Puede crear políticas de acceso independientes en IAM que controlen el acceso a ellas para controlar completamente el acceso a APIs las copias de seguridad.

Para obtener información sobre cómo crear una política de acceso para almacenes de copias de seguridad, consulte [Políticas de acceso a almacenes](#).

Roles de servicio de IAM

Una función AWS Identity and Access Management (IAM) es similar a la de un usuario, ya que es una AWS identidad con políticas de permisos que determinan lo que la identidad puede y no puede hacer en ella. AWS No obstante, en lugar de asociarse exclusivamente a una persona, la intención es que cualquier usuario pueda asumir un rol que necesite. Una función de servicio es una función que asume un AWS servicio para realizar acciones en su nombre. Como servicio que realiza las operaciones de copia de seguridad en su nombre, AWS Backup requiere transferirle un rol que debe adoptar al realizar las operaciones de copia de seguridad en su nombre. Para obtener más información acerca de los roles de IAM, consulte [Roles de IAM](#) en la guía del usuario de IAM.

El rol al que se transfiera AWS Backup debe tener una política de IAM con los permisos que le permitan realizar las acciones asociadas AWS Backup a las operaciones de copia de seguridad, como crear, restaurar o hacer caducar las copias de seguridad. Se requieren permisos diferentes para cada uno de los AWS servicios compatibles AWS Backup . El rol también debe AWS Backup figurar como entidad de confianza, lo que AWS Backup permite asumirlo.

Al asignar recursos a un plan de copia de seguridad, o si realiza una copia de seguridad, copia o restauración bajo demanda, debe asignar una función de servicio que tenga acceso para realizar las operaciones subyacentes en los recursos especificados. AWS Backup utiliza esta función para crear, etiquetar y eliminar recursos de su cuenta.

Usa AWS roles para controlar el acceso a las copias de seguridad

Puede utilizar roles para controlar el acceso a sus copias de seguridad definiendo roles muy acotados y especificando quién puede transferir dicho rol a AWS Backup. Por ejemplo, puede crear un rol que solo conceda permisos para realizar copias de seguridad de las bases de datos de Amazon Relational Database Service (Amazon RDS) y que solo conceda permiso a los propietarios de las bases de datos de Amazon RDS para transferir ese rol. AWS Backup AWS

Backup proporciona varias políticas administradas predefinidas para cada uno de los servicios compatibles. Puede asociar estas políticas administradas a los roles que cree. Esto facilita la creación de funciones específicas del servicio que tengan los permisos correctos que AWS Backup se necesitan.

Para obtener más información sobre las políticas AWS administradas para AWS Backup, consulte.

[Políticas administradas para AWS Backup](#)

Función de servicio predeterminada para AWS Backup

Cuando utilice la AWS Backup consola por primera vez, puede optar por AWS Backup crear un rol de servicio predeterminado para usted. Este rol tiene los permisos AWS Backup necesarios para crear y restaurar copias de seguridad en su nombre.

Note

El rol predeterminado se crea automáticamente si usa la Consola de administración de AWS. Puede crear el rol predeterminado con AWS Command Line Interface (AWS CLI), pero debe hacerlo manualmente.

Si prefiere usar roles personalizados, como roles independientes para diferentes tipos de recursos, también puede hacerlo y transferir sus roles personalizados a AWS Backup. Para ver ejemplos de roles que permiten la copia de seguridad y la restauración para tipos de recursos individuales, consulte la tabla [Políticas administradas por el cliente](#).

El Nombre del rol de servicio predeterminado es `AWSBackupDefaultServiceRole`. Este rol de servicio contiene dos políticas administradas [AWSBackupServiceRolePolicyForBackup](#) y [AWSBackupServiceRolePolicyForRestores](#).

`AWSBackupServiceRolePolicyForBackup` incluye una política de IAM que otorga AWS Backup permisos para describir el recurso del que se está haciendo la copia de seguridad y la posibilidad de crear, eliminar, describir o añadir etiquetas a una copia de seguridad, independientemente de la AWS KMS clave con la que esté cifrada.

`AWSBackupServiceRolePolicyForRestores` incluye una política de IAM que concede AWS Backup permisos para crear, eliminar o describir el nuevo recurso que se está creando a partir de una copia de seguridad, independientemente de la AWS KMS clave con la que esté cifrado. También incluye permisos para etiquetar el recurso recién creado.

Para restaurar una EC2 instancia de Amazon, debes lanzar una nueva instancia.

Creación del rol de servicio en la consola

Las acciones específicas que realice en la AWS Backup consola crean el rol de servicio AWS Backup predeterminado.

Para crear el rol de servicio AWS Backup predeterminado en su AWS cuenta

1. Abre la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. Para crear el rol de su cuenta, asigne recursos a un plan de copia de seguridad o cree una copia de seguridad bajo demanda.
 - a. Cree un plan de copia de seguridad y asigne recursos a la copia de seguridad. Consulte [Create a backup plan](#).
 - b. Como alternativa, cree una copia de seguridad bajo demanda. Consulte [Creación de una copia de seguridad bajo demanda](#).
3. Siga estos pasos para comprobar que ha creado `AWSBakupDefaultServiceRole` en su cuenta:
 - a. Espere unos minutos. Para obtener más información, consulte [Los cambios que realizo no están siempre visibles inmediatamente](#) en la Guía del usuario de AWS Identity and Access Management.
 - b. Inicie sesión en la consola de IAM Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/iam/>
 - c. En el menú de navegación izquierdo, elija Roles.
 - d. En la barra de búsqueda, escriba `AWSBakupDefaultServiceRole`. Si existe esta selección, ha creado el rol AWS Backup predeterminado y ha completado este procedimiento.
 - e. Si `AWSBakupDefaultServiceRole` sigue sin aparecer, agregue los siguientes permisos al usuario de IAM o al rol de IAM que utilice para acceder a la consola.

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  

```

```

    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::*:role/service-role/
AWSBackupDefaultServiceRole"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:ListRoles"
      ],
      "Resource": "*"
    }
  ]
}

```

Para las regiones de China, **aws** sustitúyalo por **aws-cn**. Para AWS GovCloud (US) las regiones, **aws** sustitúyalo por **aws-us-gov**.

- f. Si no puede agregar permisos a su usuario de IAM o rol de IAM, pida a su administrador que cree manualmente un rol con un nombre distinto de `AWSBackupDefaultServiceRole` y asocie ese rol a estas políticas administradas:

- `AWSBackupServiceRolePolicyForBackup`
- `AWSBackupServiceRolePolicyForRestores`

Políticas administradas para AWS Backup

Las políticas administradas son políticas independientes basadas en la identidad que puede adjuntar a varios usuarios, grupos y funciones de su organización. Cuenta de AWS Al asociar una política a una entidad principal, concederá a la entidad los permisos que están definidos en la política.

AWS las políticas gestionadas las crea y administra. AWS No puede cambiar los permisos definidos en las políticas AWS gestionadas. 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.

Las políticas administradas por el cliente te proporcionan controles detallados para configurar el acceso a las copias de seguridad. AWS Backup Por ejemplo, puede utilizarlas para dar acceso al administrador de copias de seguridad de su base de datos a las copias de seguridad de Amazon RDS, pero no a las de Amazon EFS.

Para obtener más información, consulte [Políticas administradas](#) en la Guía del usuario de IAM.

AWS políticas gestionadas

AWS Backup proporciona las siguientes políticas AWS administradas para casos de uso comunes. Estas políticas facilitan la definición de los permisos adecuados y controlan el acceso a sus copias de seguridad. Existen dos tipos de políticas administradas. Un tipo está diseñado para asignarlo a usuarios para controlar su acceso a AWS Backup. El otro tipo de política administrada está diseñado para asociarlo a los roles que transfiere a AWS Backup. En la siguiente tabla se muestran todas las políticas administradas que AWS Backup proporciona y describe la forma en que se definen. Encontrará estas políticas administradas en la sección Políticas de la consola de IAM.

Políticas

- [AWSBackupAuditAccess](#)
- [AWSBackupDataTransferAccess](#)
- [AWSBackupFullAccess](#)
- [AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync](#)
- [AWSBackupGuardDutyRolePolicyForScans](#)
- [AWSBackupOperatorAccess](#)
- [AWSBackupOrganizationAdminAccess](#)
- [AWSBackupRestoreAccessForSAPHANA](#)
- [AWSBackupSearchOperatorAccess](#)
- [AWSBackupServiceLinkedRolePolicyForBackup](#)
- [AWSBackupServiceLinkedRolePolicyForBackupTest](#)
- [AWSBackupServiceRolePolicyForBackup](#)
- [AWSBackupServiceRolePolicyForItemRestores](#)
- [AWSBackupServiceRolePolicyForIndexing](#)
- [AWSBackupServiceRolePolicyForRestores](#)
- [AWSBackupServiceRolePolicyForS3 Backup](#)
- [AWSBackupServiceRolePolicyForS3Restore](#)

- [AWSBackupServiceRolePolicyForScans](#)
- [AWSServiceRolePolicyForBackupReports](#)
- [AWSServiceRolePolicyForBackupRestoreTesting](#)

AWSBackupAuditAccess

Esta política otorga permisos a los usuarios para crear controles y marcos que definan sus expectativas de AWS Backup recursos y actividades, y para auditar AWS Backup los recursos y las actividades comparándolos con los controles y marcos definidos. Esta política otorga permisos AWS Config y servicios similares para describir las expectativas de los usuarios y realizar las auditorías.

Esta política también otorga permisos para entregar informes de auditoría a Amazon S3 y servicios similares, y permite a los usuarios buscar y abrir sus informes de auditoría.

Para ver los permisos de esta política, consulte [AWSBackupAuditAccess](#) en la Referencia de la política administrada de AWS .

AWSBackupDataTransferAccess

Esta política proporciona permisos para la transferencia de datos del plano de AWS Backup almacenamiento APIs, lo que permite al agente AWS Backint completar la transferencia de los datos de respaldo con el plano AWS Backup de almacenamiento. Puede adjuntar esta política a las funciones que asumen las EC2 instancias de Amazon que ejecutan SAP HANA con el agente Backint.

Para ver los permisos de esta política, consulte [AWSBackupDataTransferAccess](#) en la Referencia de la política administrada de AWS .

AWSBackupFullAccess

El administrador de copias de seguridad tiene pleno acceso a AWS Backup las operaciones, incluida la creación o edición de planes de copia de seguridad, la asignación de AWS recursos a los planes de copia de seguridad y la restauración de las copias de seguridad. Los administradores de las copias de seguridad tienen la responsabilidad de determinar e imponer medidas de conformidad definiendo planes de copias de seguridad que cumplan los requisitos empresariales y normativos de su organización. Los administradores de Backup también se aseguran de que AWS los recursos de su organización estén asignados al plan adecuado.

Para ver los permisos de esta política, consulte [AWSBackupFullAccess](#) en la Referencia de la política administrada de AWS .

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

Esta política otorga permiso a Backup Gateway para sincronizar los metadatos de las máquinas virtuales en su nombre.

Para ver los permisos de esta política, consulte

[AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync](#) en la Referencia de la política administrada de AWS .

AWSBackupGuardDutyRolePolicyForScans

Esta política debe añadirse a una nueva función de digitalización que conceda GuardDuty permiso a Amazon para leer y escanear tus copias de seguridad. Deberás adjuntar esta función de escaneo a tu plan de copias de seguridad dentro de la configuración de escaneo o protección contra malware. Cuando AWS Backup inicia un análisis, transfiere esta función de análisis a Amazon GuardDuty.

Para ver los permisos de esta política, consulte [AWSBackupGuardDutyRolePolicyForScans](#) en la Referencia de la política administrada de AWS .

AWSBackupOperatorAccess

Los operadores de copia de seguridad son usuarios que son responsables de garantizar una correcta copia de seguridad de los recursos de los que son responsables. Los operadores de backup tienen permisos para asignar AWS recursos a los planes de backup que crea el administrador de backup. También tienen permisos para crear copias de seguridad bajo demanda de sus AWS recursos y para configurar el período de retención de las copias de seguridad bajo demanda. Los operadores de copia de seguridad no tienen permisos para crear o editar los planes de copias de seguridad o eliminar copias de seguridad programadas después de que se hayan creado. Los operadores de copia de seguridad puede restaurar las copias de seguridad. Puede limitar los tipos de recursos que un operador de copia de seguridad puede asignar a un plan de copia de seguridad o restaurar desde una copia de seguridad. Para ello, se permite que solo se transfieran determinadas funciones de servicio AWS Backup que tengan permisos para un tipo de recurso determinado.

Para ver los permisos de esta política, consulte [AWSBackupOperatorAccess](#) en la Referencia de la política administrada de AWS .

AWSBackupOrganizationAdminAccess

El administrador de la organización tiene pleno acceso a AWS Organizations las operaciones, incluidas la creación, edición o eliminación de políticas de copia de seguridad, la asignación de

políticas de copia de seguridad a las cuentas y unidades organizativas y la supervisión de las actividades de copia de seguridad dentro de la organización. Los administradores de la organización son responsables de proteger las cuentas de la misma mediante la definición y asignación de políticas de copia de seguridad que cumplan con los requisitos reglamentarios y empresariales de su organización.

Para ver los permisos de esta política, consulte [AWSBackupOrganizationAdminAccess](#) en la Referencia de la política administrada de AWS .

AWSBackupRestoreAccessForSAPHANA

Esta política otorga AWS Backup permiso para restaurar una copia de seguridad de SAP HANA en Amazon EC2.

Para ver los permisos de esta política, consulte [AWSBackupRestoreAccessForSAPHANA](#) en la referencia de políticas AWS gestionadas.

AWSBackupSearchOperatorAccess

El rol de operador de búsqueda tiene acceso para crear índices de copias de seguridad y búsquedas en los metadatos de copia de seguridad indexados.

Esta política contiene los permisos necesarios para estas funciones.

Para ver los permisos de esta política, consulte [AWSBackupSearchOperatorAccess](#) en la Referencia de la política administrada de AWS .

AWSBackupServiceLinkedRolePolicyForBackup

Esta política se adjunta a la función vinculada al servicio denominada AWSServiceRoleforBackup para permitir llamar AWS Backup a los AWS servicios en su nombre para gestionar sus copias de seguridad. Para obtener más información, consulte [the section called “Copia de seguridad y copia”](#).

Para ver los permisos de esta política, consulta la Referencia [AWSBackupServiceLinkedRolePolicyforBackup](#) de políticas AWS gestionadas.

AWSBackupServiceLinkedRolePolicyForBackupTest

Para ver los permisos de esta política, consulte [AWSBackupServiceLinkedRolePolicyForBackupTest](#) en la Referencia de la política administrada de AWS .

AWSBackupServiceRolePolicyForBackup

Proporciona AWS Backup permisos para crear copias de seguridad de todos los tipos de recursos compatibles en su nombre.

Para ver los permisos de esta política, consulte [AWSBackupServiceRolePolicyForBackup](#) en la Referencia de la política administrada de AWS .

AWSBackupServiceRolePolicyForItemRestores

Descripción

Esta política otorga a los usuarios permisos para restaurar archivos y elementos individuales de una instantánea (punto de recuperación de copias de seguridad periódicas) en un bucket de Amazon S3 nuevo o existente o en un volumen de Amazon EBS nuevo. Estos permisos incluyen: permisos de lectura en Amazon EBS para instantáneas administradas mediante permisos de lectura/escritura de AWS Backup en buckets de Amazon S3, y permisos de generación y descripción para claves de AWS KMS .

Uso de esta política

Puede asociar `AWSBackupServiceRolePolicyForItemRestores` a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política AWS gestionada
- Fecha y hora de creación: 21 de noviembre de 2024 a las 22:45 UTC
- Ediciones: primera instancia
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForItemRestores`

Versión de la política: v1 (predeterminada)

La versión de esta política define los permisos para la política. Cuando el usuario o el rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud o no.

Documento de política de JSON:

AWSBackupServiceRolePolicyForItemRestores JSON

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EBSReadOnlyPermissions",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSnapshots"
      ],
      "Resource": "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid": "KMSReadOnlyPermissions",
      "Effect": "Allow",
      "Action": "kms:DescribeKey",
      "Resource": "*"
    },
    {
      "Sid": "EBSDirectReadAPIPermissions",
      "Effect": "Allow",
      "Action": [
        "ebs:ListSnapshotBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource": "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid": "S3ReadonlyPermissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket"
      ],
      "Resource": "arn:aws:s3::*:"
    },
    {
      "Sid": "S3PermissionsForFileLevelRestore",
      "Effect": "Allow",
      "Action": [
```

```

        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts"
    ],
    "Resource": "arn:aws:s3:::*/*"
  },
  {
    "Sid": "KMSSDataKeyForS3AndEC2Permissions",
    "Effect": "Allow",
    "Action": [
      "kms:Decrypt",
      "kms:GenerateDataKey"
    ],
    "Resource": "arn:aws:kms:*:key/*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "ec2.*.amazonaws.com",
          "s3.*.amazonaws.com"
        ]
      }
    }
  }
]
}

```

AWSBackupServiceRolePolicyForIndexing

Descripción

Esta política otorga a los usuarios permisos para indexar las instantáneas, también conocidas como puntos de recuperación periódicos. Estos permisos incluyen: permisos de lectura en Amazon EBS para instantáneas gestionados mediante permisos de AWS Backup lectura/escritura en buckets de Amazon S3, y permisos de generación y descripción para claves. AWS KMS

Uso de esta política

Puede asociar `AWSBackupServiceRolePolicyForIndexing` a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política AWS gestionada

- Ediciones: primera instancia
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForIndexing`

Versión de la política: v1 (predeterminada)

La versión de esta política define los permisos para la política. Cuando el usuario o el rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud o no.

Documento de política de JSON:

AWSBackupServiceRolePolicyForIndexing JSON

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EBSReadOnlyPermissions",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSnapshots"
      ],
      "Resource": "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid": "KMSReadOnlyPermissions",
      "Effect": "Allow",
      "Action": "kms:DescribeKey",
      "Resource": "*"
    },
    {
      "Sid": "EBSDirectReadAPIPermissions",
      "Effect": "Allow",
      "Action": [
        "ebs:ListSnapshotBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource": "arn:aws:ec2:*::snapshot/*"
    }
  ],
}
```

```

    {
      "Sid": "KMSTDataKeyForEC2Permissions",
      "Effect": "Allow",
      "Action": "kms:Decrypt",
      "Resource": "arn:aws:kms:*:*:key/*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}

```

AWSBackupServiceRolePolicyForRestores

Proporciona AWS Backup permisos para restaurar copias de seguridad de todos los tipos de recursos compatibles en su nombre.

Para ver los permisos de esta política, consulte [AWSBackupServiceRolePolicyForRestores](#) en la Referencia de la política administrada de AWS .

En el EC2 caso de las restauraciones, también debes incluir los siguientes permisos para lanzar la EC2 instancia:

AWSBackupServiceRolePolicyForS3 Backup

Esta política contiene los permisos necesarios AWS Backup para realizar copias de seguridad de cualquier bucket de S3. Esto incluye el acceso a todos los objetos de un depósito y a cualquier AWS KMS clave asociada.

Para ver los permisos de esta política, consulte [AWSBackupServiceRolePolicyForS3Backup](#) en la Referencia de políticas AWS gestionadas.

AWSBackupServiceRolePolicyForS3Restore

Esta política contiene los permisos necesarios AWS Backup para restaurar una copia de seguridad de S3 en un bucket. Esto incluye los permisos de lectura y escritura en los depósitos y el uso de cualquier AWS KMS clave en relación con las operaciones de S3.

Para ver los permisos de esta política, consulte [AWSBackupServiceRolePolicyForS3Restore](#) en la Referencia de políticas AWS gestionadas.

AWSBackupServiceRolePolicyForScans

La política debe estar asociada a la función de IAM que utilice en la selección de recursos de su plan de respaldo. Esta función otorga permiso a AWS Backup para iniciar escaneos en Amazon GuardDuty.

Para ver los permisos de esta política, consulte [AWSBackupServiceRolePolicyForScans](#) en la Referencia de la política administrada de AWS .

AWSServiceRolePolicyForBackupReports

AWS Backup usa esta política para el rol [AWSServiceRoleForBackupReports](#) vinculado al servicio. Esta función vinculada al servicio otorga AWS Backup permisos para supervisar e informar sobre la conformidad de la configuración, los trabajos y los recursos de las copias de seguridad con sus marcos.

Para ver los permisos de esta política, consulte [AWSServiceRolePolicyForBackupReports](#) en la Referencia de la política administrada de AWS .

AWSServiceRolePolicyForBackupRestoreTesting

Para ver los permisos de esta política, consulte [AWSServiceRolePolicyForBackupRestoreTesting](#) en la Referencia de la política administrada de AWS .

Políticas administradas por el cliente

En las siguientes secciones se describen los permisos de copia de seguridad y restauración recomendados para los AWS servicios y las aplicaciones de terceros compatibles con ellos. AWS Backup Puede utilizar las políticas AWS gestionadas existentes como modelo al crear sus propios documentos de políticas y, a continuación, personalizarlos para restringir aún más el acceso a sus AWS recursos.

Important

Cuando utilices funciones de IAM personalizadas AWS Backup, además de los permisos, debes incluir permisos específicos para cada recurso. AWS Backup Por ejemplo, al llamar a `backup:ListTags` en un recurso de Amazon RDS, su rol de IAM personalizada también

debe incluir el permiso `rds:ListTagsForResource`. Si bien estos permisos están incluidos en la función de AWS Backup servicio predeterminada, deben añadirse de forma explícita a las políticas administradas por el cliente. Los permisos de recursos subyacentes necesarios dependen del AWS servicio y la operación específicos que se estén realizando.

Amazon Aurora

Copia de seguridad

Comience con las siguientes afirmaciones de [AWSBackupServiceRolePolicyForBackup](#):

- `DynamoDBBackupPermissions`
- `RDSClusterModifyPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`
- `KMSPermissions`

Restaurar

Comience con la `RDSPermissions` declaración de [AWSBackupServiceRolePolicyForRestores](#).

Amazon Aurora DSQL

Copia de seguridad

Comience con las siguientes declaraciones de [AWSBackupServiceRolePolicyForBackup](#):

- `DSQLBackupPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`
- `KMSPermissions`

Restaurar

Comience con la `DSQLRestorePermissions` declaración de [AWSBackupServiceRolePolicyForRestores](#).

Amazon DynamoDB

Copia de seguridad

Comience con las siguientes declaraciones de [AWSBackupServiceRolePolicyForBackup](#):

- `DynamoDBPermissions`
- `DynamoDBBackupResourcePermissions`
- `DynamodbBackupPermissions`
- `KMSDynamoDBPermissions`

Restaurar

Comience con las siguientes declaraciones de [AWSBackupServiceRolePolicyForRestores](#):

- `DynamoDBPermissions`
- `DynamoDBBackupResourcePermissions`
- `DynamoDBRestorePermissions`
- `KMSPermissions`

Amazon EBS

Copia de seguridad

Comience con las siguientes declaraciones de [AWSBackupServiceRolePolicyForBackup](#):

- `EBSResourcePermissions`
- `EBSTagAndDeletePermissions`
- `EBSCopyPermissions`
- `EBSSnapshotTierPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`

Restaurar

Comience con la `EBSPermissions` declaración de [AWSBackupServiceRolePolicyForRestores](#).

Agregue la siguiente instrucción.

```
{
  "Effect": "Allow",
  "Action": [
    "ec2:DescribeSnapshots",
    "ec2:DescribeVolumes"
  ],
  "Resource": "*"
},
```

Amazon EC2

Copia de seguridad

Comience con las siguientes declaraciones de [AWSBackupServiceRolePolicyForBackup](#):

- EBSCopyPermissions
- EC2CopyPermissions
- EC2Permissions
- EC2TagPermissions
- EC2ModifyPermissions
- EBSResourcePermissions
- GetResourcesPermissions
- BackupVaultPermissions

Restaurar

Comience con las siguientes declaraciones de [AWSBackupServiceRolePolicyForRestores](#):

- EBSPermissions
- EC2DescribePermissions
- EC2RunInstancesPermissions
- EC2TerminateInstancesPermissions
- EC2CreateTagsPermissions

Agregue la siguiente instrucción.

```
{
  "Effect": "Allow",
  "Action": "iam:PassRole",
  "Resource": "arn:aws:iam::account-id:role/role-name"
},
```

role-name Sustitúyalo EC2 por el nombre del rol del perfil de la instancia que se adjuntará a la EC2 instancia restaurada. No se trata de la función de AWS Backup servicio, sino de la función de IAM que proporciona permisos a las aplicaciones que se ejecutan en la EC2 instancia.

Amazon EFS

Copia de seguridad

Comience con las siguientes afirmaciones de [AWSBackupServiceRolePolicyForBackup](#):

- EFSPermissions
- GetResourcesPermissions
- BackupVaultPermissions

Restaurar

Comience con la EFSPermissions declaración de [AWSBackupServiceRolePolicyForRestores](#).

Amazon FSx

Copia de seguridad

Comience con las siguientes declaraciones de [AWSBackupServiceRolePolicyForBackup](#):

- FsxBackupPermissions
- FsxCreateBackupPermissions
- FsxPermissions
- FsxVolumePermissions
- FsxListTagsPermissions
- FsxDeletePermissions
- FsxResourcePermissions
- KMSPermissions

Restaurar

Comience con las siguientes declaraciones de [AWSBackupServiceRolePolicyForRestores](#):

- FsxPermissions
- FsxTagPermissions
- FsxBackupPermissions
- FsxDeletePermissions
- FsxDescribePermissions
- FsxVolumeTagPermissions
- FsxBackupTagPermissions
- FsxVolumePermissions
- DSPermissions
- KMSDescribePermissions

Amazon Neptune

Copia de seguridad

Comience con las siguientes declaraciones de [AWSBackupServiceRolePolicyForBackup](#):

- DynamoDBBackupPermissions
- RDSClusterModifyPermissions
- GetResourcesPermissions
- BackupVaultPermissions
- KMSPermissions

Restaurar

Comience con la RDSPermissions declaración de [AWSBackupServiceRolePolicyForRestores](#).

Amazon RDS

Copia de seguridad

Comience con las siguientes declaraciones de [AWSBackupServiceRolePolicyForBackup](#):

- `DynamoDBBackupPermissions`
- `RDSBackupPermissions`
- `RDSClusterModifyPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`
- `KMSPermissions`

Restaurar

Comience con la `RDSPermissions` declaración de [AWSBackupServiceRolePolicyForRestores](#).

Amazon S3

Copia de seguridad

Comience con [AWSBackupServiceRolePolicyForS3Backup](#).

Añada las instrucciones `BackupVaultPermissions` y `BackupVaultCopyPermissions` si necesita copiar las copias de seguridad a una cuenta diferente.

Restaurar

[Comience con S3Restore AWSBackupServiceRolePolicyFor](#).

AWS Storage Gateway

Copia de seguridad

Comience con las siguientes declaraciones de: [AWSBackupServiceRolePolicyForBackup](#)

- `StorageGatewayPermissions`
- `EBSTagAndDeletePermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`

Agregue la siguiente instrucción.

```
{
  "Effect": "Allow",
  "Action": [
    "ec2:DescribeSnapshots"
  ],
  "Resource": "*"
},
```

Restaurar

Comience con las siguientes declaraciones de [AWSBackupServiceRolePolicyForRestores](#):

- StorageGatewayVolumePermissions
- StorageGatewayGatewayPermissions
- StorageGatewayListPermissions

Máquina virtual

Copia de seguridad

Comience con la BackupGatewayBackupPermissions declaración de [AWSBackupServiceRolePolicyForBackup](#).

Restaurar

Comience con la GatewayRestorePermissions declaración de [AWSBackupServiceRolePolicyForRestores](#).

Copia de seguridad cifrada

Para restaurar una copia de seguridad cifrada, siga uno de estos procedimientos:

- Añada su función a la lista de permitidos para la política AWS KMS clave
- Añada las siguientes instrucciones [AWSBackupServiceRolePolicyForRestores](#) a su función de IAM para las restauraciones:
 - KMSDescribePermissions
 - KMSPermissions
 - KMSCreateGrantPermissions

Actualizaciones de políticas para AWS Backup

Consulta los detalles sobre las actualizaciones de las políticas AWS gestionadas AWS Backup desde que este servicio comenzó a realizar el seguimiento de estos cambios.

Cambio	Descripción	Fecha
AWSBackupGuardDutyRolePolicyForScans : política nueva	AWS Backup se ha añadido una nueva política AWS gestionada que permite a Amazon GuardDuty leer y escanear las copias de seguridad de los clientes. AWS Backup transfiere una función con esta política GuardDuty al iniciar las operaciones <code>StartMalwareScan</code>. Esto es necesario para proporcionar todos los permisos necesarios para los escaneos de malware en los puntos de recuperación de los recursos de Amazon EC2, Amazon EBS y Amazon S3. Para obtener más información, consulte la política AWSBackupGuardDutyRolePolicyForScans gestionada.	19 de noviembre de 2025
AWSBackupServiceRolePolicyForScans : política nueva	AWS Backup se agregó una nueva política AWS administrada que permite AWS Backup iniciar escaneos de malware en los puntos de recuperación.	19 de noviembre de 2025

Cambio	Descripción	Fecha
	Esto es necesario para proporcionar todos los permisos necesarios para los escaneos de malware en los puntos de recuperación de los recursos de Amazon EC2, Amazon EBS y Amazon S3. Para obtener más información, consulte la política AWSBackupServiceRolePolicyForScans gestionada.	
AWSBackupFullAccess : actualización de una política actual	Se agregó malware-protection.guardduty.amazonaws.com a IamPassRolePermissions, lo cual es necesario para iniciar los trabajos de escaneo de malware.	19 de noviembre de 2025
AWSBackupOperatorAccess : actualización de una política actual	AWS Backup agregó los siguientes permisos a esta política: • De malware-protection.guardduty.amazonaws.com a IamPassRolePermissions • backup:StartScanJob Estos permisos son necesarios para iniciar las tareas de análisis de malware.	19 de noviembre de 2025

Cambio	Descripción	Fecha
AWSBackupFullAccess: actualización de una política actual	AWS Backup agregó los siguientes permisos a esta política: • <code>eks:ListClusters</code> • <code>eks:ListTagsForResource</code> • <code>eks:DescribeCluster</code> Estos permisos permiten AWS Backup realizar copias de seguridad y restaurar los clústeres de Amazon EKS.	10 de noviembre de 2025
AWSBackupOperatorAccess: actualización de una política actual	AWS Backup agregó los siguientes permisos a esta política: • <code>eks:ListClusters</code> • <code>eks:ListTagsForResource</code> • <code>eks:DescribeCluster</code> Estos permisos permiten AWS Backup realizar copias de seguridad y restaurar los clústeres de Amazon EKS.	10 de noviembre de 2025

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForBackup : actualización de una política actual	AWS Backup agregó los siguientes permisos a esta política: • <code>eks:ListClusters</code> • <code>eks:ListTagsForResource</code> • <code>eks:DescribeCluster</code> • <code>eks:ListAddons</code> • <code>eks:DescribeAddon</code> • <code>eks:ListNodegroups</code> • <code>eks:DescribeNodegroup</code> • <code>eks:ListPodIdentityAssociations</code> • <code>eks:DescribePodIdentityAssociation</code> • <code>eks:ListAccessEntries</code> • <code>eks:DescribeAccessEntry</code> • <code>eks:ListAssociatedAccessPolicies</code> • <code>eks:ListFargateProfiles</code> • <code>eks:DescribeFargateProfile</code> • <code>ec2:DescribeLaunchTemplateVersions</code> • <code>eks:CreateAccessEntry</code>	10 de noviembre de 2025

Cambio	Descripción	Fecha
	• <code>eks:AssociateAccessPolicy</code> • <code>eks:DisassociateAccessPolicy</code> Estos permisos permiten AWS Backup crear copias de seguridad de los clústeres de Amazon EKS y sus recursos asociados en nombre de los clientes.	

Cambio	Descripción	Fecha
AWSBackupServiceLinkedRolePolicyForBackup : actualización de una política actual	AWS Backup agregó los siguientes permisos a esta política: • <code>eks:ListClusters</code> • <code>eks:ListTagsForResource</code> • <code>eks:DescribeCluster</code> • <code>eks:ListAddons</code> • <code>eks:DescribeAddon</code> • <code>eks:ListNodegroups</code> • <code>eks:DescribeNodegroup</code> • <code>eks:ListPodIdentityAssociations</code> • <code>eks:DescribePodIdentityAssociation</code> • <code>eks:ListAccessEntries</code> • <code>eks:DescribeAccessEntry</code> • <code>eks:ListAssociatedAccessPolicies</code> • <code>eks:ListFargateProfiles</code> • <code>eks:DescribeFargateProfile</code> • <code>ec2:DescribeLaunchTemplateVersions</code> • <code>eks:CreateAccessEntry</code>	10 de noviembre de 2025

Cambio	Descripción	Fecha
	• <code>eks:AssociateAccessPolicy</code> • <code>eks:DisassociateAccessPolicy</code> Estos permisos permiten AWS Backup crear copias de seguridad de los clústeres de Amazon EKS y sus recursos asociados en nombre de los clientes.	

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForRestores : actualización de una política actual	AWS Backup agregó los siguientes permisos a esta política: • <code>eks:CreateCluster</code> • <code>eks:DescribeCluster</code> • <code>eks:CreateAccessEntry</code> • <code>eks:DescribeAccessEntry</code> • <code>eks:AssociateAccessPolicy</code> • <code>eks:ListAssociatedAccessPolicies</code> • <code>eks:CreateAddon</code> • <code>eks:DescribeAddon</code> • <code>eks:CreateNodegroup</code> • <code>eks:DescribeNodegroup</code> • <code>eks:CreateFargateProfile</code> • <code>eks:DescribeFargateProfile</code> • <code>eks:CreatePodIdentityAssociation</code> • <code>eks:DescribePodIdentityAssociation</code> • <code>eks:TagResource</code> • <code>eks:DisassociateAccessPolicy</code> • <code>iam:PassRole</code>	10 de noviembre de 2025

Cambio	Descripción	Fecha
	• <code>ec2:DescribeLaunchTemplateVersions</code> • <code>ec2:DescribeSubnets</code> • <code>ec2:RunInstances</code> • <code>ec2:CreateTags</code> • <code>iam:GetRole</code> • <code>iam:ListAttachedRolePolicies</code> • <code>backup:StartRestoreJob</code> • <code>backup:ListRestoreJobs</code> • <code>backup:ListRecoveryPointsByBackupVault</code> • <code>backup:DescribeRestoreJob</code> Estos permisos permiten AWS Backup realizar operaciones de restauración para los clústeres de Amazon EKS y sus recursos asociados en nombre de los clientes.	

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForBackup : actualización de una política actual	AWS Backup agregó el siguiente permiso a esta política: • <code>organizations:ListDelegatedAdministrators</code> Este permiso AWS Backup permite sincronizar la información del administrador delegado con Organizations para las funciones de administración multicuenta.	9 de septiembre de 2025

Cambio	Descripción	Fecha
AWSBackupGuardDutyRolePolicyForScans : política nueva	AWS Backup se ha añadido una nueva política AWS gestionada que permite a Amazon GuardDuty leer y escanear las copias de seguridad de los clientes. AWS Backup transfiere una función con esta política GuardDuty al iniciar las operaciones <code>StartMalwareScan</code>. Esto es necesario para proporcionar todos los permisos necesarios para los escaneos de malware en los puntos de recuperación de los recursos de Amazon EC2, Amazon EBS y Amazon S3. Para obtener más información, consulte la política AWSBackupGuardDutyRolePolicyForScans gestionada.	24 de noviembre de 2025

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForScans : política nueva	AWS Backup se agregó una nueva política AWS administrada que permite AWS Backup iniciar escaneos de malware en los puntos de recuperación. Esto es necesario para proporcionar todos los permisos necesarios para los escaneos de malware en los puntos de recuperación de los recursos de Amazon EC2, Amazon EBS y Amazon S3. Para obtener más información, consulte la política AWSBackupServiceRolePolicyForScans gestionada.	24 de noviembre de 2025

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForRestores : actualización de una política actual	AWS Backup agregó los siguientes permisos a esta política: • <code>dsql:UpdateCluster</code> • <code>dsql:AddPeerCluster</code> • <code>dsql:RemovePeerCluster</code> • <code>dsql:GetCluster</code> Estos permisos son necesarios AWS Backup para realizar operaciones de restauración orquestadas en varias regiones de los recursos de DSQL en nombre de los clientes.	17 de julio de 2025

Cambio	Descripción	Fecha
AWSBackupFullAccess: actualización de una política actual	AWS Backup agregó los siguientes permisos a esta política: • <code>mpa:GetApprovalTeam</code> • <code>mpa:ListApprovalTeams</code> • <code>mpa:StartSession</code> • <code>mpa:CancelSession</code> • <code>mpa:GetSession</code> • <code>mpa:ListSessions</code> Estos permisos son necesarios para la AWS Backup integración con AWS Account Management , por AWS Organizations lo que los clientes tienen la opción de obtener la aprobación multipartita (MPA) como parte de sus bóvedas cerradas de forma lógica.	17 de junio de 2025

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForRestores — Actualización de una política existente:	AWS Backup agregó los siguientes permisos a esta política: • <code>ec2:DescribeRouteTables</code> • <code>ec2:CreateTags</code> Estos permisos son necesarios para que los clientes puedan restaurar las instantáneas de las zonas de disponibilidad múltiple (Multi-AZ) de Amazon FSx for OpenZFS a través de ellas. AWS Backup	27 de mayo de 2025
AWSBackupFullAccess : actualización de una política actual	AWS Backup agregó los siguientes permisos a esta política: • <code>dsql:GetCluster</code> • <code>dsql:ListClusters</code> • <code>dsql:ListTagsForResource</code> Estos permisos permiten AWS Backup realizar copias de seguridad y restaurar los recursos de Amazon Aurora DSQL.	21 de mayo de 2025

Cambio	Descripción	Fecha
AWSBackupOperatorAccess: actualización de una política actual	AWS Backup agregó los siguientes permisos a esta política: • <code>dsql:GetCluster</code> • <code>dsql:ListClusters</code> • <code>dsql:ListTagsForResource</code> Estos permisos permiten AWS Backup realizar copias de seguridad y restaurar los recursos de Amazon Aurora DSQL.	21 de mayo de 2025

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForBackup : actualización de una política actual	AWS Backup agregó los siguientes permisos a esta política: • kms:Decrypt • kms:ReEncryptTo • kms:ReEncryptFrom • dsql:StartBackupJob • dsql:GetBackupJob • dsql:StopBackupJob • dsql:GetCluster • dsql:ListClusters • dsql:ListTagsForResource Estos permisos permiten AWS Backup crear, eliminar, recuperar y gestionar instantáneas de Amazon Aurora DSQL en nombre de los clientes.	21 de mayo de 2025

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForRestores : actualización de una política actual	AWS Backup agregó los siguientes permisos a esta política: • <code>ec2:DescribeRouteTables</code> • <code>ec2:CreateTags</code> • <code>dsql:StartRestoreJob</code> • <code>dsql:GetRestoreJob</code> • <code>dsql:StopRestoreJob</code> • <code>dsql:TagResource</code> • <code>dsql>CreateCluster</code> • <code>dsql:PutMultiRegionProperties</code> • <code>dsql:PutWitnessRegion</code> • <code>kms:DescribeKey</code> Estos permisos permiten AWS Backup crear, eliminar, recuperar, cifrar, descifrar y gestionar instantáneas de Amazon Aurora DSQL en nombre de los clientes.	21 de mayo de 2025

Cambio	Descripción	Fecha
AWSBackupServiceLinkedRolePolicyForBackup : actualización de una política actual	AWS Backup agregó los siguientes permisos a esta política: • <code>dsql:ListClusters</code> • <code>dsql:ListTagsForResource</code> Estos permisos permiten administrar AWS Backup las copias de seguridad de Aurora DSQL a intervalos especificados por el cliente.	21 de mayo de 2025

Cambio	Descripción	Fecha
AWSBackupFullAccess: actualización de una política actual	AWS Backup agregó los siguientes permisos a esta política: • <code>aws:CalledVia</code> • <code>redshift-serverless>DeleteSnapshot</code> • <code>redshift-serverless:GetNamespace</code> • <code>redshift-serverless:GetSnapshot</code> • <code>redshift-serverless:GetWorkgroup</code> • <code>redshift-serverless:ListNamespaces</code> • <code>redshift-serverless:ListSnapshots</code> • <code>redshift-serverless:ListWorkgroups</code> Estos permisos son necesarios para que los clientes designados tengan acceso total a las copias de seguridad de Amazon Redshift sin servidor, incluidos los permisos de lectura necesarios y la posibilidad de eliminar los puntos de recuperación de Amazon Redshift sin servidor (copias de seguridad de instantáneas).	31 de marzo de 2025

Cambio	Descripción	Fecha
AWSBackupOperatorAccess: actualización de una política actual	AWS Backup agregó los siguientes permisos a esta política: • <code>redshift-serverless:GetNamespace</code> • <code>redshift-serverless:GetSnapshot</code> • <code>redshift-serverless:GetWorkgroup</code> • <code>redshift-serverless:ListNamespaces</code> • <code>redshift-serverless:ListSnapshots</code> • <code>redshift-serverless:ListWorkgroups</code> Estos permisos son necesarios para que los clientes designados dispongan de todos los permisos de copia de seguridad necesarios para Amazon Redshift sin servidor, incluidos los permisos de lectura necesarios.	31 de marzo de 2025

Cambio	Descripción	Fecha
AWSBackupServiceLinkedRolePolicyForBackup : actualización de una política actual	AWS Backup agregó los siguientes permisos a esta política: • <code>redshift-serverless:DeleteSnapshot</code> • <code>redshift-serverless:GetNamespace</code> • <code>redshift-serverless:GetSnapshot</code> • <code>redshift-serverless:GetWorkgroup</code> • <code>redshift-serverless:ListNamespaces</code> • <code>redshift-serverless:ListSnapshots</code> • <code>redshift-serverless:ListTagsForResource</code> • <code>redshift-serverless:ListWorkgroups</code> Estos permisos son necesarios para AWS Backup para gestionar las instantáneas de Amazon Redshift Serverless en los intervalos especificados por el cliente.	31 de marzo de 2025

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForBackup : actualización de una política actual	AWS Backup agregó los siguientes permisos a esta política: • <code>redshift-serverless:CreateSnapshot</code> • <code>redshift-serverless>DeleteSnapshot</code> con la condición de permitir que solo se eliminen las instantáneas con la etiqueta <code>"aws:backup:source-resource"</code> . • <code>redshift-serverless:GetNamespace</code> • <code>redshift-serverless:GetSnapshot</code> • <code>redshift-serverless:ListNamespaces</code> • <code>redshift-serverless:ListSnapshots</code> • <code>redshift-serverless:ListTagsForResource</code> • <code>redshift-serverless:TagResource</code> Estos permisos son necesarios para poder crear AWS Backup , eliminar, recuperar y gestionar instantáneas de Amazon Redshift Serverless en nombre de los clientes.	31 de marzo de 2025

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForRestores : actualización de una política actual	AWS Backup agregó los siguientes permisos a esta política: • <code>redshift-serverless:GetNamespace</code> • <code>redshift-serverless:GetTableRestoreStatus</code> • <code>redshift-serverless:RestoreTableFromSnapshot</code> Estos permisos son necesarios para poder AWS Backup restaurar las instantáneas de Amazon Redshift y Amazon Redshift Serverless en nombre del cliente.	31 de marzo de 2025
AWSBackupSearchOperatorAccess — Se agregó una nueva política administrada AWS	AWS Backup agregó la política AWSBackupSearchOperatorAccess AWS gestionada.	27 de febrero de 2025

Cambio	Descripción	Fecha
AWSBackupServiceLinkedRolePolicyForBackup : actualización de una política actual	AWS Backup agregó el permiso <code>rds:AddTagsToResource</code> para admitir la copia de seguridad multicuenta de instantáneas multiusuario de Amazon RDS. Este permiso es necesario para completar las operaciones cuando un cliente decide crear una copia entre cuentas de una instantánea de RDS de varios inquilinos.	8 de enero de 2025
AWSBackupServiceRolePolicyForRestores : actualización de una política actual	AWS Backup agregó los permisos <code>rds:CreateTenantDatabase</code> y <code>rds>DeleteTenantDatabase</code> a esta política para respaldar el proceso de restauración de los recursos de Amazon RDS. Estos permisos son necesarios para completar las operaciones del cliente a fin de restaurar las instantáneas de varios inquilinos.	8 de enero de 2025
AWSBackupServiceRolePolicyForItemRestores — Se ha añadido una nueva política AWS gestionada	AWS Backup agregó la política <code>AWSBackupServiceRolePolicyForItemRestores</code> AWS gestionada.	26 de noviembre de 2024

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForIndexing — Se ha añadido una nueva política AWS gestionada	AWS Backup agregó la política AWSBackupServiceRolePolicyForIndexing AWS gestionada.	26 de noviembre de 2024
AWSBackupServiceRolePolicyForBackup : actualización de una política actual	AWS Backup ha añadido el permiso backup:TagResource a esta política. El permiso es necesario para obtener permisos de etiquetado durante la creación de un punto de recuperación.	17 de mayo de 2024
AWSBackupServiceRolePolicyForS3Backup : actualización a una política existente	AWS Backup permiso añadido backup:TagResource a esta política. El permiso es necesario para obtener permisos de etiquetado durante la creación de un punto de recuperación.	17 de mayo de 2024
AWSBackupServiceLinkedRolePolicyForBackup : actualización de una política actual	AWS Backup permiso agregado backup:TagResource a esta política. El permiso es necesario para obtener permisos de etiquetado durante la creación de un punto de recuperación.	17 de mayo de 2024

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForBackup : actualización de una política actual	Agregó el permiso <code>rds:DeleteDBInstanceAutomatedBackups</code>. Este permiso es necesario para AWS Backup para admitir copias de seguridad continuas y point-in-time-restore de instancias de Amazon RDS.	1 de mayo de 2024
AWSBackupFullAccess : actualización de una política actual	AWS Backup actualizó el nombre de recurso de Amazon (ARN) con el permiso <code>storagegateway:ListVolumes</code> de <code>arn:aws:storagegateway:*:*:gateway/*</code> a para adaptarse a un cambio * en el modelo de API de Storage Gateway.	1 de mayo de 2024
AWSBackupOperatorAccess : actualización de una política actual	AWS Backup actualizó el nombre de recurso de Amazon (ARN) con el permiso <code>storagegateway:ListVolumes</code> de <code>arn:aws:storagegateway:*:*:gateway/*</code> a para adaptarse a un cambio * en el modelo de API de Storage Gateway.	1 de mayo de 2024

Cambio	Descripción	Fecha
AWSServiceRolePolicyForBackupRestoreTesting : actualización de una política actual	Se agregaron los siguientes permisos para describir y enumerar los puntos de recuperación y los recursos protegidos a fin de llevar a cabo los planes de pruebas de restauración: <code>backup:DescribeRecoveryPoint</code> , <code>backup:DescribeProtectedResource</code> , <code>backup:ListProtectedResources</code> y <code>backup:ListRecoveryPointsByResource</code> . Se agregó el permiso <code>ec2:DescribeSnapshotTierStatus</code> para admitir el almacenamiento en niveles de archivo de Amazon EBS. Se agregó el permiso <code>rds:DescribeDBClusterAutomatedBackups</code> para admitir las copias de seguridad continuas de Amazon Aurora. Se agregaron los siguientes permisos para admitir las pruebas de restauración de las copias de seguridad de Amazon Redshift: <code>redshift:DescribeClusters</code> y	14 de febrero de 2024

Cambio	Descripción	Fecha
	<code>redshift:DeleteCluster</code> . Se agregó el permiso <code>timestream:DeleteTable</code> para admitir las pruebas de restauración de las copias de seguridad de Amazon Timestream.	
AWSBackupServiceRolePolicyForRestores: actualización de una política actual	Agregó los permisos <code>ec2:DescribeSnapshotTierStatus</code> y <code>ec2:RestoreSnapshotTier</code> . Estos permisos son necesarios para que los usuarios tengan la opción de restaurar los recursos de Amazon EBS almacenados AWS Backup desde el almacenamiento de archivos. En el EC2 caso de las restauraciones, también debe incluir los permisos, tal y como se muestra en la siguiente declaración de política, para lanzar la EC2 instancia:	27 de noviembre de 2023

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForBackup : actualización de una política actual	Agregó los permisos <code>ec2:DescribeSnapshotsTierStatus</code> y <code>ec2:ModifySnapshotTier</code> para habilitar una opción de almacenamiento adicional para que los recursos de Amazon EBS en copia de seguridad realicen la transición al nivel de almacenamiento de archivo. Estos permisos son necesarios para que los usuarios tengan la opción de realizar la transición de los recursos de Amazon EBS almacenados en AWS Backup al almacenamiento de archivos.	27 de noviembre de 2023

Cambio	Descripción	Fecha
AWSBackupServiceLinkedRolePolicyForBackup : actualización de una política actual	Agregó los permisos <code>ec2:DescribeSnapshotTierStatus</code> y <code>ec2:ModifySnapshotTier</code> para habilitar una opción de almacenamiento adicional para que los recursos de Amazon EBS en copia de seguridad realicen la transición al nivel de almacenamiento de archivo. Estos permisos son necesarios para que los usuarios tengan la opción de realizar la transición de los recursos de Amazon EBS almacenados AWS Backup al almacenamiento de archivos. Se agregaron los permisos <code>rds:DescribeDBClusterSnapshots</code> y <code>rds:RestoreDBClusterToPointInTime</code>, que son necesarios para la PITR (point-in-time restauraciones) de los clústeres de Aurora.	

Cambio	Descripción	Fecha
<u>AWSServiceRolePolicyForBackupRestoreTesting</u> : política nueva	Proporciona los permisos necesarios para realizar las pruebas de restauración. Los permisos incluyen las acciones <code>list</code> , <code>read</code> , and <code>write</code> para que los siguientes servicios se incluyan en las pruebas de restauración: Aurora, DocumentDB, DynamoDB, Amazon EBS, Amazon, EC2 Amazon EFS, para Lustre, para Windows File Server FSx , para ONTAP FSx , para FSx OpenZFS FSx , Amazon Neptune, Amazon RDS y Amazon S3.	27 de noviembre de 2023
<u>AWSBackupFullAccess</u> : actualización de una política actual	Se ha añadido <code>restore-testing.backup.amazonaws.com</code> a <code>IamPassRolePermissions</code> y <code>IamCreateServiceLinkedRolePermissions</code> . Esta adición es necesaria para realizar pruebas de restauración en nombre de los clientes. AWS Backup	27 de noviembre de 2023

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForRestores : actualización de una política actual	Se agregaron los permisos <code>rds:DescribeDBClusterSnapshots</code> y <code>rds:RestoreDBClusterToPointInTime</code> , que son necesarios para la PITR (point-in-time restauraciones) de los clústeres de Aurora.	6 de septiembre de 2023
AWSBackupFullAccess : actualización de una política actual	Se agregó el permiso <code>rds:DescribeDBClusterAutomatedBackups</code> , que es necesario para realizar copias de seguridad y point-in-time restauración continuas de los clústeres de Aurora.	6 de septiembre de 2023
AWSBackupOperatorAccess : actualización de una política actual	Se agregó el permiso <code>rds:DescribeDBClusterAutomatedBackups</code> , que es necesario para realizar copias de seguridad y point-in-time restauración continuas de los clústeres de Aurora.	6 de septiembre de 2023

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForBackup : actualización de una política actual	Agregó el permiso <code>rds:DescribeDBClusterAutomatedBackups</code>. Este permiso es necesario para AWS Backup admitir la copia de seguridad y la point-in-time restauración continuas de los clústeres de Aurora. Se agregó el permiso <code>rds:DeleteDBClusterAutomatedBackups</code> para permitir que el AWS Backup ciclo de vida elimine y desasocie los puntos de recuperación continua de Amazon Aurora cuando finalice un período de retención. Este permiso es necesario para que el punto de recuperación de Aurora evite la transición a un estado EXPIRED. Agregó el permiso <code>rds:ModifyDBCluster</code> que permite a AWS Backup interactuar con los clústeres de Aurora. Esta adición permite a los usuarios habilitar o deshabilitar las copias de seguridad continuas en función de las configuraciones deseadas.	6 de septiembre de 2023

Cambio	Descripción	Fecha
AWSBackupFullAccess: actualización de una política actual	Agregó la acción <code>ram:GetResourceShareAssociations</code> para conceder al usuario permiso para obtener asociaciones de recursos compartidos para un nuevo tipo de almacén.	8 de agosto de 2023
AWSBackupOperatorAccess: actualización de una política actual	Agregó la acción <code>ram:GetResourceShareAssociations</code> para conceder al usuario permiso para obtener asociaciones de recursos compartidos para un nuevo tipo de almacén.	8 de agosto de 2023
AWSBackupServiceRolePolicyForS3Backup: actualización a una política existente	Agregó el permiso <code>s3:PutInventoryConfiguration</code> para mejorar las velocidades de rendimiento de las copias de seguridad mediante el uso de un inventario de buckets.	1 de agosto de 2023

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForRestores : actualización de una política actual	Agregó las siguientes acciones para conceder al usuario permisos para agregar etiquetas para restaurar los recursos: <code>storagegateway:AddTagsToResource</code> , <code>elasticfilesystem:TagResource</code> , <code>ec2:CreateTags</code> solo para <code>ec2:CreateAction</code> que incluye <code>RunInstances</code> o <code>CreateVolume</code> , <code>fsx:TagResource</code> y <code>cloudformation:TagResource</code> .	22 de mayo de 2023
AWSBackupAuditAccess : actualización de una política actual	Se reemplazó la selección de recursos de la API <code>config:DescribeComplianceByConfigRule</code> por un recurso comodín para facilitar al usuario la selección de los recursos.	11 de abril de 2023
AWSBackupServiceRolePolicyForRestores : actualización de una política actual	Agregó el siguiente permiso para restaurar Amazon EFS mediante una clave administrada por el cliente: <code>kms:GenerateDataKeyWithoutPlaintext</code> . Ayuda a garantizar que los usuarios dispongan de los permisos necesarios para restaurar los recursos de Amazon EFS.	27 de marzo de 2023

Cambio	Descripción	Fecha
AWSServiceRolePolicyForBackupReports: actualización de una política actual	Se actualizaron las <code>config:DescribeConfigRuleEvaluationStatus</code> acciones <code>config:DescribeConfigRules</code> y para permitir que AWS Backup Audit Manager acceda a las reglas administradas por AWS Backup Audit Manager AWS Config .	9 de marzo de 2023
AWSBackupServiceRolePolicyForS3Restore: actualización a una política existente	Agregó los siguientes permisos: <code>kms:Decrypt</code> , <code>s3:PutBucketOwnershipControls</code> y <code>s3:GetBucketOwnershipControls</code> a la política <code>AWSBackupServiceRolePolicyForS3Restore</code> . Estos permisos son necesarios para permitir la restauración de objetos cuando se utiliza el cifrado de KMS en la copia de seguridad original y para restaurar objetos cuando la propiedad del objeto está configurada en el bucket original en lugar de en la ACL.	13 de febrero de 2023

Cambio	Descripción	Fecha
<u>AWSBackupFullAccess:</u> actualización de una política actual	Se agregaron los siguientes permisos para programar copias de seguridad mediante VMware etiquetas de máquinas virtuales y para admitir la limitación del ancho de banda basada en la programación: <code>backup-gateway:GetHypervisorPropertyMappings</code> , <code>backup-gateway:GetVirtualMachine</code> , <code>backup-gateway:PutHypervisorPropertyMappings</code> y <code>backup-gateway:GetHypervisor</code> , <code>backup-gateway:StartVirtualMachinesMetadataSync</code> , <code>backup-gateway:GetBandwidthRateLimitSchedule</code> , <code>backup-gateway:PutBandwidthRateLimitSchedule</code>	15 de diciembre de 2022

Cambio	Descripción	Fecha
AWSBackupOperatorAccess : actualización de una política actual	Se agregaron los siguientes permisos para programar copias de seguridad mediante VMware etiquetas de máquinas virtuales y para admitir la limitación del ancho de banda basada en la programación: <code>backup-gateway:GetHypervisorPropertyMappings</code> , <code>backup-gateway:GetVirtualMachine</code> , <code>backup-gateway:GetHypervisor</code> , <code>backup-gateway:GetBandwidthRateLimitSchedule</code>	15 de diciembre de 2022
AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync : política nueva	Proporciona permisos para que AWS Backup Gateway sincronice los metadatos de las máquinas virtuales de las redes locales con Backup Gateway.	15 de diciembre de 2022

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForBackup : actualización de una política actual	Se agregaron los siguientes permisos para admitir los trabajos de copia de seguridad de Timestream: <code>timestream:StartAwsBackupJob</code> , <code>timestream:GetAwsBackupStatus</code> , <code>timestream:ListTables</code> , <code>timestream:ListDatabases</code> , <code>timestream:ListTagsForResource</code> , <code>timestream:DescribeTable</code> , <code>timestream:DescribeDatabase</code> y <code>timestream:DescribeEndpoints</code> .	13 de diciembre de 2022

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForRestores : actualización de una política actual	Se agregaron los siguientes permisos para admitir los trabajos de restauración de Timestream: <code>timestream:StartAwsRestoreJob</code> , <code>timestream:GetAwsRestoreStatus</code> , <code>timestream:ListTables</code> , <code>timestream:ListTagsForResource</code> , <code>timestream:ListDatabases</code> , <code>timestream:DescribeTable</code> , <code>timestream:DescribeDatabase</code> , <code>s3:GetBucketAcl</code> y <code>timestream:DescribeEndpoints</code> .	13 de diciembre de 2022
AWSBackupFullAccess : actualización de una política actual	Se agregaron los siguientes permisos para admitir los trabajos de restauración de Timestream: <code>timestream:ListTables</code> , <code>timestream:ListDatabases</code> , <code>s3:ListAllMyBuckets</code> y <code>timestream:DescribeEndpoints</code> .	13 de diciembre de 2022

Cambio	Descripción	Fecha
AWSBackupOperatorAccess: actualización de una política actual	Se agregaron los siguientes permisos para admitir los recursos de Timestream: timestream:ListDatabases , timestream:ListTables , s3:ListAllMyBuckets y timestream:DescribeEndpoints .	13 de diciembre de 2022
AWSBackupServiceLinkedRolePolicyForBackup: actualización de una política actual	Se agregaron los siguientes permisos para admitir los recursos de Timestream: timestream:ListDatabases , timestream:ListTables , timestream:ListTagsForResource , timestream:DescribeDatabase , timestream:DescribeTable , timestream:GetAwsBackupStatus , timestream:GetAwsRestoreStatus y timestream:DescribeEndpoints .	13 de diciembre de 2022

Cambio	Descripción	Fecha
AWSBackupFullAccess: actualización de una política actual	Se agregaron los siguientes permisos para admitir los recursos de Amazon Redshift: <code>redshift:DescribeClusters</code> , <code>redshift:DescribeClusterSubnetGroups</code> , <code>redshift:DescribeNodeConfigurationOptions</code> , <code>redshift:DescribeOrderableClusterOptions</code> , <code>redshift:DescribeClusterParameterGroups</code> , <code>redshift:DescribeClusterTracks</code> , <code>redshift:DescribeSnapshotSchedules</code> y <code>ec2:DescribeAddresses</code> .	27 de noviembre de 2022

Cambio	Descripción	Fecha
AWSBackupOperatorAccess: actualización de una política actual	Se agregaron los siguientes permisos para admitir los recursos de Amazon Redshift: <code>redshift:DescribeClusters</code> , <code>redshift:DescribeClusterSubnetGroups</code> , <code>redshift:DescribeNodeConfigurationOptions</code> , <code>redshift:DescribeOrderableClusterOptions</code> , <code>redshift:DescribeClusterParameterGroups</code> , <code>redshift:DescribeClusterTracks</code> , <code>redshift:DescribeSnapshotSchedules</code> y <code>ec2:DescribeAddresses</code> .	27 de noviembre de 2022
AWSBackupServiceRolePolicyForRestores: actualización de una política actual	Se agregaron los siguientes permisos para admitir los recursos de Amazon Redshift: <code>redshift:RestoreFromClusterSnapshot</code> , <code>redshift:RestoreTableFromClusterSnapshot</code> , <code>redshift:DescribeClusters</code> y <code>redshift:DescribeTableRestoreStatus</code> .	27 de noviembre de 2022

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForBackup : actualización de una política actual	Se agregaron los siguientes permisos para admitir los trabajos de copia de seguridad de Amazon Redshift: <code>redshift:CreateClusterSnapshot</code> , <code>redshift:DescribeClusterSnapshots</code> , <code>redshift:DescribeTags</code> , <code>redshift>DeleteClusterSnapshot</code> , <code>redshift:DescribeClusters</code> y <code>redshift:CreateTags</code> .	27 de noviembre de 2022
AWSBackupFullAccess : actualización de una política actual	Se agregó el siguiente permiso para respaldar CloudFormation los recursos: <code>cloudformation:ListStacks</code> .	27 de noviembre de 2022
AWSBackupOperatorAccess : actualización de una política actual	Se agregó el siguiente permiso para respaldar CloudFormation los recursos: <code>cloudformation:ListStacks</code> .	27 de noviembre de 2022

Cambio	Descripción	Fecha
AWSBackupServiceLinkedRolePolicyForBackup : actualización de una política actual	Se agregaron los siguientes permisos para respaldar CloudFormation los recursos: redshift: DescribeClusterSnapshots redshift: DescribeTags ,redshift: DeleteClusterSnapshots ,yredshift: DescribeClusters .	27 de noviembre de 2022
AWSBackupServiceRolePolicyForBackup : actualización de una política actual	Se agregaron los siguientes permisos para admitir los trabajos de copia de seguridad de la pila de CloudFormation aplicaciones: cloudformation:GetTemplate cloudformation:DescribeStacks ,ycloudformation:ListStackResources .	16 de noviembre de 2022
AWSBackupServiceRolePolicyForRestores : actualización de una política actual	Se agregaron los siguientes permisos para admitir los trabajos de respaldo de la pila de CloudFormation aplicaciones: cloudformation:CreateChangeSet y cloudformation:DescribeChangeSet	16 de noviembre de 2022

Cambio	Descripción	Fecha
AWSBackupOrganizationAdminAccess : actualización de una política actual	Se agregaron los siguientes permisos a esta política para permitir a los administradores de la organización utilizar la característica de administrador delegado: <code>organizations:ListDelegatedAdministrator</code> , <code>organizations:RegisterDelegatedAdministrator</code> y <code>organizations:DeregisterDelegatedAdministrator</code>	27 de noviembre de 2022
AWSBackupServiceRolePolicyForBackup : actualización de una política actual	Se agregaron los siguientes permisos para admitir SAP HANA en EC2 las instancias de Amazon: <code>ssm-sap:GetOperation</code> , <code>ssm-sap:ListDatabases</code> , <code>ssm-sap:BackupDatabase</code> , <code>ssm-sap:UpdateHanaBackupSettings</code> , <code>ssm-sap:GetDatabase</code> , <code>ssm-sap:ListTagsForResource</code> .	20 de noviembre de 2022

Cambio	Descripción	Fecha
AWSBackupFullAccess : actualización de una política actual	Se agregaron los siguientes permisos para admitir SAP HANA en EC2 las instancias de Amazon: <code>ssm-sap:GetOperation</code> <code>ssm-sap:ListDatabases</code> , <code>ssm-sap:GetDatabase</code> , <code>yssm-sap:ListTagsForResource</code> .	20 de noviembre de 2022
AWSBackupOperatorAccess : actualización de una política actual	Se agregaron los siguientes permisos para admitir SAP HANA en EC2 las instancias de Amazon: <code>ssm-sap:GetOperation</code> <code>ssm-sap:ListDatabases</code> , <code>ssm-sap:GetDatabase</code> , <code>yssm-sap:ListTagsForResource</code> .	20 de noviembre de 2022
AWSBackupServiceLinkedRolePolicyForBackup : actualización de una política actual	Se agregó el siguiente permiso para admitir SAP HANA en EC2 instancias de Amazon: <code>ssm-sap:GetOperation</code> .	20 de noviembre de 2022
AWSBackupServiceRolePolicyForRestores : actualización de una política actual	Se agregó el siguiente permiso para admitir los trabajos de restauración de Backup Gateway en una EC2 instancia: <code>ec2:CreateTags</code> .	20 de noviembre de 2022

Cambio	Descripción	Fecha
AWSBackupDataTransferAccess : actualización de una política actual	Se agregaron los siguientes permisos para admitir la transferencia segura de datos de almacenamiento para EC2 los recursos de SAP HANA On Amazon: backup-storage:StartObject backup-storage:PutChunk backup-storage:GetChunk backup-storage:ListChunks backup-storage:ListObjects backup-storage:GetObjectMetadata backup-storage:NotifyObjectComplete	20 de noviembre de 2022

Cambio	Descripción	Fecha
AWSBackupRestoreAccessForSAPHANA : actualización a una política existente	Se agregaron los siguientes permisos para que los propietarios de los recursos realicen la restauración de EC2 los recursos de SAP HANA On Amazon: backup:Get* backup:List* backup:Describe* backup:StartBackupJob backup:StartRestoreJob ssm-sap:GetOperation ,ssm-sap:ListDatabases ,ssm-sap:BackupDatabase ,ssm-sap:RestoreDatabase ,ssm-sap:UpdateHanaBackupSettings ,ssm-sap:GetDatabase ,ssm-sap:ListTagsForResource .	20 de noviembre de 2022
AWSBackupServiceRolePolicyForS3Backup : actualización a una política existente	Se agregó el permiso s3:GetBucketAcl para admitir las operaciones de respaldo AWS Backup de Amazon S3.	24 de agosto de 2022

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForRestores : actualización de una política actual	Se agregaron las siguientes acciones para conceder acceso para la creación de una instancia de base de datos que admita la funcionalidad de varias zonas de disponibilidad (Multi-AZ): <code>rds:CreateDBInstance</code>	20 de julio de 2022
AWSBackupServiceLinkedRolePolicyForBackup : actualización de una política actual	Se agregó el permiso <code>s3:GetBucketTagging</code> para conceder al usuario permiso para seleccionar los buckets de los que realizar copias de seguridad con un recurso comodín. Sin este permiso, los usuarios que seleccionen los buckets de los que se va a hacer una copia de seguridad con un recurso comodín no podrán hacer esto.	6 de mayo de 2022
AWSBackupServiceRolePolicyForBackup : actualización de una política actual	Se agregaron recursos de volumen en el ámbito de <code>fsx:ListTagsForResource</code> las acciones existentes <code>fsx:CreateBackup</code> y se agregaron nuevas acciones FSx para respaldar las copias de seguridad <code>fsx:DescribeVolumes</code> a nivel de volumen de ONTAP.	27 de abril de 2022

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForRestores : actualización de una política actual	Se han añadido las siguientes acciones para conceder a los usuarios permisos de restauración de FSx los volúmenes de ONTAP: <code>fsx:DescribeVolumes</code> , <code>fsx:CreateVolumeFromBackup</code> <code>fsx:DeleteVolume</code> , y. <code>fsx:UntagResource</code>	27 de abril de 2022
AWSBackupServiceRolePolicyForS3Backup : actualización a una política existente	Se agregaron las siguientes acciones para conceder al usuario permisos para recibir notificaciones de cambios en sus buckets de Amazon S3 durante las operaciones de copia de seguridad: <code>s3:GetBucketNotification</code> y <code>s3:PutBucketNotification</code> .	25 de febrero de 2022

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForS3Backup : nueva política	Se agregó las siguientes acciones para conceder al usuario permisos para restaurar sus buckets de Amazon S3: s3:GetInventoryConfiguration , s3:PutInventoryConfiguration , s3:ListBucketVersions , s3:ListBucket , s3:GetBucketTagging , s3:GetBucketVersioning , s3:GetBucketNotification , s3:GetBucketLocation y s3:ListAllMyBuckets Se agregaron las siguientes acciones para conceder al usuario permisos para hacer copias de seguridad de sus objetos de Amazon S3: s3:GetObject , s3GetObjectAcl , s3:GetObjectVersionTagging , s3:GetObjectVersionAcl , s3:GetObjectTagging y s3:GetObjectVersion . Se agregaron las siguientes acciones para conceder al usuario permisos para hacer copias de seguridad de sus	17 de febrero de 2022

Cambio	Descripción	Fecha
	datos cifrados de Amazon S3: kms:Decrypt y kms:DescribeKey . Se agregaron las siguientes acciones para conceder al usuario permisos para realizar copias de seguridad incrementales de sus datos de Amazon S3 utilizando EventBridge las reglas de Amazon: events:DescribeRule events:EnableRule events:PutRule events:DeleteRule events:PutTargets ,events:RemoveTargets ,events:ListTargetsByRule ,events:DisableRule ,cloudwatch:GetMetricData ,events:ListRules .	

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForS3Restore: nueva política	Se agregaron las siguientes acciones para conceder al usuario permisos para restaurar sus buckets de Amazon S3: <code>s3:CreateBucket</code> , <code>s3:ListBucketVersions</code> , <code>s3:ListBucket</code> , <code>s3:GetBucketVersioning</code> , <code>s3:GetBucketLocation</code> y <code>s3:PutBucketVersioning</code> . Se agregaron las siguientes acciones para conceder al usuario permisos para restaurar sus buckets de Amazon S3: <code>s3:GetObject</code> , <code>s3:GetObjectVersion</code> , <code>s3:DeleteObject</code> , <code>s3:PutObjectVersionAcl</code> , <code>s3:GetObjectVersionAcl</code> , <code>s3:GetObjectTagging</code> , <code>s3:PutObjectTagging</code> , <code>s3:GetObjectAcl</code> , <code>s3:PutObjectAcl</code> , <code>s3:PutObject</code> y <code>s3:ListMultipartUploadParts</code> . Se agregaron las siguientes acciones para conceder al usuario permisos para cifrar	17 de febrero de 2022

Cambio	Descripción	Fecha
	sus datos de Amazon S3 restaurados: <code>kms:Decrypt</code>, <code>kms:DescribeKey</code> y <code>kms:GenerateDataKey</code>.	
AWSBackupServiceLinkedRolePolicyForBackup : actualización de una política actual	Se agregó <code>s3:ListAllMyBuckets</code> para conceder al usuario permisos para ver una lista de sus buckets y elegir cuáles asignar a un plan de copia de seguridad.	14 de febrero de 2022
AWSBackupServiceLinkedRolePolicyForBackup : actualización de una política actual	Se agregó <code>backup-gateway:ListVirtualMachines</code> para conceder al usuario permisos para ver una lista de sus máquinas virtuales y elegir cuáles asignar a un plan de copia de seguridad. Se agregó <code>backup-gateway:ListTagsForResource</code> para conceder al usuario permisos para enumerar las etiquetas de sus máquinas virtuales.	30 de noviembre de 2021

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForBackup : actualización de una política actual	Se agregó <code>backup-gateway:Backup</code> para otorgar al usuario permisos para restaurar las copias de seguridad de sus máquinas virtuales. AWS Backup también se agregó <code>backup-gateway:ListTagsForResource</code> para conceder al usuario permisos para enumerar las etiquetas asignadas a las copias de seguridad de sus máquinas virtuales.	30 de noviembre de 2021
AWSBackupServiceRolePolicyForRestores : actualización de una política actual	Se agregó <code>backup-gateway:Restore</code> para conceder al usuario permisos para restaurar las copias de seguridad de sus máquinas virtuales.	30 de noviembre de 2021

Cambio	Descripción	Fecha
<u>AWSBackupFullAccess:</u> actualización de una política actual	Se agregaron las siguientes acciones para conceder a los usuarios permisos para usar AWS Backup Gateway para realizar copias de seguridad , restaurar y administrar sus máquinas virtuales: <code>backup-gateway:AssociateGatewayToServer</code> , <code>backup-gateway:CreateGateway</code> , <code>backup-gateway:DeleteGateway</code> , <code>backup-gateway:DeleteHypervisor</code> , <code>backup-gateway:DisassociateGatewayFromServer</code> , <code>backup-gateway:ImportHypervisorConfiguration</code> , <code>backup-gateway:ListGateways</code> , <code>backup-gateway:ListHypervisors</code> , <code>backup-gateway:ListTagsForResource</code> , <code>backup-gateway:ListVirtualMachines</code> , <code>backup-gateway:PutMaintenanceStartTime</code> , <code>backup-gateway:TagResource</code> , <code>backup-gateway:TestHypervisorConfiguration</code> , <code>backup-gateway:UntagResource</code> , <code>backup-gateway:Upd</code>	30 de noviembre de 2021

Cambio	Descripción	Fecha
	ateGatewayInformat ion y backup-ga teway:UpdateHyperv isor .	
AWSBackupOperatorAccess: actualización de una política actual	Se agregó las siguientes acciones para conceder al usuario permisos para hacer copias de seguridad de sus máquinas virtuales: backup- gateway:ListGateways , backup-gateway:Lis tHypervisors , backup- gateway:ListTagsForR esource y backup-ga teway:ListVirtualM achines .	30 de noviembre de 2021
AWSBackupServiceLi nkedRolePolicyForBackup: actualización de una política actual	Se agregó dynamodb: ListTagsOfResource para conceder al usuario permisos para enumerar las etiquetas de sus tablas de DynamoDB para realizar copias de seguridad mediante las funciones avanzadas de copia AWS Backup de seguridad de DynamoDB.	23 de noviembre de 2021

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForBackup : actualización de una política actual	Se agregó dynamodb: StartAwsBackupJob para conceder al usuario permisos para hacer copias de seguridad de sus tablas de DynamoDB mediante características avanzadas de copia de seguridad. Se agregó dynamodb: ListTagsOfResource para conceder al usuario permisos para copiar etiquetas de sus tablas de DynamoDB de origen a sus copias de seguridad.	23 de noviembre de 2021
AWSBackupServiceRolePolicyForRestores : actualización de una política actual	Se ha añadido dynamodb: RestoreTableFromAwsBackup para conceder permisos al usuario para restaurar las tablas de DynamoDB de las que se ha hecho una copia de seguridad mediante las funciones avanzadas AWS Backup de copia de seguridad de DynamoDB.	23 de noviembre de 2021

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForRestores : actualización de una política actual	Se ha añadido dynamodb:RestoreTableFromAWSBackup para conceder permisos al usuario para restaurar las tablas de DynamoDB de las que se ha hecho una copia de seguridad mediante las funciones avanzadas AWS Backup de copia de seguridad de DynamoDB.	23 de noviembre de 2021
AWSBackupOperatorAccess : actualización de una política actual	Se eliminaron las acciones existentes backup:GetRecoveryPointRestoreMetadata y rds:DescribeDBSnapshots porque eran redundantes. AWS Backup no necesitaba ambas backup:GetRecoveryPointRestoreMetadata y backup:Get* formaba parte de ellas. AWSBackupOperatorAccess. Además, AWS Backup no necesitaba ambos rds:DescribeDBSnapshots y rds:describeDBSnapshots como parte deAWSBackupOperatorAccess.	23 de noviembre de 2021

Cambio	Descripción	Fecha
AWSBackupServiceLinkedRolePolicyForBackup: actualización de una política actual	Se agregaron las nuevas acciones <code>elasticfilesystem:DescribeFileSystems</code> , <code>dynamodb:ListTables</code> , <code>storagegateway:ListVolumes</code> , <code>ec2:DescribeVolumes</code> , <code>ec2:DescribeInstances</code> , <code>rds:DescribeDBInstances</code> , <code>rds:DescribeDBClusters</code> , y <code>fsx:DescribeFileSystems</code> para permitir a los clientes ver y elegir de una lista de los recursos que AWS Backup admiten al seleccionar los recursos que van a asignar a un plan de respaldo.	10 de noviembre de 2021
AWSBackupAuditAccess: política nueva	Se agregó <code>AWSBackupAuditAccess</code> para conceder al usuario permisos para usar AWS Backup Audit Manager. Los permisos incluyen la capacidad de configurar marcos de conformidad y generar informes.	24 de agosto de 2021

Cambio	Descripción	Fecha
AWSServiceRolePolicyForBackupReports : política nueva	Se agregó <code>AWSServiceRolePolicyForBackupReports</code> para conceder permisos para un rol vinculado al servicio a fin de automatizar la monitorización de la configuración, los trabajos y los recursos de la copia de seguridad para que cumplan los marcos configurados por el usuario.	24 de agosto de 2021
AWSBackupFullAccess : actualización de una política actual	Se agregó <code>iam:CreateServiceLinkedRole</code> para crear un rol vinculado al servicio (en la medida de lo posible) para automatizar la eliminación de los puntos de recuperación vencidos. Sin esta función vinculada al servicio, AWS Backup no se pueden eliminar los puntos de recuperación caducados después de que los clientes eliminen la función de IAM original que utilizaron para crear sus puntos de recuperación.	5 de julio de 2021

Cambio	Descripción	Fecha
AWSBackupServiceLinkedRolePolicyForBackup: actualización de una política actual	Se agregó la nueva acción <code>dynamodb:DeleteBackup</code> para conceder el permiso <code>DeleteRecoveryPoint</code> para automatizar la eliminación de los puntos de recuperación de DynamoDB vencidos en función de la configuración del ciclo de vida del plan de copia de seguridad.	5 de julio de 2021
AWSBackupOperatorAccess: actualización de una política actual	Se eliminaron las acciones existentes <code>backup:GetRecoveryPointRestoreMetadata</code> y <code>rds:DescribeDBSnapshots</code> porque eran redundantes. AWS Backup no necesitaba ambos <code>backup:GetRecoveryPointRestoreMetadata</code> y <code>backup:Get*</code> como parte de <code>AWSBackupOperatorAccess</code>. Además, AWS Backup no necesitaba ambos <code>rds:DescribeDBSnapshots</code> y <code>rds:describeDBSnapshots</code> como parte de <code>AWSBackupOperatorAccess</code>.	25 de mayo de 2021

Cambio	Descripción	Fecha
AWSBackupOperatorAccess: actualización de una política actual	Se eliminaron las acciones existentes <code>backup:GetRecoveryPointRestoreMetadata</code> y <code>rds:DescribeDBSnapshots</code> porque eran redundantes. AWS Backup no necesitaba ambos <code>backup:GetRecoveryPointRestoreMetadata</code> y <code>backup:Get*</code> como parte de <code>AWSBackupOperatorAccess</code>. Además, AWS Backup no necesitaba ambos <code>rds:DescribeDBSnapshots</code> y <code>rds:describeDBSnapshots</code> como parte de <code>AWSBackupOperatorAccess</code>.	25 de mayo de 2021
AWSBackupServiceRolePolicyForRestores: actualización de una política actual	Se ha añadido la nueva acción <code>fsx:TagResource</code> para conceder <code>StartRestoreJob</code> permiso que te permita aplicar etiquetas a los sistemas de FSx archivos de Amazon durante el proceso de restauración.	24 de mayo de 2021

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForRestores : actualización de una política actual	Se han añadido las nuevas acciones <code>ec2:DescribeImages</code> y <code>ec2:DescribeInstances</code> se ha concedido un <code>StartRestoreJob</code> permiso que te permita restaurar las EC2 instancias de Amazon desde los puntos de recuperación.	24 de mayo de 2021
AWSBackupServiceRolePolicyForBackup : actualización de una política actual	Se ha añadido la nueva acción <code>fsx:CopyBackup</code> para conceder <code>StartCopyJob</code> permiso que te permita copiar los puntos de FSx recuperación de Amazon entre regiones y cuentas.	12 de abril de 2021
AWSBackupServiceLinkedRolePolicyForBackup : actualización de una política actual	Se ha añadido la nueva acción <code>fsx:CopyBackup</code> para conceder <code>StartCopyJob</code> permiso que te permita copiar los puntos de FSx recuperación de Amazon entre regiones y cuentas.	12 de abril de 2021

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForBackup : actualización de una política actual	Se actualizó para cumplir con el siguiente requisito: AWS Backup Para crear una copia de seguridad de una tabla de DynamoDB cifrada, debe añadir los kms:Decrypt permisos kms:GenerateDataKey y la función de IAM utilizada para la copia de seguridad.	10 de marzo de 2021

Cambio	Descripción	Fecha
AWSBackupFullAccess: actualización de una política actual	Se actualizó para cumplir con los siguientes requisitos: AWS Backup Para configurar copias de seguridad continuas para su base de datos de Amazon RDS, compruebe que el permiso de API <code>rds:ModifyDBInstance</code> existe en la función de IAM definida en la configuración de su plan de backup. Para restaurar las copias de seguridad continuas de Amazon RDS, debe agregar el permiso <code>rds:RestoreDBInstanceToPointInTime</code> al rol de IAM que envió para el trabajo de restauración. En la AWS Backup consola, para describir el intervalo de tiempo disponible para la point-in-time recuperación, debe incluir el permiso de la <code>rds:DescribeDBInstancesAutomatedBackups</code> API en la política gestionada por IAM.	10 de marzo de 2021

Cambio	Descripción	Fecha
AWS Backup comenzó a rastrear los cambios	AWS Backup comenzó a realizar un seguimiento de los cambios de sus políticas AWS gestionadas.	10 de marzo de 2021

Cómo utilizar roles vinculados a servicios de AWS Backup

AWS Backup [usa roles vinculados al AWS Identity and Access Management servicio \(IAM\)](#). Un rol vinculado a un servicio es un tipo único de rol de IAM al que se vincula directamente. AWS Backup Los roles vinculados al servicio están predefinidos AWS Backup e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Temas

- [Uso de roles para hacer copias de seguridad y copiar](#)
- [Uso de funciones para AWS Backup Audit Manager](#)
- [Uso de roles para pruebas de restauración](#)

Uso de roles para hacer copias de seguridad y copiar

AWS Backup [usa roles vinculados al AWS Identity and Access Management servicio \(IAM\)](#). Un rol vinculado a un servicio es un tipo único de rol de IAM al que se vincula directamente. AWS Backup Los roles vinculados al servicio están predefinidos AWS Backup e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Un rol vinculado a un servicio facilita la configuración AWS Backup , ya que no es necesario añadir manualmente los permisos necesarios. AWS Backup define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo AWS Backup 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 sus recursos relacionados. Esto protege sus AWS Backup recursos porque no puede eliminar inadvertidamente el permiso de acceso a los recursos.

Para obtener información sobre otros servicios que son compatibles con los 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 servicios). Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de rol vinculados al servicio para AWS Backup

AWS Backup utiliza el rol vinculado al servicio denominado `AWSServiceRoleForBackup` para crear y eliminar copias de seguridad de sus AWS recursos en su nombre.

El rol `AWSService RoleForBackup` vinculado al servicio confía en los siguientes servicios para asumir el rol:

- `backup.amazonaws.com`

Para ver los permisos de esta política, consulte la Referencia [AWSBackupServiceLinkedRolePolicyforBackup](#) de políticas AWS administradas.

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 de AWS Backup

No necesita crear manualmente un rol vinculado a servicios. Al enumerar los recursos de los que hacer copias de seguridad, configurar copias de seguridad entre cuentas o realizar copias de seguridad en la Consola de administración de AWS, la CLI o la AWS API, se crea automáticamente la función vinculada al servicio.

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. 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. Cuando pones en una lista los recursos que deseas guardar, configuras una copia de seguridad multicuenta o realizas copias de seguridad, vuelve a AWS Backup crear el rol vinculado al servicio para ti.

Modificación de un rol vinculado a servicios de AWS Backup

AWS Backup no le permite editar el rol vinculado al AWSService RoleForBackup 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 la [Descripción sobre cómo editar un rol vinculado al servicio](#) en la Guía del usuario de IAM.

Eliminación de un rol vinculado a un servicio de AWS Backup

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma, no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa. Sin embargo, debe limpiar el rol vinculado a servicios antes de eliminarlo manualmente.

Limpiar un rol vinculado a servicios

Antes de que pueda utilizar IAM para eliminar un rol vinculado a servicios, primero debe eliminar los recursos que utiliza el rol. En primer lugar, debe eliminar todos los puntos de recuperación. Luego, debe eliminar todos sus almacenes de copias de seguridad.

Note

Si el AWS Backup servicio 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 AWS Backup los recursos utilizados por la AWSService RoleForBackup (consola)

1. Para eliminar todos los puntos de recuperación y los almacenes de copias de seguridad (excepto su almacén predeterminado), siga el procedimiento que se describe en [Eliminación de un almacén](#).
2. Para eliminar el almacén predeterminado, utilice el siguiente comando en la AWS CLI:

```
aws backup delete-backup-vault --backup-vault-name Default --region us-east-1
```

Para eliminar AWS Backup los recursos utilizados por AWSService RoleForBackup (AWS CLI)

1. Para eliminar todos los puntos de recuperación, utilice [delete-recovery-point](#).
2. Para eliminar todos los almacenes de copias de seguridad, utilice [delete-backup-vault](#).

Para eliminar AWS Backup los recursos utilizados por la AWSService RoleForBackup (API)

1. Para eliminar todos los puntos de recuperación, utilice [DeleteRecoveryPoint](#).
2. Para eliminar todos los almacenes de copias de seguridad, utilice [DeleteBackupVault](#).

Eliminación manual de un rol vinculado a servicios

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al AWSService RoleForBackup servicio. Para obtener más información, consulte [Eliminación de un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Regiones admitidas para los roles vinculados a un servicio de AWS Backup

AWS Backup admite el uso de funciones vinculadas al servicio en todas las regiones en las que el servicio está disponible. Para obtener más información, consulte [Regiones y características compatibles con AWS Backup](#).

Uso de funciones para AWS Backup Audit Manager

AWS Backup [usa roles vinculados al AWS Identity and Access Management servicio \(IAM\)](#). Un rol vinculado a un servicio es un tipo único de rol de IAM al que se vincula directamente. AWS Backup Los roles vinculados al servicio están predefinidos AWS Backup e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Un rol vinculado a un servicio facilita la configuración AWS Backup , ya que no es necesario añadir manualmente los permisos necesarios. AWS Backup define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo AWS Backup 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 sus recursos relacionados. Esto protege sus AWS Backup recursos porque no puede eliminar inadvertidamente el permiso de acceso a los recursos.

Para obtener información sobre otros servicios que son compatibles con los 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 servicios). Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de rol vinculados al servicio para AWS Backup

AWS Backup utiliza el rol vinculado al servicio denominado `AWSServiceRoleForBackupReports`: AWS Backup proporciona permiso para crear controles, marcos e informes.

El rol `AWSServiceRoleForBackupReports` vinculado al servicio confía en los siguientes servicios para asumir el rol:

- `reports.backup.amazonaws.com`

Para ver los permisos de esta política, consulte [AWSServiceRolePolicyForBackupReports](#) en la Referencia de la política administrada de AWS .

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 de AWS Backup

No necesita crear manualmente un rol vinculado a servicios. Al crear un marco o un plan de informes en la Consola de administración de AWS, la o la AWS API AWS CLI, AWS Backup crea automáticamente la función vinculada al servicio.

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. 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 un marco o un plan de informes, vuelve a AWS Backup crear el rol vinculado al servicio automáticamente.

Modificación de un rol vinculado a servicios de AWS Backup

AWS Backup no permite editar el rol vinculado al AWSService RoleForBackupReports 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 la [Edición de una descripción del rol vinculado a servicios](#) en la Guía del usuario de IAM.

Eliminación de un rol vinculado a un servicio de AWS Backup

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma, no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa. Sin embargo, debe limpiar el rol vinculado a servicios antes de eliminarlo manualmente.

Limpiar un rol vinculado a servicios

Antes de que pueda utilizar IAM para eliminar un rol vinculado a servicios, primero debe eliminar los recursos que utiliza el rol. Debe eliminar todos los marcos y los planes de informes.

Note

Si el AWS Backup servicio 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 AWS Backup los recursos utilizados por la AWSService RoleForBackupReports (consola)

1. Para eliminar todos los marcos, consulte [Eliminación de marcos](#).
2. Para eliminar todos los planes de informes, consulte [Eliminación de los planes de informes](#).

Para eliminar AWS Backup los recursos utilizados por AWSService RoleForBackupReports (AWS CLI)

1. Para eliminar todos los marcos, utilice [delete-framework](#).
2. Para eliminar todos los planes de informes, utilice [delete-report-plan](#).

Para eliminar AWS Backup los recursos utilizados por la AWSService RoleForBackupReports (API)

1. Para eliminar todos los marcos, utilice [DeleteFramework](#).
2. Para eliminar todos los planes de informes, utilice [DeleteReportPlan](#).

Eliminación manual de un rol vinculado a servicios

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al AWSService RoleForBackupReports servicio. Para obtener más información, consulte [Eliminación de un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Regiones admitidas para los roles vinculados a un servicio de AWS Backup

AWS Backup admite el uso de funciones vinculadas al servicio en todas las regiones en las que el servicio está disponible. Para obtener más información, consulte [Regiones y características compatibles con AWS Backup](#).

Uso de roles para pruebas de restauración

AWS Backup [usa roles vinculados al AWS Identity and Access Management servicio \(IAM\)](#). Un rol vinculado a un servicio es un tipo único de rol de IAM al que se vincula directamente. AWS Backup Los roles vinculados al servicio están predefinidos AWS Backup e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Un rol vinculado a un servicio facilita la configuración AWS Backup , ya que no es necesario añadir manualmente los permisos necesarios. AWS Backup define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo AWS Backup 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 sus recursos relacionados. Esto protege sus AWS Backup recursos porque no puede eliminar inadvertidamente el permiso de acceso a los recursos.

Para obtener información sobre otros servicios que son compatibles con los 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 servicios). Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de rol vinculados al servicio para AWS Backup

AWS Backup utiliza el rol vinculado al servicio denominado

`AWSServiceRoleForBackupRestoreTesting`: proporciona permisos de respaldo para realizar pruebas de restauración.

El rol vinculado al servicio `AWSServiceRoleForBackupRestoreTesting` depende de los siguientes servicios para asumir el rol:

- `restore-testing.backup.amazonaws.com`

Para ver los permisos de esta política, consulte [AWSServiceRolePolicyForBackupRestoreTesting](#) en la Referencia de la política administrada de AWS .

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 de AWS Backup

No necesita crear manualmente un rol vinculado a servicios. Al realizar pruebas de restauración en la Consola de administración de AWS, la AWS CLI API o la AWS API, AWS Backup crea automáticamente la función vinculada al servicio.

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. 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. Cuando realizas las pruebas de restauración, vuelve a AWS Backup crear el rol vinculado al servicio para ti.

Modificación de un rol vinculado a servicios de AWS Backup

AWS Backup no permite editar el rol vinculado al `AWSService RoleForBackupRestoreTesting` 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 la [Descripción sobre cómo editar un rol vinculado al servicio](#) en la Guía del usuario de IAM.

Eliminación de un rol vinculado a un servicio de AWS Backup

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma, no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa. Sin embargo, debe limpiar el rol vinculado a servicios antes de eliminarlo manualmente.

Limpiar un rol vinculado a servicios

Antes de que pueda utilizar IAM para eliminar un rol vinculado a servicios, primero debe eliminar los recursos que utiliza el rol. Debe eliminar todos los planes de prueba de restauración.

Note

Si el AWS Backup servicio 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 AWS Backup los recursos utilizados por la AWSService RoleForBackupRestoreTesting (consola)

- Para eliminar todos los planes de prueba de restauración, consulte [Pruebas de restauración](#).

Para eliminar AWS Backup los recursos utilizados por AWSService RoleForBackupRestoreTesting (AWS CLI)

- Para eliminar planes de prueba de restauración, utilice `delete-restore-testing-plan`.

Para eliminar AWS Backup los recursos utilizados por la AWSService RoleForBackupRestoreTesting (API)

- Para eliminar planes de prueba de restauración, utilice `DeleteRestoreTestingPlan`.

Eliminación manual de un rol vinculado a servicios

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al `AWSServiceRoleForBackupRestoreTesting` servicio. Para obtener más información, consulte [Eliminación de un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Regiones admitidas para los roles vinculados a un servicio de AWS Backup

AWS Backup admite el uso de funciones vinculadas al servicio en todas las regiones en las que el servicio está disponible. Para obtener más información, consulte [Regiones y características compatibles con AWS Backup](#).

Prevención de la sustitución confusa entre servicios

El problema de la sustitución confusa 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. En AWS, la suplantación de identidad entre servicios puede provocar un confuso problema de diputado. La suplantación entre servicios puede producirse cuando un servicio (el servicio que lleva a cabo las llamadas) llama a otro servicio (el servicio al que se llama). El servicio que lleva a cabo las llamadas se pueden manipular para utilizar sus permisos a fin de actuar en función de los recursos de otro cliente de una manera en la que no debe tener permiso para acceder. Para evitarlo, AWS proporciona herramientas que le ayudan a proteger los datos de todos los servicios cuyos directores de servicio tengan acceso a los recursos de su cuenta.

Recomendamos utilizar las claves de contexto de condición `aws:SourceAccount` global `aws:SourceArn` las claves contextuales en las políticas de recursos para limitar los permisos que se AWS Backup otorgan a otro servicio al recurso. Si se utilizan ambas claves contextuales de condición global, el valor `aws:SourceAccount` y la cuenta del valor `aws:SourceArn` deben utilizar el mismo ID de cuenta cuando se utilicen en la misma declaración de política.

El valor de `aws:SourceArn` debe ser una AWS Backup bóveda cuando se utilizan AWS Backup para publicar temas de Amazon SNS en su nombre.

La forma más eficaz de protegerse contra el problema de la sustitución confusa es utilizar la clave de contexto de condición global de `aws:SourceArn` con el ARN completo del recurso. Si no conoce el ARN completo del recurso o si especifica varios recursos, utiliza la clave de condición de contexto global `aws:SourceArn` con comodines (*) para las partes desconocidas del ARN. Por ejemplo, `arn:aws::servicename::123456789012:*`.

El siguiente ejemplo de política muestra cómo puede utilizar las claves de contexto `aws:SourceArn` y las condiciones `aws:SourceAccount` globales AWS Backup para evitar el confuso problema de los diputados. Esta política permite al director del servicio, `backup-storage.amazonaws.com`, realizar acciones de KMS únicamente cuando actúa en nombre de la cuenta 123456789012 en los almacenes de respaldo: AWS

Seguridad de la infraestructura en AWS Backup

Como servicio gestionado, AWS Backup está protegido por la seguridad de la red AWS global. Para obtener más 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 la infraestructura](#) en el marco de buena AWS arquitectura del pilar de la seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder a AWS Backup través de la red. Los clientes deben ser compatibles con Transport Layer Security (TLS) 1.2 o con una versión posterior. Los clientes también deben admitir conjuntos de cifrado con confidencialidad directa total (PFS) tales como Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Diffie-Hellman Ephemeral (ECDHE). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puedes utilizar [AWS Security Token Service](#) (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Integridad de los datos en AWS Backup

AWS Backup objetivo de integridad de los datos

AWS Backup busca mantener la integridad durante la transmisión, el almacenamiento y el procesamiento de sus datos. AWS Backup trata los datos de los recursos almacenados como información crítica independiente del contenido, ya que ofrecemos el mismo alto nivel de seguridad a los clientes, independientemente del tipo de datos que almacenen. Velamos por la seguridad de nuestros clientes y hemos implementado sofisticadas medidas técnicas y físicas contra el acceso no autorizado. Usted mantiene un control total sobre la forma en que se clasifican sus datos, las regiones en las que se almacenan y la forma en que se controlan, archivan y protegen contra su divulgación.

AWS Backup implementación de la integridad de los datos

AWS Backup trabaja en conjunto con otros servicios AWS y con Amazon para mantener la integridad de los datos que almacena y con los que interactúa. Las herramientas utilizadas pueden variar e incluyen, entre otras:

- Validación continua de los objetos con respecto a su suma de verificación para evitar que los objetos se corrompan
- Sumas de verificación internas para confirmar la integridad de los datos en tránsito y en reposo
- Las sumas de verificación se calculan a partir de los datos de las copias de seguridad creadas desde el almacén principal
- Intento automático de restablecer los niveles normales de redundancia del almacenamiento de objetos en caso de que el disco esté dañado o se detecte un error en el dispositivo
- Almacenamiento redundante de datos en varias ubicaciones físicas
- Mejora de la durabilidad de los objetos en varias zonas de disponibilidad durante la escritura inicial, que se combina con una mayor replicación en caso de que el dispositivo no esté disponible o se detecte una degradación de bits
- Sumas de verificación de todo el tráfico de la red para detectar paquetes de datos con daños durante el almacenamiento o la recuperación de los datos

AWS Backup almacena datos de forma nativa para Amazon DynamoDB con funciones avanzadas, Amazon EFS, Amazon S3, Amazon Timestream y máquinas virtuales que se ejecutan conectadas a través de Backup Gateway. VMware AWS Backup facilita las copias de seguridad de los datos almacenados con otros servicios, como Amazon Aurora, Amazon DocumentDB, Amazon DynamoDB, Amazon EBS, Amazon, Amazon, Amazon for Windows File Server, EC2 FSx Amazon for Lustre, FSx Amazon for OpenZFS, Amazon FSx for NetApp ONTAP, FSx Amazon Neptune, Amazon RDS y Amazon Redshift.

Confirmación objetiva y auditoría de la integridad de los datos en AWS Backup

Los datos almacenados directamente AWS Backup y los datos almacenados en asociación con otros AWS servicios con los que AWS Backup interactúa están sujetos al riguroso proceso de Amazon Simple Storage Service (Amazon S3) que sustenta la integridad de los datos. Un auditor externo independiente confirma esta integridad mediante un informe anual de auditoría de SOC, que está disponible en [AWS Artifact](#).

Obligaciones legales y AWS Backup

Descripción general de las retenciones legales

Una retención legal es una herramienta administrativa que ayuda a evitar que las copias de seguridad se eliminen mientras están retenidas. Mientras la retención esté en vigor, las copias de seguridad retenidas no se pueden eliminar y las políticas de ciclo de vida que podrían alterar el estado de las copias de seguridad (como la transición a un estado Deleted) se retrasan hasta que se elimine la retención legal.

Las retenciones legales se pueden aplicar a una o más copias de seguridad (también conocidas como puntos de recuperación) creadas AWS Backup si sus ciclos de vida lo permiten. Las retenciones legales no afectan a las [copias de seguridad continuas](#).

Cuando se crea una retención legal, puede tener en cuenta criterios de filtrado específicos, como los tipos de recursos y los recursos. IDs Además, puede definir el intervalo de fechas de creación de las copias de seguridad que desee incluir en una retención legal.

Las retenciones legales solo se aplican a la copia de seguridad original en la que se colocan. Cuando una copia de seguridad se copia entre regiones o cuentas (si el recurso lo admite), no se retiene ni lleva consigo su retención legal. Una retención legal, como otros recursos, tiene asociado un nombre de recurso de Amazon (ARN) único. Solo los puntos de recuperación creados por AWS Backup pueden formar parte de una retención legal.

Tenga en cuenta que, si bien el [Bloqueo de almacenes de AWS Backup](#) proporciona protecciones adicionales e inmutabilidad de un almacén, una retención legal ofrece adicional contra la eliminación de copias de seguridad individuales (puntos de recuperación). La retención legal no vence y retiene los datos de la copia de seguridad de forma indefinida. La retención permanece activa hasta que la libere un usuario con suficientes permisos.

Retenciones legales múltiples

Una copia de seguridad puede tener más de una retención legal. Las retenciones legales y las copias de seguridad tienen una relación de muchos a muchos, lo que significa que una copia de seguridad puede tener más de una retención legal e incluir más de una copia de seguridad.

Una copia de seguridad no se puede eliminar siempre que tenga al menos una retención legal. Una vez eliminadas todas las retenciones legales sobre una copia de seguridad, queda sujeta a las propiedades de su ciclo de vida de retención. Mantenga al menos una retención legal para evitar que

se elimine la copia de seguridad. Se pueden aplicar retenciones legales a un punto de recuperación retenido después de la fecha de retención del ciclo de vida de la copia de seguridad (debido a una retención legal existente).

Cada cuenta puede tener un máximo de 50 retenciones legales activas a la vez.

Creación de una retención legal

Se puede añadir una retención legal a una copia de seguridad existente (punto de recuperación).

Las copias de seguridad (puntos de recuperación) con un estado DELETING o EXPIRED no se incluirán en la retención legal. Es posible que los puntos de recuperación (copias de seguridad) con el estado CREATING no se incluyan en la retención legal, según el momento en que se completen.

Los usuarios que tengan los permisos de IAM necesarios pueden agregar retenciones legales.

Creación de una retención legal mediante la consola de

Para crear una retención legal

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de la izquierda de la consola, busca Mi cuenta. Seleccione Retenciones legales.
3. Seleccione Añadir retención legal.
4. Se mostrarán tres paneles: Detalles de la retención legal, Ámbito de la retención legal y Etiquetas de retención legal.
 - a. En Detalles de la retención legal, introduzca el título de la retención legal y una descripción de la misma en los cuadros de texto correspondientes.
 - b. En el panel Ámbito de la retención legal, elija cómo desea seleccionar el recurso que va a incluir en la retención. Al crear una retención, debe elegir el método que usó para seleccionar los recursos que estarán incluidos en la retención legal. Puede elegir incluir una de las siguientes opciones:
 - Tipos de recursos específicos y IDs
 - Determinados almacenes de copia de seguridad
 - Todos los tipos de recursos o todos los almacenes de copia de seguridad en su cuenta
 - c. Especifique el intervalo de fechas de la retención legal. Introduzca las fechas en el formato AAAA:MM:DD (las fechas son inclusivas).

- d. Si lo desea, puede agregar etiquetas para la retención en Etiquetas de retención legal. Las etiquetas pueden ayudar a categorizar el almacén para futura referencia y organización. Puede agregar hasta 50 etiquetas.
5. Cuando esté satisfecho con la configuración de la nueva retención legal, haga clic en el botón Agregar nueva retención.

Cree una retención legal utilizando el AWS CLI

Puede crear una retención legal mediante el [create-legal-hold](#) comando.

```
aws backup create-legal-hold --title "my title" \
  --description "my description" \
  --recovery-point-selection
  "VaultNames=string,DateRange={FromDate=timestamp,ToDate=timestamp}"
```

Visualización de las retenciones legales

Puede ver los detalles de la retención legal en la AWS Backup consola o mediante programación.

Visualización de las retenciones legales en la consola

Para ver todas las retenciones legales de una cuenta mediante la consola de Backup,

1. [Abre la AWS Backup consola en /backup. https://console.aws.amazon.com](https://console.aws.amazon.com/backup/)
2. En la parte izquierda del panel, en Mi cuenta, haga clic en Retenciones legales.
3. La tabla de retenciones legales muestra el título, el estado, la descripción, el identificador y la fecha de creación de las retenciones existentes. Haga clic en el quilate (flecha hacia abajo) situado junto al encabezado de la tabla para filtrar la tabla por la columna seleccionada.

Visualización de las retenciones legales mediante programación

Para ver todas las retenciones legales mediante programación, puedes usar las siguientes llamadas a la API: y. [ListLegalHolds](#)[GetLegalHold](#)

La siguiente plantilla de JSON se puede utilizar para `GetLegalHold`.

```
GET /legal-holds/{legalHoldId} HTTP/1.1
```


Request

empty body

Response

```
{
  Title: string,
  Status: LegalHoldStatus,
  Description: string, // 280 chars max
  CancelDescription: string, // this is provided during cancel // 280 chars max
  LegalHoldId: string,
  LegalHoldArn: string,
  CreatedTime: number,
  CanceledTime: number,

  ResourceSelection: {
    VaultArns: [ string ]
    Resources: [ string ]
  },
  ResourceFilters: {
    DateRange: {
      FromDate: number,
      ToDate: number
    }
  }
}
```

La siguiente plantilla de JSON se puede utilizar para `ListLegalHolds`.

```
GET /legal-holds/
  &maxResults=MaxResults
  &nextToken=NextToken
```

Request

empty body

url params:

```
MaxResults: number // optional,
NextToken: string // optional
```

status: Valid values: CREATING | ACTIVE | CANCELED | CANCELING

```
maxResults: 1-1000
```

Response

```
{
  NextToken: token,
  LegalHolds: [
    Title: string,
    Status: string,
    Description: string, // 280 chars max
    CancelDescription: string, // this is provided during cancel // 280 chars max
    LegalHoldId: string,
    LegalHoldArn: string,
    CreatedTime: number,
    CanceledTime: number,
  ]
}
```

A continuación se muestran los posibles valores de estado.

Status	Description (Descripción)
CREATING	Los puntos de recuperación solicitados están en proceso de retención, y las solicitudes de eliminación de esos puntos de recuperación podrían prosperar, ya que la retención no ha terminado de crearse.
ACTIVE	Se ha creado la retención legal. Se retienen todos los puntos de recuperación incluidos en esta retención legal.
CANCELADO	Las retenciones legales están en proceso de eliminación, y las solicitudes de eliminación de puntos de recuperación bajo retención podrían tener éxito.

Status	Description (Descripción)
CANCELADO	La retención legal se libera por completo y ya no surte efecto. Los puntos de recuperación se pueden eliminar.

Liberación de una retención legal

Las retenciones legales se mantendrán en vigor hasta que las elimine un usuario con suficientes permisos. La eliminación de una retención legal también se conoce como cancelación, borrado o liberación de una retención legal. Al eliminar una retención legal, se elimina de todas las copias de seguridad a las que se asoció. Todas las copias de seguridad que hayan caducado durante la retención legal se eliminarán en un plazo de 24 horas tras la retirada de la retención legal.

Liberación de una retención legal mediante la consola de

Para liberar una retención mediante la consola

1. [Abre la AWS Backup consola en /backup. https://console.aws.amazon.com](https://console.aws.amazon.com/backup/)
2. Introduzca la descripción que le gustaría asociar a la liberación.
3. Revise los detalles y, a continuación, haga clic en Liberar retención.
4. Cuando aparezca el cuadro de diálogo Liberar retención, escriba `confirm` en el cuadro de texto para confirmar su intención de liberar la retención.
 - Marque la casilla que confirma que desea cancelar la retención.

En la página Retenciones legales puede ver todas sus retenciones. Si la liberación se ha realizado correctamente, el estado de esa retención se mostrará como `Released`.

Liberación de una retención legal de forma programática

Para eliminar una retención mediante programación, use la llamada a la API [CancelLegalHold](#).

Utilice la siguiente plantilla de JSON.

```
DELETE /legal-holds/{legalHoldId}
```

Request

```
{
  CancelDescription: String
  DeleteAfterDays: number // optional
}
```

DeleteAfterDays: optional.

Defaults to 180 days. how long to keep legal hold record after canceled.

This applies to the actual legal hold record only.

Recovery points are unlocked as soon as cancelation processes and are not subject to this date.

Response

Empty body

200 if successful

other standard codes

Protección contra malware en AWS Backup

Amazon Malware Protection se encarga de analizar tus copias de seguridad con GuardDuty malware. El uso de Amazon GuardDuty Malware Protection for AWS Backup le permite automatizar el escaneo de los puntos de recuperación a través de los flujos de trabajo de respaldo existentes o iniciar escaneos bajo demanda de copias de seguridad creadas anteriormente. Esta solución AWS nativa ayuda a garantizar que sus copias de seguridad estén limpias de posibles programas maliciosos, lo que le permite cumplir con los requisitos de conformidad y responder a los incidentes maliciosos con mayor rapidez, al garantizar la recuperación de datos limpios.

Para ver una lista de los tipos de recursos y las regiones compatibles, visite la [página de disponibilidad de funciones](#).

Temas

- [Integración con Amazon GuardDuty](#)
- [Permisos de acceso instantáneo a Backup](#)
- [¿Cómo utilizar el escaneo de malware](#)
- [Acceso](#)

- [Escaneos incrementales frente a escaneos completos](#)
- [Supervisar tus escaneos de malware](#)
- [Comprender los resultados de los escaneos](#)
- [Solución de problemas de escaneo](#)
- [Medición](#)
- [Cuotas](#)
- [Pasos de uso de la consola y la CLI para los tipos de análisis de malware](#)

Integración con Amazon GuardDuty

AWS Backup se integra con Amazon GuardDuty Malware Protection para proporcionar detección de amenazas para sus puntos de recuperación. Cuando inicias un análisis de malware, llamas AWS Backup automáticamente a la `StartMalwareScan` API GuardDuty de Amazon una vez completada cada copia de seguridad y le pasas los detalles del punto de recuperación y las credenciales de tu función de escáner. Amazon comienza GuardDuty entonces a leer, descifrar y escanear todos los archivos y objetos de la copia de seguridad.

Cuando Amazon GuardDuty accede a tus datos de respaldo, se inicia sesión en ese acceso AWS CloudTrail para mayor visibilidad.

Para obtener más información sobre esta integración, consulte la [documentación de Amazon GuardDuty Malware Protection](#).

Permisos de acceso instantáneo a Backup

Al utilizar Amazon GuardDuty Malware Protection for AWS Backup con copias de seguridad de S3, Amazon GuardDuty accede a las copias de seguridad de S3 mediante tres APIs métodos: `CreateBackupAccessPoint`, `DescribeBackupAccessPoint`, y `DeleteBackupAccessPoint`.

Amazon GuardDuty utiliza `CreateBackupAccessPoint` para acceder a tus datos de copia de seguridad cifrados. Durante el trabajo de escaneo, se GuardDuty utiliza `DescribeBackupAccessPoint` para verificar que el punto de acceso se haya creado correctamente. Una vez que se complete el escaneo, GuardDuty llama `DeleteBackupAccessPoint` para eliminar su acceso a la copia de seguridad.

Este flujo de trabajo se aplica tanto a las copias de seguridad de S3 como a las copias de seguridad de EC2 /EBS almacenadas en un almacén cerrado de forma lógica.

¿Cómo utilizar el escaneo de malware

Cuando utilizas Amazon GuardDuty Malware Protection con AWS Backup, puedes escanear automáticamente tus copias de seguridad en busca de malware. Esta integración le ayuda a detectar códigos maliciosos en sus copias de seguridad e identificar puntos de recuperación limpios para las operaciones de restauración.

Amazon GuardDuty Malware Protection admite dos flujos de trabajo principales para escanear las copias de seguridad:

- Escaneo automático de malware mediante planes de respaldo: habilite el escaneo de malware en los planes de respaldo para automatizar la detección de malware con ellos AWS Backup. Cuando está activado, inicia AWS Backup automáticamente un GuardDuty escaneo de Amazon cada vez que se completa correctamente la copia de seguridad. Puedes configurar el escaneo completo o incremental según las reglas específicas del plan de copias de seguridad, que determinan la frecuencia con la que se escanean las copias de seguridad. Para obtener más información sobre los tipos de escaneo, consulte [the section called “Escaneos incrementales frente a escaneos completos”](#) a continuación. AWS Backup recomienda activar el análisis automático de malware en los planes de copia de seguridad para detectar de forma proactiva las amenazas tras la creación de la copia de seguridad.
- Escaneos bajo demanda: ejecute escaneos bajo demanda para escanear manualmente las copias de seguridad existentes, eligiendo entre escaneos completos o incrementales. AWS Backup recomienda utilizar escaneos bajo demanda para identificar la última copia de seguridad limpia. Cuando escanee antes de una operación de restauración, utilice un análisis completo para examinar toda la copia de seguridad con el modelo de detección de amenazas más reciente.

Acceso

Antes de empezar con la protección contra el malware, su cuenta debe tener los permisos necesarios para realizar las operaciones.

AWS Backup El análisis de software malicioso requiere dos funciones de IAM para analizar los puntos de recuperación en busca de posibles programas maliciosos:

- En primer lugar, la política `AWSBackupServiceRolePolicyForScans` gestionada debe estar asociada a su función de backup actual o nueva. Es la misma función que se encuentra en la asignación de recursos para su plan de respaldo en la consola o mediante la [BackupSelection](#)

[API](#). Esta política gestionada permite AWS Backup iniciar escaneos de malware con Amazon GuardDuty.

- En segundo lugar, se requiere una nueva función de escáner con una política `AWSBackupGuardDutyRolePolicyForScans` gestionada de confianza `malware-protection.guarddduty.amazonaws.com`. Es la misma función que se encuentra en la parte de protección contra el malware de su plan de respaldo en la consola o en la configuración de escaneo de su [BackupPlan API](#). Esta función se transfiere AWS Backup a Amazon GuardDuty cuando se inicia un escaneo, lo que proporciona acceso a las copias de seguridad.

Escaneos incrementales frente a escaneos completos

Con el escaneo de malware, tiene la opción de elegir entre escaneos incrementales o completos en función de sus requisitos de seguridad y consideraciones de costo.

Los escaneos incrementales analizan solo los datos que han cambiado entre el punto de recuperación objetivo y el punto de recuperación base. Estos escaneos son más rápidos y rentables para el escaneo normal, lo que los hace ideales para realizar copias de seguridad periódicas frecuentes en las que se desee escanear los datos recién respaldados.

Incluso cuando se selecciona el escaneo incremental, AWS Backup realiza un escaneo completo en las siguientes situaciones:

- **Análisis por primera vez:** el análisis inicial de un recurso es siempre un análisis completo, lo que permite GuardDuty a Amazon establecer una línea base de posibles amenazas. Los escaneos posteriores se realizarán entonces de forma incremental.
- **Línea base caducada:** si su punto de recuperación de referencia se escaneó hace más de 90 días, se realizará una exploración completa. Como Amazon GuardDuty conserva la información de búsqueda solo durante 90 días, se debe establecer un nuevo punto de referencia para garantizar la precisión de los resultados de digitalización.
- **Línea base eliminada:** si el punto de recuperación base se elimina antes de que comience el siguiente análisis incremental, se realizará automáticamente un análisis completo.

Los escaneos completos examinan todo el punto de recuperación, independientemente de los escaneos anteriores. Si bien estos escaneos ofrecen una cobertura integral, tardan más en completarse e incurrir en costos más altos. Puede realizar escaneos completos bajo demanda o programarlos a través de sus planes de respaldo. AWS Backup recomienda configurar escaneos periódicos completos en sus planes de copia de seguridad a intervalos prolongados para garantizar

que todos los datos de la copia de seguridad se escaneen periódicamente con el modelo de identificación de malware más reciente.

Para lograr una seguridad óptima frente a una gestión de costes, tenga en cuenta la frecuencia de las copias de seguridad al elegir los tipos de análisis.

 Note

Actualmente, los puntos de recuperación continua de Amazon S3 no admiten el escaneo de malware. Para escanear las copias de seguridad continuas de Amazon S3, configure las copias de seguridad periódicas de sus recursos de Amazon S3 y habilite el análisis de malware en esas copias de seguridad periódicas. Puede utilizar una [combinación de copias de seguridad continuas y periódicas](#) para sus buckets de Amazon S3.

 Note

El análisis incremental de malware no es compatible con los puntos de EC2 recuperación de Amazon que se encuentren en una [bóveda aislada de forma lógica ni con los puntos](#) de recuperación de Amazon EC2 copiados.

Supervisar tus escaneos de malware

Una vez activado el escaneo, tanto AWS Backup Amazon como Amazon GuardDuty proporcionan mecanismos de supervisión y notificación que puedes usar para realizar un seguimiento de tus resultados:

- **AWS Backup Consola:** La AWS Backup consola funciona con `ListScanJobs` y `DescribeScanJob` APIs. Puede visitar la sección Protección contra el malware para ver la lista de trabajos de escaneo, que representa el estado del trabajo y los resultados del escaneo. AWS Backup también es compatible con una `ListScanJobSummaries` API, aunque no está disponible en la consola.
- **AWS Backup Audit Manager:** puede configurar un informe de escaneo para ver todos los trabajos de escaneo de malware AWS Backup iniciados en las últimas 24 horas.
- **Amazon GuardDuty Console:** si Amazon base GuardDuty está activado, puedes ver los detalles en los resultados del análisis de malware e investigar el malware en la página de GuardDuty

hallazgos de Amazon. Puedes ver información como la amenaza y el nombre del archivo, la ruta del archivo, los datos objects/files escaneados, los bytes escaneados, etc. Ten en cuenta que esta información detallada sobre amenazas no está disponible en Internet y debes tener los GuardDuty permisos de Amazon correspondientes para verla. AWS Backup

- Amazon EventBridge: AWS Backup Tanto Amazon como Amazon GuardDuty emiten EventBridge eventos, lo que permite alertar de forma sincrónica a los administradores de copias de seguridad y seguridad. Puede configurar reglas personalizadas para recibir notificaciones cuando se completen los escaneos o se detecte malware.
- AWS CloudTrail: AWS Backup Tanto Amazon como Amazon GuardDuty emiten CloudTrail eventos, lo que te permite monitorizar el acceso a la API.

Comprender los resultados de los escaneos

Sus trabajos de escaneo AWS Backup tendrán un estado de escaneo y un resultado de escaneo.

Estados de escaneo

El estado de escaneo indica el estado de la tarea y puede tener valores de:

CREATED, COMPLETED, COMPLETED_WITH_ISSUES, RUNNING, FAILED, o CANCELED.

Existen varias situaciones en las que el trabajo de escaneo terminará con el estado COMPLETED_WITH_ISSUES siguiente:

En el caso de las copias de seguridad de Amazon S3, existen size/type limitaciones de objetos que impiden que se escaneen los objetos. Cuando se omite al menos un objeto en un escaneo, el trabajo de escaneo correspondiente se marcará como COMPLETED_WITH_ISSUES. En el caso de las copias de seguridad de EC2 Amazon/Amazon EBS, existen size/quantity limitaciones de volumen que hacen que se omitan los volúmenes durante el escaneo. Estas situaciones darán como resultado un trabajo de copia de seguridad de EC2 Amazon/Amazon EBS. COMPLETED_WITH_ISSUES

Si tu trabajo termina con el estado COMPLETED_WITH_ISSUES y necesitas más información sobre los motivos, tendrás que obtener esos detalles del trabajo de escaneo correspondiente a través de Amazon GuardDuty.

Note

Los trabajos de escaneo incremental solo escanean la diferencia de datos entre dos copias de seguridad. Por lo tanto, si un trabajo de escaneo incremental no encuentra ninguna de las

situaciones descritas anteriormente, finalizará en ese estado COMPLETE y no lo heredará del punto COMPLETED_WITH_ISSUES de recuperación base.

En raras ocasiones, Amazon GuardDuty puede experimentar problemas internos al escanear archivos y objetos, y es posible que se agoten los intentos de volver a intentarlo. Cuando esto ocurre, el trabajo de escaneo aparece como FAILED en AWS Backup y COMPLETED_WITH_ISSUES en Amazon GuardDuty. Esta diferencia de estado te permite ver los resultados de los escaneos disponibles en Amazon GuardDuty e indica que no todos los archivos y objetos compatibles se escanearon correctamente.

Resultados del escaneo

Los resultados del escaneo indican un resultado agregado de Amazon GuardDuty y pueden tener valores de: THREATS_FOUND, o NO_THREATS_FOUND.

Los resultados del análisis indican si se ha detectado un posible malware en sus puntos de recuperación. Un NO_THREATS_FOUND estado significa que no se ha detectado ningún malware potencial, mientras que THREATS_FOUND indica que se ha descubierto un malware potencial. Para obtener información detallada sobre las amenazas, acceda a los GuardDuty hallazgos completos de Amazon a través de la GuardDuty consola de Amazon o APIs. Los resultados del escaneo también están disponibles a través de EventBridge eventos, lo que le permite crear flujos de trabajo automatizados que respondan a las copias de seguridad infectadas.

Amazon GuardDuty conserva los resultados durante 90 días y rastrea los archivos u objetos mediante escaneos incrementales para monitorear si se eliminan las amenazas o si cambian las firmas del malware. Por ejemplo, si se detecta malware en la copia de seguridad 2, se mostrará el resultado del análisis THREATS_FOUND. Al realizar un análisis incremental de la copia de seguridad 3 utilizando la copia de seguridad 2 como base, el resultado del análisis se mantiene THREATS_FOUND a menos que se haya eliminado la amenaza de los datos.

Solución de problemas de escaneo

Los errores de escaneo más comunes incluyen permisos de IAM insuficientes, límites de servicio y problemas de acceso a los recursos.

Los errores de permisos se producen cuando la función de copia de seguridad carece de AWSBackupServiceRolePolicyForScans permisos o la función de escáner no tiene AWSBackupGuardDutyRolePolicyForScans las relaciones de confianza adecuadas.

Los errores del límite de servicio se producen cuando se superan los 150 escaneos simultáneos por cuenta o los 5 escaneos simultáneos por tipo de recurso; los trabajos de escaneo permanecerán intactos hasta CREATED que haya capacidad disponible.

Los errores de acceso denegado pueden indicar puntos de recuperación cifrados sin AWS KMS los permisos adecuados o puntos de recuperación principales eliminados en el caso de escaneos incrementales.

Los errores de tiempo de espera pueden producirse con puntos de recuperación muy grandes o durante períodos de alta GuardDuty carga de Amazon.

Para solucionar problemas, compruebe el estado del trabajo de escaneo mediante la DescribeScanJob API, verifique las configuraciones de las funciones de IAM, asegúrese de que los puntos de recuperación existan y sean accesibles y considere la posibilidad de cambiar a escaneos completos si faltan las referencias principales del escaneo incremental.

Supervise el uso simultáneo de escaneos e implemente la fluctuación en los flujos de trabajo automatizados para evitar sobrepasar los límites de servicio.

Medición

Amazon GuardDuty proporciona y factura la protección contra el malware. No verás ningún AWS Backup cargo relacionado con el uso de esta función. Todo el uso se puede ver en GuardDuty la facturación de Amazon. Para obtener más información, visita los [GuardDuty precios de Amazon](#).

Cuotas

AWS Backup Tanto Amazon como Amazon GuardDuty tienen límites de cuota para Amazon GuardDuty Malware Protection para AWS Backup.

Para obtener más información, visita [AWS Backup cuotas y cuotas](#) de [Amazon GuardDuty](#).

Pasos de uso de la consola y la CLI para los tipos de análisis de malware

En las siguientes secciones se muestran los pasos para configurar los diferentes tipos de análisis de malware mediante la consola y AWS CLI.

¿Cómo configurar los escaneos de malware

Consola

1. Vaya a la AWS Backup consola → Planes de backup
2. Cree un nuevo plan de respaldo o seleccione un plan existente
3. Activa la opción de protección contra malware
4. Seleccione la función de escáner para elegir una nueva función de escáner. Asegúrese de que tanto la función de copia de seguridad como la de escáner tengan los permisos adecuados, tal y como se explica en la sección [the section called “Acceso”](#).
5. Seleccione los tipos de recursos escaneables. Esto filtrará el escaneo de malware según los criterios de selección de recursos que haya elegido. Por ejemplo, si su selección de tipo de recurso escaneable es Amazon EBS, pero la selección de recursos de su plan incluye Amazon EBS y Amazon S3, solo se realizarán escaneos de malware de Amazon EBS.
6. Defina el tipo de escaneo para cada regla de respaldo. Puede elegir entre escaneo completo, incremental o sin escaneo. La selección del tipo de escaneo significa que el escaneo se realizará con la frecuencia programada de la regla de respaldo asociada.
7. Guarde el plan de respaldo

AWS CLI

CreateBackupPlan

Puede crear un plan de respaldo con el escaneo de malware habilitado mediante el [create-backup-plan](#) comando.

```
aws backup create-backup-plan \  
  --region us-west-2 \  
  --cli-input-json '{  
    "BackupPlan": {  
      "BackupPlanName": "scan-initial-test-demo",  
      "Rules": [  
        {  
          "RuleName": "full",  
          "TargetBackupVaultName": "Default",  
          "ScheduleExpression": "cron(0 * * * ? *)",  
          "StartWindowMinutes": 120,  
          "CompletionWindowMinutes": 6000,  
          "Lifecycle": {  
            "DeleteAfterDays": 3,  
            "OptInToArchiveForSupportedResources": true  
          }  
        },  
      ],  
    }  
  }'
```

```

        "RecoveryPointTags": {
            "key1": "foo",
            "key2": "foo"
        },
        "EnableContinuousBackup": true,
        "ScanActions": [
            {
                "MalwareScanner": "GUARDDUTY",
                "ScanMode": "FULL_SCAN"
            }
        ]
    },
    {
        "RuleName": "incremental",
        "TargetBackupVaultName": "Default",
        "ScheduleExpression": "cron(30 * * * ? *)",
        "StartWindowMinutes": 100,
        "CompletionWindowMinutes": 5000,
        "Lifecycle": {
            "DeleteAfterDays": 2,
            "OptInToArchiveForSupportedResources": true
        },
        "RecoveryPointTags": {
            "key1": "foo",
            "key2": "foo"
        },
        "EnableContinuousBackup": true,
        "ScanActions": [
            {
                "MalwareScanner": "GUARDDUTY",
                "ScanMode": "INCREMENTAL_SCAN"
            }
        ]
    }
],
"ScanSettings": [
    {
        "MalwareScanner": "GUARDDUTY",
        "ResourceTypes": ["EBS", "EC2", "S3"],
        "ScannerRoleArn": "arn:aws:iam::300949271314:role/
TestBackupScannerRole"
    }
]
}

```

```
}'
```

UpdateBackupPlan

Puede actualizar un plan de respaldo con la detección de malware habilitada mediante el [update-backup-plan](#) comando.

```
aws backup update-backup-plan \
  --region us-west-2 \
  --cli-input-json '{
    "BackupPlanId": "d1391282-68cf-4fce-93ad-e08bc5178bac",
    "BackupPlan": {
      "BackupPlanName": "scan-initial-test-demo",
      "Rules":
      [
        {
          "RuleName": "full",
          "TargetBackupVaultName": "Default",
          "ScheduleExpression": "cron(0 * * * ? *)",
          "StartWindowMinutes": 60,
          "CompletionWindowMinutes": 3000,
          "Lifecycle":
            {
              "DeleteAfterDays": 6,
              "OptInToArchiveForSupportedResources": false},
          "RecoveryPointTags":
            {
              "key1": "foo",
              "key2": "foo"},
          "EnableContinuousBackup": false,
          "ScanActions":
            [
              {
                "MalwareScanner": "GUARDDUTY",
                "ScanMode": "FULL_SCAN"}
            ]
        },
        {
          "RuleName": "incremental",
          "TargetBackupVaultName": "Default",
          "ScheduleExpression": "cron(30 * * * ? *)",
          "StartWindowMinutes": 120,
          "CompletionWindowMinutes": 6000,
          "Lifecycle":
            {
              "DeleteAfterDays": 9,
```

```

        "OptInToArchiveForSupportedResources": false},
    "RecoveryPointTags":
        {"key1": "foo",
         "key2": "foo"},
    "EnableContinuousBackup": false,
    "ScanActions":
        [
            {
                "MalwareScanner": "GUARDDUTY",
                "ScanMode": "INCREMENTAL_SCAN"
            }
        ]
    },
    "ScanSettings":
        [
            {
                "MalwareScanner": "GUARDDUTY",
                "ResourceTypes":
                    ["ALL", "EBS"],
                "ScannerRoleArn": "arn:aws:iam::300949271314:role/
TestBackupScannerRole"
            }
        ]
    }
}'

```

Notas clave

- Es necesario introducir el ARN de destino antes de activar las opciones de escaneo (consola)
- Todas las configuraciones requieren tanto la función de IAM de respaldo como la de IAM del escáner
- Se utiliza `aws backup list-scan-jobs` para ver todos los trabajos de escaneo (AWS CLI)
- Las implicaciones económicas varían según el tipo de escaneo (incremental o completo) y la frecuencia

AWS CLI Notas clave

- Se utiliza `aws backup list-scan-jobs` para ver todos los trabajos de escaneo (AWS CLI)

- Los resultados del escaneo están disponibles a través `describe-recovery-point` de una API con `ScanResults` campo
- Todas las configuraciones requieren tanto la función de IAM de respaldo como la de IAM de escáner
- La estructura del plan de respaldo de JSON incluye tanto `ScanSettings` a nivel del plan como en las reglas `ScanActions`

Resiliencia en AWS Backup

AWS Backup se toma muy en serio su resiliencia (y la seguridad de sus datos).

AWS Backup almacena sus copias de seguridad con al menos la misma resistencia y durabilidad que las que le proporcionaría el AWS servicio original de su recurso si lo hubiera hecho allí.

AWS Backup está diseñado para utilizar la infraestructura AWS global a fin de replicar sus copias de seguridad en varias zonas de disponibilidad y lograr una durabilidad del 99,19% (11 nueves) en un año determinado, siempre que se respete la documentación actual. AWS Backup

AWS Backup cifra sus planes de copia de seguridad en reposo y realiza copias de seguridad continuas de los mismos. También puede restringir el acceso a sus planes de respaldo mediante credenciales y políticas AWS Identity and Access Management (IAM). Para obtener más información, consulte [Autenticación](#), [Control de acceso](#) y [Prácticas recomendadas de seguridad en IAM](#).

La infraestructura AWS global se basa en zonas Regiones de AWS de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. AWS Backup almacena sus copias de seguridad en todas las zonas de disponibilidad. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples. Para obtener más información, consulte el [Acuerdo de nivel de servicio \(SLA\) de AWS Backup](#).

Además, le AWS Backup permite copiar sus copias de seguridad en todas las regiones para aumentar aún más la resiliencia. Para obtener más información sobre la función de copia AWS Backup entre regiones, consulte [Creación de una copia de seguridad](#).

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte [Infraestructura AWS global](#).

AWS Backup cuotas

Se aplican las siguientes cuotas cuando se trabaja con AWS Backup.

Cuotas

- [Copia de seguridad](#)
- [Índice de copias de seguridad y cuotas de búsqueda](#)
- [Cuotas de políticas](#)
- [Cuotas de escaneo de malware](#)
- [Cuotas de recursos de Amazon Timestream](#)
- [AWS Backup Cuotas de Audit Manager](#)
- [Cuotas del plan de pruebas de restauración](#)
- [AWS Backup gateway cuotas](#)
- [Cuotas de Amazon EKS](#)
- [Cuotas de bóvedas con huecos lógicos](#)
- [Cuotas relacionadas](#)

Copia de seguridad

Name	Predeterminado	Ajustable
Total de almacenes (de copia de seguridad y aislados lógicamente) por región y cuenta	300	Sí
Puntos de recuperación por almacén de copia de seguridad	1 000 000	Sí
Planes de copias de seguridad por región y por cuenta	300	Sí

Name	Predeterminado	Ajustable
Versiones por plan de copia de seguridad	2,000	Sí
Asignaciones de recurso por plan de copia de seguridad	100	No
Buckets de Amazon S3 por cuenta	100	Sí
Trabajos de copia simultáneos entre regiones por cuenta en la región de destino	100 ²	No
Trabajos de copia adicionales entre regiones por almacén en una región de destino tras alcanzar el límite indicado en la fila anterior. ¹	5 ²	No
Copias simultáneas entre cuentas que se pueden realizar del mismo recurso en la misma región de destino	30	No
Trabajos de copia de seguridad y copia simultáneos por recurso	1	No
Etiquetas por recurso seleccionado en una política de copias de seguridad entre cuentas	30	No. Incluya etiquetas adicionales mediante múltiples asignaciones de recursos o planes de copia de seguridad.
Hipervisores	20	No
Retenciones legales por cuenta	50	No

Name	Predeterminado	Ajustable
Capas de copia de seguridad anidadas de pilas de aplicaciones	10	No

¹ El límite de trabajos de copia simultáneos de una región a otra es de 100 por cuenta y región. Una vez alcanzado este límite, si un almacén específico de la región de destino tiene menos de cinco trabajos de copia simultáneos, se pueden iniciar nuevos trabajos de copia hasta un máximo de cinco.

² El límite solo se aplica a los tipos de recurso [completamente administrados por AWS Backup](#).

Índice de copias de seguridad y cuotas de búsqueda

Name	Predeterminado	Ajustable
Trabajos de indexación simultáneos en la cuenta (en la mayoría de las Regiones de AWS)	40	Sí
Trabajos de indexación simultáneos en cuentas en Asia Pacífico (Malasia), Canadá (Central), Asia Pacífico (Tailandia) y México (Central). Regiones de AWS	10	Sí
Trabajos de indexación simultáneos para cada recurso	5	No
Trabajo de indexación simultáneo bajo demanda	1	No
Trabajos de búsqueda simultáneos en la cuenta	10	

Name	Predeterminado	Ajustable
Trabajos de exportación simultáneos	5	
Número de puntos de recuperación incluidos en el trabajo de búsqueda	20	
Trabajos de restauración simultáneos en los archivos de Amazon EBS (en la mayoría de las Regiones de AWS)	25	
Trabajos de restauración simultáneos a nivel de archivos de Amazon EBS en Asia Pacífico (Malasia) , Canadá (Central), Asia Pacífico (Tailandia) y México (Central). Regiones de AWS	5	

Cuotas de políticas

Name	Predeterminado	Ajustable
Asignaciones de recurso por plan de copia de seguridad	100	No
Etiquetas en una selección de recursos	30	No
Selecciones de recursos que utilizan etiquetas en un plan	10	No
Reglas del plan de copia de seguridad en un plan	10	No

Name	Predeterminado	Ajustable
Etiquetas agregadas a puntos de recuperación	10	No
Acciones de copia según la regla de copia de respaldo	5	No
Condiciones de una asignación de recursos en un plan de copia de seguridad	30	No

Cuotas de escaneo de malware

En la siguiente tabla se muestran las cuotas de análisis de AWS Backup malware con Amazon GuardDuty.

Name	Predeterminado	Ajustable
Ejecutar trabajos de escaneo por recurso y por cuenta	5	Sí
Ejecutar trabajos de escaneo por punto de recuperación por cuenta	1	No
Ejecutar trabajos de escaneo por cuenta	150	Sí
Se crearon trabajos de escaneo por recurso y por cuenta	10	No
Restricción básica de escaneo incremental	1	No

Cuando alcance el límite de trabajos de escaneo creados por recurso y cuenta, no aprobaremos el trabajo más antiguo en cola.

También es posible que te encuentres con cuotas impuestas por Amazon GuardDuty. Para obtener más información, consulta [GuardDuty las cuotas de Amazon](#) en Referencia general de AWS.

Cuotas de recursos de Amazon Timestream

Name	Predeterminado	Ajustable
Trabajos de copia de seguridad simultáneos de Timestream por cuenta	4	Sí
Trabajos de restauración simultáneos de Timestream por cuenta	1	Sí

AWS Backup Cuotas de Audit Manager

Name	Predeterminado	Ajustable
Marcos por región y por cuenta	15	Sí
Controles por región y por cuenta	50	Sí
Planes de informe por cuenta	20	Sí
Marcos por plan de informes	1 000	No
[Número de cuentas] multiplicado por el [número regiones en un plan de informes]	300	No
[Número de cuentas] multiplicado por [número de regiones]	100 000	No

Name	Predeterminado	Ajustable
en un plan de informes] multiplicado por el [número de trabajos diarios más evaluacio nes en un plan de informes]		

Cuotas del plan de [pruebas de restauración](#)

Name	Predeterminado	Ajustable
Planes de prueba de restaurac ión	100	No
Etiquetas por plan	50	No
Selecciones por plan	30	No
ARNs por selección de pruebas de restauración	30	No
Condiciones por selección (ambas <code>StringEquals</code> y <code>StringNotEquals</code>)	30	No
Selectores de almacén por selección de pruebas de restauración	30	No
Valor máximo (en días) del periodo de selección	365 días	No
Límites de horas del periodo de inicio	Mínimo: 1 hora; máximo: 168 horas	No
Longitud máxima de caractere s del nombre del plan de prueba de restauración	50 caracteres (alfanuméricos y guiones bajos, sin espacios en blanco)	No

Name	Predeterminado	Ajustable
Longitud máxima de caracteres del nombre de la selección de pruebas de restauración	50 caracteres (alfanuméricos y guiones bajos, sin espacios en blanco)	No

Cada tipo de recurso tiene un límite en la cantidad de trabajos de restauración simultáneos que puede haber al mismo tiempo para los trabajos de restauración que se crean mediante un plan de prueba de restauración. Una vez alcanzado este límite, no se crearán nuevos trabajos de restauración para ese tipo de recurso hasta que un trabajo con el estado RUNNING pase al estado COMPLETED.

Si un trabajo de restauración programado no se ha iniciado debido a esta cuota, dicho trabajo recibirá el estado FAILED y se mostrará el mensaje de estado "Restore job was unable to start within the specified start window. Try increasing your start window.". Si recibe un error del trabajo con este mensaje de estado, lo primero que se recomienda hacer es aumentar el período de inicio con tiempo suficiente para permitir que los trabajos finalicen. A continuación, vuelva a intentar ejecutar los trabajos.

Tenga en cuenta que las cuotas no se aplican a los trabajos de restauración bajo demanda, sino a los trabajos de restauración creados según un [plan de prueba de restauración](#). Para algunos tipos de recurso, puede solicitar un aumento del límite de la cuota.

Name	Predeterminado	Ajustable
Amazon Aurora	40	Sí
Amazon DocumentDB	40	Sí
Amazon DynamoDB	40	No
Amazon EBS	100	Sí
Amazon EC2	100	Sí
Amazon EFS	30	Sí
Amazon FSx	40	Sí

Name	Predeterminado	Ajustable
Amazon Neptune	40	Sí
Amazon RDS	40	Sí
Amazon S3	30	Sí

AWS Backup gateway cuotas

Name	Predeterminado	Ajustable
Trabajos de copia de seguridad o restauración por puerta de enlace	4	No. Cree más puertas de enlace y conéctelas al hipervisor.

Cuotas de Amazon EKS

Name	Predeterminado	Ajustable
Espacios de nombres por copia de seguridad de clúster EKS	1 000	Sí
Copias de seguridad de almacenamiento persistente por cada copia de seguridad de un clúster	1 000	Sí
Restablece los trabajos por clúster de EKS de destino	1	No
EKS Restore los trabajos por cuenta	5	Sí

Cuotas de bóvedas con huecos lógicos

Tipo de recurso	Número máximo de copias simultáneas
EC2	El límite de copias simultáneas de EBS se aplica a todas las instantáneas copiarse como parte de una copia de la AML.
EBS	20
Aurora	20
DocumentDB	20
Neptune	20
Storage Gateway	5
FSx	5

Cuotas relacionadas

Hay [cuotas para una sola asignación de recursos](#) en una sola regla de copia de seguridad. Puede crear un plan de copia de seguridad con varias reglas de copia de seguridad.

Al administrar copias de seguridad en varias cuentas mediante AWS Organizations, es posible que se le AWS Organizations impongan cuotas. Para conocer estas cuotas, consulte [Cuotas para AWS Organizations](#) en la Guía del usuario de AWS Organizations .

También es posible que te encuentres con cuotas impuestas por un servicio AWS Backup compatible, entre las que se incluyen las siguientes:

- [Amazon Elastic File System](#)
- [Amazon Elastic Block Store](#)
- [Amazon RDS](#)
- [Amazon Aurora](#)
- [Amazon EC2](#)

- [AWS Storage Gateway](#)
- [Amazon DynamoDB](#)
- [Amazon FSx para Lustre](#)
- [Servidor FSx de archivos Amazon para Windows](#)
- [Amazon DocumentDB](#)
- [Amazon Neptune](#)
- [Amazon Simple Storage Service](#)
- [Amazon Timestream](#)

Monitorización AWS Backup

AWS Backup funciona con otras AWS herramientas para permitirle monitorear sus cargas de trabajo. Estas herramientas incluyen lo siguiente:

- [AWS Backup paneles de consola](#)
 - El panel de trabajos ofrece un monitorización de estado de los trabajos, donde puede ver métricas que muestran trabajos correctos y con error, filtradas por motivos, cuentas, región y tipo de recurso.
 - El panel de empleos está disponible en las regiones en las que se admite AWS Backup Audit Manager. Consulte estas regiones en [Disponibilidad de las funciones por Región de AWS](#). Todas las demás regiones podrán acceder al [CloudWatch Tablero](#).
- Amazon CloudWatch y Amazon EventBridge para supervisar AWS Backup los procesos.
 - Puede utilizarlos CloudWatch para realizar un seguimiento de las métricas, crear alarmas y ver los paneles.
 - Se puede usar EventBridge para ver y monitorear AWS Backup eventos.

Para obtener más información, consulte [Monitorización de AWS Backup eventos con Amazon EventBridge](#) y.

- AWS CloudTrail para supervisar las llamadas a la AWS Backup API. Puede identificar la hora, la IP de origen, los usuarios y las cuentas que realizan esas llamadas. Para obtener más información, consulte [Registrar las llamadas a AWS Backup la API con CloudTrail](#).
- Amazon Simple Notification Service (Amazon SNS) para suscribirse a temas AWS Backup relacionados, como eventos de copia de seguridad, restauración y copia. Para obtener más información, consulte [Opciones de notificación con AWS Backup](#).

AWS Backup paneles de consola

Note

El panel de trabajos está disponible en todas las regiones en las que se admite AWS Backup Audit Manager. Consulte estas regiones en [Disponibilidad de las funciones por Región de AWS](#). Todas las demás regiones podrán acceder al [CloudWatch Tablero](#).

Temas

- [Información general de los paneles de copia de seguridad](#)
- [Visualización del panel de trabajos](#)
- [Motivos para los trabajos problemáticos](#)
- [Obtención de datos del panel mediante AWS CLI](#)

Información general de los paneles de copia de seguridad

AWS Backup proporciona un panel de tareas en la consola para ayudarle a supervisar el estado de sus tareas de backup, copia y restauración. Los mismos datos que se muestran visualmente en la consola se pueden recuperar mediante la línea de comandos AWS CLI.

El panel de trabajos se puede utilizar para identificar problemas relacionados con trabajos de copia de seguridad, copia y restauración mediante monitorización de nivel de la organización o de cuentas de miembros. Con esta información puede identificar y diagnosticar eventos y posibles problemas para garantizar la fidelidad de sus actividades.

El panel de trabajos puede mostrar dos periodos. De forma predeterminada, se muestran los datos de los últimos 14 días, pero puede cambiar la vista para mostrar los 7 últimos días. Si cambias el periodo, los datos se actualizarán para reflejar el nuevo intervalo de tiempo.

Tenga en cuenta que el panel muestra los datos hasta las 0:00 UTC más recientes; es decir, no se incluyen los datos del día actual. El panel se actualiza a diario aproximadamente entre las 1:30 y las 2:30 UTC.

Visualización del panel de trabajos

Para ver el panel de tareas, [inicie sesión en la AWS Backup consola](#) y seleccione Paneles de tareas en la barra de navegación izquierda.

En la página del panel de trabajos puede seleccionar la pestaña de trabajos de copia de seguridad, copia o restauración.

La descripción general del panel de trabajos muestra la vista agregada durante el periodo de tiempo especificado para la actividad laboral, incluidos los trabajos completados, completados con problemas, vencidos y fallidos. De forma predeterminada, se muestran los datos de los últimos 14 días, pero puede cambiar la vista para mostrar 7 días.

Note

`Completed with issues` es el estado de un trabajo que se muestra en la consola y que indica un trabajo completado con un mensaje de estado.

Estado del trabajo

El gráfico de líneas muestra las líneas de tasas de trabajos correctos y con error a lo largo del tiempo. La línea de tasa de trabajos correctos muestra una suma de los trabajos completados y completados con problemas. La línea de tasa de trabajos con error muestra la suma de los trabajos con error y vencidos según el intervalo de tiempo especificado.

No se incluyen los trabajos no completados o sin error (los trabajos con estado de creados, pendientes, en ejecución, anulados, cancelando o parciales); los totales porcentuales pueden no ser iguales al 100 %.

Estado del trabajo a lo largo del tiempo

Con el gráfico de barras puede generar un gráfico de barras personalizado que muestre el número de trabajos de cada categoría (completados, completados con problemas, con error y vencidos), distribuidos por días.

En los menús desplegables, elija los estados, los tipos de recursos y AWS las regiones que desee ver en el gráfico. Si desea explorar más a fondo la selección, elija Ver trabajos para ver una parte prefiltrada de la página de monitorización de trabajos/múltiples cuentas.

Puede pasar el ratón sobre una barra para mostrar una ventana emergente con datos detallados de los trabajos correspondientes a la fecha seleccionada.

Trabajos problemáticos

Un trabajo problemático es aquel que tiene el estado Con error, Vencido o Completo con problemas. Cada gráfico muestra la métrica correspondiente que contiene las cuentas, los tipos de recursos o los principales motivos con el mayor número de trabajos problemáticos.

La pantalla predeterminada ordena el widget del panel por la métrica especificada en orden descendente, empezando por la métrica con el número más alto de trabajos problemáticos que corresponden a la métrica.

La pantalla de cuentas más problemáticas solo será visible en las cuentas que tengan acceso a través de Organizations, como las cuentas administrativas y las cuentas de administrador delegado. Si es visible, puede pasar el ratón sobre una cuenta para mostrar el número de trabajos problemáticos que corresponden a la cuenta elegida.

Puede seleccionar una barra dentro del gráfico para abrir una ventana emergente. En esta ventana puede seleccionar el estado de un trabajo para abrir una tabla de monitorización de trabajos/múltiples cuentas filtrada por el estado seleccionado.

Motivos para los trabajos problemáticos

El widget Principales motivos que ocasionan problemas muestra la categoría de códigos de mensaje a la que pertenecen los mensajes de error. Sin embargo, es posible que la categoría no explique los problemas que experimenta un trabajo. Amplíe las categorías de códigos de mensaje que aparecen a continuación para obtener más información sobre los mensajes o errores específicos que podrían surgir en sus trabajos.

"VSS_ERROR"

- "El intento de copia de seguridad de Windows VSS ha producido error porque la instancia o el agente SSM tienen un estado no válido o privilegios insuficientes."
- "El intento de copia de seguridad de Windows VSS ha producido error por falta de privilegios suficientes para realizar esta operación"
- "El intento de copia de seguridad de Windows VSS ha producido error porque ec2-vss-agent.exe no está instalado en la instancia"
- "Se ha encontrado error de trabajo de copia de seguridad de Windows VSS al intentar copia de seguridad periódica"
- "El intento de copia de seguridad de Windows VSS ha producido error porque se ha agotado el tiempo de espera en la creación de instantáneas para VSS"
- "El intento de copia de seguridad de Windows VSS ha producido error debido a una versión de Windows Server no compatible. Las versiones compatibles son Windows Server 2012 o posterior."
- "El intento de copia de seguridad de Windows VSS ha producido error porque se ha agotado el tiempo de espera en la creación de instantáneas para VSS"

"LIMIT_EXCEEDED"

- "Se ha superado el límite de suscriptores: ha alcanzado el número máximo de copias de seguridad simultáneas, que es de 300. Inténtelo de nuevo. También puedes ponerte en contacto con nosotros Soporte para solicitar un aumento de cuota».
- "Se ha superado el número máximo permitido de instantáneas en curso para un solo volumen."
- "Se ha superado el límite máximo permitido de instantáneas activas."
- "No se pueden crear más de 20 instantáneas de usuario"
- "El conjunto de etiquetas resultante no debe tener más de 50 etiquetas de usuario."
- "Ha alcanzado el número máximo de copias de seguridad admitidas para su cuenta o base de datos. Para obtener información adicional, consulte Cuotas en la Guía para desarrolladores de Timestream."
- "Ha alcanzado su cuota de 50 000 imágenes públicas y privadas permitidas en esta región. Anule el registro de las imágenes no utilizadas o solicite un aumento en su cuota de AMI."
- «Tu copia de seguridad se ha realizado correctamente, pero no hemos podido conservar NetworkInterfaces los metadatos porque su tamaño ha superado nuestros límites internos».
- "REGEX#Superado límite de suscriptores"
- "REGEX#Especificadas más de 50 etiquetas"
- "REGEX#puede tener como máximo"

"ACCESS_DENIED"

- "No está autorizado a realizar esta operación."
- «Acceso denegado al intentar llamar al AWS Backup servicio»
- «Las imágenes de AWS Marketplace no se pueden copiar a otra AWS cuenta».
- "El trabajo de copia ha producido error porque el almacén de copia de seguridad de destino está cifrado con la clave predeterminada administrada por el servicio de copia de seguridad. El contenido de este almacén no se puede copiar. Solo se puede copiar el contenido de una bóveda de Backup cifrado con una AWS KMS clave.
- Las instantáneas cifradas con la no se Clave administrada de AWS pueden compartir. Especifique otra instantánea.
- "Las instantáneas cifradas con la clave predeterminada de Amazon EBS no se pueden compartir
- "Error de trabajo de copia. La cuenta de origen y destino debe ser miembro de la misma organización."

- "REGEX#acceso denegado"
- "REGEX#no autorizado a"
- «REGEX #cannot» debe ser asumido por AWS Backup
- "REGEX#no tiene permiso"
- "REGEX#falta permiso"

"CONCURRENT_JOB"

- "El trabajo de copia de seguridad ha producido error porque había un trabajo en ejecución para el mismo recurso."

"FEATURE_NOT_ENABLED"

- "Error de trabajo de copia. La característica de copia de múltiples cuentas no está habilitada para la organización actual."

"JOB_EXPIRED"

- "El trabajo de copia de seguridad venció antes de completarse."

"INVALID_LIFECYCLE"

- "Error de trabajo de copia. La retención especificada en el trabajo no está dentro del rango especificado para el almacén de copia de seguridad de destino."
- "REGEX #no se pudo iniciar porque está dentro o demasiado cerca del periodo de mantenimiento semanal configurado"
- "REGEX#no se pudo iniciar porque está dentro o demasiado cerca del periodo de copia de seguridad automática configurado"

"INVALID_STATE"

- "REGEX#instancia no está en estado"
- "REGEX#no en el estado disponible"
- "REGEX#no en estado disponible"
- "REGEX#No puede volumen de instantáneas"

"KMS_KEY_ERROR"

- "La clave de KMS está deshabilitada o pendiente de eliminación o se ha denegado el acceso a la clave de KMS"
- "No se puede acceder al ID de clave dado"
- "Error en la copia de instantánea de AMI: no se puede acceder al ID de clave dado. Debe tener DescribeKey permisos en la clave predeterminada»
- "REGEX#clave de kms"

"ACCESS_KEY_ERROR"

- «El identificador de la clave de AWS acceso necesita una suscripción al servicio»

"HYPERVISOR_OFFLINE"

- "Esta operación no es válida para el hipervisor especificado porque no está en línea"

"RESOURCE_NOT_FOUND"

- "El volumen especificado no se ha encontrado."
- "No se encuentra la máquina virtual."
- "El ID de clave dado no existe"
- "REGEX#no existe"
- "REGEX#No se encuentra el recurso"
- "REGEX#No se encuentra cryopod"
- "REGEX#No se encuentra punto de recuperación"
- "REGEX#no se encuentra recurso"
- "REGEX#ya no está disponible"
- "REGEX#no es válido"

"RESOURCE_NOT_SUPPORTED"

- "REGEX#tipo de recurso incompatible"
- "REGEX#Tipo de recurso incompatible"

"TAG_COPY_ERROR"

- "No podemos copiar las etiquetas de recursos a la copia de seguridad debido a un error interno."
- "No podemos copiar las etiquetas de recursos a su copia de seguridad porque no está disponible el punto de recuperación de origen o destino"

"TOKEN_EXPIRED"

- "Token vencido. Inténtelo de nuevo."

"UNSUPPORTED_OPERATION"

- «CreateSnapshot El hipervisor no admite el método durante la creación de la instantánea. Trabajo de copia de seguridad cancelado"
- «UnsupportedOperation : Las copias de seguridad de Storage Gateway requieren una bóveda de respaldo creada por el usuario y una clave en el lugar de destino».
- "REGEX#Característica no compatible con el tipo de recurso proporcionado."

"FATAL_ERROR"

- "Se ha producido un error interno."
- "El trabajo de copia detectó un error grave. Póngase en contacto con AWS Support para obtener más ayuda».
- "El trabajo de copia detectó un error grave."
- "REGEX#Trabajo de copia de seguridad encontró un error grave"

Obtención de datos del panel mediante AWS CLI

Puede utilizar la línea de comandos para recuperar los mismos datos que aparecen en la consola. Utilice uno de los siguientes comandos de la CLI:

- [list-backup-job-summaries](#)
- [list-copy-job-summaries](#)
- [list-restore-job-summaries](#)

Estos son los parámetros válidos que puede incluir en cada comando:

```
BackupJobSummaries (list)
  Region (string),
  Account (string),
  State (string),
  ResourceType (string),
  MessageCategory (string),
AggregationPeriod: (string),
NextToken (string),
MaxResults (number)

CopyJobSummaries (list)
  Region (string),
  Account (string),
  State (string),
  ResourceType (string),
  MessageCategory (string),
AggregationPeriod: (string),
NextToken (string),
MaxResults (number)

RestoreJobSummaries (list)
  Region (string),
  Account (string),
  State (string),
  ResourceType (string),
AggregationPeriod: (string),
NextToken (string)
```

En este ejemplo se muestra una solicitud en la que el usuario tiene `list-backup-job-summaries` de entrada y la solicitud pide que se devuelvan todas las cuentas disponibles con un estado de `FAILED` que supere los 14 días anteriores:

```
GET /audit/backup-job-summaries/
?accountId=ANY
&state=FAILED
&aggregationPeriod=FOURTEEN_DAYS
```

Para obtener un recuento de trabajos con un estado de `completed with issues`, reste el recuento de `COMPLETED` trabajos de con una `MessageCategory` de `SUCCESS` del número total de `COMPLETED`.

Monitorización de AWS Backup eventos con Amazon EventBridge

AWS Backup envía eventos a Amazon EventBridge cuando cambia el estado de un trabajo de copia de seguridad o copia. Se puede utilizar EventBridge para monitorizar AWS Backup eventos. Por ejemplo, puede recibir una alarma cuando se produce un error en una tarea de copia de seguridad. AWS Backup emite eventos de la mejor EventBridge manera posible cada 5 minutos.

Para realizar un seguimiento de los eventos mediante EventBridge, consulte lo siguiente:

- [Crear una regla que reaccione a los eventos](#) (Guía EventBridge del usuario de Amazon)
- [Amazon CloudWatch Events and Metrics para AWS Backup](#) (blog; consulte Configurar AWS Backup eventos para enviarlos a Amazon EventBridge)

Algunos eventos informan status: COMPLETED mientras que otros informan state: COMPLETED. Esto es coherente con la AWS Backup API. Algunos estados son específicos de la consola de AWS Backup: el estado Completed with issues es una representación de los trabajos Completed con mensajes de estado. Para monitorizar eventos Completed with issues, monitorice los trabajos COMPLETED que tengan un mensaje de estado. Tenga en cuenta que esto solo es específico de los trabajos de respaldo.

También puede utilizar la API de AWS Backup notificaciones para realizar un seguimiento de AWS Backup los eventos con Amazon Simple Notification Service (Amazon SNS). Sin embargo, EventBridge rastrea más cambios que la API de notificaciones, incluidos los cambios en los almacenes de respaldo, el estado de las tareas de copia de seguridad, la configuración regional y el número de puntos de recuperación en frío o en caliente.

Eventos

- [Eventos de Trabajo de copia de seguridad](#)
- [Eventos del plan de copia de seguridad](#)
- [Eventos de Backup Vault](#)
- [Eventos de copia de trabajos](#)
- [Eventos de puntos de recuperación](#)
- [Eventos de configuración regional](#)
- [Eventos de restauración de trabajos](#)
- [Eventos de indexación del punto de recuperación](#)
- [Eventos de Job de escaneo de malware](#)

Eventos de Trabajo de copia de seguridad

Los siguientes son eventos de ejemplo.

Estado

- [State: FAILED](#)
- [State: COMPLETED](#)
- [State: RUNNING](#)
- [State: ABORTED](#)
- [State: EXPIRED](#)
- [State: PENDING](#)
- [State: CREATED](#)

State: FAILED

```
{
  "version": "0",
  "id": "710b0398-d48e-f3c3-afca-cfeb2fdaa656",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T20:15:26Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "34176239-e96d-4e1d-9fad-529dbb3c3556",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:9ab3e749-82c6-4342-9320-5edbf4918b86",
    "backupVaultName": "9ab3e749-82c6-4342-9320-5edbf4918b86",
    "bytesTransferred": "0",
    "creationDate": "2020-07-29T20:13:07.392Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
    "state": "FAILED",
    "statusMessage": "\"Backup job failed because backup vault arn:aws:backup:us-west-2:1112233445566:backup-vault:9ab3e749-82c6-4342-9320-5edbf4918b86 does not exist.\"",
    "startBy": "2020-07-30T04:13:07.392Z",
```

```
    "percentDone": 0,  
    "retryCount": 3  
  }  
}
```

State: COMPLETED

```
{  
  "version": "0",  
  "id": "dafac799-9b88-0134-26b7-fef4d54a134f",  
  "detail-type": "Backup Job State Change",  
  "source": "aws.backup",  
  "account": "1112233445566",  
  "time": "2020-07-15T21:41:17Z",  
  "region": "us-west-2",  
  "resources": [  
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:f1d966fe-a3bd-410b-b292-99f442d13b56"  
  ],  
  "detail": {  
    "backupJobId": "a827233a-d405-4a86-a440-759fa94f34dd",  
    "backupSizeInBytes": "36048",  
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:9732c1b4-1091-472a-9d9f-52e0565ee39a",  
    "backupVaultName": "9732c1b4-1091-472a-9d9f-52e0565ee39a",  
    "bytesTransferred": "36048",  
    "creationDate": "2020-07-15T21:40:31.207Z",  
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",  
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",  
    "resourceType": "type",  
    "state": "COMPLETED",  
    "completionDate": "2020-07-15T21:41:05.921Z",  
    "startBy": "2020-07-16T05:40:31.207Z",  
    "percentDone": 100,  
    "retryCount": 3  
  }  
}
```

State: RUNNING

```
{  
  "version": "0",
```

```

    "id": "44946c39-b519-3505-44e6-ba74afeb2e30",
    "detail-type": "Backup Job State Change",
    "source": "aws.backup",
    "account": "1112233445566",
    "time": "2020-07-15T21:39:13Z",
    "region": "us-west-2",
    "resources": [],
    "detail": {
      "backupJobId": "B6EC38D2-CB3C-EF0A-F5A4-3CF324EF4945",
      "backupSizeInBytes": "3221225472",
      "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:e6625738-0655-4aa9-bd37-6ec1dd183b15",
      "backupVaultName": "e6625738-0655-4aa9-bd37-6ec1dd183b15",
      "bytesTransferred": "0",
      "creationDate": "2020-07-15T21:38:31.152Z",
      "iamRoleArn": "arn:aws:iam::1112233445566:role/FullBackupTestRole",
      "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/vol-0b5ae24f2ee72d926",
      "resourceType": "EBS",
      "state": "RUNNING",
      "startBy": "2020-07-16T05:00:00Z",
      "expectedCompletionDate": "Jul 15, 2020 9:39:07 PM",
      "percentDone": 99,
      "createdBy": {
        "backupPlanId": "bde0f455-4e24-4668-aeaa-4932a97f5cc5",
        "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-plan:bde0f455-4e24-4668-aeaa-4932a97f5cc5",
        "backupPlanVersion": "YTkzNmM0MmUtMWRhNS00Y2RkLTNmZGUtNjA5NTc4NGM1YTc5",
        "backupPlanRuleId": "1f97bafa-14d6-4f39-94fd-94b51bd6d0d5"
      }
    }
  }
}

```

State: ABORTED

```

{
  "version": "0",
  "id": "4c91ceb0-b798-da82-6818-c29b3dce7543",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T21:33:16Z",
  "region": "us-west-2",
  "resources": [],

```



```

"detail": {
  "backupJobId": "58cdef95-7680-4c74-80d5-1b64093999c8",
  "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:f59bffc-d-2538-4bbe-8343-1c60dae27c27",
  "backupVaultName": "f59bffc-d-2538-4bbe-8343-1c60dae27c27",
  "bytesTransferred": "0",
  "creationDate": "2020-07-15T21:33:00.803Z",
  "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
  "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
  "resourceType": "type",
  "state": "ABORTED",
  "statusMessage": "\"Backup job was stopped by user.\",",
  "completionDate": "2020-07-15T21:33:01.621Z",
  "startBy": "2020-07-16T05:33:00.803Z",
  "percentDone": 0
}
}

```

State: EXPIRED

```

{
  "version": "0",
  "id": "1d7bbc04-6120-1145-13b9-49b0af465328",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T13:04:57Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "01EE26DC-7107-4D8E-0C54-EAC27C662BA4",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:aws/backup/AutomatedBackupVaultDel2",
    "backupVaultName": "aws/backup/AutomatedBackupVaultDel2",
    "bytesTransferred": "0",
    "creationDate": "2020-07-29T05:10:20.077Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
    "state": "EXPIRED",
    "statusMessage": "\"Backup job failed because there was a running job for the same resource.\",",
    "completionDate": "2020-07-29T13:02:15.234Z",
  }
}

```

```

    "startBy": "2020-07-29T13:00:00Z",
    "percentDone": 0,
    "createdBy": {
      "backupPlanId": "aws/efs/414a5bd4-f880-47ad-95f3-f085108a4c3b",
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-plan:aws/efs/414a5bd4-f880-47ad-95f3-f085108a4c3b",
      "backupPlanVersion": "NjBjOTUzZjYtYzZiNi00Njh1LWlzMTEtNWRjOWY0YTNjN2Vj",
      "backupPlanRuleId": "3eb0017c-f262-4211-a802-302cebb11dc2"
    }
  }
}

```

State: PENDING

```

{
  "version": "0",
  "id": "64dd1897-f863-31a3-9ee5-b05e306d81ff",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T20:03:30Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "2cfffdb68-d6ed-485f-9f9b-8b530749f1c2",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:ed1f2661-5587-48bf-8a98-fadb977bf975",
    "backupVaultName": "ed1f2661-5587-48bf-8a98-fadb977bf975",
    "bytesTransferred": "0",
    "creationDate": "2020-07-29T20:01:06.224Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
    "state": "PENDING",
    "statusMessage": "",
    "startBy": "2020-07-30T04:01:06.224Z",
    "percentDone": 0
  }
}

```

State: CREATED

```

{

```

```

"version": "0",
"id": "29af2bf2-eace-58ab-da3a-8c0bf738d692",
"detail-type": "Backup Job State Change",
"source": "aws.backup",
"account": "1112233445566",
"time": "2020-06-22T20:32:53Z",
"region": "us-west-2",
"resources": [],
"detail": {
  "backupJobId": "7e8845b5-ca30-415f-a842-e0152bf4d0ca",
  "state": "CREATED",
  "creationDate": "2020-06-22T20:32:47.466Z"
}
}

```

Eventos del plan de copia de seguridad

Los siguientes son eventos de ejemplo.

Estado

- [State: MODIFIED](#)
- [State: DELETED](#)
- [State: CREATED](#)

State: MODIFIED

```

{
  "version": "0",
  "id": "2895aefb-dd4a-0a23-6071-2652abd92c3f",
  "detail-type": "Backup Plan State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:25Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-plan:83fcb8ee-2d93-42ac-b06f-591563f3f8de"
  ],
  "detail": {
    "backupPlanId": "83fcb8ee-2d93-42ac-b06f-591563f3f8de",
    "versionId": "NjIwNDZjMDEtNmZlNC00M2JmLTkzZDgtNzNkZjQyNzkxNDk0",

```

```

    "modifiedAt": "2020-06-24T23:18:19.168Z",
    "state": "MODIFIED"
  }
}
```

State: DELETED

```

{
  "version": "0",
  "id": "33fc5c1d-6db2-b3d9-1e70-1c9a2c23645c",
  "detail-type": "Backup Plan State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:25Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-plan:83fcb8ee-2d93-42ac-b06f-591563f3f8de"
  ],
  "detail": {
    "backupPlanId": "83fcb8ee-2d93-42ac-b06f-591563f3f8de",
    "versionId": "NjIwNDFjMDEtNmZlNC00M2JmLTkzZDgtNzNkZjQyNzkxNDk0",
    "deletionDate": "2020-06-24T23:18:19.411Z",
    "state": "DELETED"
  }
}
```

State: CREATED

```

{
  "version": "0",
  "id": "b64fb2d0-ae16-ff9a-faf6-0bdd0d4bfdef",
  "detail-type": "Backup Plan State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:19Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-plan:2c103c5f-6d6e-4cac-9147-d3afa4c84f59"
  ],
  "detail": {
    "backupPlanId": "2c103c5f-6d6e-4cac-9147-d3afa4c84f59",

```

```
{
  "versionId": "N2Q40TczMzEtZmY1My00N2UwLWE30DUtMjViYWYyOTUzZWY4",
  "creationDate": "2020-06-24T23:18:15.318Z",
  "state": "CREATED"
}
```

Eventos de Backup Vault

Los siguientes son eventos de ejemplo.

Estado

- [State: CREATED](#)
- [State: MODIFIED](#)
- [State: DELETED](#)

State: CREATED

```
{
  "version": "0",
  "id": "d415609e-5f35-d9a2-76d1-613683e4e024",
  "detail-type": "Backup Vault State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:19Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:d8864642-155c-4283-a168-a04f40e12c97"
  ],
  "detail": {
    "backupVaultName": "d8864642-155c-4283-a168-a04f40e12c97",
    "state": "CREATED"
  }
}
```

State: MODIFIED

```
{
  "version": "0",
  "id": "1a2b3cd4-5e6f-7g8h-9i0j-123456k7l890",
```

```

"detail-type": "Backup Vault State Change",
"source": "aws.backup",
"account": "1112233445566",
"time": "2020-06-24T23:18:19Z",
"region": "us-west-2",
"resources": [
  "arn:aws:backup:us-west-2:1112233445566:backup-vault:nameOfTestBackup"
],
"detail": {
  "backupVaultName": "vaultName",
  "state": "MODIFIED",
  "isLocked": "true"
}
}

```

State: DELETED

```

{
  "version": "0",
  "id": "344bccc1-6d2e-da93-3adf-b3f82460294d",
  "detail-type": "Backup Vault State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-22T02:42:37Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:e8189629-1f8e-4ed2-af7d-b32415d04db1"
  ],
  "detail": {
    "backupVaultName": "e8189629-1f8e-4ed2-af7d-b32415d04db1",
    "state": "DELETED"
  }
}

```

Eventos de copia de trabajos

Los siguientes son eventos de ejemplo.

Estado

- [State: FAILED](#)
- [State: RUNNING](#)

- [State: COMPLETED](#)
- [State: CREATED](#)

State: FAILED

```
{
  "version": "0",
  "id": "4660bc92-a44d-c939-4542-cda503f14855",
  "detail-type": "Copy Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T20:37:34Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::image/ami-00179b33a7a88cac5"
  ],
  "detail": {
    "copyJobId": "47C8EF56-74D8-059D-1301-C5BE1D5C926E",
    "backupSizeInBytes": 22548578304,
    "creationDate": "2020-07-15T20:36:13.239Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/RoleForEc2BackupWithNoDescribeTagsPermissions",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:instance/i-0515aee7de03f58e1",
    "resourceType": "EC2",
    "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:55aa945e-c46a-421b-aa27-f94b074e31b7",
    "state": "FAILED",
    "statusMessage": "Access denied exception while trying to list tags",
    "completionDate": "2020-07-15T20:37:28.704Z",
    "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:55aa945e-c46a-421b-aa27-f94b074e31b7",
    "destinationRecoveryPointArn": {}
  }
}
```

State: RUNNING

```
{
  "version": "0",
  "id": "d17480ae-7042-edb2-0ff5-8b94822c58e4",
  "detail-type": "Copy Job State Change",
```

```

"source": "aws.backup",
"account": "1112233445566",
"time": "2020-07-15T22:07:48Z",
"region": "us-west-2",
"resources": [
  "arn:aws:ec2:us-west-2::snapshot/snap-03886bc8d6ef3a1f9"
],
"detail": {
  "copyJobId": "0175DE71-5784-589F-D8AC-541ACCB4CAC8",
  "backupSizeInBytes": 3221225472,
  "creationDate": "2020-07-15T22:06:27.234Z",
  "iamRoleArn": "arn:aws:iam::1112233445566:role/OrganizationCanaryTestRole",
  "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/vol-050eba21ee4d3c001",
  "resourceType": "EBS",
  "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:846869de-4589-45c3-ab60-4fbbabcbdd3ec",
  "state": "RUNNING",
  "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:846869de-4589-45c3-ab60-4fbbabcbdd3ec",
  "destinationRecoveryPointArn": {},
  "createdBy": {
    "backupPlanId": "b58e3621-1c53-4997-ad8a-afc3347a850e",
    "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-plan:b58e3621-1c53-4997-ad8a-afc3347a850e",
    "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
    "backupPlanRuleId": "78e356d3-1a11-4f61-8585-af5d6b69bb18"
  }
}
}

```

State: COMPLETED

```

{
  "version": "0",
  "id": "47deb974-6473-aef1-56c2-52c3eaedfceb",
  "detail-type": "Copy Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T22:08:04Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::snapshot/snap-03886bc8d6ef3a1f9"
  ],

```



```

"detail": {
  "copyJobId": "0175DE71-5784-589F-D8AC-541ACCB4CAC8",
  "backupSizeInBytes": 3221225472,
  "creationDate": "2020-07-15T22:06:27.234Z",
  "iamRoleArn": "arn:aws:iam::1112233445566:role/OrganizationCanaryTestRole",
  "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/vol-050eba21ee4d3c001",
  "resourceType": "EBS",
  "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:846869de-4589-45c3-ab60-4fbbabcbdd3ec",
  "state": "COMPLETED",
  "completionDate": "2020-07-15T22:07:58.111Z",
  "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:846869de-4589-45c3-ab60-4fbbabcbdd3ec",
  "destinationRecoveryPointArn": "arn:aws:ec2:us-west-2::snapshot/snap-0726fe70935586180",
  "createdBy": {
    "backupPlanId": "b58e3621-1c53-4997-ad8a-afc3347a850e",
    "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-plan:b58e3621-1c53-4997-ad8a-afc3347a850e",
    "backupPlanVersion": "Mjc4ZTRhZmUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
    "backupPlanRuleId": "78e356d3-1a11-4f61-8585-af5d6b69bb18"
  }
}
}
}

```

State: CREATED

```

{
  "version": "0",
  "id": "8398a4c4-8fe8-2b49-a4b9-fd4fdcd34a4e",
  "detail-type": "Copy Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-22T21:06:32Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::image/ami-0888b126e2170b98e"
  ],
  "detail": {
    "creationDate": "2020-06-22T21:06:25.754Z",
    "state": "CREATED",
    "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:ef09da5a-21a6-461f-a98f-857e9e621a17",

```

```
"destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:ef09da5a-21a6-461f-a98f-857e9e621a17"
}
```

Eventos de puntos de recuperación

Los siguientes son los eventos.

Estado

- [COMPLETED](#)
- PARTIAL
- ELIMINANDO
- EXPIRED
- DISPONIBLE
- STOPPED
- CREAR

State: COMPLETED

```
{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Recovery Point State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T21:39:07Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rds:us-west-2:1112233445566:cluster-snapshot:awsbackup:job-4ece7121-d60e-00c2-5c3b-49960142d03b"
  ],
  "detail": {
    "backupVaultName": "e6625738-0655-4aa9-bd37-6ec1dd183b15",
    "backupVaultArn": "arn:aws:backup:us-west-2:496821122410:backup-vault:e6625738-0655-4aa9-bd37-6ec1dd183b15",
    "creationDate": "2020-07-15T21:38:31.152Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/FullBackupTestRole",
```

```

    "resourceType": "Aurora",
    "resourceArn": "arn:aws:rds:us-west-2:1112233445566:cluster:id",
    "status": "COMPLETED",
    "isEncrypted": "false",
    "storageClass": "WARM",
    "completionDate": "2020-07-15T21:39:05.689Z",
    "createdBy": {
      "backupPlanId": "bde0f455-4e24-4668-aeaa-4932a97f5cc5",
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:bde0f455-4e24-4668-aeaa-4932a97f5cc5",
      "backupPlanVersion": "YTkzNmM0MmUtMWRhNS00Y2RkLTNmZGUtNjA5NTc4NGM1YTc5",
      "backupPlanRuleId": "1f97bafa-14d6-4f39-94fd-94b51bd6d0d5"
    },
    "lifecycle": {
      "deleteAfterDays": 100
    },
    "calculatedLifeCycle": {
      "deleteAt": "2020-10-23T21:38:31.152Z"
    }
  }
}

```

Eventos de configuración regional

El siguiente es un evento de ejemplo.

```

{
  "version": "0",
  "id": "e7ed82ba-4955-4de5-10d6-dba9cfb68b4f",
  "detail-type": "Region Setting State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T22:55:03Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "modifiedAt": "2020-06-24T22:54:57.161Z",
    "ResourceTypeOptInPreference": {
      "Aurora": true
    },
    "state": "MODIFIED"
  }
}

```

Eventos de restauración de trabajos

Los siguientes son eventos de ejemplo. Tenga en cuenta que el caso de uso de un trabajo de restauración determinará los parámetros obligatorios y opcionales que debe incluir. Por ejemplo, si el trabajo de restauración forma parte de un plan de pruebas de restauración, se incluye el parámetro `restoreTestingPlanArn`. Consulte `DescribeRestoreJob` para obtener información de posibles parámetros.

Estado

- [State: FAILED](#)
- [State: RUNNING](#)
- [State: COMPLETED](#)
- [State: PENDING](#)
- [State: CREATED](#)

State: FAILED

```
{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T20:19:29Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2:image/ami-12b3456dfb7f8cf90"
  ],
  "detail": {
    "restoreJobId": "1B234A56-789B-01CD-2A34-4567A08901FD",
    "backupSizeInBytes": "22548578304",
    "creationDate": "2020-07-15T20:19:07.303Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/TestAWSBackupRole",
    "percentDone": 0,
    "resourceType": "EC2",
    "status": "FAILED",
    "statusMessage": "AWS Backup does not permit attaching a new instance profile to an EC2 instance. Please restore using the backed up instance profile."
  }
}
```

```
}
```

State: RUNNING

```
{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T20:26:06Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::snapshot/snap-0fe123ca456cfad7c"
  ],
  "detail": {
    "restoreJobId": "1B234A56-789B-01CD-2A34-4567A08901FD",
    "backupSizeInBytes": "3221225472",
    "creationDate": "2020-07-29T20:26:00.098Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/RestoreTestRole",
    "percentDone": 0,
    "resourceType": "EBS",
    "status": "RUNNING"
  }
}
```

State: COMPLETED

```
{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T03:14:58Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rds:us-west-2:1112233445566:snapshot:awsbackup:job-1a2bcd34-567e-8901-23f4-5g6hijkl7890"
  ],
  "detail": {
    "restoreJobId": "AB123456-78C9-0123-456D-789012E34567",

```

```

    "backupSizeInBytes": "0",
    "creationDate": "2020-07-15T03:10:01.742Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/RestoreTestRole",
    "percentDone": 0,
    "resourceType": "RDS",
    "status": "COMPLETED",
    "createdResourceArn": "arn:aws:rds:us-west-2:1112233445566:db:testinginstance1a2bcd34-567e-8901-23f4-5g6hijkl7890",
    "completionDate": "2020-07-15T03:14:53.128Z"
  }
}

```

State: PENDING

```

{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T20:08:26Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:42bb8260-92cd-46a2-ab8d-b29f4edb47b1"
  ],
  "detail": {
    "restoreJobId": "123EA45F-C678-EFE9-0123-4D56FC0E789A",
    "backupSizeInBytes": "36048",
    "creationDate": "2020-07-29T20:08:21.083Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/RestoreTestRole",
    "percentDone": 0,
    "resourceType": "EC2",
    "status": "PENDING"
  }
}

```

State: CREATED

```

{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",

```

```
"detail-type": "Restore Job State Change",
"source": "aws.backup",
"account": "1112233445566",
"time": "2020-06-22T18:50:49Z",
"region": "us-west-2",
"resources": [
  "arn:aws:backup:us-west-2:1112233445566:recovery-point:a6560b33-3660-494c-8d47-efgh939ij32k"
],
"detail": {
  "restoreJobId": "123EA45F-C678-EFE9-0123-4D56FC0E789A",
  "creationDate": "2020-06-22T18:50:46.407Z",
  "state": "CREATED"
}
}
```

Eventos de indexación del punto de recuperación

Los siguientes son eventos de ejemplo.

Estado

- [Estado: ACTIVE](#)
- [State: DELETED](#)
- [State: FAILED](#)

Estado: ACTIVE

```
{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Recovery Point Index State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2023-12-15T21:39:07Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-abcdef123456"
  ],
  "detail": {
```

```

    "recoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
point:abcd1234-5678-abcd-9012-abcdef123456",
    "accountId": "1112233445566",
    "indexStatus": "ACTIVE",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/BackupIndexRole",
    "resourceType": "EBS",
    "backupVaultArn": "arn:aws:cryo:us-west-2:1112233445566:pod/backup-pod-12345",
    "indexCreationTime": "2025-05-25T21:38:31.152Z",
    "isIndexingContinuous": false,
    "sourceResourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/
vol-01234567890abcdef",
    "backupCreationTime": "2023-12-15T21:38:00.000Z",
    "indexStatusMessage": "An AWS Backup recovery point index was
successfully completed. Indexed recovery point arn : arn:aws:backup:us-
west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-abcdef123456",
    "indexCompletionTime": "2025-05-25T21:39:05.689Z",
  }
}

```

State: DELETED

```

{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Recovery Point Index State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2023-12-15T21:39:07Z",
  "region": "us-west-2",
  "resources": [
    "arn": "aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-
abcdef123456"
  ],
  "detail": {
    "recoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
point:abcd1234-5678-abcd-9012-abcdef123456",
    "accountId": "1112233445566",
    "indexStatus": "DELETED",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/BackupIndexRole",
    "resourceType": "EBS",
    "backupVaultArn": "arn:aws:cryo:us-west-2:1112233445566:pod/backup-pod-12345",
    "indexCreationTime": "2025-05-25T21:38:31.152Z",
    "isIndexingContinuous": false,
  }
}

```



```

    "sourceResourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/
vol-01234567890abcdef",
    "backupCreationTime": "2023-12-15T21:38:00.000Z",
    "indexStatusMessage": "An AWS Backup recovery point index was deleted.
Indexed recovery point arn : arn:aws:backup:us-west-2:1112233445566:recovery-
point:abcd1234-5678-abcd-9012-abcdef123456",
    "indexDeletionTime": "2025-05-27T22:39:05.689Z",
  }
}

```

State: FAILED

```

{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Recovery Point Index State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2023-12-15T21:39:07Z",
  "region": "us-west-2",
  "resources": [
    "arn": "aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-
abcdef123456"
  ],
  "detail": {
    "recoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
point:abcd1234-5678-abcd-9012-abcdef123456",
    "accountId": "1112233445566",
    "indexStatus": "FAILED",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/BackupIndexRole",
    "resourceType": "EBS",
    "backupVaultArn": "arn:aws:cryo:us-west-2:1112233445566:pod/backup-pod-12345",
    "indexCreationTime": "2025-05-25T21:38:31.152Z",
    "isIndexingContinuous": false,
    "sourceResourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/01234567890abcdef",
    "backupCreationTime": "2023-12-15T21:38:00.000Z",
    "indexStatusMessage": "An AWS Backup recovery point index failed to create.
Indexed recovery point arn : arn:aws:backup:us-west-2:1112233445566:recovery-
point:abcd1234-5678-abcd-9012-abcdef123456",
  }
}

```

Eventos de Job de escaneo de malware

Los siguientes son eventos de ejemplo.

Estado

- [State: CREATED](#)
- [State: RUNNING](#)
- [State: COMPLETED](#)
- [Estado: COMPLETADO CON PROBLEMAS](#)
- [State: FAILED](#)
- [Estado: CANCELADO](#)

State: CREATED

```
{
  "version": "0",
  "id": "60ce181d-67c7-496b-90fb-69636b42daee",
  "detail-type": "Scan Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2025-12-12T12:12:12Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-abcdef123456"
  ],
  "detail": {
    "accountId": "1112233445566",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:9ab3e749-82c6-4342-9320-5edbf4918b86",
    "backupVaultName": "9ab3e749-82c6-4342-9320-5edbf4918b86",
    "createdBy": {
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-plan:5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
      "backupPlanId": "5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
      "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMtY2IwMTY4NWQ4",
      "backupRuleId": "256ad167-f523-4cb9-93f3-f0c933efd97f"
    },
    "creationDate": "2025-12-12T12:12:00Z",
```

```

    "iamRoleArn": "arn:aws:iam::1112233445566:role/
RoleForEc2BackupWithNoDescribeTagsPermissions",
    "scannerRoleArn": "arn:aws:iam::1112233445566:role/
RoleForAwsBackupGuarddutyScanner",
    "recoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
point:abcd1234-5678-abcd-9012-abcdef123456",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:instance/
i-0515aee7de03f58e1",
    "resourceType": "EC2",
    "scanId": "43bc14a6-03e0-436a-abf5-8825d3aa6835",
    "scanJobId": "4d5fc12e-7e33-4336-a981-bbe43c300298",
    "scanBaseRecoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
point:46bd3edb-a499-4db1-8f8f-269a2ff76fab",
    "malwareScanner": "GUARDDUTY",
    "state": "CREATED"
  }
}

```

State: RUNNING

```

{
  "version": "0",
  "id": "60ce181d-67c7-496b-90fb-69636b42daee",
  "detail-type": "Scan Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2025-12-12T12:12:12Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-
abcdef123456"
  ],
  "detail": {
    "accountId": "1112233445566",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:9ab3e749-82c6-4342-9320-5edbf4918b86",
    "backupVaultName": "9ab3e749-82c6-4342-9320-5edbf4918b86",
    "createdBy": {
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
      "backupPlanId": "5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
      "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
      "backupRuleId": "256ad167-f523-4cb9-93f3-f0c933efd97f"
    }
  }
}

```

```

    },
    "creationDate": "2025-12-12T12:12:00Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/
RoleForEc2BackupWithNoDescribeTagsPermissions",
    "scannerRoleArn": "arn:aws:iam::1112233445566:role/
RoleForAwsBackupGuarddutyScanner",
    "recoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
point:abcd1234-5678-abcd-9012-abcdef123456",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:instance/
i-0515aee7de03f58e1",
    "resourceType": "EC2",
    "scanId": "43bc14a6-03e0-436a-abf5-8825d3aa6835",
    "scanJobId": "4d5fc12e-7e33-4336-a981-bbe43c300298",
    "scanBaseRecoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
point:46bd3edb-a499-4db1-8f8f-269a2ff76fab",
    "malwareScanner": "GUARDDUTY",
    "state": "RUNNING"
  }
}

```

State: COMPLETED

```

{
  "version": "0",
  "id": "60ce181d-67c7-496b-90fb-69636b42daee",
  "detail-type": "Scan Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2025-12-12T12:12:12Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-
abcdef123456"
  ],
  "detail": {
    "accountId": "1112233445566",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:9ab3e749-82c6-4342-9320-5edbf4918b86",
    "backupVaultName": "9ab3e749-82c6-4342-9320-5edbf4918b86",
    "completionDate": "2025-12-12T12:12:12Z",
    "createdBy": {
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",

```

```

        "backupPlanId": "5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
        "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
        "backupRuleId": "256ad167-f523-4cb9-93f3-f0c933efd97f"
    },
    "creationDate": "2025-12-12T12:12:00Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/RoleForEc2BackupWithNoDescribeTagsPermissions",
    "scannerRoleArn": "arn:aws:iam::1112233445566:role/RoleForAwsBackupGuarddutyScanner",
    "recoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-abcdef123456",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:instance/i-0515aee7de03f58e1",
    "resourceType": "EC2",
    "scanId": "43bc14a6-03e0-436a-abf5-8825d3aa6835",
    "scanJobId": "4d5fc12e-7e33-4336-a981-bbe43c300298",
    "scanBaseRecoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-point:46bd3edb-a499-4db1-8f8f-269a2ff76fab",
    "malwareScanner": "GUARDDUTY",
    "scanResult": {
        "scanResultStatus": "THREATS_FOUND"
    },
    "state": "COMPLETED",
    "statusMessage": "An AWS Backup scan job was successful completed."
}

```

Estado: COMPLETADO CON PROBLEMAS

```

{
    "version": "0",
    "id": "60ce181d-67c7-496b-90fb-69636b42daee",
    "detail-type": "Scan Job State Change",
    "source": "aws.backup",
    "account": "1112233445566",
    "time": "2025-12-12T12:12:12Z",
    "region": "us-west-2",
    "resources": [
        "arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-abcdef123456"
    ],
    "detail": {
        "accountId": "1112233445566",

```

```

    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:9ab3e749-82c6-4342-9320-5edbf4918b86",
    "backupVaultName": "9ab3e749-82c6-4342-9320-5edbf4918b86",
    "completionDate": "2025-12-12T12:12:12Z",
    "createdBy": {
        "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
        "backupPlanId": "5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
        "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
        "backupRuleId": "256ad167-f523-4cb9-93f3-f0c933efd97f"
    },
    "creationDate": "2025-12-12T12:12:00Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/
RoleForEc2BackupWithNoDescribeTagsPermissions",
    "scannerRoleArn": "arn:aws:iam::1112233445566:role/
RoleForAwsBackupGuarddutyScanner",
    "recoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
point:abcd1234-5678-abcd-9012-abcdef123456",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:instance/
i-0515aee7de03f58e1",
    "resourceType": "EC2",
    "scanId": "43bc14a6-03e0-436a-abf5-8825d3aa6835",
    "scanJobId": "4d5fc12e-7e33-4336-a981-bbe43c300298",
    "scanBaseRecoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
point:46bd3edb-a499-4db1-8f8f-269a2ff76fab",
    "malwareScanner": "GUARDDUTY",
    "scanResult": {
        "scanResultStatus": "NO_THREATS_FOUND"
    },
    "state": "COMPLETED_WITH_ISSUES",
    "statusMessage": "Scan job partially completed. View more details in Amazon
GuardDuty"
}
}

```

State: FAILED

```

{
    "version": "0",
    "id": "60ce181d-67c7-496b-90fb-69636b42daee",
    "detail-type": "Scan Job State Change",
    "source": "aws.backup",
    "account": "1112233445566",

```

```

    "time": "2025-12-12T12:12:12Z",
    "region": "us-west-2",
    "resources": [
        "arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-abcdef123456"
    ],
    "detail": {
        "accountId": "1112233445566",
        "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:9ab3e749-82c6-4342-9320-5edbf4918b86",
        "backupVaultName": "9ab3e749-82c6-4342-9320-5edbf4918b86",
        "completionDate": "2025-12-12T12:12:12Z",
        "createdBy": {
            "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-plan:5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
            "backupPlanId": "5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
            "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMtY2IwMTY4NWQ4",
            "backupRuleId": "256ad167-f523-4cb9-93f3-f0c933efd97f"
        },
        "creationDate": "2025-12-12T12:12:00Z",
        "iamRoleArn": "arn:aws:iam::1112233445566:role/RoleForEc2BackupWithNoDescribeTagsPermissions",
        "scannerRoleArn": "arn:aws:iam::1112233445566:role/RoleForAwsBackupGuarddutyScanner",
        "recoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-abcdef123456",
        "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:instance/i-0515aee7de03f58e1",
        "resourceType": "EC2",
        "scanId": "43bc14a6-03e0-436a-abf5-8825d3aa6835",
        "scanJobId": "4d5fc12e-7e33-4336-a981-bbe43c300298",
        "scanBaseRecoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-point:46bd3edb-a499-4db1-8f8f-269a2ff76fab",
        "malwareScanner": "GUARDDUTY",
        "state": "FAILED",
        "statusMessage": "<failure reason>"
    }
}

```

Estado: CANCELADO

```

{
    "version": "0",

```

```

    "id": "60ce181d-67c7-496b-90fb-69636b42daee",
    "detail-type": "Scan Job State Change",
    "source": "aws.backup",
    "account": "1112233445566",
    "time": "2025-12-12T12:12:12Z",
    "region": "us-west-2",
    "resources": [
      "arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-
      abcdef123456"
    ],
    "detail": {
      "accountId": "1112233445566",
      "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
      vault:9ab3e749-82c6-4342-9320-5edbf4918b86",
      "backupVaultName": "9ab3e749-82c6-4342-9320-5edbf4918b86",
      "completionDate": "2025-12-12T12:12:12Z",
      "createdBy": {
        "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
        plan:5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
        "backupPlanId": "5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
        "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
        "backupRuleId": "256ad167-f523-4cb9-93f3-f0c933efd97f"
      },
      "creationDate": "2025-12-12T12:12:00Z",
      "iamRoleArn": "arn:aws:iam::1112233445566:role/
      RoleForEc2BackupWithNoDescribeTagsPermissions",
      "scannerRoleArn": "arn:aws:iam::1112233445566:role/
      RoleForAwsBackupGuarddutyScanner",
      "recoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
      point:abcd1234-5678-abcd-9012-abcdef123456",
      "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:instance/
      i-0515aee7de03f58e1",
      "resourceType": "EC2",
      "scanId": "43bc14a6-03e0-436a-abf5-8825d3aa6835",
      "scanJobId": "4d5fc12e-7e33-4336-a981-bbe43c300298",
      "scanBaseRecoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
      point:46bd3edb-a499-4db1-8f8f-269a2ff76fab",
      "malwareScanner": "GUARDDUTY",
      "state": "CANCELED",
      "statusMessage": "Scan job was stopped by user."
    }
  }
}

```


AWS Backup métricas con Amazon CloudWatch

Temas

- [CloudWatch Tablero](#)
- [Métricas con CloudWatch](#)

CloudWatch Tablero

Note

El panel de la consola depende de la región desde la que se acceda a la consola. Consulte [Disponibilidad de las funciones por Región de AWS](#) para ver qué regiones tienen acceso al panel de trabajos. Las regiones que no figuren en la lista podrán acceder al CloudWatch panel.

La AWS Backup consola incluye un panel de control para ver las métricas de los trabajos de backup, copia y restauración completados o fallidos. En este panel, puede ver el estado del trabajo por periodo de tiempo y personalizarlo según el periodo de tiempo que desee.

PARA ACCEDER AL PANEL

1. Abre la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación izquierdo, seleccione Panel.

VISUALIZACIÓN Y COMPRENSIÓN DEL PANEL

El CloudWatch panel de control muestra varios widgets. Cada widget muestra las métricas de los trabajos por recuento. Cada widget muestra varios gráficos de líneas. Cada línea corresponde a un recurso protegido (si no ve un recurso esperado en la pantalla, asegúrese de que el recurso esté activado en Configuración). Las pantallas no muestran los trabajos en curso.

El eje y (valores verticales) muestra el recuento. El eje x (valores horizontales) muestra puntos en el tiempo. Si no hay puntos de datos que visualizar en el estado del trabajo seleccionado, el valor se establecerá en 0 con una línea horizontal en el eje x. La leyenda que muestra los recursos seguirá siendo visible.

Las métricas muestran información específica de la cuenta y de la región relacionada con el inicio de sesión actual. Para ver otras cuentas o regiones, debe iniciar sesión con la cuenta elegida.

PERSONALIZACIÓN DEL PANEL

De forma predeterminada, el periodo de tiempo que se muestra es de una semana. En el menú superior, hay opciones para redefinir el periodo de tiempo mostrado. Puede elegir entre 1 hora, 3 horas, 12 horas, 1 día, 3 días y 1 semana. Además, puede seleccionar Personalizado para especificar un valor diferente. La personalización cambiará temporalmente la vista actual a sus especificaciones.

Si pasa el ratón por encima de un widget, se mostrará el botón Ampliar en la parte superior derecha del widget. Haga clic en Ampliar para abrir el widget en pantalla completa. En pantalla completa, hay más opciones para personalizar la visualización del gráfico, como cambiar el periodo (el tiempo entre cada punto de datos). Los cambios no se retendrán una vez que se cierre la vista de pantalla completa.

Para ver solo un tipo de recurso a la vez, haga clic en el texto de la etiqueta del tipo de recurso que desee ver en la leyenda del gráfico. De este modo se anula la selección de todos los tipos de recursos. Para revertir esta situación, haga clic en el cuadro de color de un tipo de recurso en la leyenda. Para volver a la vista predeterminada de todos los tipos de recursos con todas las etiquetas seleccionadas, vuelva a hacer clic en el texto de la etiqueta de cualquier tipo de recurso seleccionado.

Al hacer clic en los tres puntos verticales de la esquina superior derecha de un widget, se abre un menú desplegable con opciones para actualizar, ampliar, ver en métricas y ver en registros. Al «Ver en métricas», se abre la métrica utilizada en el widget de la CloudWatch consola. Allí puedes realizar cualquier cambio en el widget y añadirlo a un panel personalizado en el panel de CloudWatch control. Los cambios que realices en el CloudWatch panel de control no se reflejarán en el panel de control de la AWS Backup consola. «Ver como registros» abre la página de visualización de registros en la CloudWatch consola.

Para añadir los widgets que se muestran en tu CloudWatch panel de control personalizado, haz clic en el botón Añadir al panel de control situado en la parte superior derecha del panel de control. Se abrirá la CloudWatch consola en la que podrá seleccionar en qué panel personalizado desea añadir los seis widgets.

Para obtener más información, consulta [Uso de CloudWatch las métricas de Amazon](#).

Métricas con CloudWatch

Se puede utilizar CloudWatch para monitorizar AWS Backup las métricas. El espacio de AWS/Backup nombres te permite realizar un seguimiento de las siguientes métricas. AWS Backup emite métricas actualizadas CloudWatch cada 5 minutos.

El objetivo de esta página de documentación es proporcionarle los materiales de referencia que podrá utilizar CloudWatch en el seguimiento AWS Backup. Para obtener información sobre cómo monitorear una métrica mediante CloudWatch, consulte el blog [Amazon CloudWatch Events and Metrics for AWS Backup](#) o [Céntrese en las métricas y las alarmas en un solo AWS servicio](#) en la Guía del CloudWatch usuario. Para configurar las alarmas, consulte [Uso de Amazon CloudWatch Alarms](#) en la Guía del CloudWatch usuario.

Categoría	Métricas	Dimensiones de ejemplo	Ejemplo de caso de uso
Tareas	Número de trabajos de copia de seguridad , restauración y copia en cada estado, lo que incluye CREATED, PENDING, RUNNING, ABORTED, COMPLETED , FAILED y EXPIRED. Los diferentes tipos de trabajo tienen diferentes estados disponibles.	Tipo de recurso, nombre del almacén. El nombre del almacén de los trabajos de copia es el de su almacén de destino.	Monitoree el número de trabajos de copia de seguridad que dan lugar a errores en uno o más almacenes de copia de seguridad específicos. Si hay más de cinco trabajos que tienen como resultado un error en una hora, envíe un correo electrónico o un SMS a través de Amazon SNS o abra un ticket para que el equipo de ingeniería lo investigue. Criterios del informe: hay un valor distinto de cero

Categoría	Métricas	Dimensiones de ejemplo	Ejemplo de caso de uso
Puntos de recuperación	Número de puntos de recuperación en caliente y frío en cada estado: MODIFIED, COMPLETED , PARTIAL, EXPIRED, DELETED.	Tipo de recurso, nombre del almacén.	Realice un seguimiento del número de puntos de recuperación eliminados de sus volúmenes de Amazon EBS y realice un seguimiento aparte del número de puntos de recuperación en caliente y en frío en cada almacén de copias de seguridad. Criterios del informe: hay un valor distinto de cero

 Note

El estado de la tarea Completed with issues es específico únicamente de la AWS Backup consola; no se puede rastrear a través de ella CloudWatch.

La tabla siguiente enumera todas las métricas a su disposición.

Métrica	Description (Descripción)
NumberOfBackupJobsCreated	El número de trabajos de copia de seguridad que AWS Backup se crearon.
NumberOfBackupJobsPending	El número de trabajos de copia de seguridad que están a punto de ejecutarse en AWS Backup.

Métrica	Description (Descripción)
NumberOfBackupJobsRunning	El número de trabajos de copia de seguridad que se están ejecutando actualmente AWS Backup.
NumberOfBackupJobsAborted	El número de trabajos de copia de seguridad cancelados por el usuario.
NumberOfBackupJobsCompleted	El número de trabajos de copia de seguridad AWS Backup finalizados.
NumberOfBackupJobsFailed	El número de trabajos de copia de seguridad cuyo estado esFailed. A menudo se debe a la programación de una tarea de copia de seguridad durante o 1 hora antes de un recurso de base de datos o 4 horas antes o durante una ventana de FSx mantenimiento de Amazon o una ventana de copia de seguridad automática y no se utiliza AWS Backup para realizar copias de seguridad continuas para las point-in-time restauraciones. Consulte Point-in-Time Recuperación para obtener una lista de los servicios compatibles e instrucciones sobre cómo AWS Backup utilizarlos para realizar copias de seguridad continuas o reprogramar sus tareas de copia de seguridad.
NumberOfBackupJobsExpired	El número de trabajos de copia de seguridad cuyo estado es EXPIRED. Un trabajo de copia de seguridad cambia del estado CREATED a EXPIRED si la copia de seguridad no puede iniciarse dentro del periodo de inicio.
NumberOfCopyJobsCreated	Número de trabajos de copia entre cuentas y regiones que ha creado AWS Backup .

Métrica	Description (Descripción)
NumberOfCopyJobsRunning	Número de trabajos de copia entre cuentas y regiones que se están ejecutando en la actualidad en AWS Backup.
NumberOfCopyJobsCompleted	Número de trabajos de copia entre cuentas y regiones que ha finalizado AWS Backup .
NumberOfCopyJobsFailed	El número de trabajos de copia entre cuentas y regiones que se AWS Backup intentaron realizar pero no se pudieron completar.
NumberOfRestoreJobsPending	El número de trabajos de restauración que están a punto de ejecutarse en AWS Backup.
NumberOfRestoreJobsRunning	El número de trabajos de restauración que se están ejecutando actualmente. AWS Backup
NumberOfRestoreJobsCompleted	El número de trabajos de restauración AWS Backup finalizados.
NumberOfRestoreJobsFailed	El número de trabajos de restauración que se AWS Backup intentaron realizar pero no se pudieron completar.
NumberOfRecoveryPointsCompleted	El número de puntos de recuperación que se AWS Backup crearon.
NumberOfRecoveryPointsPartial	El número de puntos de recuperación que se AWS Backup empezaron a crear pero no se pudieron terminar. AWS reintenta el proceso más adelante, pero como el reintento se produce más tarde, conserva el punto de recuperación parcial.

Métrica	Description (Descripción)
NumberOfRecoveryPointsExpired	La cantidad de puntos de recuperación que se AWS Backup intentaron eliminar en función del ciclo de vida de retención de la copia de seguridad, pero que no se pudieron eliminar. Se le facturará por el almacenamiento que consuman las copias de seguridad vencidas y deberá eliminarlas manualmente.
NumberOfRecoveryPointsDeleting	La cantidad de puntos de recuperación que AWS Backup se están eliminando.
NumberOfRecoveryPointsCold	El número de puntos de recuperación AWS Backup agrupados en almacenamiento en frío.

Hay más dimensiones disponibles además de las que se indican en la tabla. Para ver todas las dimensiones de una métrica, escriba el nombre de esa métrica en el espacio de AWS/Backup nombres de la sección de métricas de la consola. CloudWatch

Registrar las llamadas a AWS Backup la API con CloudTrail

AWS Backup está integrado con [AWS CloudTrail](#) un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio de servicio. CloudTrail captura todas las llamadas a la API AWS Backup como eventos. Las llamadas capturadas incluyen llamadas desde la AWS Backup consola y llamadas en código a las operaciones de la AWS Backup API. Con la información recopilada por CloudTrail, puede determinar a qué solicitud se realizó AWS Backup, la dirección IP desde la que se realizó la solicitud, cuándo se realizó y detalles adicionales.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales del usuario raíz o del usuario.
- Si la solicitud se realizó en nombre de un usuario de IAM Identity Center.
- 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.

CloudTrail está activo en tu cuenta Cuenta de AWS al crear la cuenta y automáticamente tienes acceso al historial de CloudTrail eventos. El historial de CloudTrail eventos proporciona un registro visible, consultable, descargable e inmutable de los últimos 90 días de eventos de gestión registrados en un. Región de AWS Para obtener más información, consulte [Uso del historial de CloudTrail eventos en la Guía del usuario](#). AWS CloudTrail La visualización del historial de eventos no conlleva ningún CloudTrail cargo.

Para tener un registro continuo de los eventos de Cuenta de AWS los últimos 90 días, crea un almacén de datos de eventos de senderos o [CloudTrail lagos](#).

CloudTrail senderos

Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. Todos los senderos creados con él Consola de administración de AWS son multirregionales. Puede crear un registro de seguimiento de una sola región o multirregionales mediante la AWS CLI. Se recomienda crear un sendero multirregional, ya que puedes capturar toda la actividad de tu Regiones de AWS cuenta. Si crea un registro de seguimiento de una sola región, solo podrá ver los eventos registrados en la Región de AWS del registro de seguimiento. Para obtener más información acerca de los registros de seguimiento, consulte [Creación de un registro de seguimiento para su Cuenta de AWS](#) y [Creación de un registro de seguimiento para una organización](#) en la Guía del usuario de AWS CloudTrail .

Puede enviar una copia de sus eventos de administración en curso a su bucket de Amazon S3 sin coste alguno CloudTrail mediante la creación de una ruta; sin embargo, hay cargos por almacenamiento en Amazon S3. Para obtener más información sobre CloudTrail los precios, consulte [AWS CloudTrail Precios](#). Para obtener información acerca de los precios de Amazon S3, consulte [Precios de Amazon S3](#).

CloudTrail Almacenes de datos de eventos en Lake

CloudTrail Lake le permite ejecutar consultas basadas en SQL en sus eventos. CloudTrail Lake convierte los eventos existentes en formato JSON basado en filas al formato [Apache](#) ORC. ORC es un formato de almacenamiento en columnas optimizado para una recuperación rápida de datos. Los eventos se agregan en almacenes de datos de eventos, que son recopilaciones inmutables de eventos en función de criterios que se seleccionan aplicando [selectores de eventos avanzados](#). Los selectores que se aplican a un almacén de datos de eventos controlan los eventos que perduran y están disponibles para la consulta. Para obtener más información sobre CloudTrail Lake, consulte Cómo [trabajar con AWS CloudTrail Lake](#) en la Guía del AWS CloudTrail usuario.

CloudTrail Los almacenes de datos y las consultas sobre eventos de Lake conllevan costes. Cuando crea un almacén de datos de eventos, debe elegir la [opción de precios](#) que desee utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como el período de retención predeterminado y máximo del almacén de datos de eventos. Para obtener más información sobre CloudTrail los precios, consulte [AWS CloudTrail Precios](#).

AWS Backup eventos en CloudTrail

AWS Backup genera estos CloudTrail eventos cuando realiza copias de seguridad, restauraciones, copias, escaneos o notificaciones. Estos eventos no se generan necesariamente por el uso del AWS Backup público APIs. Para obtener más información, consulte [Eventos de servicios de AWS](#) en la Guía del usuario de AWS CloudTrail .

- AssociateBackupVaultMpaApprovalTeamCompleted
- AssociateBackupVaultMpaApprovalTeamFailed
- BackupDeleted
- BackupJobCompleted
- BackupJobStarted
- BackupSelectionDeletedDueToSLRDeletion
- BackupTransitionedToCold
- CopyJobCompleted
- CopyJobStarted
- CreateRestoreAccessBackupVaultFailed
- DisassociateBackupVaultMpaApprovalTeamFailed
- PutBackupVaultNotifications
- RecoveryPointCreated
- ReportJobCompleted
- ReportJobStarted
- RestoreAccessBackupVaultDeleted
- RestoreCompleted
- RestoreStarted

- RevokeRestoreAccessBackupVaultFailed
- ScanJobCompleted
- ScanJobCreated
- ScanJobFailed
- ScanJobStarted

Descripción de las entradas de los archivos de AWS Backup registro

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.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que muestra las DeleteRecoveryPoint acciones y StartBackupJobStartRestoreJob, además, el BackupJobCompleted evento.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "Root",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-01-10T12:24:50Z"
      }
    }
  },
  "eventTime": "2019-01-10T13:45:24Z",
  "eventSource": "backup.amazonaws.com",
  "eventName": "StartBackupJob",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "12.34.567.89",
```

```

    "userAgent": "aws-internal/3 aws-sdk-java/1.11.465
Linux/4.9.124-0.1.ac.198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
java/1.8.0_192",
    "requestParameters": {
        "backupVaultName": "Default",
        "resourceArn": "arn:aws:ec2:us-east-1:123456789012:volume/
vol-00a422a05b9c6asd3",
        "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
        "startWindowMinutes": 60
    },
    "responseElements": {
        "backupJobId": "8a3c2a87-b23e-4d56-b045-fa9e88ede4e6",
        "creationDate": "Jan 10, 2019 1:45:24 PM"
    },
    "requestID": "98cf4d59-8c76-49f7-9201-790743931234",
    "eventID": "fe8146a5-7812-4a95-90ad-074498be1234",
    "eventType": "AwsApiCall",
    "recipientAccountId": "account-id"
},
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-01-10T12:24:50Z"
            }
        }
    },
    "eventTime": "2019-01-10T13:49:50Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "StartRestoreJob",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "12.34.567.89",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.465
Linux/4.9.124-0.1.ac.198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
java/1.8.0_192",
    "requestParameters": {
        "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-00a129455bdbc9d99",

```

```

    "metadata": {
      "volumeType": "gp2",
      "availabilityZone": "us-east-1b",
      "volumeSize": "100"
    },
    "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
    "idempotencyToken": "a9c8b4fb-d369-4a58-944b-942e442a8fe3",
    "resourceType": "EBS"
  },
  "responseElements": {
    "restoreJobId": "9808E090-8C76-CCB8-4CEA-407CF6AC4C43"
  },
  "requestID": "783ddddc-6d7e-4539-8fab-376aa9668543",
  "eventID": "ff35ddea-7577-4aec-a132-964b7e9dd423",
  "eventType": "AwsApiCall",
  "recipientAccountId": "account-id"
},
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "Root",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-01-10T12:24:50Z"
      }
    }
  },
  "eventTime": "2019-01-10T14:52:42Z",
  "eventSource": "backup.amazonaws.com",
  "eventName": "DeleteRecoveryPoint",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "12.34.567.89",
  "userAgent": "aws-internal/3 aws-sdk-java/1.11.465
Linux/4.9.124-0.1.ac.198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
java/1.8.0_192",
  "requestParameters": {
    "backupVaultName": "Default",
    "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-05f426fd9daab3433"
  },

```

```

    "responseElements": null,
    "requestID": "f1f1b33a-48da-436c-9a8f-7574f1ab5fd7",
    "eventID": "2dd70080-5aba-4a79-9a0f-92647c9f0846",
    "eventType": "AwsApiCall",
    "recipientAccountId": "account-id"
  },
  {
    "eventVersion": "1.05",
    "userIdentity": {
      "accountId": "123456789012",
      "invokedBy": "backup.amazonaws.com"
    },
    "eventTime": "2019-01-10T08:24:39Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "BackupJobCompleted",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "backup.amazonaws.com",
    "userAgent": "backup.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "2e7e4fcf-0c52-467f-9fd0-f61c2fcf7d17",
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "account-id",
    "serviceEventDetails": {
      "completionDate": {
        "seconds": 1547108091,
        "nanos": 906000000
      },
      "state": "COMPLETED",
      "percentDone": 100,
      "backupJobId": "8A8E738B-A8C5-E058-8224-90FA323A3C0E",
      "backupVaultName": "BackupVault",
      "backupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-
vault:BackupVault",
      "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-07ce8c3141d361233",
      "resourceArn": "arn:aws:ec2:us-east-1:123456789012:volume/
vol-06692095a6a421233",
      "creationDate": {
        "seconds": 1547101638,
        "nanos": 272000000
      },
      "backupSizeInBytes": 8589934592,
      "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
      "resourceType": "EBS"
    }
  }
}

```

```
}  
}
```

Registro de eventos de administración entre cuentas

Con AWS Backup, puede administrar sus copias de seguridad en todo Cuentas de AWS el interior de su [AWS Organizations](#) estructura. AWS Backup genera estos CloudTrail eventos en su cuenta de miembro cuando crea, actualiza o elimina una política de AWS Organizations respaldo (que aplica planes de respaldo a sus cuentas de miembro) o cuando hay un plan de respaldo de la organización no válido:

- `CreateOrganizationalBackupPlan`
- `UpdateOrganizationalBackupPlan`
- `DeleteOrganizationalBackupPlan`
- `InvalidOrganizationBackupPlan`

Ejemplo: entradas de archivos de AWS Backup registro para la administración de varias cuentas

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.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la `CreateOrganizationalBackupPlan` acción.

```
{  
  "eventVersion": "1.05",  
  "userIdentity": {  
    "accountId": "123456789012",  
    "invokedBy": "backup.amazonaws.com"},  
  "eventTime": "2020-06-02T00:34:00Z",  
  "eventSource": "backup.amazonaws.com",  
  "eventName": "CreateOrganizationalBackupPlan",  
  "awsRegion": "ca-central-1",
```

```

"sourceIPAddress": "backup.amazonaws.com",
"userAgent": "backup.amazonaws.com",
"requestParameters": null,
"responseElements": null,
"eventID": "f2642255-af77-4203-8c37-7ca19d898e84",
"readOnly": false,
"eventType": "AwsServiceEvent",
"recipientAccountId": "account-id",
"serviceEventDetails": {
  "backupPlanId": "orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
  "backupPlanVersionId": "ZTA1Y2ZjZDYtNmRjMy00ZTA1LWIyNTAtM2M1NzQ4OThmNzRj",
  "backupPlanArn": "arn:aws:backup:ca-central-1:123456789012:backup-
plan:orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
  "backupPlanName": "mybackupplan",
  "backupRules": "[{\"id\":\"745fd0ea-7f57-3f35-8a0e-ed4b8c48a8e2\",
  \"name\":\"hourly\", \"description\":null, \"cryopodArn\":\"arn:aws:backup:ca-
central-1:123456789012:backup-vault:ControllerCAMTestBackupVault\", \"scheduleExpression
\":\"cron(0 0/1 ? * * *)\", \"startWindow\":\"PT1H\", \"completionWindow\":\"PT2H\",
  \"lifecycle\":{\"moveToColdStorageAfterDays\":null, \"deleteAfterDays\":\"7\"}, \"tags
\":null, \"copyActions\":[]}]",
  "backupSelections": "[{\"name\":\"selectiondatatype\", \"arn\":
  \"arn:aws:backup:ca-central-1:123456789012:selection:8b40c6d9-3641-3d49-926d-
a075ea715686\", \"role\":\"arn:aws:iam::123456789012:role/OrganizationmyRoleTestRole\",
  \"resources\":[], \"notResources\":[], \"conditions\": [{\"type\":\"STRINGEQUALS\", \"key
\":\"dataType\", \"value\":\"PII\"}, {\"type\":\"STRINGEQUALS\", \"key\":\"dataType\",
  \"value\":\"RED\"}], \"creationDate\":\"2020-06-02T00:34:00.695Z\", \"creatorRequestId
\":null}]",
  "creationDate": {
    "seconds": 1591058040,
    "nanos": 695000000
  },
  "organizationId": "org-id",
  "accountId": "123456789012"
}
}

```

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la `DeleteOrganizationalBackupPlan` acción.

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",

```

```

    "invokedBy": "backup.amazonaws.com"
  },
  "eventTime": "2020-06-02T00:34:25Z",
  "eventSource": "backup.amazonaws.com",
  "eventName": "DeleteOrganizationalBackupPlan",
  "awsRegion": "ca-central-1",
  "sourceIPAddress": "backup.amazonaws.com",
  "userAgent": "backup.amazonaws.com",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "5ce66cd0-b90c-4957-8e00-96ea1077b4fa",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "account-id",
  "serviceEventDetails": {
    "backupPlanId": "orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
    "backupPlanVersionId": "ZTA1Y2ZjZDYtNmRjMy00ZTA1LWIyNTAtM2M1NzQ4OThmNzRj",
    "backupPlanArn": "arn:aws:backup:ca-central-1:123456789012:backup-
plan:orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
    "backupPlanName": "mybackupplan",
    "deletionDate": {
      "seconds": 1591058065,
      "nanos": 519000000
    },
    "organizationId": "org-id",
    "accountId": "123456789012"
  }
}

```

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra el evento `InvalidOrganizationBackupPlan`, que se envía cuando se AWS Backup recibe un plan de respaldo no válido de Organizations.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "backup.amazonaws.com"
  },
  "eventTime": "2022-06-11T13:29:23Z",
  "eventSource": "backup.amazonaws.com",
  "eventName": "InvalidOrganizationBackupPlan",
  "awsRegion": "Region",

```



```

"sourceIPAddress": "backup.amazonaws.com",
"userAgent": "backup.amazonaws.com",
"requestParameters": null,
"responseElements": null,
"eventID": "ab1de234-fg56-7890-h123-45ij678k9l01",
"readOnly": false,
"eventType": "AwsServiceEvent",
"managementEvent": true,
"recipientAccountId": "987654321098",
"serviceEventDetails": {
  "effectivePolicyVersion": 7,
  "effectivePolicyId": "12345678-a9b0-123c-45d6-78e901f23456",
  "lastUpdatedTimestamp": "Jun 11, 2022 1:29:22 PM",
  "policyType": "BACKUP_POLICY",
  "effectiveBackupPlan": {
    "logicalName": "logical-name",
    "regions": [
      "Region"
    ],
    "rules": [
      {
        "name": "test-orgs",
        "targetBackupVaultName": "vault-name",
        "ruleLifecycle": {
          "deleteAfterDays": 100
        },
        "copyActions": [],
        "enableContinuousBackup": true
      }
    ],
    "selections": {
      "tagSelections": [
        {
          "selectionName": "selection-name",
          "iamRoleArn": "arn:aws:iam::$account:role/role",
          "targetedTags": [
            {
              "tagKey": "key",
              "tagValue": "value"
            }
          ]
        }
      ]
    }
  }
},

```

```
    "backupPlanTags": {
      "key": "value"
    },
    "organizationId": "org-id",
    "accountId": "123456789012"
  },
  "eventCategory": "Management"
}
```

Opciones de notificación con AWS Backup

Hay dos formas de recibir notificaciones sobre AWS Backup:

- Notificaciones de usuario puede enviar notificaciones, incluidas CloudWatch las alarmas de Amazon y las notificaciones de otros servicios. AWS Support
- Amazon Simple Notification Service puede notificarle los AWS Backup eventos.

Notificaciones de usuario y AWS Backup

AWS Backup admite la gestión de sus notificaciones de respaldo desde la [Notificaciones de usuario consola](#). Con [Notificaciones de usuario](#), puede ver el progreso de los trabajos de copia de seguridad, copia y restauración y los cambios en las políticas de copia de seguridad, los almacenes, los puntos de recuperación y la configuración desde el Centro de notificaciones de usuario.

Amazon CloudWatch, EventBridge las alarmas de Amazon y las actualizaciones de AWS Support casos son otros tipos de notificaciones que puedes gestionar desde la consola. Además, puedes configurar varias opciones de entrega, como el correo electrónico, las notificaciones de Amazon Q Developer en las aplicaciones de chat y las notificaciones AWS Console Mobile Application push.

Amazon SNS y eventos AWS Backup

AWS Backup aprovecha las sólidas notificaciones que ofrece Amazon Simple Notification Service (Amazon SNS). Puede configurar Amazon SNS para que le notifique los AWS Backup eventos desde la consola de Amazon SNS.

Limitaciones

- Si bien el servicio Amazon SNS permite notificaciones entre cuentas, actualmente AWS Backup no admite esta función. Debe especificar su propio ID de AWS cuenta y el ARN de recurso de su tema.
- AWS Backup admite los temas estándar para la deduplicación óptima de SNS, pero actualmente no AWS Backup admite los temas de FIFO de SNS para la deduplicación estricta.

Casos de uso comunes

- Para configurar las notificaciones de los trabajos de backup fallidos, siga los pasos que se indican en [¿Cómo puedo recibir](#) las notificaciones de los trabajos fallidos? AWS Backup de AWS Premium Support.
- Consulte un ejemplo de notificación de Amazon SNS JSONs para ver los trabajos de copia de seguridad completados, fallidos o vencidos en la tabla de ejemplos de eventos que aparece a continuación.

Para obtener más información sobre Amazon SNS en general, consulte [Introducción a Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Notification Service.

AWS Backup notification APIs

Tras crear los temas con la consola de Amazon SNS o AWS Command Line Interface (AWS CLI), puede utilizar las siguientes operaciones de AWS Backup API para gestionar las notificaciones de respaldo.

- [DeleteBackupVaultNotifications](#): elimina las notificaciones de eventos para el almacén de copias de seguridad especificado.
- [GetBackupVaultNotifications](#): enumera todas las notificaciones de eventos para el almacén de copias de seguridad especificado.
- [PutBackupVaultNotifications](#): activa las notificaciones para el tema y los eventos especificados.

AWS Backup admite los siguientes eventos:

Tipo de trabajo	Event
Trabajo de copia de seguridad	BACKUP_JOB_STARTED BACKUP_JOB_COMPLETED CONTINUOUS_BACKUP_INTERRUPTED
Trabajo de copia	COPY_JOB_STARTED COPY_JOB_SUCCESSFUL COPY_JOB_FAILED
Trabajo de restauración	RESTORE_JOB_STARTED RESTORE_JOB_COMPLETED
Punto de recuperación	RECOVERY_POINT_MODIFIED
Indexación de puntos de recuperación	RECOVERY_POINT_INDEX_COMPLETED RECOVERY_POINT_INDEX_DELETED RECOVERY_POINT_INDEXING_FAILED

AWS Backup para S3 admite dos eventos adicionales:

- **S3_BACKUP_OBJECT_FAILED** le notifica cualquier objeto de S3 del que AWS Backup no haya podido realizar una copia de seguridad durante un trabajo de copia de seguridad.
- **S3_RESTORE_OBJECT_FAILED** le notifica cualquier objeto de S3 que AWS Backup no haya podido restaurar durante un trabajo de restauración.

AWS Backup for EKS admite dos eventos adicionales:

- **EKS_RESTORE_OBJECT_FAILED** le notifica cualquier objeto de EKS que AWS Backup no se haya podido restaurar durante un trabajo de restauración.
- **EKS_RESTORE_OBJECT_SKIPPED** le notifica cualquier objeto de EKS que se haya omitido durante un trabajo de restauración.

Ejemplos de eventos de

Example Ejemplo: Trabajo de copia de seguridad completado

```
{
  "Records": [{
    "EventSource": "aws:sns",
    "EventVersion": "1.0",
    "EventSubscriptionArn": "arn:aws:sns:...-a3802aa1ed45",
    "Sns": {
      "Type": "Notification",
      "MessageId": "12345678-abcd-123a-def0-abcd1a234567",
      "TopicArn": "arn:aws:sns:us-west-1:123456789012:backup-2sqs-sns-topic",
      "Subject": "Notification from AWS Backup",
      "Message": "An AWS Backup job was completed successfully. Recovery point  
ARN: arn:aws:ec2:us-west-1:123456789012:volume/vol-012f345df6789012d. Resource ARN :  
arn:aws:ec2:us-west-1:123456789012:volume/vol-012f345df6789012e. BackupJob ID :  
1b2345b2-f22c-4dab-5eb6-bbc7890ed123",
      "Timestamp": "2019-08-02T18:46:02.788Z",
      ...
      "MessageAttributes": {
        "EventType": {"Type": "String", "Value": "BACKUP_JOB"},
        "State": {"Type": "String", "Value": "COMPLETED"},
        "AccountId": {"Type": "String", "Value": "123456789012"},
        "Id": {"Type": "String", "Value": "1b2345b2-f22c-4dab-5eb6-bbc7890ed123"},
        "StartTime": {"Type": "String", "Value": "2019-09-02T13:48:52.226Z"}
      }
    }
  ]
}
```

Example Ejemplo: Trabajo de copia de seguridad con resultado de error

```
{
  "Records": [{
    "EventSource": "aws:sns",
    "EventVersion": "1.0",
    "EventSubscriptionArn": "arn:aws:sns:...-a3802aa1ed45",
    "Sns": {
      "Type": "Notification",
      "MessageId": "12345678-abcd-123a-def0-abcd1a234567",
      "TopicArn": "arn:aws:sns:us-west-1:123456789012:backup-2sqs-sns-topic",
      "Subject": "Notification from AWS Backup",
```

```

    "Message": "An AWS Backup job failed. Resource ARN : arn:aws:ec2:us-
west-1:123456789012:volume/vol-012f345df6789012e. BackupJob ID : 1b2345b2-
f22c-4dab-5eb6-bbc7890ed123",
    "Timestamp": "2019-08-02T18:46:02.788Z",
    ...
    "MessageAttributes": {
      "EventType": {"Type":"String","Value":"BACKUP_JOB"},
      "State": {"Type":"String","Value":"FAILED"},
      "AccountId": {"Type":"String","Value":"123456789012"},
      "Id": {"Type":"String","Value":"1b2345b2-f22c-4dab-5eb6-bbc7890ed123"},
      "StartTime": {"Type":"String","Value":"2019-09-02T13:48:52.226Z"}
    }
  }
}

```

Example Ejemplo: Trabajo de copia de seguridad no completado durante el intervalo de copia de seguridad

```

{
  "Records": [{
    "EventSource": "aws:sns",
    "EventVersion": "1.0",
    "EventSubscriptionArn": "arn:aws:sns:...-a3802aa1ed45",
    "Sns": {
      "Type": "Notification",
      "MessageId": "12345678-abcd-123a-def0-abcd1a234567",
      "TopicArn": "arn:aws:sns:us-west-1:123456789012:backup-2sqs-sns-topic",
      "Subject": "Notification from AWS Backup",
      "Message": "An AWS Backup job failed to complete in time. Resource ARN :
arn:aws:ec2:us-west-1:123456789012:volume/vol-012f345df6789012e. BackupJob ID :
1b2345b2-f22c-4dab-5eb6-bbc7890ed123",
      "Timestamp": "2019-08-02T18:46:02.788Z",
      ...
      "MessageAttributes" : {
        "EventType" : {"Type":"String","Value":"BACKUP_JOB"},
        "State" : {"Type":"String","Value":"EXPIRED"},
        "AccountId" : {"Type":"String","Value":"123456789012"},
        "Id" : {"Type":"String","Value":"1b2345b2-f22c-4dab-5eb6-bbc7890ed123"},
        "StartTime" : {"Type":"String","Value":"2019-09-02T13:48:52.226Z"}
      }
    }
  ]
}

```

```
}
```

Example Ejemplo: Se ha completado la indexación de puntos de recuperación

```
{
  "Records": [{
    "EventSource": "aws:sns",
    "EventVersion": "1.0",
    "EventSubscriptionArn": "arn:aws:sns:...-a3802aa1ed45",
    "Sns": {
      "Type": "Notification",
      "MessageId": "12345678-abcd-123a-def0-abcd1a234567",
      "TopicArn": "arn:aws:sns:us-west-1:123456789012:backup-2sqs-sns-topic",
      "Subject": "Notification from AWS Backup",
      "Message": "An AWS Backup backup index job was completed. Indexed recovery
point arn: arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-
abcd-9012-abcdef123456",
      "Timestamp": "2025-05-25T18:46:02.788Z",
      ...
      "MessageAttributes" : {
        "EventType" :
{"Type":"String","Value":"RECOVERY_POINT_INDEXING_COMPLETED"},
        "AccountId" : {"Type":"String","Value":"123456789012"},
        "IndexStatus" : {"Type":"String","Value":"ACTIVE"},
        "IsIndexingContinuous" : {"Type":"String","Value":"false"},
        "RecoveryPointArn" : {"Type":"String","Value":"arn:aws:backup:us-
west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-abcdef123456"}
      }
    }
  ]
}
```

AWS Backup ejemplos de comandos de notificación

Puede usar AWS CLI comandos para suscribirse a las notificaciones de Amazon SNS de sus AWS Backup eventos, enumerarlas y eliminarlas.

Ejemplo de activación de notificaciones del almacén de copias de seguridad

El siguiente comando se suscribe a un tema de Amazon SNS del almacén de copias de seguridad especificado que le notifica cuando se inicia o finaliza un trabajo de restauración o cuando se modifica un punto de recuperación.

```
aws backup put-backup-vault-notifications
  --backup-vault-name myBackupVault
  --sns-topic-arn arn:aws:sns:region:account-id:myBackupTopic
  --backup-vault-events RESTORE_JOB_STARTED RESTORE_JOB_COMPLETED
  RECOVERY_POINT_MODIFIED
```

Ejemplo de obtención de notificaciones del almacén de copias de seguridad

El siguiente comando enumera todos los eventos suscritos actualmente a un tema de Amazon SNS para el almacén de copias de seguridad especificado.

```
aws backup get-backup-vault-notifications
  --backup-vault-name myVault
```

El resultado del ejemplo es el siguiente:

```
{
  "SNSTopicArn": "arn:aws:sns:region:account-id:myBackupTopic",
  "BackupVaultEvents": [
    "RESTORE_JOB_STARTED",
    "RESTORE_JOB_COMPLETED",
    "RECOVERY_POINT_MODIFIED"
  ],
  "BackupVaultName": "myVault",
  "BackupVaultArn": "arn:aws:backup:region:account-id:backup-vault:myVault"
}
```

Ejemplo de eliminación de notificaciones del almacén de copias de seguridad

El siguiente comando cancela la suscripción a un tema de Amazon SNS para el almacén de copias de seguridad especificado.

```
aws backup delete-backup-vault-notifications
  --backup-vault-name myVault
```


Especificar AWS Backup como principal de servicio

Note

AWS Backup Para permitir la publicación de temas de SNS en su nombre, debe especificarlo AWS Backup como principal de servicio.

Incluya el siguiente JSON en la política de acceso del tema Amazon SNS que utiliza para realizar un seguimiento AWS Backup de los eventos. Debe especificar el Nombre de recurso de Amazon (ARN) del tema.

```
{
  "Sid": "My-statement-id",
  "Effect": "Allow",
  "Principal": {
    "Service": "backup.amazonaws.com"
  },
  "Action": "SNS:Publish",
  "Resource": "arn:aws:sns:region:account-id:myTopic"
}
```

Para obtener más información sobre cómo especificar un principal de servicio en una política de acceso a Amazon SNS, consulte [Permitir que cualquier AWS recurso se publique en un tema en la Guía para](#) desarrolladores de Amazon Simple Notification Service.

Note

Si su tema está cifrado, debe incluir permisos adicionales en su política AWS Backup para poder publicar en él. Para obtener más información sobre cómo permitir que los servicios publiquen en temas cifrados, consulte [Habilitar la compatibilidad entre las fuentes de eventos de AWS los servicios y los temas cifrados](#) en la Guía para desarrolladores de Amazon Simple Notification Service.

Solución de problemas AWS Backup

Cuando lo usa AWS Backup, es posible que encuentre problemas. Las siguientes secciones pueden ayudarle a solucionar algunos problemas habituales que puede encontrarse.

Si tienes preguntas generales al respecto AWS Backup, consulta las [AWS Backup preguntas frecuentes](#). También puede buscar respuestas y publicar preguntas en [AWS re:Post](#).

Temas

- [Solución de problemas generales](#)
- [Solución de problemas de creación de recursos](#)
- [Solución de problemas de eliminación de recursos](#)
- [Solución de problemas de restauración de recursos](#)
- [Solución de problemas de errores de formateo](#)

Solución de problemas generales

Al realizar copias de seguridad de los recursos y restaurarlos, debe tener permiso para usar AWS Backup y acceder a los recursos que desea proteger. La forma más sencilla de tener los permisos adecuados es elegir el rol predeterminado al [asignar recursos a un plan de copia de seguridad](#). Para obtener más información sobre el control de acceso mediante AWS Identity and Access Management (IAM) con AWS Backup, consulte [Control de acceso](#).

Si aparece un error de AccessDenied al intentar acceder a un recurso de AWS Backup, como una bóveda de copia de seguridad, significa que el recurso no existe o que no tiene permisos para acceder al recurso.

Si tiene problemas con la copia de seguridad y la restauración de un tipo de recurso concreto, puede resultar útil revisar el tema sobre solución de problemas de copia de seguridad y restauración de ese recurso. Para obtener más información, consulte los enlaces de la sección [Cómo AWS Backup funciona con AWS los servicios compatibles](#).

Si AWS Backup no puede crear o eliminar un recurso, puede obtener más información sobre el problema utilizando AWS CloudTrail para ver los mensajes de error o los registros. Para obtener más información sobre el uso CloudTrail con AWS Backup, consulte [Registrar las llamadas a AWS Backup la API con CloudTrail](#).

Solución de problemas de creación de recursos

La siguiente información puede ayudarle a solucionar problemas con la creación de copias de seguridad.

- En general, los servicios de bases de datos de AWS no pueden iniciar las copias de seguridad una hora antes o durante el intervalo de mantenimiento o el intervalo de copia de seguridad automática. Amazon FSx no puede iniciar las copias de seguridad 4 horas antes o durante el período de mantenimiento o el período de respaldo automático (Amazon Aurora está exento de esta restricción de período de mantenimiento). Las copias de seguridad instantáneas programadas durante esos periodos producirán un error. Una excepción: si opta por utilizar un servicio compatible AWS Backup para copias de seguridad instantáneas y continuas, ya no tendrá que preocuparse por esos períodos, ya que los AWS Backup programará por usted. Consulte [Point-in-Time Recovery](#) para obtener una lista de los servicios compatibles e instrucciones sobre cómo utilizarlos AWS Backup para realizar copias de seguridad continuas.
- La creación de copias de seguridad para tablas de DynamoDB producirá un error mientras se crean las tablas. La creación de una tabla de DynamoDB suele tardar un par de minutos.
- La copia de seguridad de los sistemas de archivos de Amazon EFS puede tardar hasta 7 días si los sistemas de archivos son muy grandes. Solo se puede poner en cola una copia de seguridad simultánea a la vez para un sistema de archivos de Amazon EFS. Si se pone en cola una copia de seguridad posterior mientras la anterior sigue en curso, la ventana de copia de seguridad puede caducar y no se crea ninguna copia de seguridad.
- Amazon EBS tiene una cuota flexible de 100 000 copias de seguridad Región de AWS por cuenta y las copias de seguridad adicionales fallan cuando se alcanza esta cuota. Si alcanza esta cuota, puede eliminar las copias de seguridad que sobran o solicitar un aumento. Para obtener más información acerca de cómo solicitar un aumento de cuotas, consulte [Cuotas de servicio de AWS](#).
- Al crear copias de seguridad de de Amazon Relational Database Service (RDS), tenga en cuenta lo siguiente:
 - Si no lo utiliza AWS Backup para gestionar tanto las instantáneas de Amazon RDS como las copias de seguridad continuas con point-in-time recuperación, las copias de seguridad fallarán si se inician si se programan o se realizan bajo demanda durante el período de copia de seguridad diario de 30 minutos configurable por el usuario. Para obtener más información sobre las copias de seguridad automatizadas de Amazon RDS, consulte [Trabajo con copias de seguridad](#) en la Guía del usuario de Amazon RDS. Puede evitar esta limitación si lo utiliza AWS Backup para

gestionar tanto las instantáneas de Amazon RDS como las copias de seguridad continuas con point-in-time recuperación.

- Si inicia un trabajo de copia de seguridad desde la consola de Amazon RDS, esto puede entrar en conflicto con un trabajo de copia de seguridad de clústeres Aurora y provocar el error `Backup job expired before completion`. Si ocurre esto, configure un intervalo de copias de seguridad más largo en AWS Backup.
- AWS Backup actualmente no transfiere el grupo de opciones de TDE cuando se crea un trabajo de copia. Si piensa utilizar este grupo de opciones para la creación de trabajos de copia, debe utilizar la consola de Amazon RDS o la API de Amazon RDS en lugar de las herramientas de AWS Backup. Consulte [Copia de un grupo de opciones](#) en la Guía del usuario de Amazon Relational Database Service para obtener más información.
- ERROR: las copias de seguridad bajo demanda se completan, pero las copias de seguridad programadas no se completan y dan el error "The source snapshot KMS key does not exist, is not enabled or you do not have permissions to access it". El trabajo bajo demanda se completa porque utiliza la llamada a la API `CopyDBSnapshot`, que no requiere acceso a KMS.

SOLUCIÓN: agregue el rol de IAM a su clave de KMS.

Solución de problemas de eliminación de recursos

Los puntos de recuperación creados por el recurso protegido AWS Backup no se pueden eliminar en la ventana de consola del recurso protegido. Puede eliminarlos en la AWS Backup consola seleccionándolos en el almacén donde están almacenados y, a continuación, seleccionando Eliminar.

Para eliminar un punto de recuperación o un almacén de copia de seguridad, necesita los permisos adecuados. Para obtener más información sobre el control de acceso mediante IAM with AWS Backup, consulte [Control de acceso](#).

Solución de problemas de restauración de recursos

Restauración mediante la API

Para restaurar una copia de seguridad mediante programación, utilice la operación de API [StartRestoreJob](#).

Para obtener los metadatos de configuración con los que se creó la copia de seguridad, puede llamar a [GetRecoveryPointRestoreMetadata](#).

Para obtener más información, consulte [Restauración de una copia de seguridad](#).

Restauración mediante la consola

- [Restauración de datos de Amazon S3](#)
- [Restauración de una máquina virtual](#)
- [Restauración de un sistema de FSx archivos de Amazon](#)
- [Restauración de un volumen de Amazon EBS](#)
- [Restauración de un sistema de archivos de Amazon EFS](#)
- [Restauración de una tabla de Amazon DynamoDB](#)
- [Restauración de una base de datos de Amazon RDS](#)
- [Restauración de un clúster de Aurora](#)
- [Restauración de una EC2 instancia de Amazon](#)
- [Restauración de un volumen de Storage Gateway](#)
- [Restauración de un clúster de Amazon DocumentDB](#)
- [Restauración de un clúster de Neptune](#)

Solución de problemas de errores de formateo

Cuando se incluye un comodín (*) para el valor de un parámetro, el comodín se procesa para incluir valores distintos de los espacios en blanco. Los valores de un par clave-valor que contengan espacios en blanco no se incluirán como parte del comodín.

AWS BackupAPI de

Además de utilizar la consola, puede utilizar los tipos de datos y las acciones de la API de AWS Backup para configurar y administrar AWS Backup y sus recursos mediante programación. En esta sección se describen los tipos de datos y las acciones de AWS Backup. Contiene la referencia de la API para AWS Backup.

AWS Backup API

- [Acciones de AWS Backup](#)
- [Tipos de datos de AWS Backup](#)

Acciones

Las siguientes acciones cuentan con el apoyo de AWS Backup:

- [AssociateBackupVaultMpaApprovalTeam](#)
- [CancelLegalHold](#)
- [CreateBackupPlan](#)
- [CreateBackupSelection](#)
- [CreateBackupVault](#)
- [CreateFramework](#)
- [CreateLegalHold](#)
- [CreateLogicallyAirGappedBackupVault](#)
- [CreateReportPlan](#)
- [CreateRestoreAccessBackupVault](#)
- [CreateRestoreTestingPlan](#)
- [CreateRestoreTestingSelection](#)
- [CreateTieringConfiguration](#)
- [DeleteBackupPlan](#)
- [DeleteBackupSelection](#)
- [DeleteBackupVault](#)
- [DeleteBackupVaultAccessPolicy](#)

- [DeleteBackupVaultLockConfiguration](#)
- [DeleteBackupVaultNotifications](#)
- [DeleteFramework](#)
- [DeleteRecoveryPoint](#)
- [DeleteReportPlan](#)
- [DeleteRestoreTestingPlan](#)
- [DeleteRestoreTestingSelection](#)
- [DeleteTieringConfiguration](#)
- [DescribeBackupJob](#)
- [DescribeBackupVault](#)
- [DescribeCopyJob](#)
- [DescribeFramework](#)
- [DescribeGlobalSettings](#)
- [DescribeProtectedResource](#)
- [DescribeRecoveryPoint](#)
- [DescribeRegionSettings](#)
- [DescribeReportJob](#)
- [DescribeReportPlan](#)
- [DescribeRestoreJob](#)
- [DescribeScanJob](#)
- [DisassociateBackupVaultMpaApprovalTeam](#)
- [DisassociateRecoveryPoint](#)
- [DisassociateRecoveryPointFromParent](#)
- [ExportBackupPlanTemplate](#)
- [GetBackupPlan](#)
- [GetBackupPlanFromJSON](#)
- [GetBackupPlanFromTemplate](#)
- [GetBackupSelection](#)
- [GetBackupVaultAccessPolicy](#)
- [GetBackupVaultNotifications](#)

- [GetLegalHold](#)
- [GetRecoveryPointIndexDetails](#)
- [GetRecoveryPointRestoreMetadata](#)
- [GetRestoreJobMetadata](#)
- [GetRestoreTestingInferredMetadata](#)
- [GetRestoreTestingPlan](#)
- [GetRestoreTestingSelection](#)
- [GetSupportedResourceTypes](#)
- [GetTieringConfiguration](#)
- [ListBackupJobs](#)
- [ListBackupJobSummaries](#)
- [ListBackupPlans](#)
- [ListBackupPlanTemplates](#)
- [ListBackupPlanVersions](#)
- [ListBackupSelections](#)
- [ListBackupVaults](#)
- [ListCopyJobs](#)
- [ListCopyJobSummaries](#)
- [ListFrameworks](#)
- [ListIndexedRecoveryPoints](#)
- [ListLegalHolds](#)
- [ListProtectedResources](#)
- [ListProtectedResourcesByBackupVault](#)
- [ListRecoveryPointsByBackupVault](#)
- [ListRecoveryPointsByLegalHold](#)
- [ListRecoveryPointsByResource](#)
- [ListReportJobs](#)
- [ListReportPlans](#)
- [ListRestoreAccessBackupVaults](#)
- [ListRestoreJobs](#)

- [ListRestoreJobsByProtectedResource](#)
- [ListRestoreJobSummaries](#)
- [ListRestoreTestingPlans](#)
- [ListRestoreTestingSelections](#)
- [ListScanJobs](#)
- [ListScanJobSummaries](#)
- [ListTags](#)
- [ListTieringConfigurations](#)
- [PutBackupVaultAccessPolicy](#)
- [PutBackupVaultLockConfiguration](#)
- [PutBackupVaultNotifications](#)
- [PutRestoreValidationResult](#)
- [RevokeRestoreAccessBackupVault](#)
- [StartBackupJob](#)
- [StartCopyJob](#)
- [StartReportJob](#)
- [StartRestoreJob](#)
- [StartScanJob](#)
- [StopBackupJob](#)
- [TagResource](#)
- [UntagResource](#)
- [UpdateBackupPlan](#)
- [UpdateFramework](#)
- [UpdateGlobalSettings](#)
- [UpdateRecoveryPointIndexSettings](#)
- [UpdateRecoveryPointLifecycle](#)
- [UpdateRegionSettings](#)
- [UpdateReportPlan](#)
- [UpdateRestoreTestingPlan](#)
- [UpdateRestoreTestingSelection](#)

- [UpdateTieringConfiguration](#)

Las siguientes acciones cuentan con el apoyo de AWS Backup gateway:

- [AssociateGatewayToServer](#)
- [CreateGateway](#)
- [DeleteGateway](#)
- [DeleteHypervisor](#)
- [DisassociateGatewayFromServer](#)
- [GetBandwidthRateLimitSchedule](#)
- [GetGateway](#)
- [GetHypervisor](#)
- [GetHypervisorPropertyMappings](#)
- [GetVirtualMachine](#)
- [ImportHypervisorConfiguration](#)
- [ListGateways](#)
- [ListHypervisors](#)
- [ListTagsForResource](#)
- [ListVirtualMachines](#)
- [PutBandwidthRateLimitSchedule](#)
- [PutHypervisorPropertyMappings](#)
- [PutMaintenanceStartTime](#)
- [StartVirtualMachinesMetadataSync](#)
- [TagResource](#)
- [TestHypervisorConfiguration](#)
- [UntagResource](#)
- [UpdateGatewayInformation](#)
- [UpdateGatewaySoftwareNow](#)
- [UpdateHypervisor](#)

Las siguientes acciones cuentan con el apoyo de AWS Backup:

- [GetSearchJob](#)
- [GetSearchResultExportJob](#)
- [ListSearchJobBackups](#)
- [ListSearchJobResults](#)
- [ListSearchJobs](#)
- [ListSearchResultExportJobs](#)
- [ListTagsForResource](#)
- [StartSearchJob](#)
- [StartSearchResultExportJob](#)
- [StopSearchJob](#)
- [TagResource](#)
- [UntagResource](#)

AWS Backup

Las siguientes acciones cuentan con el apoyo de AWS Backup:

- [AssociateBackupVaultMpaApprovalTeam](#)
- [CancelLegalHold](#)
- [CreateBackupPlan](#)
- [CreateBackupSelection](#)
- [CreateBackupVault](#)
- [CreateFramework](#)
- [CreateLegalHold](#)
- [CreateLogicallyAirGappedBackupVault](#)
- [CreateReportPlan](#)
- [CreateRestoreAccessBackupVault](#)
- [CreateRestoreTestingPlan](#)
- [CreateRestoreTestingSelection](#)
- [CreateTieringConfiguration](#)
- [DeleteBackupPlan](#)
- [DeleteBackupSelection](#)

- [DeleteBackupVault](#)
- [DeleteBackupVaultAccessPolicy](#)
- [DeleteBackupVaultLockConfiguration](#)
- [DeleteBackupVaultNotifications](#)
- [DeleteFramework](#)
- [DeleteRecoveryPoint](#)
- [DeleteReportPlan](#)
- [DeleteRestoreTestingPlan](#)
- [DeleteRestoreTestingSelection](#)
- [DeleteTieringConfiguration](#)
- [DescribeBackupJob](#)
- [DescribeBackupVault](#)
- [DescribeCopyJob](#)
- [DescribeFramework](#)
- [DescribeGlobalSettings](#)
- [DescribeProtectedResource](#)
- [DescribeRecoveryPoint](#)
- [DescribeRegionSettings](#)
- [DescribeReportJob](#)
- [DescribeReportPlan](#)
- [DescribeRestoreJob](#)
- [DescribeScanJob](#)
- [DisassociateBackupVaultMpaApprovalTeam](#)
- [DisassociateRecoveryPoint](#)
- [DisassociateRecoveryPointFromParent](#)
- [ExportBackupPlanTemplate](#)
- [GetBackupPlan](#)
- [GetBackupPlanFromJSON](#)
- [GetBackupPlanFromTemplate](#)
- [GetBackupSelection](#)

- [GetBackupVaultAccessPolicy](#)
- [GetBackupVaultNotifications](#)
- [GetLegalHold](#)
- [GetRecoveryPointIndexDetails](#)
- [GetRecoveryPointRestoreMetadata](#)
- [GetRestoreJobMetadata](#)
- [GetRestoreTestingInferredMetadata](#)
- [GetRestoreTestingPlan](#)
- [GetRestoreTestingSelection](#)
- [GetSupportedResourceTypes](#)
- [GetTieringConfiguration](#)
- [ListBackupJobs](#)
- [ListBackupJobSummaries](#)
- [ListBackupPlans](#)
- [ListBackupPlanTemplates](#)
- [ListBackupPlanVersions](#)
- [ListBackupSelections](#)
- [ListBackupVaults](#)
- [ListCopyJobs](#)
- [ListCopyJobSummaries](#)
- [ListFrameworks](#)
- [ListIndexedRecoveryPoints](#)
- [ListLegalHolds](#)
- [ListProtectedResources](#)
- [ListProtectedResourcesByBackupVault](#)
- [ListRecoveryPointsByBackupVault](#)
- [ListRecoveryPointsByLegalHold](#)
- [ListRecoveryPointsByResource](#)
- [ListReportJobs](#)
- [ListReportPlans](#)

- [ListRestoreAccessBackupVaults](#)
- [ListRestoreJobs](#)
- [ListRestoreJobsByProtectedResource](#)
- [ListRestoreJobSummaries](#)
- [ListRestoreTestingPlans](#)
- [ListRestoreTestingSelections](#)
- [ListScanJobs](#)
- [ListScanJobSummaries](#)
- [ListTags](#)
- [ListTieringConfigurations](#)
- [PutBackupVaultAccessPolicy](#)
- [PutBackupVaultLockConfiguration](#)
- [PutBackupVaultNotifications](#)
- [PutRestoreValidationResult](#)
- [RevokeRestoreAccessBackupVault](#)
- [StartBackupJob](#)
- [StartCopyJob](#)
- [StartReportJob](#)
- [StartRestoreJob](#)
- [StartScanJob](#)
- [StopBackupJob](#)
- [TagResource](#)
- [UntagResource](#)
- [UpdateBackupPlan](#)
- [UpdateFramework](#)
- [UpdateGlobalSettings](#)
- [UpdateRecoveryPointIndexSettings](#)
- [UpdateRecoveryPointLifecycle](#)
- [UpdateRegionSettings](#)
- [UpdateReportPlan](#)

- [UpdateRestoreTestingPlan](#)
- [UpdateRestoreTestingSelection](#)
- [UpdateTieringConfiguration](#)

AssociateBackupVaultMpaApprovalTeam

Servicio: AWS Backup

Asocia un equipo de aprobación MPA a un almacén de copias de seguridad.

Sintaxis de la solicitud

```
PUT /backup-vaults/backupVaultName/mpaApprovalTeam HTTP/1.1
Content-type: application/json

{
  "MpaApprovalTeamArn": "string",
  "RequesterComment": "string"
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupVaultName

Es el nombre del almacén de copias de seguridad que se va a asociar al equipo de aprobación MPA.

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

MpaApprovalTeamArn

Es el Nombre de recurso de Amazon (ARN) que se va a asociar al equipo de aprobación MPA.

Tipo: cadena

Obligatorio: sí

RequesterComment

Es un comentario proporcionado por el solicitante en el que se explica la solicitud de asociación.

Tipo: cadena

Requerido: no

Sintaxis de la respuesta

```
HTTP/1.1 204
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 204 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)

- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

CancelLegalHold

Servicio: AWS Backup

Elimina la retención legal especificada en un punto de recuperación. Solo puede realizar esta acción un usuario con permisos suficientes.

Sintaxis de la solicitud

```
DELETE /legal-holds/legalHoldId?  
cancelDescription=CancelDescription&retainRecordInDays=RetainRecordInDays HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

CancelDescription

Una cadena que describe el motivo de la eliminación de la retención legal.

Obligatorio: sí

legalHoldId

El identificador de la retención legal.

Obligatorio: sí

RetainRecordInDays

La cantidad entera, en días, transcurridos desde los que se elimina la retención legal.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 201
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 201 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

InvalidResourceStateException

AWS Backup ya está realizando una acción en este punto de recuperación. No es posible realizar la acción que ha solicitado hasta que finalice la primera acción. Inténtelo de nuevo más tarde.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

CreateBackupPlan

Servicio: AWS Backup

Crea un plan de copia de seguridad con el nombre del plan y las reglas de copia de seguridad. Un plan de respaldo es un documento que contiene información que se AWS Backup utiliza para programar tareas que crean puntos de recuperación para los recursos.

Si llama a CreateBackupPlan con un plan que ya existe, recibirá una excepción `AlreadyExistsException`.

Sintaxis de la solicitud

```
PUT /backup/plans/ HTTP/1.1
Content-type: application/json

{
  "BackupPlan": {
    "AdvancedBackupSettings": [
      {
        "BackupOptions": {
          "string": "string"
        },
        "ResourceType": "string"
      }
    ],
    "BackupPlanName": "string",
    "Rules": [
      {
        "CompletionWindowMinutes": number,
        "CopyActions": [
          {
            "DestinationBackupVaultArn": "string",
            "Lifecycle": {
              "DeleteAfterDays": number,
              "DeleteAfterEvent": "string",
              "MoveToColdStorageAfterDays": number,
              "OptInToArchiveForSupportedResources": boolean
            }
          }
        ],
        "EnableContinuousBackup": boolean,
        "IndexActions": [
          {
```

```

        "ResourceTypes": [ "string" ]
    },
    "Lifecycle": {
        "DeleteAfterDays": number,
        "DeleteAfterEvent": "string",
        "MoveToColdStorageAfterDays": number,
        "OptInToArchiveForSupportedResources": boolean
    },
    "RecoveryPointTags": {
        "string" : "string"
    },
    "RuleName": "string",
    "ScanActions": [
        {
            "MalwareScanner": "string",
            "ScanMode": "string"
        }
    ],
    "ScheduleExpression": "string",
    "ScheduleExpressionTimezone": "string",
    "StartWindowMinutes": number,
    "TargetBackupVaultName": "string",
    "TargetLogicallyAirGappedBackupVaultArn": "string"
    },
    "ScanSettings": [
        {
            "MalwareScanner": "string",
            "ResourceTypes": [ "string" ],
            "ScannerRoleArn": "string"
        }
    ]
},
"BackupPlanTags": {
    "string" : "string"
},
"CreatorRequestId": "string"
}

```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[BackupPlan](#)

El cuerpo de un plan de copia de seguridad. Incluye un `BackupPlanName` y uno o más conjuntos de `Rules`.

Tipo: objeto [BackupPlanInput](#)

Obligatorio: sí

[BackupPlanTags](#)

Las etiquetas que se van a asignar al plan de copia de seguridad.

Tipo: mapa de cadena a cadena

Obligatorio: no

[CreatorRequestId](#)

Identifica la solicitud y permite que se reintenten las solicitudes que han producido un error sin el riesgo de ejecutar la operación dos veces. Si la solicitud incluye un `CreatorRequestId` que coincide con un plan de copia de seguridad existente, se devuelve ese plan. Este parámetro es opcional.

Si se utiliza, este parámetro debe contener de 1 a 50 caracteres alfanuméricos o “-”. caracteres.

Tipo: cadena

Requerido: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "AdvancedBackupSettings": [
    {
      "BackupOptions": {
```

```
        "string" : "string"
      },
      "ResourceType": "string"
    }
  ],
  "BackupPlanArn": "string",
  "BackupPlanId": "string",
  "CreationDate": number,
  "VersionId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[AdvancedBackupSettings](#)

La configuración para un tipo de recurso. Esta opción solo está disponible para los trabajos de copia de seguridad de Volume Shadow Copy Service (VSS) de Windows.

Tipo: matriz de objetos [AdvancedBackupSetting](#)

[BackupPlanArn](#)

Un nombre de recurso de Amazon (ARN) que identifica de forma única un plan de copia de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Tipo: cadena

[BackupPlanId](#)

El ID del plan de copia de seguridad.

Tipo: cadena

[CreationDate](#)

La fecha y la hora en que se creó el plan de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor `1516925490.087` representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

VersionId

Cadenas cifradas en UTF-8, Unicode, únicas, generadas aleatoriamente que tienen como máximo una longitud de 1024 bytes. No es posible editarlos.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AlreadyExistsException

El recurso ya existe.

Arn

Context

CreatorRequestId

Type

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)

- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

CreateBackupSelection

Servicio: AWS Backup

Crea un documento JSON que especifica un conjunto de recursos que se asignarán a un plan de copia de seguridad. Para ver ejemplos, consulte [Asignación de recursos mediante programación](#).

Sintaxis de la solicitud

```
PUT /backup/plans/backupPlanId/selections/ HTTP/1.1
```

```
Content-type: application/json
```

```
{
  "BackupSelection": {
    "Conditions": [
      {
        "StringEquals": {
          "ConditionKey": "string",
          "ConditionValue": "string"
        }
      },
      {
        "StringLike": {
          "ConditionKey": "string",
          "ConditionValue": "string"
        }
      },
      {
        "StringNotEquals": {
          "ConditionKey": "string",
          "ConditionValue": "string"
        }
      },
      {
        "StringNotLike": {
          "ConditionKey": "string",
          "ConditionValue": "string"
        }
      }
    ],
    "IamRoleArn": "string",
    "ListOfTags": [
      {
        "ConditionKey": "string",
```

```
        "ConditionType": "string",
        "ConditionValue": "string"
    },
    ],
    "NotResources": [ "string" ],
    "Resources": [ "string" ],
    "SelectionName": "string"
},
"CreatorRequestId": "string"
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[backupPlanId](#)

El ID del plan de copia de seguridad.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[BackupSelection](#)

El cuerpo de una solicitud para asignar un conjunto de recursos a un plan de copia de seguridad.

Tipo: objeto [BackupSelection](#)

Obligatorio: sí

[CreatorRequestId](#)

Una cadena única que identifica la solicitud y permite que se reintenten las solicitudes que han producido un error sin el riesgo de ejecutar la operación dos veces. Este parámetro es opcional.

Si se utiliza, este parámetro debe contener de 1 a 50 caracteres alfanuméricos o “-_”. caracteres.

Tipo: cadena

Requerido: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupPlanId": "string",
  "CreationDate": number,
  "SelectionId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[BackupPlanId](#)

El ID del plan de copia de seguridad.

Tipo: cadena

[CreationDate](#)

La fecha y la hora en que se creó la selección de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos.

Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

[SelectionId](#)

Identifica de forma única el cuerpo de una solicitud para asignar un conjunto de recursos a un plan de copia de seguridad.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AlreadyExistsException

El recurso ya existe.

Arn

Context

CreatorRequestId

Type

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

CreateBackupVault

Servicio: AWS Backup

Crea un contenedor lógico donde se almacenan las copias de seguridad. Una solicitud `CreateBackupVault` incluye un nombre, opcionalmente una o varias etiquetas de recursos, una clave de cifrado y un ID de solicitud.

Note

No incluya datos confidenciales, como los números de pasaporte, en el nombre de un almacén de copia de seguridad.

Sintaxis de la solicitud

```
PUT /backup-vaults/backupVaultName HTTP/1.1
Content-type: application/json
```

```
{
  "BackupVaultTags": {
    "string" : "string"
  },
  "CreatorRequestId": "string",
  "EncryptionKeyArn": "string"
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon. Constan de letras minúsculas, números y guiones.

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[BackupVaultTags](#)

Las etiquetas que se van a asignar al almacén de copias de seguridad.

Tipo: mapa de cadena a cadena

Obligatorio: no

[CreatorRequestId](#)

Una cadena única que identifica la solicitud y permite que se reintenten las solicitudes que han producido un error sin el riesgo de ejecutar la operación dos veces. Este parámetro es opcional.

Si se utiliza, este parámetro debe contener de 1 a 50 caracteres alfanuméricos o “-”. caracteres.

Tipo: cadena

Requerido: no

[EncryptionKeyArn](#)

La clave de cifrado en el servidor que se utiliza para proteger sus copias de seguridad; por ejemplo, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Tipo: cadena

Requerido: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupVaultArn": "string",
  "BackupVaultName": "string",
  "CreationDate": number
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[BackupVaultArn](#)

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un almacén de copia de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

[BackupVaultName](#)

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región donde se crearon. Constan de letras minúsculas, números y guiones.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

[CreationDate](#)

La fecha y la hora en que se creó el almacén, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor `1516925490.087` representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

`AlreadyExistsException`

El recurso ya existe.

Arn

Context

CreatorRequestId

Type

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

CreateFramework

Servicio: AWS Backup

Crea un marco con uno o más controles. Un marco es un conjunto de controles que puede usar para evaluar sus prácticas de copia de seguridad. Mediante el uso de controles personalizables prediseñados para definir sus políticas, puede evaluar si sus prácticas de copia de seguridad cumplen con sus políticas y qué recursos aún no.

Sintaxis de la solicitud

```
POST /audit/frameworks HTTP/1.1
Content-type: application/json

{
  "FrameworkControls": [
    {
      "ControlInputParameters": [
        {
          "ParameterName": "string",
          "ParameterValue": "string"
        }
      ],
      "ControlName": "string",
      "ControlScope": {
        "ComplianceResourceIds": [ "string" ],
        "ComplianceResourceTypes": [ "string" ],
        "Tags": {
          "string" : "string"
        }
      }
    }
  ],
  "FrameworkDescription": "string",
  "FrameworkName": "string",
  "FrameworkTags": {
    "string" : "string"
  },
  "IdempotencyToken": "string"
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[FrameworkControls](#)

Los controles que componen el marco. Cada control de la lista tiene un nombre, parámetros de entrada y alcance.

Tipo: matriz de objetos [FrameworkControl](#)

Obligatorio: sí

[FrameworkDescription](#)

Una descripción opcional del marco con un máximo de 1024 caracteres.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `.*\S.*`

Obligatorio: no

[FrameworkName](#)

El nombre único del marco. El nombre debe contener entre 1 y 256 caracteres, comenzando por una letra, y contar con letras (a-z, A-Z), números (0-9) y guiones bajos (_).

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `[a-zA-Z][_a-zA-Z0-9]*`

Obligatorio: sí

[FrameworkTags](#)

Las etiquetas que se van a asignar al marco.

Tipo: mapa de cadena a cadena

Obligatorio: no

[IdempotencyToken](#)

Una cadena elegida por el cliente que puede utilizar para distinguir entre llamadas a `CreateFrameworkInput` que, de otro modo, serían idénticas. Si se vuelve a intentar una solicitud correcta con el mismo token de idempotencia, aparece un mensaje de confirmación y no se realiza ninguna acción.

Tipo: cadena

Requerido: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "FrameworkArn": "string",
  "FrameworkName": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[FrameworkArn](#)

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un recurso. El formato del ARN depende del tipo de recurso.

Tipo: cadena

[FrameworkName](#)

El nombre único del marco. El nombre debe contener entre 1 y 256 caracteres, comenzando por una letra, y contar con letras (a-z, A-Z), números (0-9) y guiones bajos (_).

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: [a-zA-Z][_a-zA-Z0-9]*

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AlreadyExistsException

El recurso ya existe.

Arn

Context

CreatorRequestId

Type

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

CreateLegalHold

Servicio: AWS Backup

Crea una retención legal en un punto de recuperación (copia de seguridad). Una retención legal es una restricción a la modificación o eliminación de una copia de seguridad hasta que un usuario autorizado cancele la retención legal. Toda acción que se lleve a cabo para eliminar o disociar un punto de recuperación dará lugar a un error si hay una o más retenciones legales activas en el punto de recuperación.

Sintaxis de la solicitud

```
POST /legal-holds/ HTTP/1.1
Content-type: application/json

{
  "Description": "string",
  "IdempotencyToken": "string",
  "RecoveryPointSelection": {
    "DateRange": {
      "FromDate": number,
      "ToDate": number
    },
    "ResourceIdentifiers": [ "string" ],
    "VaultNames": [ "string" ]
  },
  "Tags": {
    "string" : "string"
  },
  "Title": "string"
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

Description

La descripción de la cadena de la retención legal.

Tipo: cadena

Obligatorio: sí

[IdempotencyToken](#)

Se trata de una cadena elegida por el usuario que se utiliza para distinguir entre llamadas que, de otro modo, serían idénticas. Si se vuelve a intentar una solicitud correcta con el mismo token de idempotencia, aparece un mensaje de confirmación y no se realiza ninguna acción.

Tipo: cadena

Requerido: no

[RecoveryPointSelection](#)

Los criterios para asignar un conjunto de recursos, como los tipos de recursos o los almacenes de copias de seguridad.

Tipo: objeto [RecoveryPointSelection](#)

Obligatorio: no

[Tags](#)

Etiquetas opcionales que se incluirán. Una etiqueta es un par clave-valor que puede utilizar para administrar, filtrar y buscar sus recursos. Los caracteres permitidos incluyen espacios, números y letras en UTF-8, además de los siguientes caracteres especiales: + - = . _ : /.

Tipo: mapa de cadena a cadena

Obligatorio: no

[Title](#)

El título de la retención legal.

Tipo: cadena

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json
```

```
{
  "CreationDate": number,
  "Description": "string",
  "LegalHoldArn": "string",
  "LegalHoldId": "string",
  "RecoveryPointSelection": {
    "DateRange": {
      "FromDate": number,
      "ToDate": number
    },
    "ResourceIdentifiers": [ "string" ],
    "VaultNames": [ "string" ]
  },
  "Status": "string",
  "Title": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

CreationDate

La hora en la que se creó la retención legal.

Tipo: marca temporal

Description

La descripción de la cadena de la retención legal.

Tipo: cadena

LegalHoldArn

El nombre de recurso de Amazon (ARN) de la retención legal.

Tipo: cadena

LegalHoldId

El identificador de la retención legal.

Tipo: cadena

[RecoveryPointSelection](#)

Los criterios para asignar a un conjunto de recursos, como los tipos de recursos o los almacenes de copias de seguridad.

Tipo: objeto [RecoveryPointSelection](#)

[Status](#)

El estado de la retención legal.

Tipo: cadena

Valores válidos: CREATING | ACTIVE | CANCELING | CANCELED

[Title](#)

El título de la retención legal.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)

- [AWS SDK para Ruby V3](#)

CreateLogicallyAirGappedBackupVault

Servicio: AWS Backup

Crea un contenedor lógico en el que se pueden copiar las copias de seguridad.

Esta solicitud incluye un nombre, la región, el número máximo de días de retención y el número mínimo de días de retención y, opcionalmente, puede incluir etiquetas y un identificador de solicitud del creador.

Note

No incluya datos confidenciales, como los números de pasaporte, en el nombre de un almacén de copia de seguridad.

Sintaxis de la solicitud

```
PUT /logically-air-gapped-backup-vaults/backupVaultName HTTP/1.1
Content-type: application/json
```

```
{
  "BackupVaultTags": {
    "string" : "string"
  },
  "CreatorRequestId": "string",
  "EncryptionKeyArn": "string",
  "MaxRetentionDays": number,
  "MinRetentionDays": number
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad independientes lógicamente se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región en la que se crearon.

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[BackupVaultTags](#)

Las etiquetas que se van a asignar al almacén.

Tipo: mapa de cadena a cadena

Obligatorio: no

[CreatorRequestId](#)

El identificador de la solicitud de creación.

Este parámetro es opcional. Si se utiliza, este parámetro debe contener de 1 a 50 caracteres alfanuméricos o “-”. caracteres.

Tipo: cadena

Requerido: no

[EncryptionKeyArn](#)

El ARN de la clave KMS administrada por el cliente que se utilizará para cifrar el almacén de copias de seguridad aislado de forma lógica. Si no se especifica, el almacén se cifrará con una clave AWS propia gestionada por AWS Backup.

Tipo: cadena

Requerido: no

[MaxRetentionDays](#)

El periodo máximo de retención durante el cual el almacén retiene sus puntos de recuperación.

Tipo: largo

Obligatorio: sí

[MinRetentionDays](#)

Esta configuración especifica el periodo mínimo de retención durante el cual el almacén retiene sus puntos de recuperación.

El valor mínimo aceptado es de 7 días.

Tipo: largo

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupVaultArn": "string",
  "BackupVaultName": "string",
  "CreationDate": number,
  "VaultState": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[BackupVaultArn](#)

El nombre de recurso de Amazon (ARN) del almacén.

Tipo: cadena

[BackupVaultName](#)

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad independientes lógicamente se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región en la que se crearon.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

CreationDate

Fecha y hora en que se creó el almacén.

Este valor está en formato Unix, horario universal coordinado (UTC) y tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

VaultState

El estado actual del almacén.

Tipo: cadena

Valores válidos: CREATING | AVAILABLE | FAILED

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AlreadyExistsException

El recurso ya existe.

Arn

Context

CreatorRequestId

Type

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Context

Type

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

CreateReportPlan

Servicio: AWS Backup

Crea un plan de informe. Un plan de informes es un documento que contiene información sobre el contenido del informe y dónde AWS Backup se entregará.

Si llama a CreateReportPlan con un plan que ya existe, recibirá una excepción `AlreadyExistsException`.

Sintaxis de la solicitud

```
POST /audit/report-plans HTTP/1.1
Content-type: application/json

{
  "IdempotencyToken": "string",
  "ReportDeliveryChannel": {
    "Formats": [ "string" ],
    "S3BucketName": "string",
    "S3KeyPrefix": "string"
  },
  "ReportPlanDescription": "string",
  "ReportPlanName": "string",
  "ReportPlanTags": {
    "string" : "string"
  },
  "ReportSetting": {
    "Accounts": [ "string" ],
    "FrameworkArns": [ "string" ],
    "NumberOfFrameworks": number,
    "OrganizationUnits": [ "string" ],
    "Regions": [ "string" ],
    "ReportTemplate": "string"
  }
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

IdempotencyToken

Una cadena elegida por el cliente que puede utilizar para distinguir entre llamadas a `CreateReportPlanInput` que, de otro modo, serían idénticas. Si se vuelve a intentar una solicitud correcta con el mismo token de idempotencia, aparece un mensaje de confirmación y no se realiza ninguna acción.

Tipo: cadena

Requerido: no

ReportDeliveryChannel

Una estructura que contiene información sobre dónde y cómo entregar sus informes, específicamente el nombre del bucket de Amazon S3, el prefijo de clave de S3 y los formatos de sus informes.

Tipo: objeto [ReportDeliveryChannel](#)

Obligatorio: sí

ReportPlanDescription

Una descripción opcional del plan de informes con un máximo de 1024 caracteres.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `.*\S.*`

Obligatorio: no

ReportPlanName

El nombre único del plan de informes. El nombre debe contener entre 1 y 256 caracteres, comenzando por una letra, y contar con letras (a-z, A-Z), números (0-9) y guiones bajos (_).

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `[a-zA-Z][_a-zA-Z0-9]*`

Obligatorio: sí

[ReportPlanTags](#)

Las etiquetas que se van a asignar al plan de informe.

Tipo: mapa de cadena a cadena

Obligatorio: no

[ReportSetting](#)

Identifica la plantilla para el informe. Los informes se crean mediante una plantilla. Las plantillas de informes son:

RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT |
BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT |
SCAN_JOB_REPORT

Si la plantilla del informe es RESOURCE_COMPLIANCE_REPORT
o CONTROL_COMPLIANCE_REPORT, este recurso de API también describe la cobertura del
informe por marcos Regiones de AWS y marcos.

Tipo: objeto [ReportSetting](#)

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "CreationTime": number,
  "ReportPlanArn": "string",
  "ReportPlanName": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

CreationTime

La fecha y la hora en que se creó la lista de dominios, en formato Unix y horario universal coordinado (UTC). El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

ReportPlanArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un recurso. El formato del ARN depende del tipo de recurso.

Tipo: cadena

ReportPlanName

El nombre único del plan de informes.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `[a-zA-Z][_a-zA-Z0-9]*`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AlreadyExistsException

El recurso ya existe.

Arn

Context

CreatorRequestId

Type

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

CreateRestoreAccessBackupVault

Servicio: AWS Backup

Crea un almacén de copias de seguridad con acceso a la restauración que proporciona acceso temporal a los puntos de recuperación de un almacén de copias de seguridad aislado lógicamente y sujeto a la aprobación MPA.

Sintaxis de la solicitud

```
PUT /restore-access-backup-vaults HTTP/1.1
Content-type: application/json

{
  "BackupVaultName": "string",
  "BackupVaultTags": {
    "string" : "string"
  },
  "CreatorRequestId": "string",
  "RequesterComment": "string",
  "SourceBackupVaultArn": "string"
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

BackupVaultName

Es el nombre del almacén de copias de seguridad que se va a asociar al equipo de aprobación MPA.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: no

[BackupVaultTags](#)

Etiquetas opcionales que se van a asignar al almacén de copias de seguridad con acceso a la restauración.

Tipo: mapa de cadena a cadena

Obligatorio: no

[CreatorRequestId](#)

Es una cadena única que identifica la solicitud y permite que se reintenten las solicitudes que han generado un error sin el riesgo de ejecutar la operación dos veces.

Tipo: cadena

Requerido: no

[RequesterComment](#)

Es un comentario que explica el motivo para solicitar acceso a la restauración del almacén de copias de seguridad.

Tipo: cadena

Requerido: no

[SourceBackupVaultArn](#)

Es el ARN del almacén de copias de seguridad de origen que contiene los puntos de recuperación a los que se solicita acceso temporal.

Tipo: cadena

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "CreationDate": number,
  "RestoreAccessBackupVaultArn": "string",
```



```
"RestoreAccessBackupVaultName": "string",  
"VaultState": "string"  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

CreationDate

Es la fecha y la hora en que se creó el almacén de copias de seguridad con acceso a la restauración, expresadas en formato Unix y en horario universal coordinado (UTC).

Tipo: marca temporal

RestoreAccessBackupVaultArn

Es el ARN que identifica de forma unívoca el almacén de copias de seguridad con acceso a la restauración creado.

Tipo: cadena

RestoreAccessBackupVaultName

Es el nombre del almacén de copias de seguridad con acceso a la restauración creado.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

VaultState

Es el estado actual del almacén de copias de seguridad con acceso a la restauración.

Tipo: cadena

Valores válidos: CREATING | AVAILABLE | FAILED

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AlreadyExistsException

El recurso ya existe.

Arn

Context

CreatorRequestId

Type

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Context

Type

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)

- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

CreateRestoreTestingPlan

Servicio: AWS Backup

Crea un plan de prueba de restauración.

El primero de los dos pasos para crear un plan de prueba de restauración. Una vez que la solicitud se haya realizado correctamente, finalice el procedimiento mediante `CreateRestoreTestingSelection`.

Sintaxis de la solicitud

```
PUT /restore-testing/plans HTTP/1.1
Content-type: application/json

{
  "CreatorRequestId": "string",
  "RestoreTestingPlan": {
    "RecoveryPointSelection": {
      "Algorithm": "string",
      "ExcludeVaults": [ "string" ],
      "IncludeVaults": [ "string" ],
      "RecoveryPointTypes": [ "string" ],
      "SelectionWindowDays": number
    },
    "RestoreTestingPlanName": "string",
    "ScheduleExpression": "string",
    "ScheduleExpressionTimezone": "string",
    "StartWindowHours": number
  },
  "Tags": {
    "string" : "string"
  }
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[CreatorRequestId](#)

Es una cadena única que identifica la solicitud y permite que se reintenten las solicitudes con un error sin riesgo de ejecutar la operación dos veces. Este parámetro es opcional. Si se utiliza, este parámetro debe contener de 1 a 50 caracteres alfanuméricos o “_”. caracteres.

Tipo: cadena

Requerido: no

[RestoreTestingPlan](#)

Un plan de prueba de restauración debe contener una cadena `RestoreTestingPlanName` única que usted crea y debe contener un cron de `ScheduleExpression`. Puede incluir opcionalmente un entero de `StartWindowHours` y una cadena de `CreatorRequestId`.

`RestoreTestingPlanName` es una cadena única que es el nombre del plan de prueba de restauración. No se puede cambiar después de la creación y debe constar únicamente de caracteres alfanuméricos y guiones bajos.

Tipo: objeto [RestoreTestingPlanForCreate](#)

Obligatorio: sí

[Tags](#)

Las etiquetas que se van a asignar al plan de prueba de restauración.

Tipo: mapa de cadena a cadena

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 201
Content-type: application/json

{
  "CreationTime": number,
  "RestoreTestingPlanArn": "string",
  "RestoreTestingPlanName": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 201.

El servicio devuelve los datos siguientes en formato JSON.

[CreationTime](#)

La fecha y la hora en que se creó el plan de informes, en formato Unix y Hora universal coordinada (UTC). El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

[RestoreTestingPlanArn](#)

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva el plan de prueba de restauración creado.

Tipo: cadena

[RestoreTestingPlanName](#)

Esta cadena única es el nombre del plan de prueba de restauración.

El nombre no se puede cambiar después de crear el plan. El nombre consta de únicamente de caracteres alfanuméricos y guiones bajos. La longitud máxima es 50.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

`AlreadyExistsException`

El recurso ya existe.

Arn

Context

CreatorRequestId

Type

Código de estado HTTP: 400

ConflictException

AWS Backup no puede realizar la acción que ha solicitado hasta que termine de realizar una acción anterior. Inténtelo de nuevo más tarde.

Context

Type

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

CreateRestoreTestingSelection

Servicio: AWS Backup

Esta solicitud se puede enviar después de que la CreateRestoreTestingPlan solicitud se devuelva correctamente. Es la segunda parte de la creación de un plan de prueba de recursos y debe completarse secuencialmente.

Consta de RestoreTestingSelectionName, ProtectedResourceType y uno de los siguientes elementos:

- ProtectedResourceArns
- ProtectedResourceConditions

Cada tipo de recurso protegido puede tener un único valor.

Una selección de pruebas de restauración puede incluir un valor comodín ("*") como ProtectedResourceArns junto con ProtectedResourceConditions. Como alternativa, puede incluir hasta 30 recursos ARNs protegidos específicos ProtectedResourceArns.

No se puede seleccionar tanto por tipos de recursos protegidos como por específicos ARNs. La solicitud producirá error si se incluyen ambos.

Sintaxis de la solicitud

```
PUT /restore-testing/plans/RestoreTestingPlanName/selections HTTP/1.1
```

```
Content-type: application/json
```

```
{
  "CreatorRequestId": "string",
  "RestoreTestingSelection": {
    "IamRoleArn": "string",
    "ProtectedResourceArns": [ "string" ],
    "ProtectedResourceConditions": {
      "StringEquals": [
        {
          "Key": "string",
          "Value": "string"
        }
      ],
      "StringNotEquals": [
        {
```

```
        "Key": "string",
        "Value": "string"
    }
],
"ProtectedResourceType": "string",
"RestoreMetadataOverrides": {
    "string": "string"
},
"RestoreTestingSelectionName": "string",
"ValidationWindowHours": number
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[RestoreTestingPlanName](#)

Introduzca el nombre del plan de pruebas de restauración devuelto por la `CreateRestoreTestingPlan` solicitud relacionada.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[CreatorRequestId](#)

Es una cadena única opcional que identifica la solicitud y permite que se reintenten las solicitudes que han producido un error sin el riesgo de ejecutar la operación dos veces. Si se utiliza, este parámetro debe contener de 1 a 50 caracteres alfanuméricos o “-” o “_”. caracteres.

Tipo: cadena

Requerido: no

[RestoreTestingSelection](#)

Consta de `RestoreTestingSelectionName`, `ProtectedResourceType` y uno de los siguientes elementos:

- ProtectedResourceArns
- ProtectedResourceConditions

Cada tipo de recurso protegido puede tener un único valor.

Una selección de pruebas de restauración puede incluir un valor comodín ("*") como ProtectedResourceArns junto con ProtectedResourceConditions. Como alternativa, puede incluir hasta 30 recursos ARNs protegidos específicos ProtectedResourceArns.

Tipo: objeto [RestoreTestingSelectionForCreate](#)

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 201
Content-type: application/json

{
  "CreationTime": number,
  "RestoreTestingPlanArn": "string",
  "RestoreTestingPlanName": "string",
  "RestoreTestingSelectionName": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 201.

El servicio devuelve los datos siguientes en formato JSON.

[CreationTime](#)

La hora en la que la selección de pruebas de recursos se creó.

Tipo: marca temporal

[RestoreTestingPlanArn](#)

El ARN del plan de prueba de restauración al que está asociada la selección de pruebas de restauración.

Tipo: cadena

RestoreTestingPlanName

El nombre del plan de prueba de restauración.

El nombre no se puede cambiar después de crear el plan. El nombre consta de únicamente de caracteres alfanuméricos y guiones bajos. La longitud máxima es 50.

Tipo: cadena

RestoreTestingSelectionName

El nombre de la selección de pruebas de restauración para el plan de prueba de restauración.

El nombre no se puede cambiar después de crear el plan. El nombre consta de únicamente de caracteres alfanuméricos y guiones bajos. La longitud máxima es 50.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AlreadyExistsException

El recurso ya existe.

Arn

Context

CreatorRequestId

Type

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

CreateTieringConfiguration

Servicio: AWS Backup

Crea una configuración de estratificación.

Una configuración por niveles permite el movimiento automático de los datos de respaldo a un nivel de almacenamiento de menor costo en función de la antigüedad de los objetos respaldados en la bóveda de respaldo.

Cada almacén solo puede tener una configuración de estratificación específica para cada almacén, además de cualquier configuración global que se aplique a todos los almacenes.

Sintaxis de la solicitud

```
PUT /tiering-configurations HTTP/1.1
Content-type: application/json

{
  "CreatorRequestId": "string",
  "TieringConfiguration": {
    "BackupVaultName": "string",
    "ResourceSelection": [
      {
        "Resources": [ "string" ],
        "ResourceType": "string",
        "TieringDownSettingsInDays": number
      }
    ],
    "TieringConfigurationName": "string"
  },
  "TieringConfigurationTags": {
    "string" : "string"
  }
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[CreatorRequestId](#)

Se trata de una cadena única que identifica la solicitud y permite volver a intentar las solicitudes fallidas sin correr el riesgo de ejecutar la operación dos veces. Este parámetro es opcional. Si se utiliza, este parámetro debe contener de 1 a 50 caracteres alfanuméricos o “-”. caracteres.

Tipo: cadena

Requerido: no

[TieringConfiguration](#)

Una configuración por niveles debe contener una `TieringConfigurationName` cadena única que usted cree y debe contener una `BackupVaultName` y. `ResourceSelection` Si lo desea, puede incluir una `CreatorRequestId` cadena.

`TieringConfigurationName` Es una cadena única que es el nombre de la configuración de estratificación. No se puede cambiar después de la creación y debe constar únicamente de caracteres alfanuméricos y guiones bajos.

Tipo: objeto [TieringConfigurationInputForCreate](#)

Obligatorio: sí

[TieringConfigurationTags](#)

Las etiquetas que se van a asignar a la configuración de organización por niveles.

Tipo: mapa de cadena a cadena

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "CreationTime": number,
  "TieringConfigurationArn": "string",
  "TieringConfigurationName": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

CreationTime

La fecha y la hora en que se creó una configuración de organización por niveles, en formato Unix y en hora universal coordinada (UTC). El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

TieringConfigurationArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva la configuración de estratificación creada.

Tipo: cadena

TieringConfigurationName

Esta cadena única es el nombre de la configuración de estratificación.

El nombre no se puede cambiar después de crear el plan. El nombre consta de únicamente de caracteres alfanuméricos y guiones bajos. La longitud máxima es 200.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AlreadyExistsException

El recurso ya existe.

Arn

Context

CreatorRequestId

Type

Código de estado HTTP: 400

ConflictException

AWS Backup no puede realizar la acción que ha solicitado hasta que termine de realizar una acción anterior. Inténtelo de nuevo más tarde.

Context

Type

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DeleteBackupPlan

Servicio: AWS Backup

Elimina un plan de copia de seguridad. Solo puede eliminar un plan de copia de seguridad después de haber eliminado todas las selecciones de recursos asociadas. La eliminación de un plan de copia de seguridad elimina la versión actual del plan. Las versiones anteriores, si las hay, seguirán existiendo.

Sintaxis de la solicitud

```
DELETE /backup/plans/backupPlanId HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[backupPlanId](#)

Identifica de forma única un plan de copia de seguridad.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupPlanArn": "string",
  "BackupPlanId": "string",
  "DeletionDate": number,
  "VersionId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[BackupPlanArn](#)

Un nombre de recurso de Amazon (ARN) que identifica de forma única un plan de copia de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Tipo: cadena

[BackupPlanId](#)

Identifica de forma única un plan de copia de seguridad.

Tipo: cadena

[DeletionDate](#)

La fecha y la hora en que se eliminó el plan de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de `DeletionDate` tiene una precisión de milisegundos. Por ejemplo, el valor `1516925490.087` representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

[VersionId](#)

Cadenas cifradas en UTF-8, Unicode, únicas, generadas aleatoriamente que tienen como máximo una longitud de 1024 bytes. Los ID de versión no se pueden editar.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

`InvalidParameterValueException`

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

DeleteBackupSelection

Servicio: AWS Backup

Elimina la selección de recursos asociada a un plan de copia de seguridad especificado por `SelectionId`.

Sintaxis de la solicitud

```
DELETE /backup/plans/backupPlanId/selections/selectionId HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[backupPlanId](#)

Identifica de forma única un plan de copia de seguridad.

Obligatorio: sí

[selectionId](#)

Identifica de forma única el cuerpo de una solicitud para asignar un conjunto de recursos a un plan de copia de seguridad.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

DeleteBackupVault

Servicio: AWS Backup

Elimina el almacén de copias de seguridad identificado por su nombre. Un almacén solo se puede eliminar si está vacío.

Sintaxis de la solicitud

```
DELETE /backup-vaults/backupVaultName HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[backupVaultName](#)

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

DeleteBackupVaultAccessPolicy

Servicio: AWS Backup

Elimina el documento de política que administra los permisos en un almacén de copias de seguridad.

Sintaxis de la solicitud

```
DELETE /backup-vaults/backupVaultName/access-policy HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon. Constan de letras minúsculas, números y guiones.

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

DeleteBackupVaultLockConfiguration

Servicio: AWS Backup

Elimina el Bloqueo de almacenes de AWS Backup de un almacén de copias de seguridad especificado por un nombre de almacén de copias de seguridad.

Si la configuración del bloqueo de almacenes es inmutable, no podrá eliminar el bloqueo de almacenes mediante operaciones de API y recibirá una `InvalidRequestException` si lo intenta. Para obtener más información, consulte [Bloqueo de almacenes](#) en la Guía para desarrolladores de AWS Backup.

Sintaxis de la solicitud

```
DELETE /backup-vaults/backupVaultName/vault-lock HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[backupVaultName](#)

El nombre del almacén de copias de seguridad del que se va a eliminar el Bloqueo de almacenes de AWS Backup.

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

DeleteBackupVaultNotifications

Servicio: AWS Backup

Elimina las notificaciones de eventos para el almacén de copias de seguridad especificado.

Sintaxis de la solicitud

```
DELETE /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[backupVaultName](#)

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región donde se crearon.

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

DeleteFramework

Servicio: AWS Backup

Elimina el marco especificado por un nombre de marco.

Sintaxis de la solicitud

```
DELETE /audit/frameworks/frameworkName HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[frameworkName](#)

El nombre único de un marco.

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: [a-zA-Z][_a-zA-Z0-9]*

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

ConflictException

AWS Backup no puede realizar la acción que ha solicitado hasta que termine de realizar una acción anterior. Inténtelo de nuevo más tarde.

Context

Type

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

DeleteRecoveryPoint

Servicio: AWS Backup

Elimina el punto de recuperación especificado por un ID de punto de recuperación.

Si el ID del punto de recuperación pertenece a una copia de seguridad continua, al llamar a este punto de conexión se elimina la copia de seguridad continua existente y se detiene la copia de seguridad continua futura.

Cuando los permisos de un rol de IAM no son suficientes para llamar a esta API, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío, pero el punto de recuperación no se elimina. En su lugar, entra en un estado EXPIRED.

Los puntos de recuperación EXPIRED se pueden eliminar con esta API una vez que el rol de IAM tenga la acción `iam:CreateServiceLinkedRole`. Para obtener más información acerca de cómo agregar este rol, consulte [Solución de problemas de eliminaciones manuales](#).

Si se elimina el usuario o el rol o se quita el permiso del rol, la eliminación no se realizará correctamente y pasará a un estado EXPIRED.

Sintaxis de la solicitud

```
DELETE /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[backupVaultName](#)

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: sí

[recoveryPointArn](#)

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

`InvalidParameterValueException`

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

`InvalidRequestException`

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Context

Type

Código de estado HTTP: 400

InvalidResourceStateException

AWS Backup ya está realizando una acción en este punto de recuperación. No es posible realizar la acción que ha solicitado hasta que finalice la primera acción. Inténtelo de nuevo más tarde.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

DeleteReportPlan

Servicio: AWS Backup

Elimina el plan de informes especificado por un nombre de plan de informes.

Sintaxis de la solicitud

```
DELETE /audit/report-plans/reportPlanName HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

reportPlanName

El nombre único de un plan de informes.

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: [a-zA-Z][_a-zA-Z0-9]*

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

ConflictException

AWS Backup no puede realizar la acción que ha solicitado hasta que termine de realizar una acción anterior. Inténtelo de nuevo más tarde.

Context

Type

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

DeleteRestoreTestingPlan

Servicio: AWS Backup

Esta solicitud elimina el plan de prueba de restauración especificado.

La eliminación solo se puede realizar correctamente si se eliminan primero todas las selecciones de pruebas de restauración asociadas.

Sintaxis de la solicitud

```
DELETE /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

RestoreTestingPlanName

Nombre único obligatorio del plan de prueba de restauración que desea eliminar.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 204
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 204 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

DeleteRestoreTestingSelection

Servicio: AWS Backup

Introduzca el nombre del plan de prueba de restauración y el nombre de la selección de pruebas de restauración.

Todas las selecciones de pruebas asociadas a un plan de prueba de restauración deben eliminarse para poder eliminar el plan de prueba de restauración.

Sintaxis de la solicitud

```
DELETE /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

RestoreTestingPlanName

Nombre único obligatorio del plan de prueba de restauración que contiene la selección de pruebas de restauración que desea eliminar.

Obligatorio: sí

RestoreTestingSelectionName

Nombre único obligatorio de la selección de pruebas de restauración que desea eliminar.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 204
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 204 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)

- [AWS SDK para Ruby V3](#)

DeleteTieringConfiguration

Servicio: AWS Backup

Elimina la configuración de estratificación especificada por un nombre de configuración de estratificación.

Sintaxis de la solicitud

```
DELETE /tiering-configurations/tieringConfigurationName HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[tieringConfigurationName](#)

El nombre exclusivo de una configuración de organización por niveles.

Patrón: `^[a-zA-Z0-9_]{1,200}$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeBackupJob

Servicio: AWS Backup

Devuelve los detalles del trabajo de copia de seguridad para el BackupJobId especificado.

Sintaxis de la solicitud

```
GET /backup-jobs/backupJobId HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupJobId

Identifica de forma exclusiva una solicitud para AWS Backup hacer una copia de seguridad de un recurso.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "AccountId": "string",
  "BackupJobId": "string",
  "BackupOptions": {
    "string" : "string"
  },
  "BackupSizeInBytes": number,
  "BackupType": "string",
  "BackupVaultArn": "string",
  "BackupVaultName": "string",
  "BytesTransferred": number,
  "ChildJobsInState": {
    "string" : number
  },
}
```

```

"CompletionDate": number,
"CreatedBy": {
  "BackupPlanArn": "string",
  "BackupPlanId": "string",
  "BackupPlanName": "string",
  "BackupPlanVersion": "string",
  "BackupRuleCron": "string",
  "BackupRuleId": "string",
  "BackupRuleName": "string",
  "BackupRuleTimezone": "string"
},
"CreationDate": number,
"EncryptionKeyArn": "string",
"ExpectedCompletionDate": number,
"IamRoleArn": "string",
"InitiationDate": number,
"IsEncrypted": boolean,
"IsParent": boolean,
"MessageCategory": "string",
"NumberOfChildJobs": number,
"ParentJobId": "string",
"PercentDone": "string",
"RecoveryPointArn": "string",
"RecoveryPointLifecycle": {
  "DeleteAfterDays": number,
  "DeleteAfterEvent": "string",
  "MoveToColdStorageAfterDays": number,
  "OptInToArchiveForSupportedResources": boolean
},
"ResourceArn": "string",
"ResourceName": "string",
"ResourceType": "string",
"StartBy": number,
"State": "string",
"StatusMessage": "string",
"VaultLockState": "string",
"VaultType": "string"
}

```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[AccountId](#)

Devuelve el ID de la cuenta a la que pertenece el trabajo de copia de seguridad.

Tipo: cadena

Patrón: `^[0-9]{12}$`

[BackupJobId](#)

Identifica de forma exclusiva una solicitud para AWS Backup hacer una copia de seguridad de un recurso.

Tipo: cadena

[BackupOptions](#)

Representa las opciones especificadas como parte del plan de copia de seguridad o del trabajo de copia de seguridad bajo demanda.

Tipo: mapa de cadena a cadena

Patrón de clave: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Patrón de valores: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

[BackupSizeInBytes](#)

Es el tamaño de una copia de seguridad (punto de recuperación) en bytes.

Este valor puede representarse de forma diferente según el tipo de recurso, ya que AWS Backup extrae información de datos de otros AWS servicios. Por ejemplo, el valor devuelto puede mostrar un valor 0, que puede ser distinto al valor previsto.

A continuación se describe el comportamiento esperado de los valores por tipo de recurso:

- En Amazon Aurora, Amazon DocumentDB y Amazon Neptune, este valor no se rellena con la operación `GetBackupJobStatus`.
- En el caso de Amazon DynamoDB con características avanzadas, este valor es el tamaño del punto de recuperación (copia de seguridad).
- Amazon EC2 y Amazon EBS muestran el tamaño del volumen (almacenamiento aprovisionado) devuelto como parte de este valor. Amazon EBS no devuelve información sobre el tamaño de la copia de seguridad; el tamaño de la instantánea tendrá el mismo valor que el recurso original a partir del cual se realizó la copia de seguridad.

- En Amazon EFS, este valor hace referencia a los bytes delta transferidos durante una copia de seguridad.
- Amazon FSx no rellena este valor de la operación `GetBackupJobStatus` para sistemas de FSx archivos.
- Una instancia de Amazon RDS se mostrará como 0.
- En el caso de las máquinas virtuales en ejecución VMware, este valor se transfiere a AWS Backup través de un flujo de trabajo asíncrono, lo que puede provocar que el valor mostrado no represente el tamaño real de la copia de seguridad.

Tipo: largo

[BackupType](#)

Representa el tipo de copia de seguridad real seleccionado para un trabajo de copia de seguridad. Por ejemplo, si se realizó una copia de seguridad correcta de Volume Shadow Copy Service (VSS) de Windows, `BackupType` devuelve "WindowsVSS". Si `BackupType` está vacío, significa que el tipo de copia de seguridad era una copia de seguridad normal.

Tipo: cadena

[BackupVaultArn](#)

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un almacén de copia de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

[BackupVaultName](#)

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\ ]{2,50}$`

[BytesTransferred](#)

El tamaño en bytes transferido a un almacén de copias de seguridad en el momento en que se consultó el estado del trabajo.

Tipo: largo

[ChildJobsInState](#)

Devuelve las estadísticas de los trabajos de copia de seguridad secundarios (anidados) incluidos.

Tipo: mapa de cadena a largo

Claves válidas: CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED
| FAILED | EXPIRED | PARTIAL

[CompletionDate](#)

La fecha y la hora en que se completó un trabajo para crear un trabajo de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de `CompletionDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

[CreatedBy](#)

Contiene información de identificación sobre la creación de un trabajo de copia de seguridad, que incluye los valores de `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion` y `BackupRuleId` del plan de copia de seguridad utilizado para crearlo.

Tipo: objeto [RecoveryPointCreator](#)

[CreationDate](#)

La fecha y la hora en que se creó el trabajo de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

[EncryptionKeyArn](#)

Es el nombre de recurso de Amazon (ARN) de la clave de KMS que se utiliza para cifrar la copia de seguridad. Puede ser una clave administrada por el cliente o una clave administrada, según la AWS configuración del almacén.

Tipo: cadena

ExpectedCompletionDate

La fecha y la hora en que se espera completar un trabajo de copia de seguridad de recursos, en formato Unix y horario universal coordinado (UTC). El valor de `ExpectedCompletionDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

IamRoleArn

Especifica el ARN del rol de IAM utilizado para crear el punto de recuperación de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

InitiationDate

La fecha en que se inició un trabajo de copia de seguridad.

Tipo: marca temporal

IsEncrypted

Es un valor booleano que indica si la copia de seguridad está cifrada. Todas las copias de seguridad AWS Backup están cifradas, pero este campo indica el estado de cifrado para mayor transparencia.

Tipo: Booleano

IsParent

Esto devuelve el valor booleano de que un trabajo de copia de seguridad es un trabajo principal (compuesto).

Tipo: Booleano

MessageCategory

El recuento de trabajos de la categoría de mensajes especificada.

Las cadenas de ejemplo pueden ser `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` y `INVALIDPARAMETERS`. Consulta la [sección Supervisión](#) para ver una lista de `MessageCategory` las cadenas aceptadas.

Tipo: cadena

[NumberOfChildJobs](#)

Esto devuelve el número de trabajos de copia de seguridad secundarios (anidados).

Tipo: largo

[ParentJobId](#)

Esto devuelve el ID del trabajo de copia de seguridad del recurso principal (compuesto).

Tipo: cadena

[PercentDone](#)

Contiene el porcentaje estimado que se ha completado de un trabajo en el momento en que se consultó el estado del trabajo.

Tipo: cadena

[RecoveryPointArn](#)

Un ARN que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

[RecoveryPointLifecycle](#)

Especifica el período, en días, antes de que un punto de recuperación se transfiera al almacenamiento en frío o se elimine.

Las copias de seguridad que se transfieran a cámaras frigoríficas deben almacenarse en cámaras frigoríficas durante un mínimo de 90 días. Por lo tanto, en la consola, el valor de retención debe tener 90 días más que el valor del número de días tras los cuales se transferirá al almacenamiento en frío. El valor de "transition to cold after days" (número de días tras los cuales migrará a almacenamiento en frío) no puede cambiarse una vez que se ha migrado una copia de seguridad al almacenamiento en frío.

Los tipos de recursos que pueden pasar al almacenamiento en frío se enumeran en la tabla [Disponibilidad de funciones por recurso](#). AWS Backup omite esta expresión para otros tipos de recursos.

Para eliminar el ciclo de vida y los períodos de retención existentes y conservar los puntos de recuperación indefinidamente, especifique -1 para `MoveToColdStorageAfterDays` y `DeleteAfterDays`.

Tipo: objeto [Lifecycle](#)

[ResourceArn](#)

Un ARN que identifica de forma exclusiva un recurso guardado. El formato del ARN depende del tipo de recurso.

Tipo: cadena

[ResourceName](#)

El nombre no exclusivo del recurso que pertenece a la copia de seguridad especificada.

Tipo: cadena

[ResourceType](#)

El tipo de AWS recurso del que se va a hacer una copia de seguridad; por ejemplo, un volumen de Amazon Elastic Block Store (Amazon EBS) o una base de datos de Amazon Relational Database Service (Amazon RDS).

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

[StartBy](#)

Especifica la hora en formato Unix y horario universal coordinado (UTC) en la que se debe iniciar un trabajo de copia de seguridad antes de que se cancele. El valor se calcula agregando el periodo de inicio a la hora programada. Por lo tanto, si la hora programada fueran las 18:00 h y el periodo de inicio fuera de 2 horas, la hora `StartBy` sería las 20:00 h en la fecha especificada. El valor de `StartBy` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

[State](#)

El estado actual de un trabajo de copia de seguridad.

Tipo: cadena

Valores válidos: CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED
| FAILED | EXPIRED | PARTIAL

[StatusMessage](#)

Un mensaje detallado que explica el estado del trabajo de copia de seguridad de un recurso.

Tipo: cadena

[VaultLockState](#)

Es el estado de bloqueo del almacén de copias de seguridad. En el caso de los almacenes aislados lógicamente, indica si el almacén está bloqueado en el modo de conformidad. Los valores válidos son LOCKED y UNLOCKED.

Tipo: cadena

[VaultType](#)

Es el tipo de almacén de copias de seguridad en el que se guarda el punto de recuperación. Los valores válidos son BACKUP_VAULT para los almacenes de copias de seguridad estándar y LOGICALLY_AIR_GAPPED_BACKUP_VAULT para los almacenes aislados lógicamente.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

DependencyFailureException

Un AWS servicio o recurso dependiente devolvió un error al AWS Backup servicio y no se pudo completar la acción.

Context

Type

Código de estado HTTP: 500

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)

- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeBackupVault

Servicio: AWS Backup

Devuelve los metadatos de un almacén de copias de seguridad especificado por su nombre.

Sintaxis de la solicitud

```
GET /backup-vaults/backupVaultName?backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[BackupVaultAccountId](#)

El identificador de cuenta del almacén de copias de seguridad especificado.

[backupVaultName](#)

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupVaultArn": "string",
  "BackupVaultName": "string",
  "CreationDate": number,
  "CreatorRequestId": "string",
  "EncryptionKeyArn": "string",
  "EncryptionKeyType": "string",
  "LatestMpaApprovalTeamUpdate": {
    "ExpiryDate": number,
```

```
    "InitiationDate": number,
    "MpaSessionArn": "string",
    "Status": "string",
    "StatusMessage": "string"
  },
  "LockDate": number,
  "Locked": boolean,
  "MaxRetentionDays": number,
  "MinRetentionDays": number,
  "MpaApprovalTeamArn": "string",
  "MpaSessionArn": "string",
  "NumberOfRecoveryPoints": number,
  "SourceBackupVaultArn": "string",
  "VaultState": "string",
  "VaultType": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

BackupVaultArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un almacén de copia de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

BackupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región donde se crearon.

Tipo: cadena

CreationDate

La fecha y la hora en que se creó el almacén, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor `1516925490.087` representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

[CreatorRequestId](#)

Una cadena única que identifica la solicitud y permite que se reintenten las solicitudes que han producido un error sin el riesgo de ejecutar la operación dos veces. Este parámetro es opcional. Si se utiliza, este parámetro debe contener de 1 a 50 caracteres alfanuméricos o “-”. caracteres.

Tipo: cadena

[EncryptionKeyArn](#)

La clave de cifrado en el servidor que se utiliza para proteger sus copias de seguridad; por ejemplo, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Tipo: cadena

[EncryptionKeyType](#)

El tipo de clave de cifrado utilizada para el almacén de copias de seguridad. Los valores válidos son `CUSTOMER_MANAGED_KMS_KEY` para las claves administradas por el cliente o `_OWNED_KMS_KEY` para las claves propiedad del cliente. AWS AWS

Tipo: cadena

Valores válidos: `AWS_OWNED_KMS_KEY` | `CUSTOMER_MANAGED_KMS_KEY`

[LatestMpaApprovalTeamUpdate](#)

Información sobre la última actualización de la asociación del equipo de aprobación MPA para este almacén de copias de seguridad.

Tipo: objeto [LatestMpaApprovalTeamUpdate](#)

[LockDate](#)

La fecha y la hora en las que no se AWS Backup puede cambiar ni eliminar la configuración de Vault Lock.

Si ha aplicado el bloqueo de almacenes a su almacén sin especificar una fecha de bloqueo, puede cambiar cualquier configuración del bloqueo de almacenes o eliminarlo del almacén por completo en cualquier momento.

Este valor está en formato Unix, horario universal coordinado (UTC) y tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Locked

Un valor booleano que indica si AWS Backup Vault Lock protege actualmente el almacén de respaldo. `True` significa que Vault Lock provoca un error en las operaciones de eliminación o actualización de los puntos de recuperación almacenados en el almacén.

Tipo: Booleano

MaxRetentionDays

La configuración de bloqueo del AWS Backup almacén que especifica el período máximo de retención durante el que el almacén conserva sus puntos de recuperación. Si no se especifica este parámetro, el bloqueo de almacenes no impone un periodo de retención máximo en los puntos de recuperación del almacén (lo que permite un almacenamiento indefinido).

Si se especifica, cualquier trabajo de copia de seguridad o copia en el almacén debe tener una política de ciclo de vida con un periodo de retención igual o inferior al periodo de retención máximo. Si el periodo de retención del trabajo es superior a ese periodo de retención máximo, el almacén falla el trabajo de copia de seguridad o de copia de seguridad, y deberá modificar la configuración del ciclo de vida o utilizar un almacén diferente. Los puntos de recuperación ya almacenados en el almacén antes del bloqueo del mismo no se ven afectados.

Tipo: largo

MinRetentionDays

La configuración de bloqueo del AWS Backup almacén que especifica el período mínimo de retención durante el que el almacén conserva sus puntos de recuperación. Si no se especifica este parámetro, el bloqueo del almacén no impondrá un periodo mínimo de retención.

Si se especifica, cualquier trabajo de copia de seguridad o copia en el almacén debe tener una política de ciclo de vida con un periodo de retención igual o superior al periodo de retención mínimo. Si el periodo de retención del trabajo es más breve que ese periodo de retención mínimo, el almacén dará error en el trabajo de copia de seguridad o copia, y deberá modificar la configuración del ciclo de vida o usar un almacén diferente. Los puntos de recuperación ya almacenados en el almacén antes del bloqueo del mismo no se ven afectados.

Tipo: largo

[MpaApprovalTeamArn](#)

Es el ARN del equipo de aprobación MPA asociado con este almacén de copias de seguridad.

Tipo: cadena

[MpaSessionArn](#)

Es el ARN de la sesión de MPA asociado con este almacén de copias de seguridad.

Tipo: cadena

[NumberOfRecoveryPoints](#)

El número de puntos de recuperación que se almacenan en un almacén de copias de seguridad.

El valor del recuento de puntos de recuperación que se muestra en la consola puede ser una aproximación. Utilice la API [ListRecoveryPointsByBackupVault](#) para obtener el recuento exacto.

Tipo: largo

[SourceBackupVaultArn](#)

Es el ARN del almacén de copias de seguridad de origen a partir del cual se ha creado este almacén de copias de seguridad con acceso a la restauración.

Tipo: cadena

[VaultState](#)

El estado actual del almacén.->

Tipo: cadena

Valores válidos: CREATING | AVAILABLE | FAILED

[VaultType](#)

El tipo de almacén descrito.

Tipo: cadena

Valores válidos: BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT |
RESTORE_ACCESS_BACKUP_VAULT

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeCopyJob

Servicio: AWS Backup

Devuelve los metadatos asociados a la creación de una copia de un recurso.

Sintaxis de la solicitud

```
GET /copy-jobs/copyJobId HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[copyJobId](#)

Identifica de forma exclusiva un trabajo de copia.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "CopyJob": {
    "AccountId": "string",
    "BackupSizeInBytes": number,
    "ChildJobsInState": {
      "string" : number
    },
    "CompletionDate": number,
    "CompositeMemberIdentifier": "string",
    "CopyJobId": "string",
    "CreatedBy": {
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
```

```

    "BackupPlanName": "string",
    "BackupPlanVersion": "string",
    "BackupRuleCron": "string",
    "BackupRuleId": "string",
    "BackupRuleName": "string",
    "BackupRuleTimezone": "string"
  },
  "CreatedByBackupJobId": "string",
  "CreationDate": number,
  "DestinationBackupVaultArn": "string",
  "DestinationEncryptionKeyArn": "string",
  "DestinationRecoveryPointArn": "string",
  "DestinationRecoveryPointLifecycle": {
    "DeleteAfterDays": number,
    "DeleteAfterEvent": "string",
    "MoveToColdStorageAfterDays": number,
    "OptInToArchiveForSupportedResources": boolean
  },
  "DestinationVaultLockState": "string",
  "DestinationVaultType": "string",
  "IamRoleArn": "string",
  "IsParent": boolean,
  "MessageCategory": "string",
  "NumberOfChildJobs": number,
  "ParentJobId": "string",
  "ResourceArn": "string",
  "ResourceName": "string",
  "ResourceType": "string",
  "SourceBackupVaultArn": "string",
  "SourceRecoveryPointArn": "string",
  "State": "string",
  "StatusMessage": "string"
}
}

```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

CopyJob

Contiene información detallada acerca de un trabajo de copia.

Tipo: objeto [CopyJob](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeFramework

Servicio: AWS Backup

Devuelve los detalles del marco para el `FrameworkName` especificado.

Sintaxis de la solicitud

```
GET /audit/frameworks/frameworkName HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

frameworkName

El nombre único de un marco.

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `[a-zA-Z][_a-zA-Z0-9]*`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "CreationTime": number,
  "DeploymentStatus": "string",
  "FrameworkArn": "string",
  "FrameworkControls": [
    {
      "ControlInputParameters": [
        {
          "ParameterName": "string",
          "ParameterValue": "string"
        }
      ]
    }
  ]
}
```



```

    ],
    "ControlName": "string",
    "ControlScope": {
      "ComplianceResourceIds": [ "string" ],
      "ComplianceResourceTypes": [ "string" ],
      "Tags": {
        "string" : "string"
      }
    }
  }
},
"FrameworkDescription": "string",
"FrameworkName": "string",
"FrameworkStatus": "string",
"IdempotencyToken": "string"
}

```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[CreationTime](#)

Es la fecha y la hora en que se creó un marco con la norma ISO 8601. El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, 2020-07-10T15:00:00.000-08:00 representa el 10 de julio de 2020 a las 15:00 h, 8 horas menos que UTC.

Tipo: marca temporal

[DeploymentStatus](#)

El estado de implementación de un marco. Los estados son:

CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED
| FAILED

Tipo: cadena

[FrameworkArn](#)

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un recurso. El formato del ARN depende del tipo de recurso.

Tipo: cadena

[FrameworkControls](#)

Los controles que componen el marco. Cada control de la lista tiene un nombre, parámetros de entrada y alcance.

Tipo: matriz de objetos [FrameworkControl](#)

[FrameworkDescription](#)

Una descripción opcional del marco.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `.*\S.*`

[FrameworkName](#)

El nombre único de un marco.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `[a-zA-Z][_a-zA-Z0-9]*`

[FrameworkStatus](#)

Un marco consta de uno o varios controles. Cada control rige un recurso, como los planes de copia de seguridad, las selecciones de copia de seguridad, los almacenes de copia de seguridad o los puntos de recuperación. También puede activar o desactivar la grabación de AWS Config para cada recurso. Los estados son:

- **ACTIVE** cuando la grabación está activada para todos los recursos regidos por el marco.
- **PARTIALLY_ACTIVE** cuando la grabación está desactivada para al menos un recurso regido por el marco.
- **INACTIVE** cuando la grabación está desactivada para todos los recursos regidos por el marco.
- **UNAVAILABLE** cuando AWS Backup no puede validar el estado de la grabación en este momento.

Tipo: cadena

IdempotencyToken

Una cadena elegida por el cliente que puede utilizar para distinguir entre llamadas a `DescribeFrameworkOutput` que, de otro modo, serían idénticas. Si se vuelve a intentar una solicitud correcta con el mismo token de idempotencia, aparece un mensaje de confirmación y no se realiza ninguna acción.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

`InvalidParameterValueException`

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

`MissingParameterValueException`

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

`ResourceNotFoundException`

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeGlobalSettings

Servicio: AWS Backup

Describe si la AWS cuenta está habilitada para realizar copias de seguridad multicuenta. Devuelve un error si la cuenta no forma parte de una organización de Organizations. Ejemplo: `describe-global-settings --region us-west-2`

Sintaxis de la solicitud

```
GET /global-settings HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "GlobalSettings": {
    "string" : "string"
  },
  "LastUpdateTime": number
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

GlobalSettings

El estado de las banderas `isCrossAccountBackupEnabled` `isMpaEnabled` («Mpa» se refiere a la aprobación multipartidista) y `isDelegatedAdministratorEnabled`

Tipo: mapa de cadena a cadena

LastUpdateTime

La fecha y hora en que se actualizó por última vez el indicador `isCrossAccountBackupEnabled`. Esta actualización está en formato Unix y horario universal coordinado (UTC). El valor de `LastUpdateTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeProtectedResource

Servicio: AWS Backup

Devuelve información sobre un recurso guardado, incluida la última vez que se realizó una copia de seguridad del recurso, su nombre de recurso de Amazon (ARN) y el tipo de servicio de AWS del recurso guardado.

Sintaxis de la solicitud

```
GET /resources/resourceArn HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[resourceArn](#)

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un recurso. El formato del ARN depende del tipo de recurso.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "LastBackupTime": number,
  "LastBackupVaultArn": "string",
  "LastRecoveryPointArn": "string",
  "LatestRestoreExecutionTimeMinutes": number,
  "LatestRestoreJobCreationDate": number,
  "LatestRestoreRecoveryPointCreationDate": number,
  "ResourceArn": "string",
  "ResourceName": "string",
  "ResourceType": "string"
}
```



```
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

LastBackupTime

La fecha y la hora en que se realizó la última una copia de seguridad de un recurso, en formato Unix y horario universal coordinado (UTC). El valor de LastBackupTime tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

LastBackupVaultArn

El ARN (nombre de recurso de Amazon) del almacén de copias de seguridad que contiene el punto de recuperación de copia de seguridad más reciente.

Tipo: cadena

LastRecoveryPointArn

El ARN (nombre de recurso de Amazon) del punto de recuperación más reciente.

Tipo: cadena

LatestRestoreExecutionTimeMinutes

El tiempo en minutos que tardó en completarse el trabajo de restauración más reciente.

Tipo: Long

LatestRestoreJobCreationDate

La fecha de creación del trabajo de restauración más reciente.

Tipo: marca temporal

LatestRestoreRecoveryPointCreationDate

La fecha de creación del punto de recuperación más reciente.

Tipo: marca temporal

[ResourceArn](#)

Un ARN que identifica de forma única a un recurso. El formato del ARN depende del tipo de recurso.

Tipo: cadena

[ResourceName](#)

El nombre del recurso que pertenece a la copia de seguridad especificada.

Tipo: cadena

[ResourceType](#)

El tipo de recurso de AWS guardado como punto de recuperación; por ejemplo, un volumen de Amazon EBS o una base de datos de Amazon RDS.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)

- [AWS SDK para Ruby V3](#)

DescribeRecoveryPoint

Servicio: AWS Backup

Devuelve los metadatos asociados a un punto de recuperación, incluidos el ID, el estado, el cifrado y el ciclo de vida.

Sintaxis de la solicitud

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn?  
backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[BackupVaultAccountId](#)

El identificador de cuenta del almacén de copias de seguridad especificado.

Patrón: `^[0-9]{12}$`

[backupVaultName](#)

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: sí

[recoveryPointArn](#)

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupSizeInBytes": number,
  "BackupVaultArn": "string",
  "BackupVaultName": "string",
  "CalculatedLifecycle": {
    "DeleteAt": number,
    "MoveToColdStorageAt": number
  },
  "CompletionDate": number,
  "CompositeMemberIdentifier": "string",
  "CreatedBy": {
    "BackupPlanArn": "string",
    "BackupPlanId": "string",
    "BackupPlanName": "string",
    "BackupPlanVersion": "string",
    "BackupRuleCron": "string",
    "BackupRuleId": "string",
    "BackupRuleName": "string",
    "BackupRuleTimezone": "string"
  },
  "CreationDate": number,
  "EncryptionKeyArn": "string",
  "EncryptionKeyType": "string",
  "IamRoleArn": "string",
  "IndexStatus": "string",
  "IndexStatusMessage": "string",
  "InitiationDate": number,
  "IsEncrypted": boolean,
  "IsParent": boolean,
  "LastRestoreTime": number,
  "Lifecycle": {
    "DeleteAfterDays": number,
    "DeleteAfterEvent": "string",
    "MoveToColdStorageAfterDays": number,
    "OptInToArchiveForSupportedResources": boolean
  },
  "ParentRecoveryPointArn": "string",
  "RecoveryPointArn": "string",
  "ResourceArn": "string",
```

```

"ResourceName": "string",
"ResourceType": "string",
"ScanResults": [
  {
    "Findings": [ "string" ],
    "LastScanTimestamp": number,
    "MalwareScanner": "string",
    "ScanJobState": "string"
  }
],
"SourceBackupVaultArn": "string",
"Status": "string",
"StatusMessage": "string",
"StorageClass": "string",
"VaultType": "string"
}

```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

BackupSizeInBytes

El tamaño de una copia de seguridad, en bytes.

Tipo: largo

BackupVaultArn

Un ARN que identifica de forma exclusiva un almacén de copias de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

BackupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región donde se crearon.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

CalculatedLifecycle

Un objeto `CalculatedLifecycle` que contiene las marcas temporales `MoveToColdStorageAt` y `DeleteAt`.

Tipo: objeto [CalculatedLifecycle](#)

CompletionDate

La fecha y la hora en que se completó un trabajo para crear un punto de recuperación, en formato Unix y horario universal coordinado (UTC). El valor de `CompletionDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

CompositeMemberIdentifier

El identificador de un recurso dentro de un grupo compuesto, como un punto de recuperación anidado (secundario) que pertenece a una pila compuesta (principal). El ID se transfiere desde el [ID lógico](#) de una pila.

Tipo: cadena

CreatedBy

Contiene información de identificación sobre la creación de un punto de recuperación, que incluye los valores de `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion` y `BackupRuleId` del plan de copia de seguridad utilizado para crearlo.

Tipo: objeto [RecoveryPointCreator](#)

CreationDate

La fecha y la hora en que se creó un punto de recuperación, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

EncryptionKeyArn

La clave de cifrado en el servidor utilizada para proteger sus copias de seguridad; por ejemplo, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Tipo: cadena

[EncryptionKeyType](#)

El tipo de clave de cifrado utilizada para el punto de recuperación. Los valores válidos son `CUSTOMER_MANAGED_KMS_KEY` para las claves administradas por el cliente o `_OWNED_KMS_KEY` para las claves propiedad del cliente. AWS AWS

Tipo: cadena

Valores válidos: `AWS_OWNED_KMS_KEY` | `CUSTOMER_MANAGED_KMS_KEY`

[IamRoleArn](#)

Especifica el ARN del rol de IAM utilizado para crear el punto de recuperación de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

[IndexStatus](#)

Este es el estado actual del índice de copias de seguridad asociado al punto de recuperación especificado.

Los estados son: `PENDING` | `ACTIVE` | `FAILED` | `DELETING`

En una búsqueda se puede incluir un punto de recuperación con un índice con el estado `ACTIVE`.

Tipo: cadena

Valores válidos: `PENDING` | `ACTIVE` | `FAILED` | `DELETING`

[IndexStatusMessage](#)

Es una cadena en forma de mensaje detallado que explica el estado del índice de copias de seguridad asociado al punto de recuperación.

Tipo: cadena

[InitiationDate](#)

Fecha y hora en que se inició el trabajo de copia de seguridad que ha creado este punto de recuperación, expresadas en formato Unix y horario universal coordinado (UTC).

Tipo: marca temporal

IsEncrypted

Un valor booleano que se devuelve como TRUE si el punto de recuperación especificado está cifrado o como FALSE si el punto de recuperación no está cifrado.

Tipo: Booleano

IsParent

Esto devuelve el valor booleano de que un punto de recuperación es un trabajo principal (compuesto).

Tipo: Booleano

LastRestoreTime

La fecha y hora en que se restauró por última vez un punto de recuperación, en formato Unix y horario universal coordinado (UTC). El valor de LastRestoreTime tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Lifecycle

El ciclo de vida define cuándo un recurso protegido pasa a almacenamiento en frío y cuándo caduca. AWS Backup cambia y vence las copias de seguridad automáticamente de acuerdo con el ciclo de vida que usted defina.

Las copias de seguridad que se han migrado al almacenamiento en frío deben permanecer en él durante un mínimo de 90 días. Por lo tanto, el valor de retención debe tener 90 días más que el valor del número de días tras los cuales se transferirá al almacenamiento en frío. El valor de “número de días tras los cuales migrará a almacenamiento en frío” no puede cambiarse una vez que se ha migrado una copia de seguridad al almacenamiento en frío.

Los tipos de recursos que pueden pasar al almacenamiento en frío se muestran en la tabla [Disponibilidad de funciones por recurso](#). AWS Backup omite esta expresión para otros tipos de recursos.

Tipo: objeto [Lifecycle](#)

[ParentRecoveryPointArn](#)

Un ARN que identifica de forma exclusiva un punto de recuperación principal (compuesto); por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

[RecoveryPointArn](#)

Un ARN que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

[ResourceArn](#)

Un ARN que identifica de forma exclusiva un recurso guardado. El formato del ARN depende del tipo de recurso.

Tipo: cadena

[ResourceName](#)

El nombre del recurso que pertenece a la copia de seguridad especificada.

Tipo: cadena

[ResourceType](#)

El tipo de AWS recurso que se va a guardar como punto de recuperación; por ejemplo, un volumen de Amazon Elastic Block Store (Amazon EBS) o una base de datos de Amazon Relational Database Service (Amazon RDS).

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

[ScanResults](#)

Contiene los resultados de escaneo más recientes comparados con el punto de recuperación y, actualmente `MalwareScanner`, incluye, `ScanJobState` y `Findings LastScanTimestamp`

Tipo: matriz de objetos [ScanResult](#)

Miembros de la matriz: número mínimo de 0 artículos. La cantidad máxima es de 5 artículos.

SourceBackupVaultArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva el almacén de origen en el que se realizó la copia de seguridad original del recurso; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`. Si la recuperación se restaura en la misma AWS cuenta o región, este valor será `null`.

Tipo: cadena

Status

Un código de estado que especifica el estado del punto de recuperación. Para obtener más información, consulta el [estado de los puntos de recuperación](#) en la Guía para AWS Backup desarrolladores.

- **CREATING**El estado indica que se ha iniciado un AWS Backup trabajo para un recurso. El proceso de copia de seguridad se ha iniciado y está procesando activamente un trabajo de copia de seguridad para el punto de recuperación asociado.
- El estado **AVAILABLE** indica que la copia de seguridad se ha creado correctamente para el punto de recuperación. El proceso de copia de seguridad se ha completado sin problemas y el punto de recuperación ya está listo para su uso.
- El estado **PARTIAL** indica que un punto de recuperación compuesto tiene uno o más puntos de recuperación anidados que no estaban en la copia de seguridad.
- **EXPIRED**El estado indica que el punto de recuperación ha superado su período de retención, pero AWS Backup carece de permiso o no puede eliminarlo por algún motivo. Para eliminar estos puntos de recuperación manualmente, consulte el [Paso 3: elimine los puntos de recuperación](#) en la sección Depuración de recursos de la Introducción.
- El estado **STOPPED** se produce en una copia de seguridad continua cuando un usuario ha realizado alguna acción que provoca la desactivación de la copia de seguridad continua. Esto puede deberse a la eliminación de los permisos, a la desactivación del control de versiones, a la desactivación de los eventos a EventBridge los que se envían o a la desactivación de EventBridge las reglas establecidas por. AWS Backup En el caso de los puntos de recuperación de los recursos de Amazon S3, Amazon RDS y Amazon Aurora, este estado se produce cuando se cambia el período de retención de una regla de copia de seguridad continua.

Para resolver el estado **STOPPED**, asegúrese de que todos los permisos solicitados estén en vigor y de que el control de versiones esté activado en el bucket de S3. Una vez que se

cumplan estas condiciones, la siguiente instancia de una regla de copia de seguridad que se ejecute provocará la creación de un nuevo punto de recuperación continuo. No es necesario eliminar los puntos de recuperación con el estado STOPPED.

En el caso de SAP HANA on Amazon, el EC2 STOPPED estado se debe a una acción del usuario, a una mala configuración de la aplicación o a un error en la copia de seguridad. Para garantizar que las futuras copias de seguridad continuas se realicen correctamente, consulte el estado del punto de recuperación y consulte SAP HANA para obtener más información.

Tipo: cadena

Valores válidos: COMPLETED | PARTIAL | DELETING | EXPIRED | AVAILABLE | STOPPED | CREATING

[StatusMessage](#)

Un mensaje de estado que explica el estado del punto de recuperación.

Tipo: cadena

[StorageClass](#)

Especifica la clase de almacenamiento del punto de recuperación. Los valores válidos son WARM o COLD.

Tipo: cadena

Valores válidos: WARM | COLD | DELETED

[VaultType](#)

El tipo de almacén en el que se guarda el punto de recuperación descrito.

Tipo: cadena

Valores válidos: BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT | RESTORE_ACCESS_BACKUP_VAULT

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeRegionSettings

Servicio: AWS Backup

Devuelve la configuración actual de suscripción del servicio para la región. Si la suscripción al servicio está habilitada para un servicio, AWS Backup intenta proteger los recursos de ese servicio en esta región cuando el recurso esté incluido en un plan de copia de seguridad bajo demanda o programada. De no ser así, AWS Backup no intenta proteger los recursos de ese servicio en esta región.

Sintaxis de la solicitud

```
GET /account-settings HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "ResourceTypeManagementPreference": {
    "string" : boolean
  },
  "ResourceTypeOptInPreference": {
    "string" : boolean
  }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[ResourceTypeManagementPreference](#)

Devuelve si AWS Backup administra completamente las copias de seguridad de un tipo de recurso.

Para conocer las ventajas de una administración completa de AWS Backup, consulte [Administración completa de AWS Backup](#).

Para obtener una lista de los tipos de recursos y saber si cada uno de ellos admite la administración completa de AWS Backup, consulte la tabla [Disponibilidad de características por recurso](#).

Si "DynamoDB": false, puede habilitar la administración completa de AWS Backup para las copias de seguridad de DynamoDB al habilitar las [características avanzadas de copia de seguridad de DynamoDB de AWS Backup](#).

Tipo: mapa de cadena a booleano

Patrón de clave: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

[ResourceTypeOptInPreference](#)

Los servicios junto con las preferencias de suscripción de la región.

Tipo: mapa de cadena a booleano

Patrón de clave: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeReportJob

Servicio: AWS Backup

Devuelve los detalles asociados a la creación de un informe especificado por su `ReportJobId`.

Sintaxis de la solicitud

```
GET /audit/report-jobs/reportJobId HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

reportJobId

El identificador del trabajo de informes. Una única cadena cifrada en UTF-8, Unicode, generada aleatoriamente que tiene como máximo una longitud de 1024 bytes. El ID del trabajo de informes no se puede editar.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "ReportJob": {
    "CompletionTime": number,
    "CreationTime": number,
    "ReportDestination": {
      "S3BucketName": "string",
      "S3Keys": [ "string" ]
    },
    "ReportJobId": "string",
    "ReportPlanArn": "string",
    "ReportTemplate": "string",
    "Status": "string",
```

```
    "StatusMessage": "string"  
  }  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[ReportJob](#)

La información sobre un trabajo de informes, que incluye las horas de finalización y creación, el destino del informe, el ID único del trabajo de informes, el nombre de recurso de Amazon (ARN), la plantilla del informe, el estado y el mensaje de estado.

Tipo: objeto [ReportJob](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeReportPlan

Servicio: AWS Backup

Devuelve una lista de todos los planes de informes para una Cuenta de AWS y Región de AWS.

Sintaxis de la solicitud

```
GET /audit/report-plans/reportPlanName HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

reportPlanName

El nombre único de un plan de informes.

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `[a-zA-Z][_a-zA-Z0-9]*`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "ReportPlan": {
    "CreationTime": number,
    "DeploymentStatus": "string",
    "LastAttemptedExecutionTime": number,
    "LastSuccessfulExecutionTime": number,
    "ReportDeliveryChannel": {
      "Formats": [ "string" ],
      "S3BucketName": "string",
```

```
    "S3KeyPrefix": "string"
  },
  "ReportPlanArn": "string",
  "ReportPlanDescription": "string",
  "ReportPlanName": "string",
  "ReportSetting": {
    "Accounts": [ "string" ],
    "FrameworkArns": [ "string" ],
    "NumberOfFrameworks": number,
    "OrganizationUnits": [ "string" ],
    "Regions": [ "string" ],
    "ReportTemplate": "string"
  }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[ReportPlan](#)

Devuelve detalles sobre el plan de informes especificado por su nombre. Estos detalles incluyen el nombre de recurso de Amazon (ARN) del plan de informes, la descripción, la configuración, el canal de entrega, el estado de implementación, la hora de creación y las últimas veces que se intentó ejecutar y se ejecutó correctamente.

Tipo: objeto [ReportPlan](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)

- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeRestoreJob

Servicio: AWS Backup

Devuelve los metadatos asociados a un trabajo de restauración especificado mediante un ID de trabajo.

Sintaxis de la solicitud

```
GET /restore-jobs/restoreJobId HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

restoreJobId

Identifica de forma exclusiva el trabajo que restaura un punto de recuperación.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "AccountId": "string",
  "BackupSizeInBytes": number,
  "BackupVaultArn": "string",
  "CompletionDate": number,
  "CreatedBy": {
    "RestoreTestingPlanArn": "string"
  },
  "CreatedResourceArn": "string",
  "CreationDate": number,
  "DeletionStatus": "string",
  "DeletionStatusMessage": "string",
  "ExpectedCompletionTimeMinutes": number,
  "IamRoleArn": "string",
```

```
"IsParent": boolean,
"ParentJobId": "string",
"PercentDone": "string",
"RecoveryPointArn": "string",
"RecoveryPointCreationDate": number,
"ResourceType": "string",
"RestoreJobId": "string",
"SourceResourceArn": "string",
"Status": "string",
"StatusMessage": "string",
"ValidationStatus": "string",
"ValidationStatusMessage": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

AccountId

Devuelve el ID de la cuenta a la que pertenece el trabajo de restauración.

Tipo: cadena

Patrón: `^[0-9]{12}$`

BackupSizeInBytes

El tamaño del recurso restaurado, en bytes.

Tipo: largo

BackupVaultArn

Es el Nombre de recurso de Amazon (ARN) del almacén de copias de seguridad que contiene el punto de recuperación que se va a restaurar. Esto ayuda a identificar las políticas y los permisos de acceso al almacén.

Tipo: cadena

CompletionDate

La fecha y la hora en que se completó un trabajo para restaurar un punto de recuperación, en formato Unix y horario universal coordinado (UTC). El valor de `CompletionDate` tiene una

precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

CreatedBy

Contiene información de identificación sobre la creación de un trabajo de restauración.

Tipo: objeto [RestoreJobCreator](#)

CreatedResourceArn

El nombre de recurso de Amazon (ARN) del recurso que creó el trabajo de restauración.

El formato del ARN depende del tipo de recurso del que se ha hecho copia de seguridad.

Tipo: cadena

CreationDate

La fecha y la hora en que se creó un trabajo de restauración, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

DeletionStatus

El estado de los datos generados por la prueba de restauración.

Tipo: cadena

Valores válidos: DELETING | FAILED | SUCCESSFUL

DeletionStatusMessage

Describe el estado de eliminación del trabajo de restauración.

Tipo: cadena

ExpectedCompletionTimeMinutes

La cantidad de tiempo en minutos que se espera que tarde un trabajo de restauración de un punto de recuperación.

Tipo: largo

[IamRoleArn](#)

Especifica el ARN del rol de IAM utilizado para crear el punto de recuperación de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

[IsParent](#)

Se trata de un valor booleano que indica si el trabajo de restauración es un trabajo de restauración principal (compuesto).

Tipo: Booleano

[ParentJobId](#)

Es el identificador único del trabajo de restauración principal del trabajo de restauración seleccionado.

Tipo: cadena

[PercentDone](#)

Contiene el porcentaje estimado que se ha completado de un trabajo en el momento en que se consultó el estado del trabajo.

Tipo: cadena

[RecoveryPointArn](#)

Un ARN que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

[RecoveryPointCreationDate](#)

La fecha de creación del punto de recuperación creado por el trabajo de restauración especificado.

Tipo: marca temporal

[ResourceType](#)

Devuelve los metadatos asociados a un trabajo de restauración enumerados por tipo de recurso.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

[RestoreJobId](#)

Identifica de forma exclusiva el trabajo que restaura un punto de recuperación.

Tipo: cadena

[SourceResourceArn](#)

Es el Nombre de recurso de Amazon (ARN) del recurso original del que se ha realizado la copia de seguridad. Proporciona un contexto sobre el recurso que se está restaurando.

Tipo: cadena

[Status](#)

Código de estado que especifica el estado del trabajo que se inicia AWS Backup para restaurar un punto de recuperación.

Tipo: cadena

Valores válidos: PENDING | RUNNING | COMPLETED | ABORTED | FAILED

[StatusMessage](#)

Un mensaje que muestra el estado de un trabajo para restaurar un punto de recuperación.

Tipo: cadena

[ValidationStatus](#)

El estado de la validación ejecutada en el trabajo de restauración indicado.

Tipo: cadena

Valores válidos: FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING

[ValidationStatusMessage](#)

Mensaje del estado.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

DependencyFailureException

Un AWS servicio o recurso dependiente devolvió un error al AWS Backup servicio y la acción no se pudo completar.

Context

Type

Código de estado HTTP: 500

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeScanJob

Servicio: AWS Backup

Devuelve los detalles del trabajo de escaneo para el ScanJob ID especificado.

Sintaxis de la solicitud

```
GET /scan/jobs/ScanJobId HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

ScanJobId

Identifica de forma exclusiva una solicitud AWS Backup para escanear un recurso.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "AccountId": "string",
  "BackupVaultArn": "string",
  "BackupVaultName": "string",
  "CompletionDate": number,
  "CreatedBy": {
    "BackupPlanArn": "string",
    "BackupPlanId": "string",
    "BackupPlanVersion": "string",
    "BackupRuleId": "string"
  },
  "CreationDate": number,
  "IamRoleArn": "string",
  "MalwareScanner": "string",
```

```

"RecoveryPointArn": "string",
"ResourceArn": "string",
"ResourceName": "string",
"ResourceType": "string",
"ScanBaseRecoveryPointArn": "string",
"ScanId": "string",
"ScanJobId": "string",
"ScanMode": "string",
"ScannerRoleArn": "string",
"ScanResult": {
  "ScanResultStatus": "string"
},
"State": "string",
"StatusMessage": "string"
}

```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

AccountId

Devuelve el ID de cuenta propietario del trabajo de escaneo.

Patrón: `^[0-9]{12}$`

Tipo: cadena

BackupVaultArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un almacén de copias de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`

Tipo: cadena

BackupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de Backup se identifican con nombres que son exclusivos de la cuenta utilizada para crearlos y de la AWS región en la que se crearon.

Patrón: `^[a-zA-Z0-9\-\_\.\.]{2,50}$`

Tipo: cadena

CompletionDate

Es la fecha y la hora en que ha finalizado la creación del índice de copias de seguridad, expresadas en formato Unix y en horario universal coordinado (UTC). El valor de `CompletionDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

CreatedBy

Contiene información de identificación sobre la creación de un trabajo de escaneo, incluidos el plan de respaldo y la regla que inició el escaneo.

Tipo: objeto [ScanJobCreator](#)

CreationDate

Es la fecha y la hora en que ha finalizado la creación del índice de copias de seguridad, expresadas en formato Unix y en horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

IamRoleArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un almacén de copia de seguridad; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

MalwareScanner

El motor de escaneo utilizado para el trabajo de escaneo correspondiente. En la actualidad, solo se admite GUARDUTY.

Tipo: cadena

Valores válidos: GUARDDUTY

[RecoveryPointArn](#)

Un ARN que identifica de forma exclusiva el punto de recuperación objetivo para el escaneo.; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

Tipo: cadena

[ResourceArn](#)

Un ARN que identifica de forma exclusiva el recurso de origen del ARN del punto de recuperación correspondiente.

Tipo: cadena

[ResourceName](#)

El nombre no exclusivo del recurso que pertenece a la copia de seguridad especificada.

Tipo: cadena

[ResourceType](#)

El tipo de AWS recurso del que se va a hacer una copia de seguridad; por ejemplo, un volumen de Amazon Elastic Block Store (Amazon EBS).

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Tipo: cadena

Valores válidos: EBS | EC2 | S3

[ScanBaseRecoveryPointArn](#)

Un ARN que identifica de forma exclusiva el punto de recuperación base para el escaneo. Este campo solo se rellenará cuando se haya realizado un trabajo de escaneo incremental.

Tipo: cadena

[ScanId](#)

El ID de escaneo generado por Amazon GuardDuty para la solicitud de Scan Job ID correspondiente desde AWS Backup.

Tipo: cadena

[ScanJobId](#)

El identificador del trabajo de escaneo que identificó de forma exclusiva la solicitud AWS Backup.

Tipo: cadena

[ScanMode](#)

Especifica el tipo de escaneo utilizado para el trabajo de escaneo.

Tipo: cadena

Valores válidos: FULL_SCAN | INCREMENTAL_SCAN

[ScannerRoleArn](#)

Especifica la función de IAM del escáner (ARN) que se utiliza para el trabajo de digitalización.

Tipo: cadena

[ScanResult](#)

Contiene el ScanResultsStatus correspondiente al trabajo de digitalización y devuelve THREATS_FOUND o NO_THREATS_FOUND corresponde a los trabajos finalizados.

Tipo: objeto [ScanResultInfo](#)

[State](#)

El estado actual de un trabajo de escaneo.

Tipo: cadena

Valores válidos: CANCELED | COMPLETED | COMPLETED_WITH_ISSUES | CREATED | FAILED | RUNNING

[StatusMessage](#)

Un mensaje detallado que explica el estado del trabajo de copia de seguridad de un recurso.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DisassociateBackupVaultMpaApprovalTeam

Servicio: AWS Backup

Elimina la asociación entre un equipo de aprobación MPA y un almacén de copias de seguridad, lo que desactiva el flujo de trabajo de aprobación MPA para las operaciones de restauración.

Sintaxis de la solicitud

```
POST /backup-vaults/backupVaultName/mpaApprovalTeam?delete HTTP/1.1
Content-type: application/json

{
  "RequesterComment": "string"
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[backupVaultName](#)

Es el nombre del almacén de copias de seguridad del que se va a desasociar el equipo de aprobación MPA.

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[RequesterComment](#)

Es un comentario opcional que explica el motivo por el que se desasocia al equipo de aprobación MPA del almacén de copias de seguridad.

Tipo: cadena

Requerido: no

Sintaxis de la respuesta

```
HTTP/1.1 204
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 204 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

DisassociateRecoveryPoint

Servicio: AWS Backup

Elimina el punto de recuperación de la copia de seguridad continua especificado en AWS Backup y transfiere el control de esa copia de seguridad continua al servicio de origen, como Amazon RDS. El servicio de origen seguirá creando y reteniendo copias de seguridad continuas según el ciclo de vida que haya especificado en su plan de copia de seguridad original.

No admite puntos de recuperación de copias de seguridad instantáneas.

Sintaxis de la solicitud

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/disassociate
HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupVaultName

El nombre exclusivo de un almacén de AWS Backup.

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: sí

recoveryPointArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un punto de recuperación de AWS Backup.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Context

Type

Código de estado HTTP: 400

InvalidResourceStateException

AWS Backup ya está realizando una acción en este punto de recuperación. No es posible realizar la acción que ha solicitado hasta que finalice la primera acción. Inténtelo de nuevo más tarde.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)

- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

DisassociateRecoveryPointFromParent

Servicio: AWS Backup

Esta acción dirigida a un punto de recuperación secundario (anidado) específico elimina la relación entre el punto de recuperación especificado y su punto de recuperación principal (compuesto).

Sintaxis de la solicitud

```
DELETE /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/parentAssociation HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[backupVaultName](#)

El nombre de un contenedor lógico en el que se almacena el punto de recuperación secundario (anidado). Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: sí

[recoveryPointArn](#)

El nombre de recurso de Amazon (ARN) que identifica de forma exclusiva el punto de recuperación secundario (anidado); por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 204
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 204 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ExportBackupPlanTemplate

Servicio: AWS Backup

Devuelve el plan de copia de seguridad especificado por el ID del plan como plantilla de copia de seguridad.

Sintaxis de la solicitud

```
GET /backup/plans/backupPlanId/toTemplate/ HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[backupPlanId](#)

Identifica de forma única un plan de copia de seguridad.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupPlanTemplateJson": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[BackupPlanTemplateJson](#)

El cuerpo de una plantilla de plan de copia de seguridad en formato JSON.

 Note

Se trata de un documento JSON firmado que no se puede modificar antes de pasarlo a `GetBackupPlanFromJSON`.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

`InvalidParameterValueException`

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

`MissingParameterValueException`

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

`ResourceNotFoundException`

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

GetBackupPlan

Servicio: AWS Backup

Devuelve los detalles del BackupPlan para el BackupPlanId especificado. Los detalles son el cuerpo de un plan de copia de seguridad en formato JSON, además de los metadatos del plan.

Sintaxis de la solicitud

```
GET /backup/plans/backupPlanId?  
MaxScheduledRunsPreview=MaxScheduledRunsPreview&versionId=VersionId HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupPlanId

Identifica de forma única un plan de copia de seguridad.

Obligatorio: sí

MaxScheduledRunsPreview

Número de ejecuciones de copias de seguridad programadas futuras para previsualizar. Si se establece en 0 (valor predeterminado), no se incluye ninguna vista previa de ejecuciones programadas en la respuesta. El rango válido es de 0 a 10.

Rango válido: valor mínimo de 0. Valor máximo de 10.

VersionId

Cadenas cifradas en UTF-8, Unicode, únicas, generadas aleatoriamente que tienen como máximo una longitud de 1024 bytes. La versión IDs no se puede editar.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200  
Content-type: application/json  
  
{
```

```

    "AdvancedBackupSettings": [
      {
        "BackupOptions": {
          "string" : "string"
        },
        "ResourceType": "string"
      }
    ],
    "BackupPlan": {
      "AdvancedBackupSettings": [
        {
          "BackupOptions": {
            "string" : "string"
          },
          "ResourceType": "string"
        }
      ],
      "BackupPlanName": "string",
      "Rules": [
        {
          "CompletionWindowMinutes": number,
          "CopyActions": [
            {
              "DestinationBackupVaultArn": "string",
              "Lifecycle": {
                "DeleteAfterDays": number,
                "DeleteAfterEvent": "string",
                "MoveToColdStorageAfterDays": number,
                "OptInToArchiveForSupportedResources": boolean
              }
            }
          ],
          "EnableContinuousBackup": boolean,
          "IndexActions": [
            {
              "ResourceTypes": [ "string" ]
            }
          ],
          "Lifecycle": {
            "DeleteAfterDays": number,
            "DeleteAfterEvent": "string",
            "MoveToColdStorageAfterDays": number,
            "OptInToArchiveForSupportedResources": boolean
          }
        }
      ]
    }
  ],
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "Version": "string"
}

```

```

    "RecoveryPointTags": {
      "string" : "string"
    },
    "RuleId": "string",
    "RuleName": "string",
    "ScanActions": [
      {
        "MalwareScanner": "string",
        "ScanMode": "string"
      }
    ],
    "ScheduleExpression": "string",
    "ScheduleExpressionTimezone": "string",
    "StartWindowMinutes": number,
    "TargetBackupVaultName": "string",
    "TargetLogicallyAirGappedBackupVaultArn": "string"
  }
],
"ScanSettings": [
  {
    "MalwareScanner": "string",
    "ResourceTypes": [ "string" ],
    "ScannerRoleArn": "string"
  }
]
},
"BackupPlanArn": "string",
"BackupPlanId": "string",
"CreationDate": number,
"CreatorRequestId": "string",
"DeletionDate": number,
"LastExecutionDate": number,
"ScheduledRunsPreview": [
  {
    "ExecutionTime": number,
    "RuleExecutionType": "string",
    "RuleId": "string"
  }
],
"VersionId": "string"
}

```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[AdvancedBackupSettings](#)

Contiene una lista de BackupOptions para cada tipo de recurso. La lista se rellena solo si se ha configurado la opción avanzada para el plan de copia de seguridad.

Tipo: matriz de objetos [AdvancedBackupSetting](#)

[BackupPlan](#)

Especifica el cuerpo de un plan de copia de seguridad. Incluye un BackupPlanName y uno o más conjuntos de Rules.

Tipo: objeto [BackupPlan](#)

[BackupPlanArn](#)

Un nombre de recurso de Amazon (ARN) que identifica de forma única un plan de copia de seguridad; por ejemplo, arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50.

Tipo: cadena

[BackupPlanId](#)

Identifica de forma única un plan de copia de seguridad.

Tipo: cadena

[CreationDate](#)

La fecha y la hora en que se creó el plan de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de CreationDate tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

[CreatorRequestId](#)

Una cadena única que identifica la solicitud y permite que se reintenten las solicitudes que han producido un error sin el riesgo de ejecutar la operación dos veces.

Tipo: cadena

[DeletionDate](#)

La fecha y la hora en que se eliminó el plan de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de `DeletionDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

[LastExecutionDate](#)

La última vez que se ejecutó este plan de copia de seguridad. Una fecha y hora, en formato Unix y horario universal coordinado (UTC). El valor de `LastExecutionDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

[ScheduledRunsPreview](#)

Lista de las próximas ejecuciones de copias de seguridad programadas. Solo se incluye cuando el parámetro `MaxScheduledRunsPreview` sea mayor que 0. Contiene hasta 10 futuras ejecuciones de copias de seguridad con sus horarios programados, tipos de ejecución y regla asociada IDs.

Tipo: matriz de objetos [ScheduledPlanExecutionMember](#)

[VersionId](#)

Cadenas cifradas en UTF-8, Unicode, únicas, generadas aleatoriamente que tienen como máximo una longitud de 1024 bytes. La versión IDs no se puede editar.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

GetBackupPlanFromJSON

Servicio: AWS Backup

Devuelve un documento JSON válido que especifica un plan de copia de seguridad o un error.

Sintaxis de la solicitud

```
POST /backup/template/json/toPlan HTTP/1.1
Content-type: application/json
```

```
{
  "BackupPlanTemplateJson": "string"
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[BackupPlanTemplateJson](#)

Un documento del plan de copia de seguridad proporcionado por el cliente en formato JSON.

Tipo: cadena

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupPlan": {
    "AdvancedBackupSettings": [
      {
        "BackupOptions": {
          "string" : "string"
        },
        "ResourceType": "string"
      }
    ]
  }
}
```

```

    }
  ],
  "BackupPlanName": "string",
  "Rules": [
    {
      "CompletionWindowMinutes": number,
      "CopyActions": [
        {
          "DestinationBackupVaultArn": "string",
          "Lifecycle": {
            "DeleteAfterDays": number,
            "DeleteAfterEvent": "string",
            "MoveToColdStorageAfterDays": number,
            "OptInToArchiveForSupportedResources": boolean
          }
        }
      ],
      "EnableContinuousBackup": boolean,
      "IndexActions": [
        {
          "ResourceTypes": [ "string" ]
        }
      ],
      "Lifecycle": {
        "DeleteAfterDays": number,
        "DeleteAfterEvent": "string",
        "MoveToColdStorageAfterDays": number,
        "OptInToArchiveForSupportedResources": boolean
      },
      "RecoveryPointTags": {
        "string" : "string"
      },
      "RuleId": "string",
      "RuleName": "string",
      "ScanActions": [
        {
          "MalwareScanner": "string",
          "ScanMode": "string"
        }
      ],
      "ScheduleExpression": "string",
      "ScheduleExpressionTimezone": "string",
      "StartWindowMinutes": number,
      "TargetBackupVaultName": "string",

```

```
        "TargetLogicallyAirGappedBackupVaultArn": "string"
    },
    ],
    "ScanSettings": [
        {
            "MalwareScanner": "string",
            "ResourceTypes": [ "string " ],
            "ScannerRoleArn": "string"
        }
    ]
}
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[BackupPlan](#)

Especifica el cuerpo de un plan de copia de seguridad. Incluye un BackupPlanName y uno o más conjuntos de Rules.

Tipo: objeto [BackupPlan](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Context

Type

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

GetBackupPlanFromTemplate

Servicio: AWS Backup

Devuelve la plantilla especificada por su `templateId` como plan de copia de seguridad.

Sintaxis de la solicitud

```
GET /backup/template/plans/templateId/toPlan HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[templateId](#)

Identifica de forma exclusiva una plantilla de plan de copia de seguridad almacenada.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupPlanDocument": {
    "AdvancedBackupSettings": [
      {
        "BackupOptions": {
          "string" : "string"
        },
        "ResourceType": "string"
      }
    ],
    "BackupPlanName": "string",
    "Rules": [
      {
        "CompletionWindowMinutes": number,
        "CopyActions": [
```

```

    {
      "DestinationBackupVaultArn": "string",
      "Lifecycle": {
        "DeleteAfterDays": number,
        "DeleteAfterEvent": "string",
        "MoveToColdStorageAfterDays": number,
        "OptInToArchiveForSupportedResources": boolean
      }
    },
    "EnableContinuousBackup": boolean,
    "IndexActions": [
      {
        "ResourceTypes": [ "string" ]
      }
    ],
    "Lifecycle": {
      "DeleteAfterDays": number,
      "DeleteAfterEvent": "string",
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
    },
    "RecoveryPointTags": {
      "string" : "string"
    },
    "RuleId": "string",
    "RuleName": "string",
    "ScanActions": [
      {
        "MalwareScanner": "string",
        "ScanMode": "string"
      }
    ],
    "ScheduleExpression": "string",
    "ScheduleExpressionTimezone": "string",
    "StartWindowMinutes": number,
    "TargetBackupVaultName": "string",
    "TargetLogicallyAirGappedBackupVaultArn": "string"
  }
],
"ScanSettings": [
  {
    "MalwareScanner": "string",
    "ResourceTypes": [ "string" ],

```

```
    "ScannerRoleArn": "string"  
  }  
]  
}  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[BackupPlanDocument](#)

Devuelve el cuerpo de un plan de copia de seguridad en función de la plantilla de destino, incluidos el nombre, las reglas y el almacén de copias de seguridad del plan.

Tipo: objeto [BackupPlan](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

GetBackupSelection

Servicio: AWS Backup

Devuelve los metadatos de selección y un documento en formato JSON que especifica una lista de recursos asociados a un plan de copia de seguridad.

Sintaxis de la solicitud

```
GET /backup/plans/backupPlanId/selections/selectionId HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[backupPlanId](#)

Identifica de forma única un plan de copia de seguridad.

Obligatorio: sí

[selectionId](#)

Identifica de forma única el cuerpo de una solicitud para asignar un conjunto de recursos a un plan de copia de seguridad.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupPlanId": "string",
  "BackupSelection": {
    "Conditions": {
      "StringEquals": [
        {
          "ConditionKey": "string",
```

```

        "ConditionValue": "string"
    },
    ],
    "StringLike": [
        {
            "ConditionKey": "string",
            "ConditionValue": "string"
        }
    ],
    "StringNotEquals": [
        {
            "ConditionKey": "string",
            "ConditionValue": "string"
        }
    ],
    "StringNotLike": [
        {
            "ConditionKey": "string",
            "ConditionValue": "string"
        }
    ]
},
"IamRoleArn": "string",
"ListOfTags": [
    {
        "ConditionKey": "string",
        "ConditionType": "string",
        "ConditionValue": "string"
    }
],
"NotResources": [ "string" ],
"Resources": [ "string" ],
"SelectionName": "string"
},
"CreationDate": number,
"CreatorRequestId": "string",
"SelectionId": "string"
}

```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[BackupPlanId](#)

Identifica de forma única un plan de copia de seguridad.

Tipo: cadena

[BackupSelection](#)

Especifica el cuerpo de una solicitud para asignar un conjunto de recursos a un plan de copia de seguridad.

Tipo: objeto [BackupSelection](#)

[CreationDate](#)

La fecha y la hora en que se creó la selección de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

[CreatorRequestId](#)

Una cadena única que identifica la solicitud y permite que se reintenten las solicitudes que han producido un error sin el riesgo de ejecutar la operación dos veces.

Tipo: cadena

[SelectionId](#)

Identifica de forma única el cuerpo de una solicitud para asignar un conjunto de recursos a un plan de copia de seguridad.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)

- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

GetBackupVaultAccessPolicy

Servicio: AWS Backup

Devuelve el documento de política de acceso asociado al almacén de copias de seguridad indicado.

Sintaxis de la solicitud

```
GET /backup-vaults/backupVaultName/access-policy HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupVaultArn": "string",
  "BackupVaultName": "string",
  "Policy": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[BackupVaultArn](#)

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un almacén de copia de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

[BackupVaultName](#)

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región donde se crearon.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

[Policy](#)

El documento de política de acceso al almacén de copias de seguridad en formato JSON.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)

- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

GetBackupVaultNotifications

Servicio: AWS Backup

Devuelve notificaciones de eventos para el almacén de copias de seguridad especificado.

Sintaxis de la solicitud

```
GET /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupVaultArn": "string",
  "BackupVaultEvents": [ "string" ],
  "BackupVaultName": "string",
  "SNSTopicArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[BackupVaultArn](#)

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un almacén de copia de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

[BackupVaultEvents](#)

Una matriz de eventos que indica el estado de los trabajos para realizar copias de seguridad de recursos en el almacén de copia de seguridad.

Tipo: matriz de cadenas

Valores válidos: `BACKUP_JOB_STARTED` | `BACKUP_JOB_COMPLETED` | `BACKUP_JOB_SUCCESSFUL` | `BACKUP_JOB_FAILED` | `BACKUP_JOB_EXPIRED` | `RESTORE_JOB_STARTED` | `RESTORE_JOB_COMPLETED` | `RESTORE_JOB_SUCCESSFUL` | `RESTORE_JOB_FAILED` | `COPY_JOB_STARTED` | `COPY_JOB_SUCCESSFUL` | `COPY_JOB_FAILED` | `RECOVERY_POINT_MODIFIED` | `BACKUP_PLAN_CREATED` | `BACKUP_PLAN_MODIFIED` | `S3_BACKUP_OBJECT_FAILED` | `S3_RESTORE_OBJECT_FAILED` | `CONTINUOUS_BACKUP_INTERRUPTED` | `RECOVERY_POINT_INDEX_COMPLETED` | `RECOVERY_POINT_INDEX_DELETED` | `RECOVERY_POINT_INDEXING_FAILED`

[BackupVaultName](#)

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región donde se crearon.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

[SNSTopicArn](#)

Un ARN que identifica de forma exclusiva un tema de Amazon Simple Notification Service (Amazon SNS); por ejemplo, `arn:aws:sns:us-west-2:111122223333:MyTopic`.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

GetLegalHold

Servicio: AWS Backup

Esta acción devuelve los detalles de una retención legal concreta. Los detalles son el cuerpo de una retención legal en formato JSON, además de los metadatos.

Sintaxis de la solicitud

```
GET /legal-holds/legalHoldId/ HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

legalHoldId

El identificador de la retención legal.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "CancelDescription": "string",
  "CancellationDate": number,
  "CreationDate": number,
  "Description": "string",
  "LegalHoldArn": "string",
  "LegalHoldId": "string",
  "RecoveryPointSelection": {
    "DateRange": {
      "FromDate": number,
      "ToDate": number
    },
    "ResourceIdentifiers": [ "string" ],
  },
}
```

```
    "VaultNames": [ "string" ]  
  },  
  "RetainRecordUntil": number,  
  "Status": "string",  
  "Title": "string"  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[CancelDescription](#)

El motivo de la eliminación de la retención legal.

Tipo: cadena

[CancellationDate](#)

Hora a la que se canceló la retención legal.

Tipo: marca temporal

[CreationDate](#)

La hora en la que se creó la retención legal.

Tipo: marca temporal

[Description](#)

La descripción de la cadena de la retención legal.

Tipo: cadena

[LegalHoldArn](#)

El ARN del marco para la retención legal especificada. El formato del ARN depende del tipo de recurso.

Tipo: cadena

[LegalHoldId](#)

El identificador de la retención legal.

Tipo: cadena

[RecoveryPointSelection](#)

Los criterios para asignar un conjunto de recursos, como los tipos de recursos o los almacenes de copias de seguridad.

Tipo: objeto [RecoveryPointSelection](#)

[RetainRecordUntil](#)

La fecha y la hora hasta las que se conservará el registro de la retención legal.

Tipo: marca temporal

[Status](#)

El estado de la retención legal.

Tipo: cadena

Valores válidos: CREATING | ACTIVE | CANCELING | CANCELED

[Title](#)

El título de la retención legal.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)

- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

GetRecoveryPointIndexDetails

Servicio: AWS Backup

Esta operación devuelve los metadatos y los detalles específicos del índice de copias de seguridad asociados al punto de recuperación especificado.

Sintaxis de la solicitud

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/index HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región donde se crearon.

Los caracteres permitidos son: letras minúsculas, números y guiones.

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: sí

recoveryPointArn

Un ARN que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Content-type: application/json

```
{
  "BackupVaultArn": "string",
  "IndexCompletionDate": number,
  "IndexCreationDate": number,
  "IndexDeletionDate": number,
  "IndexStatus": "string",
  "IndexStatusMessage": "string",
  "RecoveryPointArn": "string",
  "SourceResourceArn": "string",
  "TotalItemsIndexed": number
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[BackupVaultArn](#)

Es un ARN que identifica de forma unívoca el almacén de copias de seguridad en el que se almacena el índice de puntos de recuperación.

Por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

[IndexCompletionDate](#)

Es la fecha y la hora en que ha finalizado la creación del índice de copias de seguridad, expresadas en formato Unix y en horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor `1516925490.087` representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

[IndexCreationDate](#)

Es la fecha y la hora de creación de un índice de copias de seguridad, expresadas en formato Unix y en horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de

milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

[IndexDeletionDate](#)

Es la fecha y la hora de eliminación de un índice de copias de seguridad, expresadas en formato Unix y en horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

[IndexStatus](#)

Este es el estado actual del índice de copias de seguridad asociado al punto de recuperación especificado.

Los estados son: PENDING | ACTIVE | FAILED | DELETING

En una búsqueda se puede incluir un punto de recuperación con un índice con el estado ACTIVE.

Tipo: cadena

Valores válidos: PENDING | ACTIVE | FAILED | DELETING

[IndexStatusMessage](#)

Es un mensaje detallado que explica el estado del índice de copias de seguridad asociado al punto de recuperación.

Tipo: cadena

[RecoveryPointArn](#)

Un ARN que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

[SourceResourceArn](#)

Es una cadena de un Nombre de recurso de Amazon (ARN) que identifica de forma unívoca un recurso de origen.

Tipo: cadena

TotalItemsIndexed

Cantidad de elementos del índice de copias de seguridad asociado al punto de recuperación.

Tipo: Long

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

GetRecoveryPointRestoreMetadata

Servicio: AWS Backup

Devuelve un conjunto de pares clave-valor de metadatos que se utilizaron para crear la copia de seguridad.

Sintaxis de la solicitud

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/restore-metadata?
backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[BackupVaultAccountId](#)

El identificador de cuenta del almacén de copias de seguridad especificado.

Patrón: `^[0-9]{12}$`

[backupVaultName](#)

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: sí

[recoveryPointArn](#)

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupVaultArn": "string",
  "RecoveryPointArn": "string",
  "ResourceType": "string",
  "RestoreMetadata": {
    "string" : "string"
  }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[BackupVaultArn](#)

Un ARN que identifica de forma exclusiva un almacén de copias de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

[RecoveryPointArn](#)

Un ARN que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

[ResourceType](#)

El tipo de recurso del punto de recuperación.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\.\-]{1,50}$`

RestoreMetadata

El conjunto de pares clave-valor de metadatos que describen la configuración original del recurso del que se ha hecho una copia de seguridad. Estos valores varían en función del servicio que se esté restaurando.

Tipo: mapa de cadena a cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

GetRestoreJobMetadata

Servicio: AWS Backup

Esta solicitud devuelve los metadatos del trabajo de restauración especificado.

Sintaxis de la solicitud

```
GET /restore-jobs/restoreJobId/metadata HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[restoreJobId](#)

Es un identificador único de un trabajo de restauración de AWS Backup.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "Metadata": {
    "string" : "string"
  },
  "RestoreJobId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[Metadata](#)

Contiene los metadatos del trabajo de copia de seguridad especificado.

Tipo: mapa de cadena a cadena

[RestoreJobId](#)

Es un identificador único de un trabajo de restauración de AWS Backup.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

GetRestoreTestingInferredMetadata

Servicio: AWS Backup

Esta solicitud devuelve el conjunto mínimo de metadatos necesario para iniciar un trabajo de restauración con una configuración predeterminada segura. BackupVaultName y RecoveryPointArn son parámetros obligatorios. BackupVaultAccountId es un parámetro opcional.

Sintaxis de la solicitud

```
GET /restore-testing/inferred-metadata?  
BackupVaultAccountId=BackupVaultAccountId&BackupVaultName=BackupVaultName&RecoveryPointArn=RecoveryPointArn  
HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

BackupVaultAccountId

El identificador de cuenta del almacén de copias de seguridad especificado.

BackupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon. Constan de letras minúsculas, números y guiones.

Obligatorio: sí

RecoveryPointArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "InferredMetadata": {
    "string" : "string"
  }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[InferredMetadata](#)

Es un mapa de cadenas de los metadatos inferidos de la solicitud.

Tipo: mapa de cadena a cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)

- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

GetRestoreTestingPlan

Servicio: AWS Backup

Devuelve los detalles del `RestoreTestingPlan` para el `RestoreTestingPlanName` especificado. Los detalles son el cuerpo de un plan de prueba de restauración en formato JSON, además de los metadatos del plan.

Sintaxis de la solicitud

```
GET /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

RestoreTestingPlanName

Nombre único obligatorio del plan de prueba de restauración.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "RestoreTestingPlan": {
    "CreationTime": number,
    "CreatorRequestId": "string",
    "LastExecutionTime": number,
    "LastUpdateTime": number,
    "RecoveryPointSelection": {
      "Algorithm": "string",
      "ExcludeVaults": [ "string" ],
      "IncludeVaults": [ "string" ],
      "RecoveryPointTypes": [ "string" ],
      "SelectionWindowDays": number
    }
  }
}
```

```
    },  
    "RestoreTestingPlanArn": "string",  
    "RestoreTestingPlanName": "string",  
    "ScheduleExpression": "string",  
    "ScheduleExpressionTimezone": "string",  
    "StartWindowHours": number  
  }  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[RestoreTestingPlan](#)

Especifica el cuerpo de un plan de prueba de restauración. Incluye `RestoreTestingPlanName`.

Tipo: objeto [RestoreTestingPlanForGet](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

GetRestoreTestingSelection

Servicio: AWS Backup

Devuelve `RestoreTestingSelection`, que muestra los recursos y los elementos del plan de prueba de restauración.

Sintaxis de la solicitud

```
GET /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[RestoreTestingPlanName](#)

Nombre único obligatorio del plan de prueba de restauración.

Obligatorio: sí

[RestoreTestingSelectionName](#)

Nombre único obligatorio de la selección de pruebas de restauración.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "RestoreTestingSelection": {
    "CreationTime": number,
    "CreatorRequestId": "string",
    "IamRoleArn": "string",
    "ProtectedResourceArns": [ "string" ],
    "ProtectedResourceConditions": {
```

```

    "StringEquals": [
      {
        "Key": "string",
        "Value": "string"
      }
    ],
    "StringNotEquals": [
      {
        "Key": "string",
        "Value": "string"
      }
    ]
  },
  "ProtectedResourceType": "string",
  "RestoreMetadataOverrides": {
    "string" : "string"
  },
  "RestoreTestingPlanName": "string",
  "RestoreTestingSelectionName": "string",
  "ValidationWindowHours": number
}
}

```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

RestoreTestingSelection

Nombre único de la selección de pruebas de restauración.

Tipo: objeto [RestoreTestingSelectionForGet](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

GetSupportedResourceTypes

Servicio: AWS Backup

Devuelve los tipos de recursos de AWS admitidos por AWS Backup.

Sintaxis de la solicitud

```
GET /supported-resource-types HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "ResourceTypes": [ "string" ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[ResourceTypes](#)

Contiene una cadena con los tipos de recursos de AWS admitidos:

- Aurora para Amazon Aurora
- CloudFormation para AWS CloudFormation
- DocumentDB para Amazon DocumentDB (compatible con MongoDB)
- DynamoDB para Amazon DynamoDB
- EBS para Amazon Elastic Block Store (EBS)

- EC2 para Amazon Elastic Compute Cloud
- EFS para Amazon Elastic File System
- FSx para Amazon FSx
- Neptune para Amazon Neptune
- RDS para Amazon Relational Database Service
- Redshift para Amazon Redshift
- S3 para Amazon Simple Storage Service (Amazon S3)
- SAP HANA on Amazon EC2 para bases de datos de SAP HANA en instancias de Amazon Elastic Compute Cloud
- Storage Gateway para AWS Storage Gateway
- Timestream para Amazon Timestream
- VirtualMachine para máquinas virtuales de VMware

Tipo: matriz de cadenas

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

GetTieringConfiguration

Servicio: AWS Backup

Devuelve los detalles del `TieringConfiguration` para el `TieringConfigurationName` especificado. Los detalles son el cuerpo de una configuración por niveles en formato JSON, además de los metadatos de configuración.

Sintaxis de la solicitud

```
GET /tiering-configurations/tieringConfigurationName HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

tieringConfigurationName

El nombre exclusivo de una configuración de organización por niveles.

Patrón: `^[a-zA-Z0-9_]{1,200}$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "TieringConfiguration": {
    "BackupVaultName": "string",
    "CreationTime": number,
    "CreatorRequestId": "string",
    "LastUpdatedTime": number,
    "ResourceSelection": [
      {
        "Resources": [ "string" ],
        "ResourceType": "string",
```



```
        "TieringDownSettingsInDays": number
      }
    ],
    "TieringConfigurationArn": "string",
    "TieringConfigurationName": "string"
  }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[TieringConfiguration](#)

Especifica el cuerpo de una configuración de estratificación. Incluye `TieringConfigurationName`.

Tipo: objeto [TieringConfiguration](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)

- [AWS SDK para Ruby V3](#)

ListBackupJobs

Servicio: AWS Backup

Devuelve una lista de los trabajos de copia de seguridad existentes para una cuenta autenticada durante los últimos 30 días. Para un periodo de tiempo más prolongado, considere la posibilidad de utilizar estas [herramientas de monitorización](#).

Sintaxis de la solicitud

```
GET /backup-jobs/?  
accountId=ByAccountId&backupVaultName=ByBackupVaultName&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore  
HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[ByAccountId](#)

El ID de la cuenta desde la que se van a enumerar los trabajos. Devuelve solo los trabajos de copia de seguridad asociados al ID de cuenta especificado.

Si se usa desde una cuenta AWS Organizations de administración, la * transferencia devuelve todos los trabajos de la organización.

Patrón: `^[0-9]{12}$`

[ByBackupVaultName](#)

Devuelve solo los trabajos de copia de seguridad que se almacenarán en el almacén de copias de seguridad especificado. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

[ByCompleteAfter](#)

Devuelve solo los trabajos de copia de seguridad completados después de una fecha expresada en formato Unix y horario universal coordinado (UTC).

[ByCompleteBefore](#)

Devuelve solo los trabajos de copia de seguridad completados antes de una fecha expresada en formato Unix y horario universal coordinado (UTC).

[ByCreatedAfter](#)

Devuelve solo los trabajos de copia de seguridad que se crearon después de la fecha especificada.

[ByCreatedBefore](#)

Devuelve solo los trabajos de copia de seguridad que se crearon antes de la fecha especificada.

[ByMessageCategory](#)

Se trata de un parámetro opcional que se puede utilizar para filtrar los trabajos con un valor `MessageCategory` que coincida con el valor introducido.

Las cadenas de ejemplo pueden ser `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` y `InvalidParameters`.

Vista [Monitorización](#)

El comodín () devuelve el recuento de todas las categorías de mensajes.

`AGGREGATE_ALL` suma los recuentos de trabajos de todas las categorías de mensajes y devuelve la suma.

[ByParentJobId](#)

Se trata de un filtro para enumerar los trabajos secundarios (anidados) en función del ID del trabajo principal.

[ByResourceArn](#)

Devuelve solo los trabajos de copia de seguridad que coinciden con el nombre de recurso de Amazon (ARN) del recurso especificado.

[ByResourceType](#)

Devuelve únicamente los trabajos de copia de seguridad de los recursos especificados:

- `Aurora` para Amazon Aurora
- `CloudFormation` para AWS CloudFormation
- `DocumentDB` para Amazon DocumentDB (compatible con MongoDB)
- `DynamoDB` para Amazon DynamoDB
- `EBS` para Amazon Elastic Block Store (EBS)

- EC2 para Amazon Elastic Compute Cloud
- EFS para Amazon Elastic File System
- FSx para Amazon FSx
- Neptune para Amazon Neptune
- RDS para Amazon Relational Database Service
- Redshift para Amazon Redshift
- S3 para Amazon Simple Storage Service (Amazon S3)
- SAP HANA on Amazon EC2 para bases de datos de SAP HANA en instancias de Amazon Elastic Compute Cloud
- Storage Gateway para AWS Storage Gateway
- Timestream para Amazon Timestream
- VirtualMachine para máquinas VMware virtuales

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

[ByState](#)

Devuelve solo los trabajos de copia de seguridad que se encuentran en el estado especificado.

`Completed with issues` es un estado que solo se encuentra en la consola de AWS Backup. En el caso de la API, este estado se refiere a los trabajos con un estado de `MessageCategory` y una `SUCCESS` con un valor distinto de `COMPLETED`; es decir, el estado se ha completado pero genera un mensaje de estado.

Para obtener el recuento de trabajos de `Completed with issues`, ejecute dos solicitudes `GET` y reste el segundo número, más pequeño:

```
GET /backup-jobs/?state=COMPLETED
```

```
GET /backup-jobs/?messageCategory=SUCCESS&state=COMPLETED
```

Valores válidos: `CREATED` | `PENDING` | `RUNNING` | `ABORTING` | `ABORTED` | `COMPLETED` | `FAILED` | `EXPIRED` | `PARTIAL`

[MaxResults](#)

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupJobs": [
    {
      "AccountId": "string",
      "BackupJobId": "string",
      "BackupOptions": {
        "string" : "string"
      },
      "BackupSizeInBytes": number,
      "BackupType": "string",
      "BackupVaultArn": "string",
      "BackupVaultName": "string",
      "BytesTransferred": number,
      "CompletionDate": number,
      "CreatedBy": {
        "BackupPlanArn": "string",
        "BackupPlanId": "string",
        "BackupPlanName": "string",
        "BackupPlanVersion": "string",
        "BackupRuleCron": "string",
        "BackupRuleId": "string",
        "BackupRuleName": "string",
        "BackupRuleTimezone": "string"
      },
      "CreationDate": number,
      "EncryptionKeyArn": "string",
      "ExpectedCompletionDate": number,
      "IamRoleArn": "string",
```

```

    "InitiationDate": number,
    "IsEncrypted": boolean,
    "IsParent": boolean,
    "MessageCategory": "string",
    "ParentJobId": "string",
    "PercentDone": "string",
    "RecoveryPointArn": "string",
    "RecoveryPointLifecycle": {
        "DeleteAfterDays": number,
        "DeleteAfterEvent": "string",
        "MoveToColdStorageAfterDays": number,
        "OptInToArchiveForSupportedResources": boolean
    },
    "ResourceArn": "string",
    "ResourceName": "string",
    "ResourceType": "string",
    "StartBy": number,
    "State": "string",
    "StatusMessage": "string",
    "VaultLockState": "string",
    "VaultType": "string"
  },
  ],
  "NextToken": "string"
}

```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[BackupJobs](#)

Una matriz de estructuras que contiene metadatos sobre trabajos de copia de seguridad devueltos en formato JSON.

Tipo: matriz de objetos [BackupJob](#)

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)

- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListBackupJobSummaries

Servicio: AWS Backup

Es una solicitud de resumen de trabajos de copia de seguridad creados o en ejecución en los 30 últimos días. Puede incluir los parámetros AccountID, State, ResourceType, MessageCategory, AggregationPeriod, MaxResults o NextToken para filtrar los resultados.

La solicitud devuelve un resumen que contiene Region, Account, State, ResourceType, MessageCategory, StartTime, EndTime y Count de los trabajos incluidos.

Sintaxis de la solicitud

```
GET /audit/backup-job-summaries?  
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&MessageCategory=M  
HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

AccountId

Devuelve el recuento de trabajos de la cuenta especificada.

Si la solicitud se envía desde una cuenta de miembro o una cuenta que no forma parte de AWS Organizations, se devolverán los trabajos de la cuenta del solicitante.

Las cuentas raíz, de administrador y de administrador delegado pueden utilizar el valor ANY para devolver recuentos de trabajos de todas las cuentas de la organización.

AGGREGATE_ALL suma los recuentos de trabajos de todas las cuentas de la organización autenticada y, a continuación, devuelve la suma.

Patrón: `^[0-9]{12}$`

AggregationPeriod

El período de los resultados devueltos.

- ONE_DAY: el recuento de trabajos diarios de los 14 días anteriores.
- SEVEN_DAYS: el recuento total de trabajos de los 7 días anteriores.
- FOURTEEN_DAYS: el recuento total de trabajos de los 14 días anteriores.

Valores válidos: ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS

MaxResults

Número máximo de elementos que se van a devolver.

El valor es un entero. El rango de valores aceptados está entre 1 y 500.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

MessageCategory

Este parámetro devuelve el recuento de trabajos de la categoría de mensajes especificada.

Ejemplos de cadenas aceptadas son AccessDenied, Success y InvalidParameters.

Consulte en [Monitorización](#) una lista de cadenas de MessageCategory aceptadas.

El valor ANY devuelve el recuento de todas las categorías de mensajes.

AGGREGATE_ALL suma los recuentos de trabajos de todas las categorías de mensajes y devuelve la suma.

NextToken

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos MaxResults, NextToken permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

ResourceType

Devuelve el recuento de trabajos del tipo de recurso especificado. Utilice GetSupportedResourceTypes de solicitud para obtener cadenas para los tipos de recursos compatibles.

El valor ANY devuelve el recuento de todos los tipos de recursos.

AGGREGATE_ALL suma los recuentos de trabajos de todos los tipos de recursos y devuelve la suma.

El tipo de recurso de AWS del que se va a hacer la copia de seguridad; por ejemplo, un volumen de Amazon Elastic Block Store (Amazon EBS) o una base de datos de Amazon Relational Database Service (Amazon RDS).

Patrón: `^[a-zA-Z0-9\-\_\.\]{1,50}$`

State

Este parámetro devuelve el recuento de los trabajos con el estado especificado.

El valor ANY devuelve el recuento de todos los estados.

AGGREGATE_ALL suma los recuentos de trabajos de todos los tipos de estados y devuelve la suma.

Completed with issues es un estado que solo se encuentra en la consola de AWS Backup. En el caso de la API, este estado se refiere a los trabajos con un estado de MessageCategory y una SUCCESS con un valor distinto de COMPLETED; es decir, el estado se ha completado pero genera un mensaje de estado. Para obtener el recuento de trabajos de Completed with issues, ejecute dos solicitudes GET y reste el segundo número, más pequeño:

GET /audit/backup-job-summaries?AggregationPeriod=FOURTEEN_DAYS&State=COMPLETED

GET /audit/backup-job-summaries?

AggregationPeriod=FOURTEEN_DAYS&MessageCategory=SUCCESS&State=COMPLETED

Valores válidos: CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED
| FAILED | EXPIRED | PARTIAL | AGGREGATE_ALL | ANY

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "AggregationPeriod": "string",
  "BackupJobSummaries": [
    {
      "AccountId": "string",
      "Count": number,
      "EndTime": number,
      "MessageCategory": "string",
      "Region": "string",
```

```
    "ResourceType": "string",
    "StartTime": number,
    "State": "string"
  },
  "NextToken": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[AggregationPeriod](#)

El período de los resultados devueltos.

- ONE_DAY: el recuento de trabajos diarios de los 14 días anteriores.
- SEVEN_DAYS: el recuento total de trabajos de los 7 días anteriores.
- FOURTEEN_DAYS: el recuento total de trabajos de los 14 días anteriores.

Tipo: cadena

[BackupJobSummaries](#)

La información del resumen.

Tipo: matriz de objetos [BackupJobSummary](#)

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ListBackupPlans

Servicio: AWS Backup

Muestra los planes de copia de seguridad activos de la cuenta.

Sintaxis de la solicitud

```
GET /backup/plans/?  
includeDeleted=IncludeDeleted&maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[IncludeDeleted](#)

Un valor booleano con un valor predeterminado de FALSE que devuelve los planes de copia de seguridad eliminados si se establece en TRUE.

[MaxResults](#)

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200  
Content-type: application/json  
  
{  
  "BackupPlansList": [  
    {  
      "AdvancedBackupSettings": [  

```



```
{
  "BackupOptions": {
    "string": "string"
  },
  "ResourceType": "string"
},
"BackupPlanArn": "string",
"BackupPlanId": "string",
"BackupPlanName": "string",
"CreationDate": number,
"CreatorRequestId": "string",
"DeletionDate": number,
"LastExecutionDate": number,
"VersionId": "string"
},
"NextToken": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

BackupPlansList

Información sobre los planes de copia de seguridad.

Tipo: matriz de objetos [BackupPlansListMember](#)

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ListBackupPlanTemplates

Servicio: AWS Backup

Muestra las plantillas del plan de copia de seguridad.

Sintaxis de la solicitud

```
GET /backup/template/plans?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[MaxResults](#)

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupPlanTemplatesList": [
    {
      "BackupPlanTemplateId": "string",
      "BackupPlanTemplateName": "string"
    }
  ],
  "NextToken": "string"
}
```

```
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[BackupPlanTemplatesList](#)

Una matriz de elementos de la lista de plantillas que contiene metadatos sobre las plantillas guardadas.

Tipo: matriz de objetos [BackupPlanTemplatesListMember](#)

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

`InvalidParameterValueException`

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

`MissingParameterValueException`

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)

- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ListBackupPlanVersions

Servicio: AWS Backup

Devuelve los metadatos de las versiones de sus planes de copia de seguridad, incluidos los nombres de recursos de Amazon (ARN), los ID de los planes de copia de seguridad, las fechas de creación y eliminación, los nombres de los planes y los ID de versión.

Sintaxis de la solicitud

```
GET /backup/plans/backupPlanId/versions/?maxResults=MaxResults&nextToken=NextToken  
HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupPlanId

Identifica de forma única un plan de copia de seguridad.

Obligatorio: sí

MaxResults

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200  
Content-type: application/json
```



```

{
  "BackupPlanVersionsList": [
    {
      "AdvancedBackupSettings": [
        {
          "BackupOptions": {
            "string": "string"
          },
          "ResourceType": "string"
        }
      ],
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
      "BackupPlanName": "string",
      "CreationDate": number,
      "CreatorRequestId": "string",
      "DeletionDate": number,
      "LastExecutionDate": number,
      "VersionId": "string"
    }
  ],
  "NextToken": "string"
}

```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[BackupPlanVersionsList](#)

Una matriz de elementos de la lista de versiones que contiene metadatos sobre sus planes de copia de seguridad.

Tipo: matriz de objetos [BackupPlansListMember](#)

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ListBackupSelections

Servicio: AWS Backup

Devuelve una matriz que contiene los metadatos de los recursos asociados al plan de copia de seguridad de destino.

Sintaxis de la solicitud

```
GET /backup/plans/backupPlanId/selections/?maxResults=MaxResults&nextToken=NextToken  
HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[backupPlanId](#)

Identifica de forma única un plan de copia de seguridad.

Obligatorio: sí

[MaxResults](#)

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200  
Content-type: application/json  
  
{
```

```
"BackupSelectionsList": [  
  {  
    "BackupPlanId": "string",  
    "CreationDate": number,  
    "CreatorRequestId": "string",  
    "IamRoleArn": "string",  
    "SelectionId": "string",  
    "SelectionName": "string"  
  },  
  "NextToken": "string"  
]
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[BackupSelectionsList](#)

Una matriz de elementos de la lista de selección de copias de seguridad que contiene metadatos sobre cada recurso de la lista.

Tipo: matriz de objetos [BackupSelectionsListMember](#)

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

`InvalidParameterValueException`

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)

- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ListBackupVaults

Servicio: AWS Backup

Devuelve una lista de contenedores de almacenamiento de puntos de recuperación junto con información sobre ellos.

Sintaxis de la solicitud

```
GET /backup-vaults/?  
maxResults=MaxResults&nextToken=NextToken&shared=ByShared&vaultType=ByVaultType  
HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[ByShared](#)

Este parámetro ordenará la lista de almacenes por almacenes compartidos.

[ByVaultType](#)

Este parámetro ordenará la lista de almacenes por tipo de almacén.

Valores válidos: BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT |
RESTORE_ACCESS_BACKUP_VAULT

[MaxResults](#)

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupVaultList": [
    {
      "BackupVaultArn": "string",
      "BackupVaultName": "string",
      "CreationDate": number,
      "CreatorRequestId": "string",
      "EncryptionKeyArn": "string",
      "EncryptionKeyType": "string",
      "LockDate": number,
      "Locked": boolean,
      "MaxRetentionDays": number,
      "MinRetentionDays": number,
      "NumberOfRecoveryPoints": number,
      "VaultState": "string",
      "VaultType": "string"
    }
  ],
  "NextToken": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

BackupVaultList

Una matriz de miembros de la lista del almacén de copias de seguridad que contiene metadatos del almacén, como el nombre de recurso de Amazon (ARN), el nombre de visualización, la fecha de creación, el número de puntos de recuperación guardados y la información de cifrado si los recursos guardados en el almacén de copias de seguridad están cifrados.

Tipo: matriz de objetos [BackupVaultListMember](#)

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

`InvalidParameterValueException`

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

`MissingParameterValueException`

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

`ResourceNotFoundException`

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListCopyJobs

Servicio: AWS Backup

Devuelve los metadatos de los trabajos de copia.

Sintaxis de la solicitud

```
GET /copy-jobs/?  
accountId=ByAccountId&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore&createdAfter=ByCreatedAfter&createdBefore=ByCreatedBefore&destinationVaultArn=ByDestinationVaultArn  
HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[ByAccountId](#)

El ID de la cuenta desde la que se van a enumerar los trabajos. Devuelve solo los trabajos de copia asociados al ID de cuenta especificado.

Patrón: `^[0-9]{12}$`

[ByCompleteAfter](#)

Devuelve solo los trabajos de copia completados después de una fecha expresada en formato Unix y horario universal coordinado (UTC).

[ByCompleteBefore](#)

Devuelve solo los trabajos de copia completados antes de una fecha expresada en formato Unix y horario universal coordinado (UTC).

[ByCreatedAfter](#)

Devuelve solo los trabajos de copia que se crearon después de la fecha especificada.

[ByCreatedBefore](#)

Devuelve solo los trabajos de copia que se crearon antes de la fecha especificada.

[ByDestinationVaultArn](#)

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un almacén de copias de seguridad de origen desde el que realizar copias; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

[ByMessageCategory](#)

Se trata de un parámetro opcional que se puede utilizar para filtrar los trabajos con un valor MessageCategory que coincida con el valor introducido.

Las cadenas de ejemplo pueden ser AccessDenied, SUCCESS, AGGREGATE_ALL y INVALIDPARAMETERS.

Consulte en [Monitorización](#) una lista de cadenas aceptadas.

El valor ANY devuelve el recuento de todas las categorías de mensajes.

AGGREGATE_ALL suma los recuentos de trabajos de todas las categorías de mensajes y devuelve la suma.

[ByParentJobId](#)

Se trata de un filtro para enumerar los trabajos secundarios (anidados) en función del ID del trabajo principal.

[ByResourceArn](#)

Devuelve solo los trabajos de copia que coinciden con el nombre de recurso de Amazon (ARN) del recurso especificado.

[ByResourceType](#)

Devuelve únicamente los trabajos de copia de seguridad de los recursos especificados:

- Aurora para Amazon Aurora
- CloudFormation para AWS CloudFormation
- DocumentDB para Amazon DocumentDB (compatible con MongoDB)
- DynamoDB para Amazon DynamoDB
- EBS para Amazon Elastic Block Store (EBS)
- EC2 para Amazon Elastic Compute Cloud
- EFS para Amazon Elastic File System
- FSx para Amazon FSx
- Neptune para Amazon Neptune
- RDS para Amazon Relational Database Service
- Redshift para Amazon Redshift
- S3 para Amazon Simple Storage Service (Amazon S3)

- SAP HANA on Amazon EC2 para bases de datos de SAP HANA en instancias de Amazon Elastic Compute Cloud
- Storage Gateway para AWS Storage Gateway
- Timestream para Amazon Timestream
- VirtualMachine para máquinas VMware virtuales

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

[BySourceRecoveryPointArn](#)

Filtra los trabajos de copia por el punto de recuperación de origen especificado (ARN).

[ByState](#)

Devuelve solo los trabajos de copia que se encuentran en el estado especificado.

Valores válidos: CREATED | RUNNING | COMPLETED | FAILED | PARTIAL

[MaxResults](#)

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el MaxResults número de artículos NextToken , podrá devolver más artículos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "CopyJobs": [
    {
      "AccountId": "string",
      "BackupSizeInBytes": number,
```

```

    "ChildJobsInState": {
      "string" : number
    },
    "CompletionDate": number,
    "CompositeMemberIdentifier": "string",
    "CopyJobId": "string",
    "CreatedBy": {
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
      "BackupPlanName": "string",
      "BackupPlanVersion": "string",
      "BackupRuleCron": "string",
      "BackupRuleId": "string",
      "BackupRuleName": "string",
      "BackupRuleTimezone": "string"
    },
    "CreatedByBackupJobId": "string",
    "CreationDate": number,
    "DestinationBackupVaultArn": "string",
    "DestinationEncryptionKeyArn": "string",
    "DestinationRecoveryPointArn": "string",
    "DestinationRecoveryPointLifecycle": {
      "DeleteAfterDays": number,
      "DeleteAfterEvent": "string",
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
    },
    "DestinationVaultLockState": "string",
    "DestinationVaultType": "string",
    "IamRoleArn": "string",
    "IsParent": boolean,
    "MessageCategory": "string",
    "NumberOfChildJobs": number,
    "ParentJobId": "string",
    "ResourceArn": "string",
    "ResourceName": "string",
    "ResourceType": "string",
    "SourceBackupVaultArn": "string",
    "SourceRecoveryPointArn": "string",
    "State": "string",
    "StatusMessage": "string"
  }
],
"NextToken": "string"

```

```
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[CopyJobs](#)

Una matriz de estructuras que contiene metadatos sobre trabajos de copia devueltos en formato JSON.

Tipo: matriz de objetos [CopyJob](#)

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el MaxResults número de NextToken artículos, podrás devolver más artículos de la lista empezando por la ubicación que indique el siguiente token.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListCopyJobSummaries

Servicio: AWS Backup

Esta solicitud obtiene una lista de trabajos de copia creados o en ejecución en los 30 últimos días. Puede incluir los parámetros AccountID, State, ResourceType, MessageCategory, AggregationPeriod, MaxResults o NextToken para filtrar los resultados.

La solicitud devuelve un resumen que contiene Region, Account, State, ResourceType, MessageCategory, StartTime, EndTime y Count de los trabajos incluidos.

Sintaxis de la solicitud

```
GET /audit/copy-job-summaries?  
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&MessageCategory=M  
HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[AccountId](#)

Devuelve el recuento de trabajos de la cuenta especificada.

Si la solicitud se envía desde una cuenta de miembro o una cuenta que no forma parte de AWS Organizations, se devolverán los trabajos de la cuenta del solicitante.

Las cuentas raíz, de administrador y de administrador delegado pueden utilizar el valor ANY para devolver recuentos de trabajos de todas las cuentas de la organización.

AGGREGATE_ALL suma los recuentos de trabajos de todas las cuentas de la organización autenticada y, a continuación, devuelve la suma.

Patrón: `^[0-9]{12}$`

[AggregationPeriod](#)

El período de los resultados devueltos.

- ONE_DAY: el recuento de trabajos diarios de los 14 días anteriores.
- SEVEN_DAYS: el recuento total de trabajos de los 7 días anteriores.
- FOURTEEN_DAYS: el recuento total de trabajos de los 14 días anteriores.

Valores válidos: ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS

[MaxResults](#)

Este parámetro establece el número máximo de elementos que se van a devolver.

El valor es un entero. El rango de valores aceptados está entre 1 y 500.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

[MessageCategory](#)

Este parámetro devuelve el recuento de trabajos de la categoría de mensajes especificada.

Ejemplos de cadenas aceptadas son AccessDenied, Success y InvalidParameters.

Consulte en [Monitorización](#) una lista de cadenas de MessageCategory aceptadas.

El valor ANY devuelve el recuento de todas las categorías de mensajes.

AGGREGATE_ALL suma los recuentos de trabajos de todas las categorías de mensajes y devuelve la suma.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos MaxResults, NextToken permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

[ResourceType](#)

Devuelve el recuento de trabajos del tipo de recurso especificado. Utilice GetSupportedResourceTypes de solicitud para obtener cadenas para los tipos de recursos compatibles.

El valor ANY devuelve el recuento de todos los tipos de recursos.

AGGREGATE_ALL suma los recuentos de trabajos de todos los tipos de recursos y devuelve la suma.

El tipo de recurso de AWS del que se va a hacer la copia de seguridad; por ejemplo, un volumen de Amazon Elastic Block Store (Amazon EBS) o una base de datos de Amazon Relational Database Service (Amazon RDS).

Patrón: `^[a-zA-Z0-9\-\_\.\]{1,50}$`

State

Este parámetro devuelve el recuento de los trabajos con el estado especificado.

El valor ANY devuelve el recuento de todos los estados.

AGGREGATE_ALL suma los recuentos de trabajos de todos los tipos de estados y devuelve la suma.

Valores válidos: CREATED | RUNNING | ABORTING | ABORTED | COMPLETING | COMPLETED | FAILING | FAILED | PARTIAL | AGGREGATE_ALL | ANY

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "AggregationPeriod": "string",
  "CopyJobSummaries": [
    {
      "AccountId": "string",
      "Count": number,
      "EndTime": number,
      "MessageCategory": "string",
      "Region": "string",
      "ResourceType": "string",
      "StartTime": number,
      "State": "string"
    }
  ],
  "NextToken": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[AggregationPeriod](#)

El período de los resultados devueltos.

- ONE_DAY: el recuento de trabajos diarios de los 14 días anteriores.
- SEVEN_DAYS: el recuento total de trabajos de los 7 días anteriores.
- FOURTEEN_DAYS: el recuento total de trabajos de los 14 días anteriores.

Tipo: cadena

[CopyJobSummaries](#)

Devuelve un resumen que contiene Region, Account, State, ResourceType, MessageCategory, StartTime, EndTime y Count de los trabajos incluidos.

Tipo: matriz de objetos [CopyJobSummary](#)

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos MaxResults, NextToken permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ListFrameworks

Servicio: AWS Backup

Devuelve una lista de todos los marcos de una Cuenta de AWS y Región de AWS.

Sintaxis de la solicitud

```
GET /audit/frameworks?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[MaxResults](#)

El número de resultados deseados va de 1 a 1000. Opcional. Si no se especifica, la consulta devolverá 1 MB de datos.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

[NextToken](#)

Un identificador que se devolvió de la llamada anterior a esta operación, que se puede usar para devolver el siguiente conjunto de elementos de la lista.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "Frameworks": [
    {
      "CreationTime": number,
      "DeploymentStatus": "string",
      "FrameworkArn": "string",
      "FrameworkDescription": "string",
      "FrameworkName": "string",
```

```
    "NumberOfControls": number
  },
  "NextToken": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[Frameworks](#)

Los marcos con detalles de cada marco, incluidos el nombre del marco, el nombre de recurso de Amazon (ARN), la descripción, el número de controles, la hora de creación y el estado de la implementación.

Tipo: matriz de objetos [Framework](#)

[NextToken](#)

Un identificador que se devolvió de la llamada anterior a esta operación, que se puede usar para devolver el siguiente conjunto de elementos de la lista.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ListIndexedRecoveryPoints

Servicio: AWS Backup

Esta operación devuelve una lista de puntos de recuperación que tienen un índice asociado que pertenece a la cuenta especificada.

Los parámetros opcionales que puede incluir son: MaxResults; NextToken; SourceResourceArns; CreatedBefore; CreatedAfter y ResourceType.

Sintaxis de la solicitud

```
GET /indexes/recovery-point/?
createdAfter=CreatedAfter&createdBefore=CreatedBefore&indexStatus=IndexStatus&maxResults=MaxRes
HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[CreatedAfter](#)

Devuelve solo los puntos de recuperación indexados creados tras la fecha especificada.

[CreatedBefore](#)

Devuelve solo los puntos de recuperación indexados creados antes de la fecha especificada.

[IndexStatus](#)

Incluya este parámetro para filtrar la lista devuelta según los estados indicados.

Valores aceptados: PENDING | ACTIVE | FAILED | DELETING

En una búsqueda se puede incluir un punto de recuperación con un índice con el estado ACTIVE.

Valores válidos: PENDING | ACTIVE | FAILED | DELETING

[MaxResults](#)

Número máximo de elementos de la lista de recursos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

[NextToken](#)

Es el elemento que sigue a una lista parcial de los puntos de recuperación devueltos.

Por ejemplo, si se solicita que se devuelva el número `MaxResults` de puntos de recuperación indexados, `NextToken` le permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

[ResourceType](#)

Devuelve una lista de puntos de recuperación indexados para el tipo o los tipos de recurso especificados.

Los valores aceptados son:

- EBS para Amazon Elastic Block Store (EBS)
- S3 para Amazon Simple Storage Service (Amazon S3)

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

[SourceResourceArn](#)

Es una cadena de un Nombre de recurso de Amazon (ARN) que identifica de forma unívoca un recurso de origen.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "IndexedRecoveryPoints": [
    {
      "BackupCreationDate": number,
      "BackupVaultArn": "string",
      "IamRoleArn": "string",
      "IndexCreationDate": number,
      "IndexStatus": "string",
      "IndexStatusMessage": "string",
      "RecoveryPointArn": "string",
      "ResourceType": "string",
      "SourceResourceArn": "string"
    }
  ]
}
```

```
] ,  
  "NextToken": "string"  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[IndexedRecoveryPoints](#)

Es una lista de puntos de recuperación que tienen un índice asociado que pertenece a la cuenta especificada.

Tipo: matriz de objetos [IndexedRecoveryPoint](#)

[NextToken](#)

Es el elemento que sigue a una lista parcial de los puntos de recuperación devueltos.

Por ejemplo, si se solicita que se devuelva el número `MaxResults` de puntos de recuperación indexados, `NextToken` le permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

`InvalidParameterValueException`

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ListLegalHolds

Servicio: AWS Backup

Esta acción devuelve metadatos sobre las retenciones legales activas y anteriores.

Sintaxis de la solicitud

```
GET /legal-holds/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[MaxResults](#)

Número máximo de elementos de la lista de recursos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "LegalHolds": [
    {
      "CancellationDate": number,
      "CreationDate": number,
      "Description": "string",
      "LegalHoldArn": "string",
      "LegalHoldId": "string",
```

```
    "Status": "string",  
    "Title": "string"  
  },  
],  
"NextToken": "string"  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[LegalHolds](#)

Se trata de una matriz de retenciones legales devueltas, tanto activas como anteriores.

Tipo: matriz de objetos [LegalHold](#)

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

`InvalidParameterValueException`

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ListProtectedResources

Servicio: AWS Backup

Devuelve una matriz de recursos de la que AWS Backup realizó una copia de seguridad correcta, incluida la hora en que se guardó el recurso, el nombre de recurso de Amazon (ARN) del recurso y el tipo de recurso.

Sintaxis de la solicitud

```
GET /resources/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[MaxResults](#)

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "Results": [
    {
      "LastBackupTime": number,
```

```
    "LastBackupVaultArn": "string",
    "LastRecoveryPointArn": "string",
    "ResourceArn": "string",
    "ResourceName": "string",
    "ResourceType": "string"
  }
]
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

[Results](#)

Una matriz de recursos de la que AWS Backup realizó una copia de seguridad correcta, incluida la hora en que se guardó el recurso, el nombre de recurso de Amazon (ARN) del recurso y el tipo de recurso.

Tipo: matriz de objetos [ProtectedResource](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

`InvalidParameterValueException`

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ListProtectedResourcesByBackupVault

Servicio: AWS Backup

En esta solicitud se enumeran los recursos protegidos correspondientes a cada almacén de copias de seguridad.

Sintaxis de la solicitud

```
GET /backup-vaults/backupVaultName/resources/?  
backupVaultAccountId=BackupVaultAccountId&maxResults=MaxResults&nextToken=NextToken  
HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

BackupVaultAccountId

La lista de recursos protegidos por almacén de copias de seguridad dentro de los almacenes que especifique mediante el identificador de cuenta.

Patrón: `^[0-9]{12}$`

backupVaultName

La lista de recursos protegidos por almacén de copias de seguridad dentro de los almacenes que especifique por nombre.

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: sí

MaxResults

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "Results": [
    {
      "LastBackupTime": number,
      "LastBackupVaultArn": "string",
      "LastRecoveryPointArn": "string",
      "ResourceArn": "string",
      "ResourceName": "string",
      "ResourceType": "string"
    }
  ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Results

Estos son los resultados devueltos para la solicitud `ListProtectedResourcesByBackupVault`.

Tipo: matriz de objetos [ProtectedResource](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)

- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ListRecoveryPointsByBackupVault

Servicio: AWS Backup

Devuelve información detallada sobre los puntos de recuperación almacenados en un almacén de copias de seguridad.

Sintaxis de la solicitud

```
GET /backup-vaults/backupVaultName/recovery-points/?  
backupPlanId=ByBackupPlanId&backupVaultAccountId=BackupVaultAccountId&createdAfter=ByCreatedAfter  
HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[BackupVaultAccountId](#)

Este parámetro ordenará la lista de puntos de recuperación por ID de cuenta.

Patrón: `^[0-9]{12}$`

[backupVaultName](#)

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Note

Es posible que el nombre del almacén de copias de seguridad no esté disponible cuando un servicio compatible cree la copia de seguridad.

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: sí

[ByBackupPlanId](#)

Devuelve solo los puntos de recuperación que coinciden con el identificador del plan de copia de seguridad especificado.

[ByCreatedAfter](#)

Devuelve solo los puntos de recuperación que se crearon después de la marca de tiempo especificada.

[ByCreatedBefore](#)

Devuelve solo los puntos de recuperación que se crearon antes de la marca de tiempo especificada.

[ByParentRecoveryPointArn](#)

Devuelve solo los puntos de recuperación que coinciden con el nombre de recurso de Amazon (ARN) del punto de recuperación principal (compuesto) especificado.

[ByResourceArn](#)

Devuelve solo los puntos de recuperación que coinciden con el nombre de recurso de Amazon (ARN) del recurso especificado.

[ByResourceType](#)

Devuelve solo los puntos de recuperación que coinciden con el tipo o los tipos de recurso especificados.

- Aurora para Amazon Aurora
- CloudFormation para AWS CloudFormation
- DocumentDB para Amazon DocumentDB (compatible con MongoDB)
- DynamoDB para Amazon DynamoDB
- EBS para Amazon Elastic Block Store (EBS)
- EC2 para Amazon Elastic Compute Cloud
- EFS para Amazon Elastic File System
- FSx para Amazon FSx
- Neptune para Amazon Neptune
- RDS para Amazon Relational Database Service
- Redshift para Amazon Redshift
- S3 para Amazon Simple Storage Service (Amazon S3)
- SAP HANA on Amazon EC2 para bases de datos de SAP HANA en instancias de Amazon Elastic Compute Cloud
- Storage Gateway para AWS Storage Gateway

- Timestream para Amazon Timestream
- VirtualMachine para máquinas VMware virtuales

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

[MaxResults](#)

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "RecoveryPoints": [
    {
      "AggregatedScanResult": {
        "FailedScan": boolean,
        "Findings": [ "string" ],
        "LastComputed": number
      },
      "BackupSizeInBytes": number,
      "BackupVaultArn": "string",
      "BackupVaultName": "string",
      "CalculatedLifecycle": {
        "DeleteAt": number,
        "MoveToColdStorageAt": number
      },
      "CompletionDate": number,
      "CompositeMemberIdentifier": "string",
```

```

    "CreatedBy": {
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
      "BackupPlanName": "string",
      "BackupPlanVersion": "string",
      "BackupRuleCron": "string",
      "BackupRuleId": "string",
      "BackupRuleName": "string",
      "BackupRuleTimezone": "string"
    },
    "CreationDate": number,
    "EncryptionKeyArn": "string",
    "EncryptionKeyType": "string",
    "IamRoleArn": "string",
    "IndexStatus": "string",
    "IndexStatusMessage": "string",
    "InitiationDate": number,
    "IsEncrypted": boolean,
    "IsParent": boolean,
    "LastRestoreTime": number,
    "Lifecycle": {
      "DeleteAfterDays": number,
      "DeleteAfterEvent": "string",
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
    },
    "ParentRecoveryPointArn": "string",
    "RecoveryPointArn": "string",
    "ResourceArn": "string",
    "ResourceName": "string",
    "ResourceType": "string",
    "SourceBackupVaultArn": "string",
    "Status": "string",
    "StatusMessage": "string",
    "VaultType": "string"
  }
]
}

```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

[RecoveryPoints](#)

Una matriz de objetos que contiene información detallada sobre los puntos de recuperación guardados en un almacén de copias de seguridad.

Tipo: matriz de objetos [RecoveryPointByBackupVault](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

`InvalidParameterValueException`

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

`MissingParameterValueException`

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

`ResourceNotFoundException`

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListRecoveryPointsByLegalHold

Servicio: AWS Backup

Esta acción devuelve los ARN (nombres de recursos de Amazon) de los puntos de recuperación de la retención legal especificada.

Sintaxis de la solicitud

```
GET /legal-holds/legalHoldId/recovery-points?maxResults=MaxResults&nextToken=NextToken  
HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[legalHoldId](#)

El identificador de la retención legal.

Obligatorio: sí

[MaxResults](#)

Número máximo de elementos de la lista de recursos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200  
Content-type: application/json
```

```
{
  "NextToken": "string",
  "RecoveryPoints": [
    {
      "BackupVaultName": "string",
      "RecoveryPointArn": "string",
      "ResourceArn": "string",
      "ResourceType": "string"
    }
  ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de recursos devueltos.

Tipo: cadena

[RecoveryPoints](#)

Los puntos de recuperación.

Tipo: matriz de objetos [RecoveryPointMember](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ListRecoveryPointsByResource

Servicio: AWS Backup

La información detallada sobre todos los puntos de recuperación del tipo especificado por el nombre de recurso de Amazon (ARN) de un recurso.

Note

Para Amazon EFS y Amazon EC2, esta acción solo muestra los puntos de recuperación creados por AWS Backup.

Sintaxis de la solicitud

```
GET /resources/resourceArn/recovery-points/?  
managedByAWSBackupOnly=ManagedByAWSBackupOnly&maxResults=MaxResults&nextToken=NextToken  
HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

ManagedByAWSBackupOnly

Este atributo filtra los puntos de recuperación en función de la propiedad.

Si se establece en TRUE, la respuesta contendrá los puntos de recuperación asociados a los recursos seleccionados administrados por AWS Backup.

Si se establece en FALSE, la respuesta contendrá todos los puntos de recuperación asociados al recurso.

Tipo: Booleano

MaxResults

Número máximo de elementos que se van a devolver.

Note

Amazon RDS requiere un valor mínimo de 20.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

[resourceArn](#)

Un ARN que identifica de forma única a un recurso. El formato del ARN depende del tipo de recurso.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "RecoveryPoints": [
    {
      "AggregatedScanResult": {
        "FailedScan": boolean,
        "Findings": [ "string" ],
        "LastComputed": number
      },
      "BackupSizeBytes": number,
      "BackupVaultName": "string",
      "CreationDate": number,
      "EncryptionKeyArn": "string",
      "EncryptionKeyType": "string",
      "IndexStatus": "string",
      "IndexStatusMessage": "string",
      "IsParent": boolean,
      "ParentRecoveryPointArn": "string",
      "RecoveryPointArn": "string",
```

```
    "ResourceName": "string",  
    "Status": "string",  
    "StatusMessage": "string",  
    "VaultType": "string"  
  }  
]  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

[RecoveryPoints](#)

Una matriz de objetos que contiene información detallada sobre los puntos de recuperación del tipo de recurso especificado.

Note

Solo se devuelven Amazon EFS y los puntos EC2 de recuperación de Amazon BackupVaultName.

Tipo: matriz de objetos [RecoveryPointByResource](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListReportJobs

Servicio: AWS Backup

Devuelve detalles sobre sus trabajos de informes.

Sintaxis de la solicitud

```
GET /audit/report-jobs?  
CreationAfter=ByCreationAfter&CreationBefore=ByCreationBefore&MaxResults=MaxResults&NextToken=N  
HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[ByCreationAfter](#)

Devuelve solo los trabajos de informes que se crearon después de la fecha y la hora especificadas en formato Unix y horario universal coordinado (UTC). Por ejemplo, el valor 1516925490 representa el viernes 26 de enero de 2018 a las 12:11:30 h

[ByCreationBefore](#)

Devuelve solo los trabajos de informes que se crearon antes de la fecha y la hora, expresadas en formato Unix y horario universal coordinado (UTC). Por ejemplo, el valor 1516925490 representa el viernes 26 de enero de 2018 a las 12:11:30 h

[ByReportPlanName](#)

Devuelve solo los trabajos de informe con el nombre del plan de informes especificado.

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: [a-zA-Z][_a-zA-Z0-9]*

[ByStatus](#)

Devuelve solo los trabajos de informes que se encuentran en el estado especificado. Los estados son:

CREATED | RUNNING | COMPLETED | FAILED | COMPLETED_WITH_ISSUES

Tenga en cuenta que solo los trabajos de escaneo terminan con el estado completado con problemas. En el caso de los trabajos de copia de seguridad, se trata de una interpretación en consola de un trabajo que finaliza y que tiene un mensaje de estado.

MaxResults

El número de resultados deseados va de 1 a 1000. Opcional. Si no se especifica, la consulta devolverá 1 MB de datos.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

Un identificador que se devolvió de la llamada anterior a esta operación, que se puede usar para devolver el siguiente conjunto de elementos de la lista.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "ReportJobs": [
    {
      "CompletionTime": number,
      "CreationTime": number,
      "ReportDestination": {
        "S3BucketName": "string",
        "S3Keys": [ "string" ]
      },
      "ReportJobId": "string",
      "ReportPlanArn": "string",
      "ReportTemplate": "string",
      "Status": "string",
      "StatusMessage": "string"
    }
  ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[NextToken](#)

Un identificador que se devolvió de la llamada anterior a esta operación, que se puede usar para devolver el siguiente conjunto de elementos de la lista.

Tipo: cadena

[ReportJobs](#)

Detalles sobre sus trabajos de informes en formato JSON.

Tipo: matriz de objetos [ReportJob](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListReportPlans

Servicio: AWS Backup

Devuelve una lista de los planes de informes. Para obtener información detallada sobre un plan de informes único, utilice DescribeReportPlan.

Sintaxis de la solicitud

```
GET /audit/report-plans?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[MaxResults](#)

El número de resultados deseados va de 1 a 1000. Opcional. Si no se especifica, la consulta devolverá 1 MB de datos.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

[NextToken](#)

Un identificador que se devolvió de la llamada anterior a esta operación, que se puede usar para devolver el siguiente conjunto de elementos de la lista.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "ReportPlans": [
    {
      "CreationTime": number,
      "DeploymentStatus": "string",
```

```

    "LastAttemptedExecutionTime": number,
    "LastSuccessfulExecutionTime": number,
    "ReportDeliveryChannel": {
      "Formats": [ "string" ],
      "S3BucketName": "string",
      "S3KeyPrefix": "string"
    },
    "ReportPlanArn": "string",
    "ReportPlanDescription": "string",
    "ReportPlanName": "string",
    "ReportSetting": {
      "Accounts": [ "string" ],
      "FrameworkArns": [ "string" ],
      "NumberOfFrameworks": number,
      "OrganizationUnits": [ "string" ],
      "Regions": [ "string" ],
      "ReportTemplate": "string"
    }
  }
]
}

```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[NextToken](#)

Un identificador que se devolvió de la llamada anterior a esta operación, que se puede usar para devolver el siguiente conjunto de elementos de la lista.

Tipo: cadena

[ReportPlans](#)

Los planes de informes con información detallada de cada plan. Esta información incluye el nombre de recurso de Amazon (ARN), el nombre del plan de informes, la descripción, la configuración, el canal de entrega, el estado de implementación, la hora de creación y las últimas veces que el plan de informes se intentó ejecutar y se ejecutó correctamente.

Tipo: matriz de objetos [ReportPlan](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)

- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ListRestoreAccessBackupVaults

Servicio: AWS Backup

Devuelve una lista de los almacenes de copias de seguridad con acceso a la restauración asociadas a un almacén de copias de seguridad específico.

Sintaxis de la solicitud

```
GET /logically-air-gapped-backup-vaults/backupVaultName/restore-access-backup-vaults/?
maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupVaultName

Es el nombre del almacén de copias de seguridad a partir del cual se enumeran los almacenes de copias de seguridad con acceso a la restauración asociados.

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: sí

MaxResults

Es el número máximo de elementos que se devuelve en la respuesta.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

Es el token de paginación de una solicitud anterior para obtener el siguiente conjunto de resultados.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json
```

```
{
  "NextToken": "string",
  "RestoreAccessBackupVaults": [
    {
      "ApprovalDate": number,
      "CreationDate": number,
      "LatestRevokeRequest": {
        "ExpiryDate": number,
        "InitiationDate": number,
        "MpaSessionArn": "string",
        "Status": "string",
        "StatusMessage": "string"
      },
      "RestoreAccessBackupVaultArn": "string",
      "VaultState": "string"
    }
  ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[NextToken](#)

Es el token de paginación que se debe utilizar en una solicitud subsiguiente para obtener el siguiente conjunto de resultados.

Tipo: cadena

[RestoreAccessBackupVaults](#)

Es una lista de los almacenes de copias de seguridad con acceso a la restauración asociadas a un almacén de copias de seguridad específico.

Tipo: matriz de objetos [RestoreAccessBackupVaultListMember](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ListRestoreJobs

Servicio: AWS Backup

Devuelve una lista de los trabajos que AWS Backup se iniciaron para restaurar un recurso guardado, incluidos los detalles del proceso de recuperación.

Sintaxis de la solicitud

```
GET /restore-jobs/?  
accountId=ByAccountId&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore&createdAfter=ByCreatedAfter  
HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[ByAccountId](#)

El ID de la cuenta desde la que se van a enumerar los trabajos. Devuelve solo los trabajos de restauración asociados al ID de cuenta especificado.

Patrón: `^[0-9]{12}$`

[ByCompleteAfter](#)

Devuelve solo los trabajos de copia completados después de una fecha expresada en formato Unix y horario universal coordinado (UTC).

[ByCompleteBefore](#)

Devuelve solo los trabajos de copia completados antes de una fecha expresada en formato Unix y horario universal coordinado (UTC).

[ByCreatedAfter](#)

Devuelve solo los trabajos de restauración que se crearon después de la fecha especificada.

[ByCreatedBefore](#)

Devuelve solo los trabajos de restauración que se crearon antes de la fecha especificada.

[ByParentJobId](#)

Se trata de un filtro para enumerar los trabajos de restauración secundarios (anidados) en función del identificador del trabajo de restauración principal.

[ByResourceType](#)

Incluya este parámetro para devolver únicamente los trabajos de restauración de los recursos especificados:

- Aurora para Amazon Aurora
- CloudFormation para AWS CloudFormation
- DocumentDB para Amazon DocumentDB (compatible con MongoDB)
- DynamoDB para Amazon DynamoDB
- EBS para Amazon Elastic Block Store (EBS)
- EC2 para Amazon Elastic Compute Cloud
- EFS para Amazon Elastic File System
- FSx para Amazon FSx
- Neptune para Amazon Neptune
- RDS para Amazon Relational Database Service
- Redshift para Amazon Redshift
- S3 para Amazon Simple Storage Service (Amazon S3)
- SAP HANA on Amazon EC2 para bases de datos de SAP HANA en instancias de Amazon Elastic Compute Cloud
- Storage Gateway para AWS Storage Gateway
- Timestream para Amazon Timestream
- VirtualMachine para máquinas VMware virtuales

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

[ByRestoreTestingPlanArn](#)

Devuelve solo los trabajos de restauración que coinciden con el nombre de recurso de Amazon (ARN) del recurso especificado.

[ByStatus](#)

Devuelve solo los trabajos de restauración asociados al estado de trabajo especificado.

Valores válidos: PENDING | RUNNING | COMPLETED | ABORTED | FAILED

[MaxResults](#)

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "RestoreJobs": [
    {
      "AccountId": "string",
      "BackupSizeInBytes": number,
      "BackupVaultArn": "string",
      "CompletionDate": number,
      "CreatedBy": {
        "RestoreTestingPlanArn": "string"
      },
      "CreatedResourceArn": "string",
      "CreationDate": number,
      "DeletionStatus": "string",
      "DeletionStatusMessage": "string",
      "ExpectedCompletionTimeMinutes": number,
      "IamRoleArn": "string",
      "IsParent": boolean,
      "ParentJobId": "string",
      "PercentDone": "string",
      "RecoveryPointArn": "string",
      "RecoveryPointCreationDate": number,
      "ResourceType": "string",
      "RestoreJobId": "string",
      "SourceResourceArn": "string",
      "Status": "string",
```

```
    "StatusMessage": "string",  
    "ValidationStatus": "string",  
    "ValidationStatusMessage": "string"  
  }  
]  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

[RestoreJobs](#)

Una matriz de objetos que contiene información detallada sobre los trabajos para restaurar los recursos guardados.

Tipo: matriz de objetos [RestoreJobsListMember](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

`InvalidParameterValueException`

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)

- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListRestoreJobsByProtectedResource

Servicio: AWS Backup

Devuelve los trabajos de restauración que contienen el recurso protegido especificado.

Debe incluir `ResourceArn`. Opcionalmente, puede incluir `NextToken`, `ByStatus`, `MaxResults`, `ByRecoveryPointCreationDateAfter` y `ByRecoveryPointCreationDateBefore`.

Sintaxis de la solicitud

```
GET /resources/resourceArn/restore-jobs/?  
maxResults=MaxResults&nextToken=NextToken&recoveryPointCreationDateAfter=ByRecoveryPointCreationDateAfter  
HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[ByRecoveryPointCreationDateAfter](#)

Devuelve solo los trabajos de restauración de puntos de recuperación que se crearon después de la fecha especificada.

[ByRecoveryPointCreationDateBefore](#)

Devuelve solo los trabajos de restauración de puntos de recuperación que se crearon antes de la fecha especificada.

[ByStatus](#)

Devuelve solo los trabajos de restauración asociados al estado de trabajo especificado.

Valores válidos: PENDING | RUNNING | COMPLETED | ABORTED | FAILED

[MaxResults](#)

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

resourceArn

Devuelve solo los trabajos de restauración que coinciden con el nombre de recurso de Amazon (ARN) del recurso especificado.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "RestoreJobs": [
    {
      "AccountId": "string",
      "BackupSizeInBytes": number,
      "BackupVaultArn": "string",
      "CompletionDate": number,
      "CreatedBy": {
        "RestoreTestingPlanArn": "string"
      },
      "CreatedResourceArn": "string",
      "CreationDate": number,
      "DeletionStatus": "string",
      "DeletionStatusMessage": "string",
      "ExpectedCompletionTimeMinutes": number,
      "IamRoleArn": "string",
      "IsParent": boolean,
      "ParentJobId": "string",
      "PercentDone": "string",
      "RecoveryPointArn": "string",
      "RecoveryPointCreationDate": number,
      "ResourceType": "string",
      "RestoreJobId": "string",
      "SourceResourceArn": "string",
      "Status": "string",
      "StatusMessage": "string",
```

```
    "ValidationStatus": "string",  
    "ValidationStatusMessage": "string"  
  }  
]  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token

Tipo: cadena

[RestoreJobs](#)

Una matriz de objetos que contiene información detallada sobre los trabajos para restaurar los recursos guardados.>

Tipo: matriz de objetos [RestoreJobsListMember](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

`InvalidParameterValueException`

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)

- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListRestoreJobSummaries

Servicio: AWS Backup

Esta solicitud obtiene un resumen de los trabajos de restauración creados o en ejecución en los 30 últimos días. Puede incluir los parámetros AccountID, State, ResourceType, AggregationPeriod, MaxResults o NextToken para filtrar los resultados.

La solicitud devuelve un resumen que contiene Region, Account, State, ResourceType, MessageCategory, StartTime, EndTime y Count de los trabajos incluidos.

Sintaxis de la solicitud

```
GET /audit/restore-job-summaries?  
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&NextToken=NextTok  
HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

AccountId

Devuelve el recuento de trabajos de la cuenta especificada.

Si la solicitud se envía desde una cuenta de miembro o una cuenta que no forma parte de AWS Organizations, se devolverán los trabajos de la cuenta del solicitante.

Las cuentas raíz, de administrador y de administrador delegado pueden utilizar el valor ANY para devolver recuentos de trabajos de todas las cuentas de la organización.

AGGREGATE_ALL suma los recuentos de trabajos de todas las cuentas de la organización autenticada y, a continuación, devuelve la suma.

Patrón: `^[0-9]{12}$`

AggregationPeriod

El período de los resultados devueltos.

- ONE_DAY: el recuento de trabajos diarios de los 14 días anteriores.
- SEVEN_DAYS: el recuento total de trabajos de los 7 días anteriores.

- `FOURTEEN_DAYS`: el recuento total de trabajos de los 14 días anteriores.

Valores válidos: `ONE_DAY` | `SEVEN_DAYS` | `FOURTEEN_DAYS`

MaxResults

Este parámetro establece el número máximo de elementos que se van a devolver.

El valor es un entero. El rango de valores aceptados está entre 1 y 500.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

ResourceType

Devuelve el recuento de trabajos del tipo de recurso especificado. Utilice `GetSupportedResourceTypes` de solicitud para obtener cadenas para los tipos de recursos compatibles.

El valor `ANY` devuelve el recuento de todos los tipos de recursos.

`AGGREGATE_ALL` suma los recuentos de trabajos de todos los tipos de recursos y devuelve la suma.

El tipo de recurso de AWS del que se va a hacer la copia de seguridad; por ejemplo, un volumen de Amazon Elastic Block Store (Amazon EBS) o una base de datos de Amazon Relational Database Service (Amazon RDS).

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

State

Este parámetro devuelve el recuento de los trabajos con el estado especificado.

El valor `ANY` devuelve el recuento de todos los estados.

`AGGREGATE_ALL` suma los recuentos de trabajos de todos los tipos de estados y devuelve la suma.

Valores válidos: CREATED | PENDING | RUNNING | ABORTED | COMPLETED | FAILED | AGGREGATE_ALL | ANY

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "AggregationPeriod": "string",
  "NextToken": "string",
  "RestoreJobSummaries": [
    {
      "AccountId": "string",
      "Count": number,
      "EndTime": number,
      "Region": "string",
      "ResourceType": "string",
      "StartTime": number,
      "State": "string"
    }
  ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

AggregationPeriod

El período de los resultados devueltos.

- ONE_DAY: el recuento de trabajos diarios de los 14 días anteriores.
- SEVEN_DAYS: el recuento total de trabajos de los 7 días anteriores.
- FOURTEEN_DAYS: el recuento total de trabajos de los 14 días anteriores.

Tipo: cadena

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

[RestoreJobSummaries](#)

Devuelve un resumen que contiene `Region`, `Account`, `State`, `ResourceType`, `MessageCategory`, `StartTime`, `EndTime` y `Count` de los trabajos incluidos.

Tipo: matriz de objetos [RestoreJobSummary](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

`InvalidParameterValueException`

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

`ServiceUnavailableException`

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ListRestoreTestingPlans

Servicio: AWS Backup

Devuelve una lista de los planes de prueba de restauración.

Sintaxis de la solicitud

```
GET /restore-testing/plans?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[MaxResults](#)

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "RestoreTestingPlans": [
    {
      "CreationTime": number,
      "LastExecutionTime": number,
      "LastUpdateTime": number,
      "RestoreTestingPlanArn": "string",
```

```
"RestoreTestingPlanName": "string",  
"ScheduleExpression": "string",  
"ScheduleExpressionTimezone": "string",  
"StartWindowHours": number  
}  
]  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

[RestoreTestingPlans](#)

Es una lista devuelta de planes de prueba de restauración.

Tipo: matriz de objetos [RestoreTestingPlanForList](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

`InvalidParameterValueException`

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ListRestoreTestingSelections

Servicio: AWS Backup

Devuelve una lista de selecciones de pruebas de restauración. Se puede filtrar por `MaxResults` y `RestoreTestingPlanName`.

Sintaxis de la solicitud

```
GET /restore-testing/plans/RestoreTestingPlanName/selections?  
MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[MaxResults](#)

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

[RestoreTestingPlanName](#)

Devuelve las selecciones de pruebas de restauración por el nombre del plan de prueba de restauración especificado.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200  
Content-type: application/json  
  
{
```

```
"NextToken": "string",
"RestoreTestingSelections": [
  {
    "CreationTime": number,
    "IamRoleArn": "string",
    "ProtectedResourceType": "string",
    "RestoreTestingPlanName": "string",
    "RestoreTestingSelectionName": "string",
    "ValidationWindowHours": number
  }
]
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

[RestoreTestingSelections](#)

Las selecciones de pruebas de restauración devueltas asociadas al plan de prueba de restauración.

Tipo: matriz de objetos [RestoreTestingSelectionForList](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

`InvalidParameterValueException`

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)

- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ListScanJobs

Servicio: AWS Backup

Devuelve una lista de los trabajos de escaneo existentes para una cuenta autenticada durante los últimos 30 días.

Sintaxis de la solicitud

```
GET /scan/jobs?
```

```
ByAccountId=ByAccountId&ByBackupVaultName=ByBackupVaultName&ByCompleteAfter=ByCompleteAfter&ByC
```

```
HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[ByAccountId](#)

El ID de la cuenta desde la que se van a enumerar los trabajos. Devuelve solo los trabajos de copia de seguridad asociados al ID de cuenta especificado.

Si se usa desde una AWS cuenta de administración de Organizations, la * transferencia devuelve todos los trabajos de la organización.

Patrón: `^[0-9]{12}$`

[ByBackupVaultName](#)

Devuelve solo los trabajos de escaneo que se almacenarán en la bóveda de respaldo especificada. Los almacenes de Backup se identifican con nombres que son exclusivos de la cuenta utilizada para crearlos y de la AWS región en la que se crearon.

Patrón: `^[a-zA-Z0-9\-\_\.\]{2,50}$`

[ByCompleteAfter](#)

Solo devuelve los trabajos de escaneo completados después de una fecha expresada en formato Unix y en la hora universal coordinada (UTC).

[ByCompleteBefore](#)

Devuelve solo los trabajos de copia de seguridad completados antes de una fecha expresada en formato Unix y horario universal coordinado (UTC).

[ByMalwareScanner](#)

Devuelve solo los trabajos de escaneo del escáner de malware especificado. Actualmente solo es compatible GUARDDUTY.

Valores válidos: GUARDDUTY

[ByRecoveryPointArn](#)

Devuelve solo los trabajos de escaneo que se ejecutan en el punto de recuperación especificado.

[ByResourceArn](#)

Devuelve solo los trabajos de escaneo que coinciden con el nombre de recurso Amazon (ARN) del recurso especificado.

[ByResourceType](#)

Devuelve las selecciones de pruebas de restauración por el nombre del plan de prueba de restauración especificado.

- EBS para Amazon Elastic Block Store
- EC2 para Amazon Elastic Compute Cloud
- S3 para Amazon Simple Storage Service (Amazon S3)

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Valores válidos: EBS | EC2 | S3

[ByScanResultStatus](#)

Devuelve solo los trabajos de escaneo para los resultados de escaneo especificados:

- THREATS_FOUND
- NO_THREATS_FOUND

Valores válidos: NO_THREATS_FOUND | THREATS_FOUND

[ByState](#)

Devuelve solo los trabajos de escaneo para el estado del trabajo de escaneo especificado.

Valores válidos: CANCELED | COMPLETED | COMPLETED_WITH_ISSUES | CREATED | FAILED | RUNNING

[MaxResults](#)

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "ScanJobs": [
    {
      "AccountId": "string",
      "BackupVaultArn": "string",
      "BackupVaultName": "string",
      "CompletionDate": number,
      "CreatedBy": {
        "BackupPlanArn": "string",
        "BackupPlanId": "string",
        "BackupPlanVersion": "string",
        "BackupRuleId": "string"
      },
      "CreationDate": number,
      "IamRoleArn": "string",
      "MalwareScanner": "string",
      "RecoveryPointArn": "string",
      "ResourceArn": "string",
      "ResourceName": "string",
      "ResourceType": "string",
      "ScanBaseRecoveryPointArn": "string",
      "ScanId": "string",
      "ScanJobId": "string",
```

```
    "ScanMode": "string",
    "ScannerRoleArn": "string",
    "ScanResult": {
        "ScanResultStatus": "string"
    },
    "State": "string",
    "StatusMessage": "string"
}
]
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

[ScanJobs](#)

Un conjunto de estructuras que contienen metadatos sobre sus trabajos de escaneo devueltos en formato JSON.

Tipo: matriz de objetos [ScanJob](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

`InvalidParameterValueException`

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListScanJobSummaries

Servicio: AWS Backup

Se trata de una solicitud de resumen de los trabajos de digitalización creados o en ejecución en los últimos 30 días.

Sintaxis de la solicitud

```
GET /audit/scan-job-summaries?  
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MalwareScanner=MalwareScanner&MaxResult  
HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

AccountId

Devuelve el recuento de trabajos de la cuenta especificada.

Si la solicitud se envía desde una cuenta de miembro o desde una cuenta que no forma parte de AWS Organizations, se devolverán los trabajos de la cuenta del solicitante.

Las cuentas raíz, de administrador y de administrador delegado pueden usar el valor ANY para devolver los recuentos de puestos de trabajo de todas las cuentas de la organización.

AGGREGATE_ALL suma los recuentos de trabajos de todas las cuentas de la organización autenticada y, a continuación, devuelve la suma.

Patrón: `^[0-9]{12}$`

AggregationPeriod

El período de los resultados devueltos.

- ONE_DAY El recuento diario de trabajos del día anterior.
- SEVEN_DAY El recuento diario de trabajos de los 7 días anteriores.
- FOURTEEN_DAY El recuento diario de trabajos de los 14 días anteriores.

Valores válidos: ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS

[MalwareScanner](#)

Devuelve solo los trabajos de escaneo del escáner de malware especificado. Actualmente, el único MalwareScanner es GUARDDUTY. Pero el campo también apoya ANY, y AGGREGATE_ALL.

Valores válidos: GUARDDUTY

[MaxResults](#)

Número máximo de elementos que se van a devolver.

El valor es un entero. El rango de valores aceptados está entre 1 y 500.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos MaxResults, NextToken permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

[ResourceType](#)

Devuelve el recuento de trabajos del tipo de recurso especificado. Utilice GetSupportedResourceTypes de solicitud para obtener cadenas para los tipos de recursos compatibles.

El valor ANY devuelve el recuento de todos los tipos de recursos.

AGGREGATE_ALL suma los recuentos de trabajos de todos los tipos de recursos y devuelve la suma.

Patrón: `^[a-zA-Z0-9\-\_\.\]{1,50}$`

[ScanResultStatus](#)

Devuelve solo los trabajos de escaneo para los resultados de escaneo especificados.

Valores válidos: NO_THREATS_FOUND | THREATS_FOUND

[State](#)

Devuelve solo los trabajos de escaneo para el estado del trabajo de escaneo especificado.

Valores válidos: CREATED | COMPLETED | COMPLETED_WITH_ISSUES | RUNNING | FAILED | CANCELED | AGGREGATE_ALL | ANY

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "AggregationPeriod": "string",
  "NextToken": "string",
  "ScanJobSummaries": [
    {
      "AccountId": "string",
      "Count": number,
      "EndTime": number,
      "MalwareScanner": "string",
      "Region": "string",
      "ResourceType": "string",
      "ScanResultStatus": "string",
      "StartTime": number,
      "State": "string"
    }
  ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

AggregationPeriod

El período de los resultados devueltos.

- ONE_DAY El recuento de trabajos diarios del día anterior.
- SEVEN_DAY El recuento diario de trabajos de los 7 días anteriores.
- FOURTEEN_DAY El recuento diario de trabajos de los 14 días anteriores.

Valores válidos: 'ONE_DAY' | 'SEVEN_DAYS' | 'FOURTEEN_DAYS'

Tipo: cadena

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

[ScanJobSummaries](#)

La información del resumen.

Tipo: matriz de objetos [ScanJobSummary](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

`InvalidParameterValueException`

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

`ServiceUnavailableException`

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListTags

Servicio: AWS Backup

Devuelve las etiquetas asignadas al recurso, como un punto de recuperación, plan de copia de seguridad o almacén de copias de seguridad de destino.

Esta operación devuelve resultados en función del tipo de recurso utilizado en el valor de `resourceArn`. Por ejemplo, los puntos de recuperación de Amazon DynamoDB con configuración avanzada tienen un ARN (nombre de recurso de Amazon) que comienza por `arn:aws:backup`. Los puntos de recuperación (copias de seguridad) de DynamoDB sin la configuración avanzada activada tienen un ARN que comienza por `arn:aws:dynamodb`.

Cuando se llama a esta operación y se incluyen valores de `resourceArn` que tienen un ARN distinto de `arn:aws:backup`, es posible que devuelva una de las excepciones que se enumera a continuación. Para evitar esta excepción, incluya únicamente los valores que representen los tipos de recursos completamente administrados por AWS Backup. Estos valores tienen un ARN que comienza por `arn:aws:backup` y se incluyen en la tabla [Disponibilidad de características por recurso](#).

Sintaxis de la solicitud

```
GET /tags/resourceArn?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[MaxResults](#)

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

[resourceArn](#)

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un recurso. El formato del ARN depende del tipo de recurso. Los destinos válidos de `ListTags` son los puntos de recuperación, los planes de copia de seguridad y los almacenes de copias de seguridad.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "Tags": {
    "string" : "string"
  }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

[Tags](#)

Información acerca de las etiquetas.

Tipo: mapa de cadena a cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ListTieringConfigurations

Servicio: AWS Backup

Devuelve una lista de configuraciones de estratificación.

Sintaxis de la solicitud

```
GET /tiering-configurations/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[MaxResults](#)

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "TieringConfigurations": [
    {
      "BackupVaultName": "string",
      "CreationTime": number,
      "LastUpdatedTime": number,
      "TieringConfigurationArn": "string",
```

```
    "TieringConfigurationName": "string"  
  }  
]  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

[TieringConfigurations](#)

Un conjunto de configuraciones de estratificación devueltas por la `ListTieringConfigurations` llamada.

Tipo: matriz de objetos [TieringConfigurationsListMember](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

`InvalidParameterValueException`

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

PutBackupVaultAccessPolicy

Servicio: AWS Backup

Establece una política basada en recursos que se utiliza para administrar los permisos de acceso en el almacén de copias de seguridad de destino. Requiere un nombre de almacén de copias de seguridad y un documento de política de acceso en formato JSON.

Sintaxis de la solicitud

```
PUT /backup-vaults/backupVaultName/access-policy HTTP/1.1
Content-type: application/json

{
  "Policy": "string"
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[backupVaultName](#)

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[Policy](#)

El documento de política de acceso al almacén de copias de seguridad en formato JSON.

Tipo: cadena

Requerido: no

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

PutBackupVaultLockConfiguration

Servicio: AWS Backup

Aplica el Bloqueo de almacenes de AWS Backup a un almacén de copias de seguridad, lo que impide que se intente eliminar cualquier punto de recuperación almacenado o creado en un almacén de copias de seguridad. El bloqueo de almacenes también impide los intentos de actualizar la política de ciclo de vida que controla el periodo de retención de cualquier punto de recuperación almacenado actualmente en un almacén de copias de seguridad. Si se especifica, el bloqueo de almacenes impone un periodo de retención mínimo y máximo a los futuros trabajos de copia y copia de seguridad que tengan como destino un almacén de copias de seguridad.

Note

Cohasset Associates ha evaluado el uso del Bloqueo de almacenes de AWS Backup en entornos sujetos a las normativas SEC 17a-4, CFTC y FINRA. Para obtener más información acerca de cómo el Bloqueo de almacenes de AWS Backup está relacionado con estas regulaciones, consulte la [Cohasset Associates Compliance Assessment](#).

Para obtener más información, consulte [Bloqueo de almacenes de AWS Backup](#).

Sintaxis de la solicitud

```
PUT /backup-vaults/backupVaultName/vault-lock HTTP/1.1
Content-type: application/json

{
  "ChangeableForDays": number,
  "MaxRetentionDays": number,
  "MinRetentionDays": number
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[backupVaultName](#)

La configuración del Bloqueo de almacenes de AWS Backup que especifica el nombre del almacén de copias de seguridad que protege.

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[ChangeableForDays](#)

La configuración de bloqueo de almacenes de AWS Backup que especifica el número de días antes de la fecha de bloqueo. Por ejemplo, si se fija `ChangeableForDays` en 30 el 1 de enero de 2022 a las 20:00 UTC, la fecha de bloqueo será el 31 de enero de 2022 a las 20:00 UTC.

AWS Backup impone un periodo de reflexión de 72 horas antes de que el bloqueo de almacenes surta efecto y se convierta en inmutable. Por tanto, debe establecer `ChangeableForDays` a 3 o mayor.

Antes de la fecha de bloqueo, puede eliminar el bloqueo de almacenes mediante `DeleteBackupVaultLockConfiguration` o cambiar la configuración de este mediante `PutBackupVaultLockConfiguration`. A partir de la fecha de bloqueo, el bloqueo de almacenes pasa a ser inmutable y no se puede cambiar ni eliminar.

Si no se especifica este parámetro, puede eliminar el bloqueo de almacenes mediante `DeleteBackupVaultLockConfiguration` o cambiar la configuración del bloqueo de almacenes mediante `PutBackupVaultLockConfiguration` en cualquier momento.

Tipo: Long

Obligatorio: no

[MaxRetentionDays](#)

La configuración de bloqueo de almacenes de AWS Backup que especifica el periodo máximo de retención durante el que el almacén retiene sus puntos de recuperación. Esta configuración puede resultar útil si, por ejemplo, las políticas de su organización requieren que destruya ciertos datos después de retenerlos durante cuatro años (1460 días).

Si no se incluye este parámetro, el bloqueo de almacenes no impone un periodo de retención máximo en los puntos de recuperación del almacén. Si este parámetro se incluye sin un valor, el bloqueo de almacenes no aplicará un periodo de retención máximo.

Si se especifica este parámetro, cualquier trabajo de copia de seguridad o copia en el almacén debe tener una política de ciclo de vida con un periodo de retención igual o inferior al periodo de retención máximo. Si el periodo de retención del trabajo es superior a ese periodo de retención máximo, el almacén falla el trabajo de copia de seguridad o de copia de seguridad, y deberá modificar la configuración del ciclo de vida o utilizar un almacén diferente. El periodo de retención máximo más largo que puede especificar es de 36 500 días (aproximadamente 100 años). Los puntos de recuperación ya guardados en el almacén antes del bloqueo del mismo no se ven afectados.

Tipo: Long

Obligatorio: no

MinRetentionDays

La configuración de bloqueo de almacenes de AWS Backup que especifica el periodo de retención mínimo durante el cual el almacén retiene sus puntos de recuperación. Esta configuración puede ser útil si, por ejemplo, las políticas de su organización requieren que se retengan ciertos datos durante al menos siete años (2555 días).

Este parámetro es obligatorio cuando se crea un bloqueo de bóveda mediante él AWS CloudFormation; de lo contrario, este parámetro es opcional. Si no se especifica este parámetro, el bloqueo del almacén no impondrá un periodo mínimo de retención.

Si se especifica este parámetro, cualquier trabajo de copia de seguridad o copia en el almacén debe tener una política de ciclo de vida con un periodo de retención igual o superior al periodo de retención mínimo. Si el periodo de retención del trabajo es más corto que ese periodo de retención mínimo, el almacén no supera ese trabajo de copia o copia, y debe modificar la configuración del ciclo de vida o usar un almacén diferente. El periodo de retención mínimo más corto que puede especificar es de 1 día. Los puntos de recuperación ya guardados en el almacén antes del bloqueo del mismo no se ven afectados.

Tipo: Long

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

PutBackupVaultNotifications

Servicio: AWS Backup

Activa las notificaciones en un almacén de copias de seguridad para el tema y los eventos especificados.

Sintaxis de la solicitud

```
PUT /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
Content-type: application/json

{
  "BackupVaultEvents": [ "string" ],
  "SNSTopicArn": "string"
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

BackupVaultEvents

Una matriz de eventos que indica el estado de los trabajos para realizar copias de seguridad de recursos en el almacén de copia de seguridad. Para ver la lista de eventos compatibles, casos de uso habituales y ejemplos de código, consulte [Opciones de notificación con AWS Backup](#).

 Note

La siguiente lista incluye eventos compatibles y obsoletos que ya no se utilizan (como referencia). Los eventos obsoletos no devolverán estados ni notificaciones.

Tipo: matriz de cadenas

Valores válidos: BACKUP_JOB_STARTED | BACKUP_JOB_COMPLETED |
BACKUP_JOB_SUCCESSFUL | BACKUP_JOB_FAILED | BACKUP_JOB_EXPIRED |
RESTORE_JOB_STARTED | RESTORE_JOB_COMPLETED | RESTORE_JOB_SUCCESSFUL
| RESTORE_JOB_FAILED | COPY_JOB_STARTED | COPY_JOB_SUCCESSFUL |
COPY_JOB_FAILED | RECOVERY_POINT_MODIFIED | BACKUP_PLAN_CREATED
| BACKUP_PLAN_MODIFIED | S3_BACKUP_OBJECT_FAILED |
S3_RESTORE_OBJECT_FAILED | CONTINUOUS_BACKUP_INTERRUPTED |
RECOVERY_POINT_INDEX_COMPLETED | RECOVERY_POINT_INDEX_DELETED |
RECOVERY_POINT_INDEXING_FAILED

Obligatorio: sí

SNSTopicArn

El nombre de recurso de Amazon (ARN) que especifica el tema de los eventos de un almacén de copias de seguridad; por ejemplo, `arn:aws:sns:us-west-2:111122223333:MyVaultTopic`.

Tipo: cadena

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

PutRestoreValidationResult

Servicio: AWS Backup

Esta solicitud permite enviar los resultados de validación de pruebas de restauración independientes que se ejecutan automáticamente. RestoreJobId y ValidationStatus son obligatorios. Si lo desea, puede introducir un ValidationStatusMessage.

Sintaxis de la solicitud

```
PUT /restore-jobs/restoreJobId/validations HTTP/1.1
Content-type: application/json

{
  "ValidationStatus": "string",
  "ValidationStatusMessage": "string"
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

restoreJobId

Es un identificador único de un trabajo de restauración de AWS Backup.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

ValidationStatus

El estado de validación de la restauración.

Tipo: cadena

Valores válidos: FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING

Obligatorio: sí

ValidationStatusMessage

Es una cadena de mensaje opcional que puede introducir para describir el estado de validación de la prueba de restauración.

Tipo: cadena

Requerido: no

Sintaxis de la respuesta

```
HTTP/1.1 204
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 204 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)

- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

RevokeRestoreAccessBackupVault

Servicio: AWS Backup

Revoca el acceso a un almacén de copias de seguridad con acceso a la restauración, lo que elimina la posibilidad de restaurar a partir de sus puntos de recuperación y elimina el almacén de forma permanente.

Sintaxis de la solicitud

```
DELETE /logically-air-gapped-backup-vaults/backupVaultName/restore-access-backup-vaults/restoreAccessBackupVaultArn?requesterComment=RequesterComment HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[backupVaultName](#)

Es el nombre del almacén de copias de seguridad de origen asociado al almacén de copias de seguridad con acceso a la restauración que se va a revocar.

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: sí

[RequesterComment](#)

Es un comentario que explica el motivo de la revocación del acceso al almacén de copias de seguridad con acceso a la restauración.

[restoreAccessBackupVaultArn](#)

Es el ARN del almacén de copias de seguridad con acceso a la restauración que se va a revocar.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

StartBackupJob

Servicio: AWS Backup

Inicia un trabajo de copia de seguridad bajo demanda para el recurso especificado.

Sintaxis de la solicitud

```
PUT /backup-jobs HTTP/1.1
Content-type: application/json

{
  "BackupOptions": {
    "string" : "string"
  },
  "BackupVaultName": "string",
  "CompleteWindowMinutes": number,
  "IamRoleArn": "string",
  "IdempotencyToken": "string",
  "Index": "string",
  "Lifecycle": {
    "DeleteAfterDays": number,
    "DeleteAfterEvent": "string",
    "MoveToColdStorageAfterDays": number,
    "OptInToArchiveForSupportedResources": boolean
  },
  "LogicallyAirGappedBackupVaultArn": "string",
  "RecoveryPointTags": {
    "string" : "string"
  },
  "ResourceArn": "string",
  "StartWindowMinutes": number
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[BackupOptions](#)

La opción de copia de seguridad para un recurso seleccionado. Esta opción solo está disponible para los trabajos de copia de seguridad de Windows Volume Shadow Copy Service (VSS).

Valores válidos: configure "WindowsVSS": "enabled" para habilitar la opción de copia de seguridad de WindowsVSS y crear una copia de seguridad de Windows VSS. Configure "WindowsVSS": "disabled" para crear una copia de seguridad normal. La opción WindowsVSS no está habilitada de forma predeterminada.

Tipo: mapa de cadena a cadena

Patrón de clave: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Patrón de valores: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatorio: no

[BackupVaultName](#)

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\.]{2,50}$`

Obligatorio: sí

[CompleteWindowMinutes](#)

Un valor en minutos durante el cual debe completarse una copia de seguridad que se haya iniciado correctamente o, de lo contrario, AWS Backup cancelará el trabajo. Este valor es opcional. Este valor comienza la cuenta regresiva a partir del momento en que se programó la copia de seguridad. No agrega tiempo adicional para StartWindowMinutes o si la copia de seguridad se inició más tarde de lo programado.

Como StartWindowMinutes, este parámetro tiene un valor máximo de 100 años (52 560 000 minutos).

Tipo: largo

Obligatorio: no

[IamRoleArn](#)

Especifica el ARN del rol de IAM utilizado para crear el punto de recuperación de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

Obligatorio: sí

[IdempotencyToken](#)

Una cadena elegida por el cliente que puede utilizar para distinguir entre llamadas a `StartBackupJob` que, de otro modo, serían idénticas. Si se vuelve a intentar una solicitud correcta con el mismo token de idempotencia, aparece un mensaje de confirmación y no se realiza ninguna acción.

Tipo: cadena

Requerido: no

[Index](#)

Incluya este parámetro para activar la creación de índices si su trabajo de copia de seguridad tiene un tipo de recurso que admite índices de copia de seguridad.

Los tipos de recurso que admiten índices de copia de seguridad son:

- EBS para Amazon Elastic Block Store (EBS)
- S3 para Amazon Simple Storage Service (Amazon S3)

El índice puede tener uno o dos valores posibles, `ENABLED` o `DISABLED`.

Para crear un índice de copias de seguridad para un punto de recuperación `ACTIVE` elegible que aún no tiene un índice de copia de seguridad, establezca el valor en `ENABLED`.

Para eliminar un índice de copias de seguridad, defina el valor en `DISABLED`.

Tipo: cadena

Valores válidos: `ENABLED` | `DISABLED`

Obligatorio: no

Lifecycle

El ciclo de vida define cuándo un recurso protegido pasa a almacenamiento en frío y cuándo caduca. AWS Backup realizará la transición y caducará las copias de seguridad automáticamente según el ciclo de vida que usted defina.

Las copias de seguridad que se transfieran al almacenamiento en frío deben almacenarse en un almacenamiento en frío durante un mínimo de 90 días. Por lo tanto, el valor de retención debe tener 90 días más que el valor del número de días tras los cuales se transferirá al almacenamiento en frío. El valor de “número de días tras los cuales migrará a almacenamiento en frío” no puede cambiarse una vez que se ha migrado una copia de seguridad al almacenamiento en frío.

Los tipos de recursos que pueden pasar al almacenamiento en frío se enumeran en la tabla [Disponibilidad de funciones por recurso](#). AWS Backup omite esta expresión para otros tipos de recursos.

Este parámetro tiene un valor máximo de 100 años (36 500 días).

Tipo: objeto [Lifecycle](#)

Obligatorio: no

LogicallyAirGappedBackupVaultArn

El ARN de una bóveda con huecos de aire lógicos. El ARN debe estar en la misma cuenta y región. Si se proporcionan, los recursos compatibles totalmente gestionados realizan copias de seguridad directamente en un almacén aislado de forma lógica, mientras que otros recursos compatibles crean una instantánea temporal (facturable) en el almacén de respaldo y, a continuación, la copian en un almacén aislado de forma lógica. Los recursos no compatibles solo se respaldan en el almacén de respaldo especificado.

Tipo: cadena

Requerido: no

RecoveryPointTags

Las etiquetas para asignar a los recursos.

Tipo: mapa de cadena a cadena

Obligatorio: no

[ResourceArn](#)

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un recurso. El formato del ARN depende del tipo de recurso.

Tipo: cadena

Obligatorio: sí

[StartWindowMinutes](#)

Un valor en minutos después del que una copia de seguridad está programada antes de que se cancele el trabajo si no se ha iniciado correctamente. El valor es opcional y el valor predeterminado es 8 horas. Si se incluye este valor, debe ser de al menos 60 minutos para evitar errores.

Este parámetro tiene un valor máximo de 100 años (52 560 000 minutos).

Durante el intervalo de inicio, el estado del trabajo de copia de seguridad permanece en ese estado CREATED hasta que comience correctamente o hasta que se agote el tiempo del intervalo de inicio. Si dentro de la ventana de inicio, Time AWS Backup recibe un error que permite volver a intentar el trabajo, AWS Backup volverá a intentarlo automáticamente al menos cada 10 minutos hasta que la copia de seguridad comience correctamente (el estado del trabajo cambia a RUNNING) o hasta que el estado del trabajo cambie a EXPIRED (lo que se espera que ocurra cuando finalice el tiempo de la ventana de inicio).

Tipo: largo

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupJobId": "string",
  "CreationDate": number,
  "IsParent": boolean,
  "RecoveryPointArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[BackupJobId](#)

Identifica de forma exclusiva una solicitud para AWS Backup hacer una copia de seguridad de un recurso.

Tipo: cadena

[CreationDate](#)

La fecha y la hora en que se creó el trabajo de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

[IsParent](#)

Se trata de un valor booleano devuelto que indica que es un trabajo de copia de seguridad principal (compuesto).

Tipo: Booleano

[RecoveryPointArn](#)

Nota: Este campo solo se devuelve para los recursos avanzados de DynamoDB y Amazon EFS.

Un ARN que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Context

Type

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

StartCopyJob

Servicio: AWS Backup

Inicia un trabajo para crear una copia única del recurso especificado.

No admite copias de seguridad continuas.

Consulte [Reintentar tareas de copia](#) para obtener información sobre cómo se AWS Backup reintentan las operaciones de copia de tareas.

Sintaxis de la solicitud

```
PUT /copy-jobs HTTP/1.1
Content-type: application/json

{
  "DestinationBackupVaultArn": "string",
  "IamRoleArn": "string",
  "IdempotencyToken": "string",
  "Lifecycle": {
    "DeleteAfterDays": number,
    "DeleteAfterEvent": "string",
    "MoveToColdStorageAfterDays": number,
    "OptInToArchiveForSupportedResources": boolean
  },
  "RecoveryPointArn": "string",
  "SourceBackupVaultName": "string"
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[DestinationBackupVaultArn](#)

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un almacén de copias de seguridad de destino al que copiar; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

Obligatorio: sí

[IamRoleArn](#)

Especifica el ARN del rol de IAM utilizado para copiar el punto de recuperación de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

Obligatorio: sí

[IdempotencyToken](#)

Una cadena elegida por el cliente que puede utilizar para distinguir entre llamadas a `StartCopyJob` que, de otro modo, serían idénticas. Si se vuelve a intentar una solicitud correcta con el mismo token de idempotencia, aparece un mensaje de confirmación y no se realiza ninguna acción.

Tipo: cadena

Requerido: no

[Lifecycle](#)

Especifica el período, en días, antes de que un punto de recuperación se transfiera al almacenamiento en frío o se elimine.

Las copias de seguridad que se transfieran al almacenamiento en frío deben almacenarse en un almacenamiento en frío durante un mínimo de 90 días. Por lo tanto, en la consola, el valor de retención debe tener 90 días más que el valor del número de días tras los cuales se transferirá al almacenamiento en frío. El valor de "transition to cold after days" (número de días tras los cuales migrará a almacenamiento en frío) no puede cambiarse una vez que se ha migrado una copia de seguridad al almacenamiento en frío.

Los tipos de recursos que pueden pasar al almacenamiento en frío se enumeran en la tabla [Disponibilidad de funciones por recurso](#). AWS Backup omite esta expresión para otros tipos de recursos.

Para eliminar el ciclo de vida y los períodos de retención existentes y conservar los puntos de recuperación indefinidamente, especifique -1 para `MoveToColdStorageAfterDays` y `DeleteAfterDays`.

Tipo: objeto [Lifecycle](#)

Obligatorio: no

[RecoveryPointArn](#)

Un ARN que identifica de forma exclusiva un punto de recuperación para usarlo en el trabajo de copia; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1 B5E7-9EB0-435A-A80B-108B488B0D45. EB3`

Tipo: cadena

Obligatorio: sí

[SourceBackupVaultName](#)

El nombre de un contenedor de origen lógico donde se almacenan las copias de seguridad. Los almacenes de Backup se identifican con nombres que son exclusivos de la cuenta utilizada para crearlos y de la AWS región en la que se crearon.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "CopyJobId": "string",
  "CreationDate": number,
  "IsParent": boolean
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

CopyJobId

Identifica de forma exclusiva un trabajo de copia.

Tipo: cadena

CreationDate

La fecha y la hora en que se creó el trabajo de copia, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

IsParent

Se trata de un valor booleano devuelto que indica que es un trabajo de copia principal (compuesto).

Tipo: Booleano

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Context

Type

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

StartReportJob

Servicio: AWS Backup

Inicia un trabajo de informes bajo demanda para el plan de informes especificado.

Sintaxis de la solicitud

```
POST /audit/report-jobs/reportPlanName HTTP/1.1
Content-type: application/json

{
  "IdempotencyToken": "string"
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

reportPlanName

El nombre único de un plan de informes.

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: [a-zA-Z][_a-zA-Z0-9]*

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

IdempotencyToken

Una cadena elegida por el cliente que puede utilizar para distinguir entre llamadas a `StartReportJobInput` que, de otro modo, serían idénticas. Si se vuelve a intentar una solicitud correcta con el mismo token de idempotencia, aparece un mensaje de confirmación y no se realiza ninguna acción.

Tipo: cadena

Requerido: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "ReportJobId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[ReportJobId](#)

El identificador del trabajo de informes. Una única cadena cifrada en UTF-8, Unicode, generada aleatoriamente que tiene como máximo una longitud de 1024 bytes. El ID del trabajo de informes no se puede editar.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)

- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

StartRestoreJob

Servicio: AWS Backup

Recupera el recurso guardado identificado por un nombre de recurso de Amazon (ARN).

Sintaxis de la solicitud

```
PUT /restore-jobs HTTP/1.1
Content-type: application/json

{
  "CopySourceTagsToRestoredResource": boolean,
  "IamRoleArn": "string",
  "IdempotencyToken": "string",
  "Metadata": {
    "string" : "string"
  },
  "RecoveryPointArn": "string",
  "ResourceType": "string"
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

CopySourceTagsToRestoredResource

Se trata de un parámetro opcional. Si es igual a `True`, las etiquetas incluidas en la copia de seguridad se copiarán en el recurso restaurado.

Esto solo se puede aplicar a las copias de seguridad creadas mediante AWS Backup.

Tipo: Booleano

Obligatorio: no

IamRoleArn

El nombre de recurso de Amazon (ARN) del rol de IAM que AWS Backup utiliza para crear el recurso de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

Requerido: no

[IdempotencyToken](#)

Una cadena elegida por el cliente que puede utilizar para distinguir entre llamadas a `StartRestoreJob` que, de otro modo, serían idénticas. Si se vuelve a intentar una solicitud correcta con el mismo token de idempotencia, aparece un mensaje de confirmación y no se realiza ninguna acción.

Tipo: cadena

Requerido: no

[Metadata](#)

Un conjunto de pares clave-valor de metadatos.

Para obtener los metadatos de configuración de un recurso en el momento en que se realizó la copia de seguridad, solo tiene que llamar a `GetRecoveryPointRestoreMetadata`. Sin embargo, es posible que para restaurar un recurso se necesiten valores adicionales a los proporcionados por el recurso `GetRecoveryPointRestoreMetadata`. Por ejemplo, puede que tenga que proporcionar un nombre de recurso nuevo si el original ya existe.

Para obtener más información sobre los metadatos de cada recurso, consulte lo siguiente:

- [Metadata for Amazon Aurora](#)
- [Metadata for Amazon DocumentDB](#)
- [Metadata for AWS CloudFormation](#)
- [Metadata for Amazon DynamoDB](#)
- [Metadata for Amazon EBS](#)
- [Metadata for Amazon EC2](#)
- [Metadata for Amazon EFS](#)
- [Metadata for Amazon FSx](#)
- [Metadata for Amazon Neptune](#)
- [Metadata for Amazon RDS](#)
- [Metadata for Amazon Redshift](#)
- [Metadata for AWS Storage Gateway](#)

- [Metadata for Amazon S3](#)
- [Metadata for Amazon Timestream](#)
- [Metadata for virtual machines](#)

Tipo: mapa de cadena a cadena

Obligatorio: sí

[RecoveryPointArn](#)

Un ARN que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

Obligatorio: sí

[ResourceType](#)

Inicia un trabajo para restaurar un punto de recuperación para uno de los siguientes recursos:

- Aurora - Amazon Aurora
- DocumentDB - Amazon DocumentDB
- CloudFormation - AWS CloudFormation
- DynamoDB - Amazon DynamoDB
- EBS - Amazon Elastic Block Store
- EC2 - Amazon Elastic Compute Cloud
- EFS - Amazon Elastic File System
- FSx - Amazon FSx
- Neptune - Amazon Neptune
- RDS - Amazon Relational Database Service
- Redshift - Amazon Redshift
- Storage Gateway - AWS Storage Gateway
- S3 - Amazon Simple Storage Service
- Timestream - Amazon Timestream
- VirtualMachine - Máquinas virtuales

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "RestoreJobId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[RestoreJobId](#)

Identifica de forma exclusiva el trabajo que restaura un punto de recuperación.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

StartScanJob

Servicio: AWS Backup

Comienza a escanear trabajos en busca de recursos específicos.

Sintaxis de la solicitud

```
PUT /scan/job HTTP/1.1
Content-type: application/json

{
  "BackupVaultName": "string",
  "IamRoleArn": "string",
  "IdempotencyToken": "string",
  "MalwareScanner": "string",
  "RecoveryPointArn": "string",
  "ScanBaseRecoveryPointArn": "string",
  "ScanMode": "string",
  "ScannerRoleArn": "string"
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

BackupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de Backup se identifican con nombres que son exclusivos de la cuenta utilizada para crearlos y de la AWS región en la que se crearon.

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Tipo: cadena

Obligatorio: sí

[IamRoleArn](#)

Especifica el ARN del rol de IAM utilizado para crear el punto de recuperación de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

Obligatorio: sí

[IdempotencyToken](#)

Una cadena elegida por el cliente que puede utilizar para distinguir entre llamadas a `StartScanJob` que, de otro modo, serían idénticas. Si se vuelve a intentar una solicitud correcta con el mismo token de idempotencia, aparece un mensaje de confirmación y no se realiza ninguna acción.

Tipo: cadena

Requerido: no

[MalwareScanner](#)

Especifica el escáner de malware utilizado durante el trabajo de escaneo. Actualmente solo es compatible `GUARDDUTY`.

Tipo: cadena

Valores válidos: `GUARDDUTY`

Obligatorio: sí

[RecoveryPointArn](#)

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un punto de recuperación. Este es el punto de recuperación objetivo para un análisis completo. Si está realizando un análisis incremental, este será el punto de recuperación que se haya creado después de seleccionar el punto de recuperación base.

Tipo: cadena

Obligatorio: sí

[ScanBaseRecoveryPointArn](#)

Un ARN que identifica de forma exclusiva el punto de recuperación base que se utilizará para el escaneo incremental.

Tipo: cadena

Requerido: no

[ScanMode](#)

Especifica el tipo de escaneo que se utilizará para el trabajo de escaneo.

Incluye:

- `FULL_SCAN` Escaneará todo el linaje de datos de la copia de seguridad.
- `INCREMENTAL_SCAN` Escaneará la diferencia de datos entre el punto de recuperación objetivo y el ARN del punto de recuperación base.

Tipo: cadena

Valores válidos: `FULL_SCAN` | `INCREMENTAL_SCAN`

Obligatorio: sí

[ScannerRoleArn](#)

Especificó el ARN del rol del escáner de IAM.

Tipo: cadena

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 201
Content-type: application/json

{
  "CreationDate": number,
  "ScanJobId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 201.

El servicio devuelve los datos siguientes en formato JSON.

CreationDate

La fecha y la hora en que se creó el trabajo de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

ScanJobId

Identifica de forma exclusiva una solicitud para AWS Backup hacer una copia de seguridad de un recurso.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Context

Type

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

StopBackupJob

Servicio: AWS Backup

Intenta cancelar un trabajo para crear una copia de seguridad única de un recurso.

Esta acción no es compatible con los siguientes servicios:

- Amazon Aurora
- Amazon DocumentDB (con compatibilidad con MongoDB)
- Amazon FSx for Lustre
- Amazon FSx for ONTAP de NetApp
- Amazon FSx for OpenZFS
- Amazon FSx for Windows File Server
- Amazon Neptune
- Bases de datos de SAP HANA en instancias de Amazon EC2
- Amazon RDS

Sintaxis de la solicitud

```
POST /backup-jobs/backupJobId HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupJobId

Identifica de forma exclusiva una solicitud de AWS Backup para hacer una copia de seguridad de un recurso.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

TagResource

Servicio: AWS Backup

Asigna un conjunto de pares clave-valor a un recurso.

Sintaxis de la solicitud

```
POST /tags/resourceArn HTTP/1.1
Content-type: application/json

{
  "Tags": {
    "string" : "string"
  }
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

resourceArn

Es un ARN que identifica de forma unívoca un recurso.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

Tags

Pares clave-valor que se utiliza para ayudar a organizar los recursos. Puede asignar sus propios metadatos a los recursos que cree. Para mayor claridad, esta es la estructura para asignar etiquetas: [{"Key": "string", "Value": "string"}].

Tipo: mapa de cadena a cadena

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

UntagResource

Servicio: AWS Backup

Elimina un conjunto de pares clave-valor de un punto de recuperación, plan de copia de seguridad o almacén de copias de seguridad identificado por un nombre de recurso de Amazon (ARN).

Esta API no es compatible con los puntos de recuperación de tipos de recursos, incluidos Aurora y Amazon DocumentDB. Amazon EBS, Amazon FSx, Neptune y Amazon RDS.

Sintaxis de la solicitud

```
POST /untag/resourceArn HTTP/1.1
Content-type: application/json
```

```
{
  "TagKeyList": [ "string" ]
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

resourceArn

Un ARN que identifica de forma única a un recurso. El formato del ARN depende del tipo de recurso etiquetado.

Los ARN que no incluyen backup son incompatibles con el etiquetado. TagResource y UntagResource con ARN no válidos generarán un error. Un contenido de ARN aceptable puede ser `arn:aws:backup:us-east`. Un contenido de ARN no válido puede ser `arn:aws:ec2:us-east`.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

TagKeyList

Las claves para identificar qué etiquetas clave-valor se deben eliminar de un recurso.

Tipo: matriz de cadenas

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateBackupPlan

Servicio: AWS Backup

Actualiza el plan de copia de seguridad especificado. La nueva versión se identifica únicamente con su ID.

Sintaxis de la solicitud

POST /backup/plans/*backupPlanId* HTTP/1.1

Content-type: application/json

```
{
  "BackupPlan": {
    "AdvancedBackupSettings": [
      {
        "BackupOptions": {
          "string": "string"
        },
        "ResourceType": "string"
      }
    ],
    "BackupPlanName": "string",
    "Rules": [
      {
        "CompletionWindowMinutes": number,
        "CopyActions": [
          {
            "DestinationBackupVaultArn": "string",
            "Lifecycle": {
              "DeleteAfterDays": number,
              "DeleteAfterEvent": "string",
              "MoveToColdStorageAfterDays": number,
              "OptInToArchiveForSupportedResources": boolean
            }
          }
        ],
        "EnableContinuousBackup": boolean,
        "IndexActions": [
          {
            "ResourceTypes": [ "string" ]
          }
        ],
        "Lifecycle": {
```

```

        "DeleteAfterDays": number,
        "DeleteAfterEvent": "string",
        "MoveToColdStorageAfterDays": number,
        "OptInToArchiveForSupportedResources": boolean
    },
    "RecoveryPointTags": {
        "string" : "string"
    },
    "RuleName": "string",
    "ScanActions": [
        {
            "MalwareScanner": "string",
            "ScanMode": "string"
        }
    ],
    "ScheduleExpression": "string",
    "ScheduleExpressionTimezone": "string",
    "StartWindowMinutes": number,
    "TargetBackupVaultName": "string",
    "TargetLogicallyAirGappedBackupVaultArn": "string"
}
],
"ScanSettings": [
    {
        "MalwareScanner": "string",
        "ResourceTypes": [ "string" ],
        "ScannerRoleArn": "string"
    }
]
}
}

```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupPlanId

El ID del plan de copia de seguridad.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[BackupPlan](#)

El cuerpo de un plan de copia de seguridad. Incluye un BackupPlanName y uno o más conjuntos de Rules.

Tipo: objeto [BackupPlanInput](#)

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "AdvancedBackupSettings": [
    {
      "BackupOptions": {
        "string" : "string"
      },
      "ResourceType": "string"
    }
  ],
  "BackupPlanArn": "string",
  "BackupPlanId": "string",
  "CreationDate": number,
  "ScanSettings": [
    {
      "MalwareScanner": "string",
      "ResourceTypes": [ "string" ],
      "ScannerRoleArn": "string"
    }
  ],
  "VersionId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[AdvancedBackupSettings](#)

Contiene una lista de BackupOptions para cada tipo de recurso.

Tipo: matriz de objetos [AdvancedBackupSetting](#)

[BackupPlanArn](#)

Un nombre de recurso de Amazon (ARN) que identifica de forma única un plan de copia de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Tipo: cadena

[BackupPlanId](#)

Identifica de forma única un plan de copia de seguridad.

Tipo: cadena

[CreationDate](#)

La fecha y la hora en que se creó el plan de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de CreationDate tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

[ScanSettings](#)

Contiene la configuración de escaneo para el plan de respaldo e incluye el escáner de malware, los recursos seleccionados y la función del escáner.

Tipo: matriz de objetos [ScanSetting](#)

[VersionId](#)

Cadenas cifradas en UTF-8, Unicode, únicas, generadas aleatoriamente que tienen como máximo una longitud de 1024 bytes. Los ID de versión no se pueden editar.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateFramework

Servicio: AWS Backup

Actualiza el marco especificado.

Sintaxis de la solicitud

```
PUT /audit/frameworks/frameworkName HTTP/1.1
Content-type: application/json

{
  "FrameworkControls": [
    {
      "ControlInputParameters": [
        {
          "ParameterName": "string",
          "ParameterValue": "string"
        }
      ],
      "ControlName": "string",
      "ControlScope": {
        "ComplianceResourceIds": [ "string" ],
        "ComplianceResourceTypes": [ "string" ],
        "Tags": {
          "string" : "string"
        }
      }
    }
  ],
  "FrameworkDescription": "string",
  "IdempotencyToken": "string"
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

frameworkName

El nombre único de un marco. Este nombre debe contener entre 1 y 256 caracteres, comenzando por una letra, y contar con letras (a-z, A-Z), números (0-9) y guiones bajos (_).

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `[a-zA-Z][_a-zA-Z0-9]*`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[FrameworkControls](#)

Los controles que componen el marco. Cada control de la lista tiene un nombre, parámetros de entrada y alcance.

Tipo: matriz de objetos [FrameworkControl](#)

Obligatorio: no

[FrameworkDescription](#)

Una descripción opcional del marco con un máximo de 1024 caracteres.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `.*\S.*`

Obligatorio: no

[IdempotencyToken](#)

Una cadena elegida por el cliente que puede utilizar para distinguir entre llamadas a `UpdateFrameworkInput` que, de otro modo, serían idénticas. Si se vuelve a intentar una solicitud correcta con el mismo token de idempotencia, aparece un mensaje de confirmación y no se realiza ninguna acción.

Tipo: cadena

Requerido: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json
```

```
{
  "CreationTime": number,
  "FrameworkArn": "string",
  "FrameworkName": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

CreationTime

Es la fecha y la hora en que se creó un marco con la norma ISO 8601. El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, 2020-07-10T15:00:00.000-08:00 representa el 10 de julio de 2020 a las 15:00 h, 8 horas menos que UTC.

Tipo: marca temporal

FrameworkArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un recurso. El formato del ARN depende del tipo de recurso.

Tipo: cadena

FrameworkName

El nombre único de un marco. Este nombre debe contener entre 1 y 256 caracteres, comenzando por una letra, y contar con letras (a-z, A-Z), números (0-9) y guiones bajos (_).

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `[a-zA-Z][_a-zA-Z0-9]*`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AlreadyExistsException

El recurso ya existe.

Arn

Context

CreatorRequestId

Type

Código de estado HTTP: 400

ConflictException

AWS Backup no puede realizar la acción que ha solicitado hasta que termine de realizar una acción anterior. Inténtelo de nuevo más tarde.

Context

Type

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)

- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateGlobalSettings

Servicio: AWS Backup

Actualiza si la AWS cuenta está habilitada para la copia de seguridad multicuenta. Devuelve un error si la cuenta no es una cuenta de administración de Organizations. Utilice la API `DescribeGlobalSettings` para determinar la configuración actual.

Sintaxis de la solicitud

```
PUT /global-settings HTTP/1.1
Content-type: application/json

{
  "GlobalSettings": {
    "string" : "string"
  }
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[GlobalSettings](#)

Las entradas pueden ser:

Un valor para `isCrossAccountBackupEnabled` y una región. Ejemplo: `update-global-settings --global-settings isCrossAccountBackupEnabled=false --region us-west-2`.

Un valor para la aprobación de varias partes denominado MPA: `isMpaEnabled`. Los valores pueden ser `true` o `false`. Ejemplo: `update-global-settings --global-settings isMpaEnabled=false --region us-west-2`.

Un valor para la creación de roles vinculados a Backup Service-Linked, con el estilo. `isDelegatedAdministratorEnabled` Los valores pueden ser `true` o `false`. Ejemplo: `update-global-settings --global-settings isDelegatedAdministratorEnabled=false --region us-west-2`.

Tipo: mapa de cadena a cadena

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateRecoveryPointIndexSettings

Servicio: AWS Backup

Esta operación actualiza la configuración de un índice de puntos de recuperación.

Obligatorios: BackupVaultName, RecoveryPointArn y IAMRoleArn

Sintaxis de la solicitud

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/index HTTP/1.1
Content-type: application/json
```

```
{
  "IamRoleArn": "string",
  "Index": "string"
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región donde se crearon.

Los caracteres permitidos son: letras minúsculas, números y guiones.

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: sí

recoveryPointArn

Un ARN que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[IamRoleArn](#)

Especifica el ARN del rol de IAM utilizado para esta operación.

Por ejemplo, `arn:aws:iam::123456789012:role/S3Access`

Tipo: cadena

Requerido: no

[Index](#)

El índice puede tener uno o dos valores posibles, `ENABLED` o `DISABLED`.

Para crear un índice de copias de seguridad para un punto de recuperación `ACTIVE` elegible que aún no tiene un índice de copia de seguridad, establezca el valor en `ENABLED`.

Para eliminar un índice de copias de seguridad, defina el valor en `DISABLED`.

Tipo: cadena

Valores válidos: `ENABLED` | `DISABLED`

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupVaultName": "string",
  "Index": "string",
  "IndexStatus": "string",
  "RecoveryPointArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

BackupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región donde se crearon.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Index

El índice puede tener uno o dos valores posibles, ENABLED o DISABLED.

Un valor ENABLED significa que se ha creado un índice de copias de seguridad para un punto de recuperación ACTIVE elegible.

Un valor DISABLED significa que se ha eliminado un índice de copias de seguridad.

Tipo: cadena

Valores válidos: ENABLED | DISABLED

IndexStatus

Este es el estado actual del índice de copias de seguridad asociado al punto de recuperación especificado.

Los estados son: PENDING | ACTIVE | FAILED | DELETING

En una búsqueda se puede incluir un punto de recuperación con un índice con el estado ACTIVE.

Tipo: cadena

Valores válidos: PENDING | ACTIVE | FAILED | DELETING

RecoveryPointArn

Un ARN que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateRecoveryPointLifecycle

Servicio: AWS Backup

Establece el ciclo de vida de transferencia de un punto de recuperación.

El ciclo de vida define cuándo un recurso protegido pasa a almacenamiento en frío y cuándo caduca. AWS Backup cambia y vence las copias de seguridad automáticamente de acuerdo con el ciclo de vida que usted defina.

Los tipos de recursos que pueden pasar al almacenamiento en frío se muestran en la tabla [Disponibilidad de funciones por recurso](#). AWS Backup omite esta expresión para otros tipos de recursos.

Las copias de seguridad que se transfieran al almacenamiento en frío deben almacenarse en un almacenamiento en frío durante un mínimo de 90 días. Por lo tanto, el valor de retención debe tener 90 días más que el valor del número de días tras los cuales se transferirá al almacenamiento en frío. El valor de “número de días tras los cuales migrará a almacenamiento en frío” no puede cambiarse una vez que se ha migrado una copia de seguridad al almacenamiento en frío.

Important

Si su ciclo de vida utiliza actualmente los parámetros `DeleteAfterDays` y `MoveToColdStorageAfterDays`, incluya estos parámetros y sus valores cuando llame a esta operación. Si no los incluye, es posible que su plan se actualice con valores nulos.

Esta operación no admite copias de seguridad continuas.

Sintaxis de la solicitud

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
Content-type: application/json
```

```
{
  "Lifecycle": {
    "DeleteAfterDays": number,
    "DeleteAfterEvent": "string",
    "MoveToColdStorageAfterDays": number,
    "OptInToArchiveForSupportedResources": boolean
  }
}
```



```
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[backupVaultName](#)

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: sí

[recoveryPointArn](#)

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[Lifecycle](#)

El ciclo de vida define cuándo un recurso protegido pasa a almacenamiento en frío y cuándo caduca. AWS Backup cambia y vence las copias de seguridad automáticamente de acuerdo con el ciclo de vida que usted defina.

Las copias de seguridad que se transfieran al almacenamiento en frío deben almacenarse en un almacenamiento en frío durante un mínimo de 90 días. Por lo tanto, el valor de retención debe tener 90 días más que el valor del número de días tras los cuales se transferirá al almacenamiento en frío. El valor de “número de días tras los cuales migrará a almacenamiento en frío” no puede cambiarse una vez que se ha migrado una copia de seguridad al almacenamiento en frío.

Tipo: objeto [Lifecycle](#)

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupVaultArn": "string",
  "CalculatedLifecycle": {
    "DeleteAt": number,
    "MoveToColdStorageAt": number
  },
  "Lifecycle": {
    "DeleteAfterDays": number,
    "DeleteAfterEvent": "string",
    "MoveToColdStorageAfterDays": number,
    "OptInToArchiveForSupportedResources": boolean
  },
  "RecoveryPointArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[BackupVaultArn](#)

Un ARN que identifica de forma exclusiva un almacén de copias de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

[CalculatedLifecycle](#)

Un objeto `CalculatedLifecycle` que contiene las marcas temporales `MoveToColdStorageAt` y `DeleteAt`.

Tipo: objeto [CalculatedLifecycle](#)

Lifecycle

El ciclo de vida define cuándo un recurso protegido pasa a almacenamiento en frío y cuándo caduca. AWS Backup cambia y vence las copias de seguridad automáticamente de acuerdo con el ciclo de vida que usted defina.

Las copias de seguridad que se transfieran al almacenamiento en frío deben almacenarse en un almacenamiento en frío durante un mínimo de 90 días. Por lo tanto, el valor de retención debe tener 90 días más que el valor del número de días tras los cuales se transferirá al almacenamiento en frío. El valor de “número de días tras los cuales migrará a almacenamiento en frío” no puede cambiarse una vez que se ha migrado una copia de seguridad al almacenamiento en frío.

Los tipos de recursos que pueden pasar al almacenamiento en frío se enumeran en la tabla [Disponibilidad de funciones por recurso](#). AWS Backup omite esta expresión para otros tipos de recursos.

Tipo: objeto [Lifecycle](#)

RecoveryPointArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateRegionSettings

Servicio: AWS Backup

Actualiza la configuración actual de suscripción del servicio para la región.

Utilice la API `DescribeRegionSettings` para determinar los tipos de recursos compatibles.

Sintaxis de la solicitud

```
PUT /account-settings HTTP/1.1
Content-type: application/json

{
  "ResourceTypeManagementPreference": {
    "string" : boolean
  },
  "ResourceTypeOptInPreference": {
    "string" : boolean
  }
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[ResourceTypeManagementPreference](#)

Habilita o deshabilita la administración completa de AWS Backup de las copias de seguridad para un tipo de recurso. Para habilitar la administración completa de AWS Backup para DynamoDB junto con las [características avanzadas de copia de seguridad de DynamoDB de AWS Backup](#), siga el procedimiento para [habilitar la copia de seguridad avanzada de DynamoDB mediante programación](#).

Tipo: mapa de cadena a booleano

Patrón de clave: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatorio: no

[ResourceTypeOptInPreference](#)

Actualiza la lista de servicios junto con las preferencias de suscripción de la región.

Si las asignaciones de recursos se basan únicamente en etiquetas, se aplica la configuración de suscripción al servicio. Si un tipo de recurso se asigna explícitamente a un plan de copia de seguridad, como Amazon S3, Amazon EC2 o Amazon RDS, se incluirá en la copia de seguridad incluso si la suscripción no está habilitada para ese servicio en particular. Si en una asignación de recursos se especifican tanto el tipo de recurso como las etiquetas, el tipo de recurso especificado en el plan de copia de seguridad tiene prioridad sobre la condición de la etiqueta. En esta situación no se tiene en cuenta la configuración de suscripción al servicio.

Tipo: mapa de cadena a booleano

Patrón de clave: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateReportPlan

Servicio: AWS Backup

Actualiza el plan de informes especificado.

Sintaxis de la solicitud

```
PUT /audit/report-plans/reportPlanName HTTP/1.1
Content-type: application/json
```

```
{
  "IdempotencyToken": "string",
  "ReportDeliveryChannel": {
    "Formats": [ "string" ],
    "S3BucketName": "string",
    "S3KeyPrefix": "string"
  },
  "ReportPlanDescription": "string",
  "ReportSetting": {
    "Accounts": [ "string" ],
    "FrameworkArns": [ "string" ],
    "NumberOfFrameworks": number,
    "OrganizationUnits": [ "string" ],
    "Regions": [ "string" ],
    "ReportTemplate": "string"
  }
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

reportPlanName

El nombre único del plan de informes. Este nombre debe contener entre 1 y 256 caracteres, comenzando por una letra, y contar con letras (a-z, A-Z), números (0-9) y guiones bajos (_).

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: [a-zA-Z][_a-zA-Z0-9]*

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[IdempotencyToken](#)

Una cadena elegida por el cliente que puede utilizar para distinguir entre llamadas a `UpdateReportPlanInput` que, de otro modo, serían idénticas. Si se vuelve a intentar una solicitud correcta con el mismo token de idempotencia, aparece un mensaje de confirmación y no se realiza ninguna acción.

Tipo: cadena

Requerido: no

[ReportDeliveryChannel](#)

La información sobre dónde entregar sus informes, específicamente el nombre del bucket de Amazon S3, el prefijo de clave de S3 y los formatos de sus informes.

Tipo: objeto [ReportDeliveryChannel](#)

Obligatorio: no

[ReportPlanDescription](#)

Una descripción opcional del plan de informes con un máximo de 1024 caracteres.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `.*\S.*`

Obligatorio: no

[ReportSetting](#)

La plantilla para el informe. Los informes se crean mediante una plantilla. Las plantillas de informes son:

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT |
BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Si la plantilla de informe es `RESOURCE_COMPLIANCE_REPORT` o `CONTROL_COMPLIANCE_REPORT`, este recurso de la API también describe la cobertura de informes por Regiones de AWS y marcos.

Tipo: objeto [ReportSetting](#)

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "CreationTime": number,
  "ReportPlanArn": "string",
  "ReportPlanName": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[CreationTime](#)

La fecha y la hora en que se creó el plan de informes, en formato Unix y horario universal coordinado (UTC). El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

[ReportPlanArn](#)

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un recurso. El formato del ARN depende del tipo de recurso.

Tipo: cadena

[ReportPlanName](#)

El nombre único del plan de informes.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: [a-zA-Z][_a-zA-Z0-9]*

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

ConflictException

AWS Backup no puede realizar la acción que ha solicitado hasta que termine de realizar una acción anterior. Inténtelo de nuevo más tarde.

Context

Type

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateRestoreTestingPlan

Servicio: AWS Backup

Esta solicitud enviará los cambios al plan de prueba de restauración especificado.

RestoreTestingPlanName no se puede actualizar después de crearlo.

RecoveryPointSelection puede contener:

- Algorithm
- ExcludeVaults
- IncludeVaults
- RecoveryPointTypes
- SelectionWindowDays

Sintaxis de la solicitud

```
PUT /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
```

```
Content-type: application/json
```

```
{
  "RestoreTestingPlan": {
    "RecoveryPointSelection": {
      "Algorithm": "string",
      "ExcludeVaults": [ "string" ],
      "IncludeVaults": [ "string" ],
      "RecoveryPointTypes": [ "string" ],
      "SelectionWindowDays": number
    },
    "ScheduleExpression": "string",
    "ScheduleExpressionTimezone": "string",
    "StartWindowHours": number
  }
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[RestoreTestingPlanName](#)

El nombre del plan de prueba de restauración.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[RestoreTestingPlan](#)

Especifica el cuerpo de un plan de prueba de restauración.

Tipo: objeto [RestoreTestingPlanForUpdate](#)

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "CreationTime": number,
  "RestoreTestingPlanArn": "string",
  "RestoreTestingPlanName": "string",
  "UpdateTime": number
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[CreationTime](#)

El momento en que se creó el plan de prueba de recursos.

Tipo: marca temporal

[RestoreTestingPlanArn](#)

ARN (Amazon Resource Name) único del plan de prueba de restauración.

Tipo: cadena

RestoreTestingPlanName

El nombre no se puede cambiar después de crear el plan. El nombre consta de únicamente de caracteres alfanuméricos y guiones bajos. La longitud máxima es 50.

Tipo: cadena

UpdateTime

La hora en la que se completó la actualización del plan de prueba de restauración.

Tipo: marca temporal

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

ConflictException

AWS Backup no puede realizar la acción que ha solicitado hasta que termine de realizar una acción anterior. Inténtelo de nuevo más tarde.

Context

Type

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)

- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateRestoreTestingSelection

Servicio: AWS Backup

Actualiza la selección de pruebas de restauración especificada.

La mayoría de los elementos, salvo el `RestoreTestingSelectionName`, se pueden actualizar con esta solicitud.

Puede utilizar ARN de recursos protegidos o condiciones, pero no ambos.

Sintaxis de la solicitud

```
PUT /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
Content-type: application/json
```

```
{
  "RestoreTestingSelection": {
    "IamRoleArn": "string",
    "ProtectedResourceArns": [ "string" ],
    "ProtectedResourceConditions": {
      "StringEquals": [
        {
          "Key": "string",
          "Value": "string"
        }
      ],
      "StringNotEquals": [
        {
          "Key": "string",
          "Value": "string"
        }
      ]
    },
    "RestoreMetadataOverrides": {
      "string" : "string"
    },
    "ValidationWindowHours": number
  }
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[RestoreTestingPlanName](#)

El nombre del plan de prueba de restauración es obligatorio para actualizar el plan de prueba indicado.

Obligatorio: sí

[RestoreTestingSelectionName](#)

El nombre de la selección de pruebas de restauración obligatorias que desea actualizar.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[RestoreTestingSelection](#)

Para actualizar la selección de pruebas de restauración puede utilizar ARN de recursos protegidos o condiciones, pero no ambos. Es decir, si su selección tiene `ProtectedResourceArns`, no podrá solicitar una actualización con el parámetro `ProtectedResourceConditions`.

Tipo: objeto [RestoreTestingSelectionForUpdate](#)

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "CreationTime": number,
  "RestoreTestingPlanArn": "string",
  "RestoreTestingPlanName": "string",
  "RestoreTestingSelectionName": "string",
```

```
"UpdateTime": number
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[CreationTime](#)

La hora en la que la selección de pruebas de recursos se actualizó correctamente.

Tipo: marca temporal

[RestoreTestingPlanArn](#)

Cadena única que es el nombre del plan de prueba de restauración.

Tipo: cadena

[RestoreTestingPlanName](#)

El plan de prueba de restauración al que está asociada la selección de pruebas de restauración actualizada.

Tipo: cadena

[RestoreTestingSelectionName](#)

El nombre de la selección de pruebas de restauración devuelta.

Tipo: cadena

[UpdateTime](#)

La hora en la que se completó la actualización de la selección de pruebas de restauración.

Tipo: marca temporal

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

ConflictException

AWS Backup no puede realizar la acción que ha solicitado hasta que termine de realizar una acción anterior. Inténtelo de nuevo más tarde.

Context

Type

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateTieringConfiguration

Servicio: AWS Backup

Esta solicitud enviará los cambios a la configuración de estratificación especificada. TieringConfigurationName no se puede actualizar una vez creada.

ResourceSelection puede contener:

- Resources
- TieringDownSettingsInDays
- ResourceType

Sintaxis de la solicitud

```
PUT /tiering-configurations/tieringConfigurationName HTTP/1.1
Content-type: application/json

{
  "TieringConfiguration": {
    "BackupVaultName": "string",
    "ResourceSelection": [
      {
        "Resources": [ "string" ],
        "ResourceType": "string",
        "TieringDownSettingsInDays": number
      }
    ]
  }
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

tieringConfigurationName

El nombre de la configuración de estratificación que se va a actualizar.

Patrón: `^[a-zA-Z0-9_]{1,200}$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[TieringConfiguration](#)

Especifica el cuerpo de una configuración de estratificación.

Tipo: objeto [TieringConfigurationInputForUpdate](#)

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "CreationTime": number,
  "LastUpdatedTime": number,
  "TieringConfigurationArn": "string",
  "TieringConfigurationName": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[CreationTime](#)

Fecha y hora en que se creó una configuración de organización por niveles, en formato Unix y en hora universal coordinada (UTC). El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

[LastUpdatedTime](#)

Fecha y hora en que se actualizó la configuración de organización por niveles, en formato Unix y en hora universal coordinada (UTC). El valor de `LastUpdatedTime` tiene una precisión de

milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

[TieringConfigurationArn](#)

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva la configuración de estratificación actualizada.

Tipo: cadena

[TieringConfigurationName](#)

Esta cadena única es el nombre de la configuración de estratificación.

Tipo: cadena

Patrón: `^[a-zA-Z0-9_]{1,200}$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AlreadyExistsException

El recurso ya existe.

Arn

Context

CreatorRequestId

Type

Código de estado HTTP: 400

ConflictException

AWS Backup no puede realizar la acción que ha solicitado hasta que termine de realizar una acción anterior. Inténtelo de nuevo más tarde.

Context

Type

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Context

Type

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Context

Type

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Context

Type

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Context

Type

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Context

Type

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

AWS Backup gateway

AWS Backup gateway admiten las siguientes acciones:

- [AssociateGatewayToServer](#)
- [CreateGateway](#)

- [DeleteGateway](#)
- [DeleteHypervisor](#)
- [DisassociateGatewayFromServer](#)
- [GetBandwidthRateLimitSchedule](#)
- [GetGateway](#)
- [GetHypervisor](#)
- [GetHypervisorPropertyMappings](#)
- [GetVirtualMachine](#)
- [ImportHypervisorConfiguration](#)
- [ListGateways](#)
- [ListHypervisors](#)
- [ListTagsForResource](#)
- [ListVirtualMachines](#)
- [PutBandwidthRateLimitSchedule](#)
- [PutHypervisorPropertyMappings](#)
- [PutMaintenanceStartTime](#)
- [StartVirtualMachinesMetadataSync](#)
- [TagResource](#)
- [TestHypervisorConfiguration](#)
- [UntagResource](#)
- [UpdateGatewayInformation](#)
- [UpdateGatewaySoftwareNow](#)
- [UpdateHypervisor](#)

AssociateGatewayToServer

Servicio: AWS Backup gateway

Asocia una puerta de enlace de copia de seguridad a su servidor. Tras completar el proceso de asociación, puede realizar copias de seguridad de sus máquinas virtuales y restaurarlas a través de la puerta de enlace.

Sintaxis de la solicitud

```
{
  "GatewayArn": "string",
  "ServerArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[GatewayArn](#)

El nombre de recurso de Amazon (ARN) de la puerta de enlace. Utilice la operación `ListGateways` para devolver una lista de puertas de enlace para su cuenta y Región de AWS.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 180 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\[/code>`

Obligatorio: sí

[ServerArn](#)

El nombre de recurso de Amazon (ARN) del servidor que aloja la máquina virtual.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\/[a-zA-Z-0-9]{1,63}`

Obligatorio: sí

Sintaxis de la respuesta

```
{
  "GatewayArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

GatewayArn

El nombre de recurso de Amazon (ARN) de una puerta de enlace.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 180 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\/[a-zA-Z-0-9]{1,63}`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

ConflictException

La operación no puede continuar porque no se admite.

ErrorCode

Es una descripción de los motivos por los que no se admite la operación.

Código de estado HTTP: 400

InternalServerError

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

ErrorCode

Es una descripción del error interno que se ha producido.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

ErrorCode

Es la descripción del motivo por el que no se ha encontrado el recurso.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

ErrorCode

Error: Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

ErrorCode

Es una descripción de la causa del error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

CreateGateway

Servicio: AWS Backup gateway

Crea una puerta de enlace de copia de seguridad. Después de crear una puerta de enlace, puede asociarla a un servidor mediante la operación AssociateGatewayToServer.

Sintaxis de la solicitud

```
{
  "ActivationKey": "string",
  "GatewayDisplayName": "string",
  "GatewayType": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[ActivationKey](#)

La clave de activación de la puerta de enlace creada.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 50 caracteres.

Patrón: [0-9a-zA-Z\ -]+

Obligatorio: sí

[GatewayDisplayName](#)

El nombre de visualización de la puerta de enlace creada.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `[a-zA-Z0-9-]*`

Obligatorio: sí

[GatewayType](#)

El tipo de puerta de enlace creada.

Tipo: cadena

Valores válidos: `BACKUP_VM`

Obligatorio: sí

[Tags](#)

Una lista de hasta 50 etiquetas que se asignarán a la puerta de enlace. Cada etiqueta es un par clave-valor.

Tipo: matriz de objetos [Tag](#)

Obligatorio: no

Sintaxis de la respuesta

```
{
  "GatewayArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[GatewayArn](#)

El nombre de recurso de Amazon (ARN) de la puerta de enlace que crea.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 180 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\\[a-zA-Z-0-9]+`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalServerError

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

ErrorCode

Es una descripción del error interno que se ha producido.

Código de estado HTTP: 500

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

ErrorCode

Error: Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

ErrorCode

Es una descripción de la causa del error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

DeleteGateway

Servicio: AWS Backup gateway

Elimina una puerta de enlace de copia de seguridad.

Sintaxis de la solicitud

```
{
  "GatewayArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[GatewayArn](#)

El nombre de recurso de Amazon (ARN) de la puerta de enlace que se va a eliminar.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 180 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\[/code>`

Obligatorio: sí

Sintaxis de la respuesta

```
{
  "GatewayArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace que ha eliminado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 180 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]){3}\/[a-zA-Z-0-9]+`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalServerError

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

ErrorCode

Es una descripción del error interno que se ha producido.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

ErrorCode

Es la descripción del motivo por el que no se ha encontrado el recurso.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

ErrorCode

Error: Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

ErrorCode

Es una descripción de la causa del error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

DeleteHypervisor

Servicio: AWS Backup gateway

Elimina un hipervisor.

Sintaxis de la solicitud

```
{  
  "HypervisorArn": "string"  
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[HypervisorArn](#)

El nombre de recurso de Amazon (ARN) del hipervisor que se va a eliminar.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\[/code>`

Obligatorio: sí

Sintaxis de la respuesta

```
{  
  "HypervisorArn": "string"  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

HypervisorArn

El nombre de recurso de Amazon (ARN) del hipervisor que ha eliminado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\/[a-zA-Z-0-9]{+}`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

La operación no puede continuar porque no tiene permisos suficientes.

ErrorCode

Es una descripción del motivo por el que no tiene permisos suficientes.

Código de estado HTTP: 400

ConflictException

La operación no puede continuar porque no se admite.

ErrorCode

Es una descripción de los motivos por los que no se admite la operación.

Código de estado HTTP: 400

InternalServerErrorException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

ErrorCode

Es una descripción del error interno que se ha producido.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

ErrorCode

Es la descripción del motivo por el que no se ha encontrado el recurso.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

ErrorCode

Error: Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

ErrorCode

Es una descripción de la causa del error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)

- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

DisassociateGatewayFromServer

Servicio: AWS Backup gateway

Disocia una puerta de enlace de copia de seguridad del servidor especificado. Una vez finalizado el proceso de disociación, la puerta de enlace ya no podrá acceder a las máquinas virtuales del servidor.

Sintaxis de la solicitud

```
{  
  "GatewayArn": "string"  
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace que se va a disociar.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 180 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\[/code>`

Obligatorio: sí

Sintaxis de la respuesta

```
{  
  "GatewayArn": "string"  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace que ha disociado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 180 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\[a-zA-Z-0-9]+`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

ConflictException

La operación no puede continuar porque no se admite.

ErrorCode

Es una descripción de los motivos por los que no se admite la operación.

Código de estado HTTP: 400

InternalServerError

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

ErrorCode

Es una descripción del error interno que se ha producido.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

ErrorCode

Es la descripción del motivo por el que no se ha encontrado el recurso.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

ErrorCode

Error: Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

ErrorCode

Es una descripción de la causa del error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

GetBandwidthRateLimitSchedule

Servicio: AWS Backup gateway

Recupera la programación de límite de velocidad de ancho de banda de una puerta de enlace especificada. De forma predeterminada, las puertas de enlace no tienen una programación de límite de velocidad de ancho de banda, lo que significa que no hay ningún límite de velocidad de ancho de banda en vigor. Use esto para obtener la programación de límite de velocidad de ancho de banda de una puerta de enlace.

Sintaxis de la solicitud

```
{
  "GatewayArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[GatewayArn](#)

El nombre de recurso de Amazon (ARN) de la puerta de enlace. Utilice la operación [ListGateways](#) para devolver una lista de puertas de enlace para su cuenta y Región de AWS.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 180 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\/[a-zA-Z-0-9]{+}`

Obligatorio: sí

Sintaxis de la respuesta

```
{
  "BandwidthRateLimitIntervals": [
    {
```



```

    "AverageUploadRateLimitInBitsPerSec": number,
    "DaysOfWeek": [ number ],
    "EndHourOfDay": number,
    "EndMinuteOfHour": number,
    "StartHourOfDay": number,
    "StartMinuteOfHour": number
  }
],
"GatewayArn": "string"
}

```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[BandwidthRateLimitIntervals](#)

Una matriz que contiene los intervalos de programación de límite de velocidad de ancho de banda para una puerta de enlace. Cuando no se ha programado ningún intervalo de límite de velocidad de ancho de banda, la matriz está vacía.

Tipo: matriz de objetos [BandwidthRateLimitInterval](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 20 artículos.

[GatewayArn](#)

El nombre de recurso de Amazon (ARN) de la puerta de enlace. Utilice la operación [ListGateways](#) para devolver una lista de puertas de enlace para su cuenta y Región de AWS.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 180 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\[/code>`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalServerError

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

ErrorCode

Es una descripción del error interno que se ha producido.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

ErrorCode

Es la descripción del motivo por el que no se ha encontrado el recurso.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

ErrorCode

Error: Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

ErrorCode

Es una descripción de la causa del error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

GetGateway

Servicio: AWS Backup gateway

Al proporcionar el ARN (nombre de recurso de Amazon), esta API devuelve la puerta de enlace.

Sintaxis de la solicitud

```
{  
  "GatewayArn": "string"  
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 180 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\[/code>`

Obligatorio: sí

Sintaxis de la respuesta

```
{  
  "Gateway": {  
    "GatewayArn": "string",  
    "GatewayDisplayName": "string",  
    "GatewayType": "string",  
    "HypervisorId": "string",  
    "LastSeenTime": number,  
    "MaintenanceStartTime": {  
      "DayOfMonth": number,
```

```
    "DayOfWeek": number,
    "HourOfDay": number,
    "MinuteOfHour": number
  },
  "NextUpdateAvailabilityTime": number,
  "VpcEndpoint": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[Gateway](#)

Al proporcionar el ARN (nombre de recurso de Amazon), esta API devuelve la puerta de enlace.

Tipo: objeto [GatewayDetails](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalServerError

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

ErrorCode

Es una descripción del error interno que se ha producido.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

ErrorCode

Es la descripción del motivo por el que no se ha encontrado el recurso.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

ErrorCode

Error: Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

ErrorCode

Es una descripción de la causa del error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

GetHypervisor

Servicio: AWS Backup gateway

Esta acción solicita información sobre el hipervisor especificado al que se conectará la puerta de enlace. Un hipervisor es un hardware, software o firmware que crea y administra máquinas virtuales y les asigna recursos.

Sintaxis de la solicitud

```
{  
  "HypervisorArn": "string"  
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[HypervisorArn](#)

El nombre de recurso de Amazon (ARN) del hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\\[a-zA-Z-0-9]+`

Obligatorio: sí

Sintaxis de la respuesta

```
{  
  "Hypervisor": {  
    "Host": "string",  
    "HypervisorArn": "string",  
    "KmsKeyArn": "string",  
    "LastSuccessfulMetadataSyncTime": number,  
  }
```

```
"LatestMetadataSyncStatus": "string",  
"LatestMetadataSyncStatusMessage": "string",  
"LogGroupArn": "string",  
"Name": "string",  
"State": "string"  
}  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[Hypervisor](#)

Detalles sobre el hipervisor solicitado.

Tipo: objeto [HypervisorDetails](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalServerError

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

ErrorCode

Es una descripción del error interno que se ha producido.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

ErrorCode

Es la descripción del motivo por el que no se ha encontrado el recurso.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

ErrorCode

Error: Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

ErrorCode

Es una descripción de la causa del error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

GetHypervisorPropertyMappings

Servicio: AWS Backup gateway

Esta acción recupera las asignaciones de propiedades del hipervisor especificado. La asignación de propiedades de un hipervisor muestra la relación entre las propiedades de la entidad disponibles en el hipervisor y las propiedades disponibles en AWS.

Sintaxis de la solicitud

```
{  
  "HypervisorArn": "string"  
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[HypervisorArn](#)

El nombre de recurso de Amazon (ARN) del hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Obligatorio: sí

Sintaxis de la respuesta

```
{  
  "HypervisorArn": "string",  
  "IamRoleArn": "string",  
  "VmwareToAwsTagMappings": [  
    {  
      "AwsTagKey": "string",  
      "AwsTagValue": "string",
```

```
    "VmwareCategory": "string",  
    "VmwareTagName": "string"  
  }  
]  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[HypervisorArn](#)

El nombre de recurso de Amazon (ARN) del hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

[IamRoleArn](#)

El nombre de recurso de Amazon (ARN) del rol de IAM.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 2048 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):iam:([0-9]+):role/(\S+)`

[VmwareToAwsTagMappings](#)

Esta es una visualización de las asignaciones de las etiquetas de VMware a las etiquetas de AWS.

Tipo: matriz de objetos [VmwareToAwsTagMapping](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalServerError

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

ErrorCode

Es una descripción del error interno que se ha producido.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

ErrorCode

Es la descripción del motivo por el que no se ha encontrado el recurso.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

ErrorCode

Error: Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

ErrorCode

Es una descripción de la causa del error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

GetVirtualMachine

Servicio: AWS Backup gateway

Al proporcionar el ARN (nombre de recurso de Amazon), esta API devuelve la máquina virtual.

Sintaxis de la solicitud

```
{
  "ResourceArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[ResourceArn](#)

El nombre de recurso de Amazon (ARN) de la máquina virtual.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\[/code>`

Obligatorio: sí

Sintaxis de la respuesta

```
{
  "VirtualMachine": {
    "HostName": "string",
    "HypervisorId": "string",
    "LastBackupDate": number,
    "Name": "string",
    "Path": "string",
    "ResourceArn": "string",
    "VmwareTags": [
```

```
{
  {
    "VmwareCategory": "string",
    "VmwareTagDescription": "string",
    "VmwareTagName": "string"
  }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[VirtualMachine](#)

Este objeto contiene los atributos básicos de las `VirtualMachine` contenidas en el resultado de `GetVirtualMachine`.

Tipo: objeto [VirtualMachineDetails](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalServerError

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

ErrorCode

Es una descripción del error interno que se ha producido.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

ErrorCode

Es la descripción del motivo por el que no se ha encontrado el recurso.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

ErrorCode

Error: Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

ErrorCode

Es una descripción de la causa del error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ImportHypervisorConfiguration

Servicio: AWS Backup gateway

Conéctese a un hipervisor importando su configuración.

Sintaxis de la solicitud

```
{
  "Host": "string",
  "KmsKeyArn": "string",
  "Name": "string",
  "Password": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "Username": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

Host

El host del servidor del hipervisor. Puede ser una dirección IP o un nombre de dominio completo (FQDN).

Tipo: cadena

Limitaciones de longitud: longitud mínima de 3. Longitud máxima de 128.

Patrón: . +

Obligatorio: sí

KmsKeyArn

El AWS Key Management Service para el hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)`

Obligatorio: no

Name

El nombre del hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `[a-zA-Z0-9-]*`

Obligatorio: sí

Password

La contraseña del hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `[-~]+`

Obligatorio: no

Tags

Las etiquetas de configuración del hipervisor que se van a importar.

Tipo: matriz de objetos [Tag](#)

Obligatorio: no

Username

El nombre de usuario del hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `[ -\\.0-\\[\\]-~]*[!-\\.0-\\[\\]-~][ -\\.0-\\[\\]-~]*`

Obligatorio: no

Sintaxis de la respuesta

```
{
  "HypervisorArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[HypervisorArn](#)

El nombre de recurso de Amazon (ARN) del hipervisor que ha disociado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\\/[a-zA-Z-0-9]{+}`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

La operación no puede continuar porque no tiene permisos suficientes.

ErrorCode

Es una descripción del motivo por el que no tiene permisos suficientes.

Código de estado HTTP: 400

ConflictException

La operación no puede continuar porque no se admite.

ErrorCode

Es una descripción de los motivos por los que no se admite la operación.

Código de estado HTTP: 400

InternalServerError

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

ErrorCode

Es una descripción del error interno que se ha producido.

Código de estado HTTP: 500

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

ErrorCode

Error: Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

ErrorCode

Es una descripción de la causa del error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ListGateways

Servicio: AWS Backup gateway

Enumera las puertas de enlace de copia de seguridad propiedad de una Cuenta de AWS en una Región de AWS. La lista obtenida se ordena por el nombre de recurso de Amazon (ARN) de la puerta de enlace.

Sintaxis de la solicitud

```
{
  "MaxResults": number,
  "NextToken": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[MaxResults](#)

El número máximo de puertas de enlace que se van a enumerar.

Tipo: número entero

Rango válido: valor mínimo de 1.

Obligatorio: no

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 1000 caracteres.

Patrón: . +

Obligatorio: no

Sintaxis de la respuesta

```
{
  "Gateways": [
    {
      "GatewayArn": "string",
      "GatewayDisplayName": "string",
      "GatewayType": "string",
      "HypervisorId": "string",
      "LastSeenTime": number
    }
  ],
  "NextToken": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Gateways

Una lista de sus puertas de enlace.

Tipo: matriz de objetos [Gateway](#)

NextToken

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos `maxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 1000 caracteres.

Patrón: . +

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalServerErrorException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

ErrorCode

Es una descripción del error interno que se ha producido.

Código de estado HTTP: 500

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

ErrorCode

Error: Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

ErrorCode

Es una descripción de la causa del error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)

- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ListHypervisors

Servicio: AWS Backup gateway

Enumera los hipervisores.

Sintaxis de la solicitud

```
{
  "MaxResults": number,
  "NextToken": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[MaxResults](#)

El número máximo de hipervisores que se van a enumerar.

Tipo: número entero

Rango válido: valor mínimo de 1.

Obligatorio: no

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos `maxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 1000 caracteres.

Patrón: `.+`

Obligatorio: no

Sintaxis de la respuesta

```
{
  "Hypervisors": [
    {
      "Host": "string",
      "HypervisorArn": "string",
      "KmsKeyArn": "string",
      "Name": "string",
      "State": "string"
    }
  ],
  "NextToken": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Hypervisors

Una lista de sus objetos Hypervisor, ordenados por sus nombres de recurso de Amazon (ARN).

Tipo: matriz de objetos [Hypervisor](#)

NextToken

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos `maxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 1000 caracteres.

Patrón: `.+`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalServerErrorException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

ErrorCode

Es una descripción del error interno que se ha producido.

Código de estado HTTP: 500

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

ErrorCode

Error: Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

ErrorCode

Es una descripción de la causa del error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)

- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ListTagsForResource

Servicio: AWS Backup gateway

Enumera las etiquetas aplicadas al recurso identificado por su nombre de recurso de Amazon (ARN).

Sintaxis de la solicitud

```
{  
  "ResourceArn": "string"  
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

ResourceArn

El nombre de recurso de Amazon (ARN) de las etiquetas del recurso a enumerar.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\[/code>`

Obligatorio: sí

Sintaxis de la respuesta

```
{  
  "ResourceArn": "string",  
  "Tags": [  
    {  
      "Key": "string",  
      "Value": "string"  
    }  
  ]  
}
```

```
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[ResourceArn](#)

El nombre de recurso de Amazon (ARN) de las etiquetas del recurso que ha enumerado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\[a-zA-Z-0-9\]+`

[Tags](#)

Una lista de las etiquetas del recurso.

Tipo: matriz de objetos [Tag](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalServerError

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

ErrorCode

Es una descripción del error interno que se ha producido.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

ErrorCode

Es la descripción del motivo por el que no se ha encontrado el recurso.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

ErrorCode

Error: Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

ErrorCode

Es una descripción de la causa del error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)

- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ListVirtualMachines

Servicio: AWS Backup gateway

Enumera sus máquinas virtuales.

Sintaxis de la solicitud

```
{
  "HypervisorArn": "string",
  "MaxResults": number,
  "NextToken": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[HypervisorArn](#)

El nombre de recurso de Amazon (ARN) del hipervisor conectado a la máquina virtual.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Obligatorio: no

[MaxResults](#)

El número máximo de máquinas virtuales que se van a enumerar.

Tipo: número entero

Rango válido: valor mínimo de 1.

Obligatorio: no

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos `maxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 1000 caracteres.

Patrón: `.+`

Obligatorio: no

Sintaxis de la respuesta

```
{
  "NextToken": "string",
  "VirtualMachines": [
    {
      "HostName": "string",
      "HypervisorId": "string",
      "LastBackupDate": number,
      "Name": "string",
      "Path": "string",
      "ResourceArn": "string"
    }
  ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[NextToken](#)

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos `maxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 1000 caracteres.

Patrón: . +

[VirtualMachines](#)

Una lista de sus objetos `VirtualMachine`, ordenados por sus nombres de recurso de Amazon (ARN).

Tipo: matriz de objetos [VirtualMachine](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalServerErrorException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

`ErrorCode`

Es una descripción del error interno que se ha producido.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

`ErrorCode`

Es la descripción del motivo por el que no se ha encontrado el recurso.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

`ErrorCode`

Error: Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

ErrorCode

Es una descripción de la causa del error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

PutBandwidthRateLimitSchedule

Servicio: AWS Backup gateway

Esta acción establece la programación de límite de velocidad de ancho de banda para una puerta de enlace especificada. De forma predeterminada, las puertas de enlace no tienen una programación de límite de velocidad de ancho de banda, lo que significa que no hay ningún límite de velocidad de ancho de banda en vigor. Use esto para iniciar la programación de límite de velocidad de ancho de banda de una puerta de enlace.

Sintaxis de la solicitud

```
{
  "BandwidthRateLimitIntervals": [
    {
      "AverageUploadRateLimitInBitsPerSec": number,
      "DaysOfWeek": [ number ],
      "EndHourOfDay": number,
      "EndMinuteOfHour": number,
      "StartHourOfDay": number,
      "StartMinuteOfHour": number
    }
  ],
  "GatewayArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[BandwidthRateLimitIntervals](#)

Una matriz que contiene los intervalos de programación de límite de velocidad de ancho de banda para una puerta de enlace. Cuando no se ha programado ningún intervalo de límite de velocidad de ancho de banda, la matriz está vacía.

Tipo: matriz de objetos [BandwidthRateLimitInterval](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 20 artículos.

Obligatorio: sí

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace. Utilice la operación [ListGateways](#) para devolver una lista de puertas de enlace para su cuenta y Región de AWS.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 180 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Obligatorio: sí

Sintaxis de la respuesta

```
{
  "GatewayArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace. Utilice la operación [ListGateways](#) para devolver una lista de puertas de enlace para su cuenta y Región de AWS.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 180 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalServerError

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

ErrorCode

Es una descripción del error interno que se ha producido.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

ErrorCode

Es la descripción del motivo por el que no se ha encontrado el recurso.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

ErrorCode

Error: Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

ErrorCode

Es una descripción de la causa del error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

PutHypervisorPropertyMappings

Servicio: AWS Backup gateway

Esta acción establece las asignaciones de propiedades del hipervisor especificado. La asignación de propiedades de un hipervisor muestra la relación entre las propiedades de la entidad disponibles en el hipervisor y las propiedades disponibles en AWS.

Sintaxis de la solicitud

```
{
  "HypervisorArn": "string",
  "IamRoleArn": "string",
  "VmwareToAwsTagMappings": [
    {
      "AwsTagKey": "string",
      "AwsTagValue": "string",
      "VmwareCategory": "string",
      "VmwareTagName": "string"
    }
  ]
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[HypervisorArn](#)

El nombre de recurso de Amazon (ARN) del hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\[/code>`

Obligatorio: sí

[IamRoleArn](#)

El nombre de recurso de Amazon (ARN) del rol de IAM.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 2048 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):iam:([0-9]+):role/(\S+)`

Obligatorio: sí

[VmwareToAwsTagMappings](#)

Esta acción solicita la asignación de las etiquetas de VMware a las etiquetas de AWS.

Tipo: matriz de objetos [VmwareToAwsTagMapping](#)

Obligatorio: sí

Sintaxis de la respuesta

```
{
  "HypervisorArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[HypervisorArn](#)

El nombre de recurso de Amazon (ARN) del hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

La operación no puede continuar porque no tiene permisos suficientes.

ErrorCode

Es una descripción del motivo por el que no tiene permisos suficientes.

Código de estado HTTP: 400

ConflictException

La operación no puede continuar porque no se admite.

ErrorCode

Es una descripción de los motivos por los que no se admite la operación.

Código de estado HTTP: 400

InternalServerError

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

ErrorCode

Es una descripción del error interno que se ha producido.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

ErrorCode

Es la descripción del motivo por el que no se ha encontrado el recurso.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

ErrorCode

Error: Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

ErrorCode

Es una descripción de la causa del error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

PutMaintenanceStartTime

Servicio: AWS Backup gateway

Establece la hora de inicio del mantenimiento de una puerta de enlace.

Sintaxis de la solicitud

```
{
  "DayOfMonth": number,
  "DayOfWeek": number,
  "GatewayArn": "string",
  "HourOfDay": number,
  "MinuteOfHour": number
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[DayOfMonth](#)

El día del mes de inicio del mantenimiento de una puerta de enlace.

Los valores válidos van de Sunday a Saturday.

Tipo: número entero

Rango válido: valor mínimo de 1. Valor máximo de 31.

Obligatorio: no

[DayOfWeek](#)

El día de la semana de inicio del mantenimiento de una puerta de enlace.

Tipo: número entero

Rango válido: valor mínimo de 0. Valor máximo de 6.

Obligatorio: no

[GatewayArn](#)

El nombre de recurso de Amazon (ARN) de la puerta de enlace, que se utiliza para especificar la hora de inicio del mantenimiento.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 180 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\/[a-zA-Z-0-9]{+}`

Obligatorio: sí

[HourOfDay](#)

La hora del día de inicio del mantenimiento de una puerta de enlace.

Tipo: número entero

Rango válido: valor mínimo de 0. Valor máximo de 23.

Obligatorio: sí

[MinuteOfHour](#)

El minuto de la hora de inicio del mantenimiento de una puerta de enlace.

Tipo: número entero

Rango válido: valor mínimo de 0. Valor máximo de 59.

Obligatorio: sí

Sintaxis de la respuesta

```
{
  "GatewayArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

GatewayArn

El nombre de recurso de Amazon (ARN) de una puerta de enlace para la que haya establecido la hora de inicio del mantenimiento.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 180 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]){3}\/[a-zA-Z-0-9]+`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

ConflictException

La operación no puede continuar porque no se admite.

ErrorCode

Es una descripción de los motivos por los que no se admite la operación.

Código de estado HTTP: 400

InternalServerError

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

ErrorCode

Es una descripción del error interno que se ha producido.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

ErrorCode

Es la descripción del motivo por el que no se ha encontrado el recurso.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

ErrorCode

Error: Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

ErrorCode

Es una descripción de la causa del error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

StartVirtualMachinesMetadataSync

Servicio: AWS Backup gateway

Esta acción envía una solicitud para sincronizar los metadatos en las máquinas virtuales especificadas.

Sintaxis de la solicitud

```
{  
  "HypervisorArn": "string"  
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[HypervisorArn](#)

El nombre de recurso de Amazon (ARN) del hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\[/code>`

Obligatorio: sí

Sintaxis de la respuesta

```
{  
  "HypervisorArn": "string"  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

HypervisorArn

El nombre de recurso de Amazon (ARN) del hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\[a-zA-Z-0-9]+`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

La operación no puede continuar porque no tiene permisos suficientes.

ErrorCode

Es una descripción del motivo por el que no tiene permisos suficientes.

Código de estado HTTP: 400

InternalServerError

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

ErrorCode

Es una descripción del error interno que se ha producido.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

ErrorCode

Es la descripción del motivo por el que no se ha encontrado el recurso.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

ErrorCode

Error: Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

ErrorCode

Es una descripción de la causa del error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

TagResource

Servicio: AWS Backup gateway

Etiqueta el recurso.

Sintaxis de la solicitud

```
{
  "ResourceARN": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[ResourceARN](#)

El nombre de recurso de Amazon (ARN) del recurso que se va a etiquetar.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\/[a-zA-Z-0-9]{+}`

Obligatorio: sí

[Tags](#)

Una lista de etiquetas que se asignarán al recurso.

Tipo: matriz de objetos [Tag](#)

Obligatorio: sí

Sintaxis de la respuesta

```
{  
  "ResourceARN": "string"  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[ResourceARN](#)

El nombre de recurso de Amazon (ARN) del recurso que ha etiquetado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\[a-zA-Z-0-9]+`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalServerError

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

ErrorCode

Es una descripción del error interno que se ha producido.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

ErrorCode

Es la descripción del motivo por el que no se ha encontrado el recurso.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

ErrorCode

Error: Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

ErrorCode

Es una descripción de la causa del error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)

- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

TestHypervisorConfiguration

Servicio: AWS Backup gateway

Prueba la configuración del hipervisor para validar que la puerta de enlace de copia de seguridad pueda conectarse con el hipervisor y sus recursos.

Sintaxis de la solicitud

```
{
  "GatewayArn": "string",
  "Host": "string",
  "Password": "string",
  "Username": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[GatewayArn](#)

El nombre de recurso de Amazon (ARN) de la puerta de enlace al hipervisor que se va a probar.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 180 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\/[a-zA-Z-0-9]{+}`

Obligatorio: sí

[Host](#)

El host del servidor del hipervisor. Puede ser una dirección IP o un nombre de dominio completo (FQDN).

Tipo: cadena

Limitaciones de longitud: longitud mínima de 3. Longitud máxima de 128.

Patrón: . +

Obligatorio: sí

Password

La contraseña del hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: [-~] +

Obligatorio: no

Username

El nombre de usuario del hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: [-\.\0-\[\] -~] * [!-\.\0-\[\] -~] [-\.\0-\[\] -~] *

Obligatorio: no

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

ConflictException

La operación no puede continuar porque no se admite.

ErrorCode

Es una descripción de los motivos por los que no se admite la operación.

Código de estado HTTP: 400

InternalServerError

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

ErrorCode

Es una descripción del error interno que se ha producido.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

ErrorCode

Es la descripción del motivo por el que no se ha encontrado el recurso.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

ErrorCode

Error: Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

ErrorCode

Es una descripción de la causa del error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

UntagResource

Servicio: AWS Backup gateway

Elimina etiquetas del recurso.

Sintaxis de la solicitud

```
{  
  "ResourceARN": "string",  
  "TagKeys": [ "string" ]  
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[ResourceARN](#)

El nombre de recurso de Amazon (ARN) del recurso del que se van a eliminar etiquetas.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Obligatorio: sí

[TagKeys](#)

La lista de claves de etiquetas que especifica las etiquetas que se van a eliminar.

Tipo: matriz de cadenas

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: `([\\p{L}\\p{Z}\\p{N}_.:\\/=+\\-@]*)`

Obligatorio: sí

Sintaxis de la respuesta

```
{  
  "ResourceARN": "string"  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[ResourceARN](#)

El nombre de recurso de Amazon (ARN) del recurso del que ha eliminado etiquetas.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\/[a-zA-Z-0-9]{+}`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalServerError

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

ErrorCode

Es una descripción del error interno que se ha producido.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

ErrorCode

Es la descripción del motivo por el que no se ha encontrado el recurso.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

ErrorCode

Error: Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

ErrorCode

Es una descripción de la causa del error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)

- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateGatewayInformation

Servicio: AWS Backup gateway

Actualiza el nombre de una puerta de enlace. Especifique la puerta de enlace que desea actualizar mediante el nombre de recurso de Amazon (ARN) de la puerta de enlace en su solicitud.

Sintaxis de la solicitud

```
{  
  "GatewayArn": "string",  
  "GatewayDisplayName": "string"  
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[GatewayArn](#)

El nombre de recurso de Amazon (ARN) de la puerta de enlace que se va a actualizar.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 180 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z0-9+]{3})\/[a-zA-Z0-9]+`

Obligatorio: sí

[GatewayDisplayName](#)

El nombre de visualización actualizado de la puerta de enlace.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `[a-zA-Z0-9-]*`

Obligatorio: no

Sintaxis de la respuesta

```
{  
  "GatewayArn": "string"  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[GatewayArn](#)

El nombre de recurso de Amazon (ARN) de la puerta de enlace que ha actualizado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 180 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

ConflictException

La operación no puede continuar porque no se admite.

ErrorCode

Es una descripción de los motivos por los que no se admite la operación.

Código de estado HTTP: 400

InternalServerErrorException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

ErrorCode

Es una descripción del error interno que se ha producido.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

ErrorCode

Es la descripción del motivo por el que no se ha encontrado el recurso.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

ErrorCode

Error: Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

ErrorCode

Es una descripción de la causa del error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)

- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateGatewaySoftwareNow

Servicio: AWS Backup gateway

Esta operación actualiza el software de máquina virtual (VM) de la puerta de enlace. La solicitud activa inmediatamente la actualización del software.

Note

Al realizar esta solicitud, se obtiene inmediatamente una respuesta 200 OK de confirmación. Sin embargo, es posible que la actualización tarde algún tiempo en completarse.

Sintaxis de la solicitud

```
{
  "GatewayArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace que se va a actualizar.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 180 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\[/code>`

Obligatorio: sí

Sintaxis de la respuesta

```
{
```

```
"GatewayArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace que ha actualizado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 180 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalServerError

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

ErrorCode

Es una descripción del error interno que se ha producido.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

ErrorCode

Es la descripción del motivo por el que no se ha encontrado el recurso.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

ErrorCode

Error: Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

ErrorCode

Es una descripción de la causa del error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateHypervisor

Servicio: AWS Backup gateway

Actualiza los metadatos de un hipervisor, lo que incluye el host, el nombre de usuario y la contraseña. Especifique el hipervisor que desea actualizar mediante el nombre de recurso de Amazon (ARN) del hipervisor en su solicitud.

Sintaxis de la solicitud

```
{  
  "Host": "string",  
  "HypervisorArn": "string",  
  "LogGroupArn": "string",  
  "Name": "string",  
  "Password": "string",  
  "Username": "string"  
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[Host](#)

El host actualizado del hipervisor. Puede ser una dirección IP o un nombre de dominio completo (FQDN).

Tipo: cadena

Limitaciones de longitud: longitud mínima de 3. Longitud máxima de 128.

Patrón: . +

Obligatorio: no

[HypervisorArn](#)

El nombre de recurso de Amazon (ARN) del hipervisor que se va a actualizar.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\/[a-zA-Z-0-9]+`

Obligatorio: sí

LogGroupArn

El nombre de recurso de Amazon (ARN) de grupo de puertas de enlace dentro del registro solicitado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0 caracteres. La longitud máxima es de 2048 caracteres.

Patrón: `$|^arn:(aws|aws-cn|aws-us-gov):logs:([a-zA-Z0-9-]):([0-9]+):log-group:[a-zA-Z0-9_-\./\.:]*`

Obligatorio: no

Name

El nombre actualizado del hipervisor

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `[a-zA-Z0-9-]*`

Obligatorio: no

Password

La contraseña actualizada del hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `[-~]+`

Obligatorio: no

Username

El nombre de usuario actualizado del hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: [-\.0-\[\]-~]*[!-\.0-\[\]-~][-\.0-\[\]-~]*

Obligatorio: no

Sintaxis de la respuesta

```
{  
  "HypervisorArn": "string"  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

HypervisorArn

El nombre de recurso de Amazon (ARN) del hipervisor que ha actualizado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

La operación no puede continuar porque no tiene permisos suficientes.

ErrorCode

Es una descripción del motivo por el que no tiene permisos suficientes.

Código de estado HTTP: 400

ConflictException

La operación no puede continuar porque no se admite.

ErrorCode

Es una descripción de los motivos por los que no se admite la operación.

Código de estado HTTP: 400

InternalServerError

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

ErrorCode

Es una descripción del error interno que se ha producido.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

ErrorCode

Es la descripción del motivo por el que no se ha encontrado el recurso.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

ErrorCode

Error: Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

ErrorCode

Es una descripción de la causa del error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

AWS Backup

AWS Backup admiten las siguientes acciones:

- [GetSearchJob](#)
- [GetSearchResultExportJob](#)
- [ListSearchJobBackups](#)
- [ListSearchJobResults](#)
- [ListSearchJobs](#)
- [ListSearchResultExportJobs](#)

- [ListTagsForResource](#)
- [StartSearchJob](#)
- [StartSearchResultExportJob](#)
- [StopSearchJob](#)
- [TagResource](#)
- [UntagResource](#)

GetSearchJob

Servicio: AWS Backup

Esta operación obtiene los metadatos de un trabajo de búsqueda, incluido su progreso.

Sintaxis de la solicitud

```
GET /search-jobs/SearchJobIdentifier HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

SearchJobIdentifier

Cadena única requerida que especifica el trabajo de búsqueda.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "CompletionTime": number,
  "CreationTime": number,
  "CurrentSearchProgress": {
    "ItemsMatchedCount": number,
    "ItemsScannedCount": number,
    "RecoveryPointsScannedCount": number
  },
  "EncryptionKeyArn": "string",
  "ItemFilters": {
    "EBSItemFilters": [
      {
        "CreationTimes": [
          {
            "Operator": "string",
```

```

        "Value": number
    }
],
"FilePaths": [
    {
        "Operator": "string",
        "Value": "string"
    }
],
"LastModificationTimes": [
    {
        "Operator": "string",
        "Value": number
    }
],
"Sizes": [
    {
        "Operator": "string",
        "Value": number
    }
]
}
],
"S3ItemFilters": [
    {
        "CreationTimes": [
            {
                "Operator": "string",
                "Value": number
            }
        ],
        "ETags": [
            {
                "Operator": "string",
                "Value": "string"
            }
        ],
        "ObjectKeys": [
            {
                "Operator": "string",
                "Value": "string"
            }
        ],
        "Sizes": [

```

```

        {
            "Operator": "string",
            "Value": number
        }
    ],
    "VersionIds": [
        {
            "Operator": "string",
            "Value": "string"
        }
    ]
}
],
},
"Name": "string",
"SearchJobArn": "string",
"SearchJobIdentifier": "string",
"SearchScope": {
    "BackupResourceArns": [ "string" ],
    "BackupResourceCreationTime": {
        "CreatedAfter": number,
        "CreatedBefore": number
    },
    "BackupResourceTags": {
        "string" : "string"
    },
    "BackupResourceTypes": [ "string" ],
    "SourceResourceArns": [ "string" ]
},
"SearchScopeSummary": {
    "TotalItemsToScanCount": number,
    "TotalRecoveryPointsToScanCount": number
},
"Status": "string",
"StatusMessage": "string"
}

```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

CompletionTime

Fecha y hora en que se completó el trabajo de búsqueda, en formato Unix y en la hora universal coordinada (UTC). El valor de `CompletionTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

CreationTime

Fecha y hora en que se creó el trabajo de búsqueda, en formato Unix y en la hora universal coordinada (UTC). El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

CurrentSearchProgress

Devuelve números que representan `BackupsScannedCount`, `ItemsScanned` e `ItemsMatched`.

Tipo: objeto [CurrentSearchProgress](#)

EncryptionKeyArn

Es la clave de cifrado del trabajo de búsqueda especificado.

Ejemplo: `:arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Tipo: cadena

ItemFilters

Son los filtros de elementos que representan todas las propiedades de los elementos de entrada especificados al crear la búsqueda.

Tipo: objeto [ItemFilters](#)

Name

Nombre devuelto del trabajo de búsqueda especificado.

Tipo: cadena

[SearchJobArn](#)

Cadena única que identifica el nombre de recurso de Amazon (ARN) del trabajo de búsqueda especificado.

Tipo: cadena

[SearchJobIdentifier](#)

Cadena única que identifica el trabajo de búsqueda especificado.

Tipo: cadena

[SearchScope](#)

Ámbito de búsqueda que incluye todas las propiedades de copia de seguridad introducidas en una búsqueda.

Tipo: objeto [SearchScope](#)

[SearchScopeSummary](#)

Devuelve un resumen del ámbito del trabajo de búsqueda especificado, que incluye:

- TotalBackupsToScanCount, que es el número de puntos de recuperación que devuelve la búsqueda.
- TotalItemsToScanCount, que es el número de elementos que devuelve la búsqueda.

Tipo: objeto [SearchScopeSummary](#)

[Status](#)

Estado actual del trabajo de búsqueda especificado.

Un trabajo de búsqueda puede tener uno de los siguientes estados: RUNNING; COMPLETED; STOPPED; FAILED TIMED_OUT o EXPIRED.

Tipo: cadena

Valores válidos: RUNNING | COMPLETED | STOPPING | STOPPED | FAILED

[StatusMessage](#)

Se devolverá un mensaje de estado para cada trabajo de búsqueda con un estado ERRORRED o un estado de trabajos COMPLETED con problemas.

Por ejemplo, un mensaje puede indicar que una búsqueda contiene puntos de recuperación que no se han podido analizar debido a un problema con permisos.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

No tiene acceso suficiente para realizar esta acción.

message

El usuario no tiene acceso suficiente para realizar esta acción.

Código de estado HTTP: 403

InternalServerError

Se ha producido un error interno del servidor. Vuelva a enviar la solicitud.

message

Error inesperado durante el procesamiento de la solicitud.

retryAfterSeconds

Vuelva a intentar la llamada pasados varios segundos.

Código de estado HTTP: 500

ResourceNotFoundException

No se ha encontrado el recurso para esta solicitud.

Confirme que la información del recurso, como el ARN o el tipo, es correcta y existe y, a continuación, vuelva a intentar la solicitud.

message

La solicitud hace referencia a un recurso que no existe.

resourceId

Identificador hipotético del recurso afectado.

resourceType

Tipo hipotético del recurso afectado.

Código de estado HTTP: 404

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

message

La solicitud ha dado error debido a la limitación de la solicitud.

quotaCode

Este es el código unívoco del servicio de origen con la cuota.

retryAfterSeconds

Vuelva a intentar la llamada pasados varios segundos.

serviceCode

Este es el código unívoco del servicio de origen.

Código de estado HTTP: 429

ValidationException

La entrada no satisface las limitaciones que especifica un servicio.

message

La entrada no satisface las limitaciones que especifica un servicio de Amazon.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)

- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

GetSearchResultExportJob

Servicio: AWS Backup

Esta operación obtiene los metadatos de un trabajo de exportación.

Un trabajo de exportación es una operación que transmite los resultados de un trabajo de búsqueda a un bucket de S3 específico en un archivo .csv.

Un trabajo de exportación le permite conservar los resultados de una búsqueda más allá de los siete días programados para el trabajo de búsqueda.

Sintaxis de la solicitud

```
GET /export-search-jobs/ExportJobIdentifier HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[ExportJobIdentifier](#)

Esta es la cadena unívoca que identifica un trabajo de exportación específico.

Es obligatoria para esta operación.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "CompletionTime": number,
  "CreationTime": number,
  "ExportJobArn": "string",
  "ExportJobIdentifier": "string",
  "ExportSpecification": { ... },
  "SearchJobArn": "string",
```

```
"Status": "string",  
"StatusMessage": "string"  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[CompletionTime](#)

Fecha y hora en que se completó el trabajo de exportación, expresadas en formato Unix y en horario universal coordinado (UTC). El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

[CreationTime](#)

Fecha y hora en que se creó un trabajo de exportación, expresadas en formato Unix y en horario universal coordinado (UTC). El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

[ExportJobArn](#)

Es el Nombre de recurso de Amazon (ARN) unívoco que identifica de forma exclusiva el trabajo de exportación.

Tipo: cadena

[ExportJobIdentifier](#)

Esta es la cadena unívoca que identifica un trabajo de exportación específico.

Tipo: cadena

[ExportSpecification](#)

La especificación de exportación consta del bucket de S3 de destino al que se exportaron los resultados de la búsqueda, junto con el prefijo de destino.

Tipo: objeto [ExportSpecification](#)

Nota: Este objeto es una unión. Solo se puede especificar o devolver un miembro de este objeto.

[SearchJobArn](#)

Cadena única que identifica el nombre de recurso de Amazon (ARN) del trabajo de búsqueda especificado.

Tipo: cadena

[Status](#)

Este es el estado actual del trabajo de exportación.

Tipo: cadena

Valores válidos: RUNNING | FAILED | COMPLETED

[StatusMessage](#)

Un mensaje de estado es una cadena que se devuelve para el trabajo de búsqueda con un estado FAILED, junto con los pasos para corregir y volver a intentar la operación.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

No tiene acceso suficiente para realizar esta acción.

message

El usuario no tiene acceso suficiente para realizar esta acción.

Código de estado HTTP: 403

InternalServerErrorException

Se ha producido un error interno del servidor. Vuelva a enviar la solicitud.

message

Error inesperado durante el procesamiento de la solicitud.

retryAfterSeconds

Vuelva a intentar la llamada pasados varios segundos.

Código de estado HTTP: 500

ResourceNotFoundException

No se ha encontrado el recurso para esta solicitud.

Confirme que la información del recurso, como el ARN o el tipo, es correcta y existe y, a continuación, vuelva a intentar la solicitud.

message

La solicitud hace referencia a un recurso que no existe.

resourceId

Identificador hipotético del recurso afectado.

resourceType

Tipo hipotético del recurso afectado.

Código de estado HTTP: 404

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

message

La solicitud ha dado error debido a la limitación de la solicitud.

quotaCode

Este es el código único del servicio de origen con la cuota.

retryAfterSeconds

Vuelva a intentar la llamada pasados varios segundos.

serviceCode

Este es el código único del servicio de origen.

Código de estado HTTP: 429

ValidationException

La entrada no satisface las limitaciones que especifica un servicio.

message

La entrada no satisface las limitaciones que especifica un servicio de Amazon.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ListSearchJobBackups

Servicio: AWS Backup

Esta operación devuelve una lista de todas las copias de seguridad (puntos de recuperación) en formato paginado que se han incluido en el trabajo de búsqueda.

Si una búsqueda no muestra la copia de seguridad esperada en los resultados, puede llamar a esta operación para que se muestren todas las copias de seguridad incluidas en la búsqueda. Se mostrarán todas las copias de seguridad que no se hayan incluido porque tenían el estado FAILED de un problema de permisos, junto con un mensaje de estado.

En los resultados de búsqueda solo se incluyen puntos de recuperación con un índice de copias de seguridad con el estado ACTIVE. Si el índice tiene otro estado, este se mostrará junto con un mensaje de estado.

Sintaxis de la solicitud

```
GET /search-jobs/SearchJobIdentifier/backups?maxResults=MaxResults&nextToken=NextToken  
HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[MaxResults](#)

Número máximo de elementos de la lista de recursos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

[NextToken](#)

Es el siguiente elemento tras una lista parcial de copias de seguridad devueltas que se incluyen en un trabajo de búsqueda.

Por ejemplo, si se solicita que se devuelva el número de copias de seguridad `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

[SearchJobIdentifier](#)

Cadena unívoca que especifica el trabajo de búsqueda.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "Results": [
    {
      "BackupCreationTime": number,
      "BackupResourceArn": "string",
      "IndexCreationTime": number,
      "ResourceType": "string",
      "SourceResourceArn": "string",
      "Status": "string",
      "StatusMessage": "string"
    }
  ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

NextToken

Es el siguiente elemento tras una lista parcial de copias de seguridad devueltas que se incluyen en un trabajo de búsqueda.

Por ejemplo, si se solicita que se devuelva el número de copias de seguridad MaxResults, NextToken permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Results

Los puntos de recuperación devuelven los resultados de un trabajo de búsqueda.

Tipo: matriz de objetos [SearchJobBackupsResult](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

No tiene acceso suficiente para realizar esta acción.

message

El usuario no tiene acceso suficiente para realizar esta acción.

Código de estado HTTP: 403

InternalServerError

Se ha producido un error interno del servidor. Vuelva a enviar la solicitud.

message

Error inesperado durante el procesamiento de la solicitud.

retryAfterSeconds

Vuelva a intentar la llamada pasados varios segundos.

Código de estado HTTP: 500

ResourceNotFoundException

No se ha encontrado el recurso para esta solicitud.

Confirme que la información del recurso, como el ARN o el tipo, es correcta y existe y, a continuación, vuelva a intentar la solicitud.

message

La solicitud hace referencia a un recurso que no existe.

`resourceId`

Identificador hipotético del recurso afectado.

`resourceType`

Tipo hipotético del recurso afectado.

Código de estado HTTP: 404

`ThrottlingException`

La solicitud fue denegada debido a una limitación de la solicitud.

`message`

La solicitud ha dado error debido a la limitación de la solicitud.

`quotaCode`

Este es el código unívoco del servicio de origen con la cuota.

`retryAfterSeconds`

Vuelva a intentar la llamada pasados varios segundos.

`serviceCode`

Este es el código unívoco del servicio de origen.

Código de estado HTTP: 429

`ValidationException`

La entrada no satisface las limitaciones que especifica un servicio.

`message`

La entrada no satisface las limitaciones que especifica un servicio de Amazon.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)

- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ListSearchJobResults

Servicio: AWS Backup

Esta operación devuelve una lista de un trabajo de búsqueda especificado.

Sintaxis de la solicitud

```
GET /search-jobs/SearchJobIdentifier/search-results?  
maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[MaxResults](#)

Número máximo de elementos de la lista de recursos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

[NextToken](#)

Es el elemento que sigue a una lista parcial de los resultados del trabajo de búsqueda devueltos.

Por ejemplo, si se solicita que se devuelva el número `MaxResults` de resultados del trabajo de búsqueda, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

[SearchJobIdentifier](#)

Cadena unívoca que especifica el trabajo de búsqueda.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200  
Content-type: application/json
```



```
{
  "NextToken": "string",
  "Results": [
    { ... }
  ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[NextToken](#)

Es el elemento que sigue a una lista parcial de los resultados del trabajo de búsqueda.

Por ejemplo, si se solicita que se devuelva el número de copias de seguridad `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

[Results](#)

Los resultados constan de `EBSResultItem` o `S3ResultItem`.

Tipo: matriz de objetos [ResultItem](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

`AccessDeniedException`

No tiene acceso suficiente para realizar esta acción.

message

El usuario no tiene acceso suficiente para realizar esta acción.

Código de estado HTTP: 403

InternalServerErrorException

Se ha producido un error interno del servidor. Vuelva a enviar la solicitud.

message

Error inesperado durante el procesamiento de la solicitud.

retryAfterSeconds

Vuelva a intentar la llamada pasados varios segundos.

Código de estado HTTP: 500

ResourceNotFoundException

No se ha encontrado el recurso para esta solicitud.

Confirme que la información del recurso, como el ARN o el tipo, es correcta y existe y, a continuación, vuelva a intentar la solicitud.

message

La solicitud hace referencia a un recurso que no existe.

resourceId

Identificador hipotético del recurso afectado.

resourceType

Tipo hipotético del recurso afectado.

Código de estado HTTP: 404

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

message

La solicitud ha dado error debido a la limitación de la solicitud.

quotaCode

Este es el código unívoco del servicio de origen con la cuota.

retryAfterSeconds

Vuelva a intentar la llamada pasados varios segundos.

`serviceCode`

Este es el código unívoco del servicio de origen.

Código de estado HTTP: 429

`ValidationException`

La entrada no satisface las limitaciones que especifica un servicio.

`message`

La entrada no satisface las limitaciones que especifica un servicio de Amazon.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ListSearchJobs

Servicio: AWS Backup

Esta operación devuelve una lista de los trabajos de búsqueda que pertenecen a una cuenta.

Sintaxis de la solicitud

```
GET /search-jobs?MaxResults=MaxResults&NextToken=NextToken&Status=ByStatus HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[ByStatus](#)

Incluya este parámetro para filtrar la lista por estado del trabajo de búsqueda.

Valores válidos: RUNNING | COMPLETED | STOPPING | STOPPED | FAILED

[MaxResults](#)

Número máximo de elementos de la lista de recursos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

[NextToken](#)

Es el elemento que sigue a una lista parcial de los resultados del trabajo de búsqueda devueltos.

Por ejemplo, si se solicita que se devuelva el número de copias de seguridad `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200  
Content-type: application/json
```

```
{
  "NextToken": "string",
  "SearchJobs": [
    {
      "CompletionTime": number,
      "CreationTime": number,
      "Name": "string",
      "SearchJobArn": "string",
      "SearchJobIdentifier": "string",
      "SearchScopeSummary": {
        "TotalItemsToScanCount": number,
        "TotalRecoveryPointsToScanCount": number
      },
      "Status": "string",
      "StatusMessage": "string"
    }
  ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

NextToken

Es el siguiente elemento tras una lista parcial de copias de seguridad devueltas que se incluyen en un trabajo de búsqueda.

Por ejemplo, si se solicita que se devuelva el número de copias de seguridad `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

SearchJobs

Son los trabajos de búsqueda de la lista que incluyen detalles de los trabajos de búsqueda devueltos.

Tipo: matriz de objetos [SearchJobSummary](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

No tiene acceso suficiente para realizar esta acción.

message

El usuario no tiene acceso suficiente para realizar esta acción.

Código de estado HTTP: 403

InternalServerError

Se ha producido un error interno del servidor. Vuelva a enviar la solicitud.

message

Error inesperado durante el procesamiento de la solicitud.

retryAfterSeconds

Vuelva a intentar la llamada pasados varios segundos.

Código de estado HTTP: 500

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

message

La solicitud ha dado error debido a la limitación de la solicitud.

quotaCode

Este es el código unívoco del servicio de origen con la cuota.

retryAfterSeconds

Vuelva a intentar la llamada pasados varios segundos.

serviceCode

Este es el código unívoco del servicio de origen.

Código de estado HTTP: 429

ValidationException

La entrada no satisface las limitaciones que especifica un servicio.

message

La entrada no satisface las limitaciones que especifica un servicio de Amazon.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ListSearchResultExportJobs

Servicio: AWS Backup

Esta operación exporta los resultados de búsqueda de un trabajo de búsqueda a un bucket de S3 de destino específico.

Sintaxis de la solicitud

```
GET /export-search-jobs?  
MaxResults=MaxResults&NextToken=NextToken&SearchJobIdentifier=SearchJobIdentifier&Status=Status  
HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[MaxResults](#)

Número máximo de elementos de la lista de recursos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

[NextToken](#)

Es el siguiente elemento tras una lista parcial de copias de seguridad devueltas que se incluyen en un trabajo de búsqueda.

Por ejemplo, si se solicita que se devuelva el número de copias de seguridad `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

[SearchJobIdentifier](#)

Cadena unívoca que especifica el trabajo de búsqueda.

[Status](#)

Los trabajos de búsqueda que se van a incluir en el trabajo de exportación se pueden filtrar mediante la inclusión de este parámetro.

Valores válidos: `RUNNING` | `FAILED` | `COMPLETED`

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "ExportJobs": [
    {
      "CompletionTime": number,
      "CreationTime": number,
      "ExportJobArn": "string",
      "ExportJobIdentifier": "string",
      "SearchJobArn": "string",
      "Status": "string",
      "StatusMessage": "string"
    }
  ],
  "NextToken": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[ExportJobs](#)

La operación devuelve los trabajos de exportación incluidos.

Tipo: matriz de objetos [ExportJobSummary](#)

[NextToken](#)

Es el siguiente elemento tras una lista parcial de copias de seguridad devueltas que se incluyen en un trabajo de búsqueda.

Por ejemplo, si se solicita que se devuelva el número de copias de seguridad `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

No tiene acceso suficiente para realizar esta acción.

message

El usuario no tiene acceso suficiente para realizar esta acción.

Código de estado HTTP: 403

InternalServerError

Se ha producido un error interno del servidor. Vuelva a enviar la solicitud.

message

Error inesperado durante el procesamiento de la solicitud.

retryAfterSeconds

Vuelva a intentar la llamada pasados varios segundos.

Código de estado HTTP: 500

ResourceNotFoundException

No se ha encontrado el recurso para esta solicitud.

Confirme que la información del recurso, como el ARN o el tipo, es correcta y existe y, a continuación, vuelva a intentar la solicitud.

message

La solicitud hace referencia a un recurso que no existe.

resourceId

Identificador hipotético del recurso afectado.

resourceType

Tipo hipotético del recurso afectado.

Código de estado HTTP: 404

ServiceQuotaExceededException

La solicitud se ha denegado debido a que se han superado los límites de cuota permitidos.

message

Esta solicitud no se ha realizado correctamente debido a que la cuota de servicio ha superado los límites.

quotaCode

Este es el código específico del tipo de cuota.

resourceId

Es el identificador del recurso.

resourceType

Tipo de recurso.

serviceCode

Este es el código unívoco del servicio de origen con la cuota.

Código de estado HTTP: 402

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

message

La solicitud ha dado error debido a la limitación de la solicitud.

quotaCode

Este es el código unívoco del servicio de origen con la cuota.

retryAfterSeconds

Vuelva a intentar la llamada pasados varios segundos.

`serviceCode`

Este es el código unívoco del servicio de origen.

Código de estado HTTP: 429

`ValidationException`

La entrada no satisface las limitaciones que especifica un servicio.

`message`

La entrada no satisface las limitaciones que especifica un servicio de Amazon.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

ListTagsForResource

Servicio: AWS Backup

Esta operación devuelve las etiquetas de un tipo de recurso.

Sintaxis de la solicitud

```
GET /tags/ResourceArn HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[ResourceArn](#)

Es el Nombre de recurso de Amazon (ARN) que identifica de forma unívoca el recurso.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "Tags": {
    "string" : "string"
  }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[Tags](#)

Es la lista de etiquetas que devuelve la operación.

Tipo: mapa de cadena a cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

No tiene acceso suficiente para realizar esta acción.

message

El usuario no tiene acceso suficiente para realizar esta acción.

Código de estado HTTP: 403

InternalServerError

Se ha producido un error interno del servidor. Vuelva a enviar la solicitud.

message

Error inesperado durante el procesamiento de la solicitud.

retryAfterSeconds

Vuelva a intentar la llamada pasados varios segundos.

Código de estado HTTP: 500

ResourceNotFoundException

No se ha encontrado el recurso para esta solicitud.

Confirme que la información del recurso, como el ARN o el tipo, es correcta y existe y, a continuación, vuelva a intentar la solicitud.

message

La solicitud hace referencia a un recurso que no existe.

resourceId

Identificador hipotético del recurso afectado.

resourceType

Tipo hipotético del recurso afectado.

Código de estado HTTP: 404

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

message

La solicitud ha dado error debido a la limitación de la solicitud.

quotaCode

Este es el código unívoco del servicio de origen con la cuota.

retryAfterSeconds

Vuelva a intentar la llamada pasados varios segundos.

serviceCode

Este es el código unívoco del servicio de origen.

Código de estado HTTP: 429

ValidationException

La entrada no satisface las limitaciones que especifica un servicio.

message

La entrada no satisface las limitaciones que especifica un servicio de Amazon.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)

- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

StartSearchJob

Servicio: AWS Backup

Esta operación crea un trabajo de búsqueda que devuelve los puntos de recuperación filtrados por SearchScope y los elementos filtrados por ItemFilters.

Si lo desea, puede incluir ClientToken, EncryptionKeyArn, Name o Tags.

Sintaxis de la solicitud

```
PUT /search-jobs HTTP/1.1
Content-type: application/json

{
  "ClientToken": "string",
  "EncryptionKeyArn": "string",
  "ItemFilters": {
    "EBSItemFilters": [
      {
        "CreationTimes": [
          {
            "Operator": "string",
            "Value": number
          }
        ],
        "FilePaths": [
          {
            "Operator": "string",
            "Value": "string"
          }
        ],
        "LastModificationTimes": [
          {
            "Operator": "string",
            "Value": number
          }
        ],
        "Sizes": [
          {
            "Operator": "string",
            "Value": number
          }
        ]
      }
    ]
  }
}
```

```

    }
  ],
  "S3ItemFilters": [
    {
      "CreationTimes": [
        {
          "Operator": "string",
          "Value": number
        }
      ],
      "ETags": [
        {
          "Operator": "string",
          "Value": "string"
        }
      ],
      "ObjectKeys": [
        {
          "Operator": "string",
          "Value": "string"
        }
      ],
      "Sizes": [
        {
          "Operator": "string",
          "Value": number
        }
      ],
      "VersionIds": [
        {
          "Operator": "string",
          "Value": "string"
        }
      ]
    }
  ]
},
"Name": "string",
"SearchScope": {
  "BackupResourceArns": [ "string" ],
  "BackupResourceCreationTime": {
    "CreatedAfter": number,
    "CreatedBefore": number
  }
},

```

```
"BackupResourceTags": {
  "string" : "string"
},
"BackupResourceTypes": [ "string" ],
"SourceResourceArns": [ "string" ]
},
"Tags": {
  "string" : "string"
}
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[ClientToken](#)

Incluya este parámetro para permitir múltiples llamadas idénticas de idempotencia.

Un token de cliente es válido durante ocho horas desde el momento en que finaliza la primera solicitud que lo utiliza. Pasado ese tiempo, cualquier solicitud con el mismo token se considera una solicitud nueva.

Tipo: cadena

Requerido: no

[EncryptionKeyArn](#)

Es la clave de cifrado del trabajo de búsqueda especificado.

Tipo: cadena

Requerido: no

[ItemFilters](#)

Son los filtros de elementos que representan todas las propiedades de los elementos de entrada especificados al crear la búsqueda.

Contiene `EBSItemFilters` o `S3ItemFilters`.

Tipo: objeto [ItemFilters](#)

Obligatorio: no

[Name](#)

Incluye caracteres alfanuméricos para crear un nombre para este trabajo de búsqueda.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 500 caracteres.

Obligatorio: no

[SearchScope](#)

Este objeto puede contener `BackupResourceTypes`, `BackupResourceArns`, `BackupResourceCreationTime`, `BackupResourceTags` y `SourceResourceArns` para filtrar los puntos de recuperación devueltos por el trabajo de búsqueda.

Tipo: objeto [SearchScope](#)

Obligatorio: sí

[Tags](#)

Es la lista de etiquetas que devuelve la operación.

Tipo: mapa de cadena a cadena

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "CreationTime": number,
  "SearchJobArn": "string",
  "SearchJobIdentifier": "string"
```

```
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[CreationTime](#)

Fecha y hora en que se creó el trabajo, expresadas en formato Unix y en horario universal coordinado (UTC). El valor de `CompletionTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

[SearchJobArn](#)

Cadena única que identifica el nombre de recurso de Amazon (ARN) del trabajo de búsqueda especificado.

Tipo: cadena

[SearchJobIdentifier](#)

Cadena unívoca que especifica el trabajo de búsqueda.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

`AccessDeniedException`

No tiene acceso suficiente para realizar esta acción.

message

El usuario no tiene acceso suficiente para realizar esta acción.

Código de estado HTTP: 403

ConflictException

Esta excepción se produce cuando se detecta un conflicto con una operación anterior completada correctamente. Esto suele ocurrir cuando la operación anterior no ha podido propagarse al host que atiende la solicitud actual.

La respuesta recomendada a esta excepción es intentarlo de nuevo (con la lógica de retroceso adecuada).

message

Actualizar o eliminar un recurso puede generar un estado incoherente.

resourceId

Es el identificador del recurso afectado.

resourceType

Es el tipo de recurso afectado.

Código de estado HTTP: 409

InternalServerError

Se ha producido un error interno del servidor. Vuelva a enviar la solicitud.

message

Error inesperado durante el procesamiento de la solicitud.

retryAfterSeconds

Vuelva a intentar la llamada pasados varios segundos.

Código de estado HTTP: 500

ResourceNotFoundException

No se ha encontrado el recurso para esta solicitud.

Confirme que la información del recurso, como el ARN o el tipo, es correcta y existe y, a continuación, vuelva a intentar la solicitud.

message

La solicitud hace referencia a un recurso que no existe.

resourceId

Identificador hipotético del recurso afectado.

resourceType

Tipo hipotético del recurso afectado.

Código de estado HTTP: 404

ServiceQuotaExceededException

La solicitud se ha denegado debido a que se han superado los límites de cuota permitidos.

message

Esta solicitud no se ha realizado correctamente debido a que la cuota de servicio ha superado los límites.

quotaCode

Este es el código específico del tipo de cuota.

resourceId

Es el identificador del recurso.

resourceType

Tipo de recurso.

serviceCode

Este es el código unívoco del servicio de origen con la cuota.

Código de estado HTTP: 402

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

message

La solicitud ha dado error debido a la limitación de la solicitud.

quotaCode

Este es el código unívoco del servicio de origen con la cuota.

`retryAfterSeconds`

Vuelva a intentar la llamada pasados varios segundos.

`serviceCode`

Este es el código único del servicio de origen.

Código de estado HTTP: 429

`ValidationException`

La entrada no satisface las limitaciones que especifica un servicio.

`message`

La entrada no satisface las limitaciones que especifica un servicio de Amazon.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

StartSearchResultExportJob

Servicio: AWS Backup

Esta operación inicia un trabajo para exportar los resultados del trabajo de búsqueda a un bucket de S3 designado.

Sintaxis de la solicitud

```
PUT /export-search-jobs HTTP/1.1
Content-type: application/json

{
  "ClientToken": "string",
  "ExportSpecification": { ... },
  "RoleArn": "string",
  "SearchJobIdentifier": "string",
  "Tags": {
    "string" : "string"
  }
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

ClientToken

Incluya este parámetro para permitir múltiples llamadas idénticas de idempotencia.

Un token de cliente es válido durante ocho horas desde el momento en que finaliza la primera solicitud que lo utiliza. Pasado ese tiempo, cualquier solicitud con el mismo token se considera una solicitud nueva.

Tipo: cadena

Requerido: no

[ExportSpecification](#)

Esta especificación contiene una cadena obligatoria del bucket de destino; si lo desea, puede incluir el prefijo de destino.

Tipo: objeto [ExportSpecification](#)

Nota: Este objeto es una unión. Solo se puede especificar o devolver un miembro de este objeto.

Obligatorio: sí

[RoleArn](#)

Este parámetro especifica el ARN del rol que se utiliza para iniciar los trabajos de exportación de los resultados de la búsqueda.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 2048 caracteres.

Patrón: `arn:(?:aws|aws-cn|aws-us-gov):iam::[a-z0-9-]+:role/(.+)`

Obligatorio: no

[SearchJobIdentifier](#)

Cadena unívoca que especifica el trabajo de búsqueda.

Tipo: cadena

Obligatorio: sí

[Tags](#)

Etiquetas opcionales que se incluirán. Una etiqueta es un par clave-valor que puede utilizar para administrar, filtrar y buscar sus recursos. Los caracteres permitidos incluyen espacios, números y letras en UTF-8, además de los siguientes caracteres especiales: + - = . _ : /.

Tipo: mapa de cadena a cadena

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json
```

```
{  
  "ExportJobArn": "string",  
  "ExportJobIdentifier": "string"  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[ExportJobArn](#)

Este es el ARN (Nombre de recurso de Amazon) exclusivo que pertenece al nuevo trabajo de exportación.

Tipo: cadena

[ExportJobIdentifier](#)

Este es el identificador único que especifica el nuevo trabajo de exportación.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

No tiene acceso suficiente para realizar esta acción.

message

El usuario no tiene acceso suficiente para realizar esta acción.

Código de estado HTTP: 403

ConflictException

Esta excepción se produce cuando se detecta un conflicto con una operación anterior completada correctamente. Esto suele ocurrir cuando la operación anterior no ha podido propagarse al host que atiende la solicitud actual.

La respuesta recomendada a esta excepción es intentarlo de nuevo (con la lógica de retroceso adecuada).

message

Actualizar o eliminar un recurso puede generar un estado incoherente.

resourceId

Es el identificador del recurso afectado.

resourceType

Es el tipo de recurso afectado.

Código de estado HTTP: 409

InternalServerErrorException

Se ha producido un error interno del servidor. Vuelva a enviar la solicitud.

message

Error inesperado durante el procesamiento de la solicitud.

retryAfterSeconds

Vuelva a intentar la llamada pasados varios segundos.

Código de estado HTTP: 500

ResourceNotFoundException

No se ha encontrado el recurso para esta solicitud.

Confirme que la información del recurso, como el ARN o el tipo, es correcta y existe y, a continuación, vuelva a intentar la solicitud.

message

La solicitud hace referencia a un recurso que no existe.

resourceId

Identificador hipotético del recurso afectado.

resourceType

Tipo hipotético del recurso afectado.

Código de estado HTTP: 404

ServiceQuotaExceededException

La solicitud se ha denegado debido a que se han superado los límites de cuota permitidos.

message

Esta solicitud no se ha realizado correctamente debido a que la cuota de servicio ha superado los límites.

quotaCode

Este es el código específico del tipo de cuota.

resourceId

Es el identificador del recurso.

resourceType

Tipo de recurso.

serviceCode

Este es el código unívoco del servicio de origen con la cuota.

Código de estado HTTP: 402

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

message

La solicitud ha dado error debido a la limitación de la solicitud.

quotaCode

Este es el código unívoco del servicio de origen con la cuota.

retryAfterSeconds

Vuelva a intentar la llamada pasados varios segundos.

serviceCode

Este es el código unívoco del servicio de origen.

Código de estado HTTP: 429

ValidationException

La entrada no satisface las limitaciones que especifica un servicio.

message

La entrada no satisface las limitaciones que especifica un servicio de Amazon.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

StopSearchJob

Servicio: AWS Backup

Esta operación finaliza un trabajo de búsqueda.

Solo se puede detener un trabajo de búsqueda que tenga el estado RUNNING.

Sintaxis de la solicitud

```
PUT /search-jobs/SearchJobIdentifier/actions/cancel HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

SearchJobIdentifier

Cadena unívoca que especifica el trabajo de búsqueda.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

No tiene acceso suficiente para realizar esta acción.

message

El usuario no tiene acceso suficiente para realizar esta acción.

Código de estado HTTP: 403

ConflictException

Esta excepción se produce cuando se detecta un conflicto con una operación anterior completada correctamente. Esto suele ocurrir cuando la operación anterior no ha podido propagarse al host que atiende la solicitud actual.

La respuesta recomendada a esta excepción es intentarlo de nuevo (con la lógica de retroceso adecuada).

message

Actualizar o eliminar un recurso puede generar un estado incoherente.

resourceId

Es el identificador del recurso afectado.

resourceType

Es el tipo de recurso afectado.

Código de estado HTTP: 409

InternalServerErrorException

Se ha producido un error interno del servidor. Vuelva a enviar la solicitud.

message

Error inesperado durante el procesamiento de la solicitud.

retryAfterSeconds

Vuelva a intentar la llamada pasados varios segundos.

Código de estado HTTP: 500

ResourceNotFoundException

No se ha encontrado el recurso para esta solicitud.

Confirme que la información del recurso, como el ARN o el tipo, es correcta y existe y, a continuación, vuelva a intentar la solicitud.

message

La solicitud hace referencia a un recurso que no existe.

resourceId

Identificador hipotético del recurso afectado.

resourceType

Tipo hipotético del recurso afectado.

Código de estado HTTP: 404

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

message

La solicitud ha dado error debido a la limitación de la solicitud.

quotaCode

Este es el código unívoco del servicio de origen con la cuota.

retryAfterSeconds

Vuelva a intentar la llamada pasados varios segundos.

serviceCode

Este es el código unívoco del servicio de origen.

Código de estado HTTP: 429

ValidationException

La entrada no satisface las limitaciones que especifica un servicio.

message

La entrada no satisface las limitaciones que especifica un servicio de Amazon.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

TagResource

Servicio: AWS Backup

Esta operación coloca etiquetas en el recurso que indique.

Sintaxis de la solicitud

```
POST /tags/ResourceArn HTTP/1.1
Content-type: application/json

{
  "Tags": {
    "string" : "string"
  }
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

ResourceArn

Es el Nombre de recurso de Amazon (ARN) que identifica de forma unívoca el recurso.

Este es el recurso que tendrá las etiquetas indicadas.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

Tags

Son las etiquetas que se deben incluir. Una etiqueta es un par clave-valor que puede utilizar para administrar, filtrar y buscar sus recursos. Los caracteres permitidos incluyen espacios, números y letras en UTF-8, además de los siguientes caracteres especiales: + - = . _ : /.

Tipo: mapa de cadena a cadena

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

No tiene acceso suficiente para realizar esta acción.

message

El usuario no tiene acceso suficiente para realizar esta acción.

Código de estado HTTP: 403

InternalServerError

Se ha producido un error interno del servidor. Vuelva a enviar la solicitud.

message

Error inesperado durante el procesamiento de la solicitud.

retryAfterSeconds

Vuelva a intentar la llamada pasados varios segundos.

Código de estado HTTP: 500

ResourceNotFoundException

No se ha encontrado el recurso para esta solicitud.

Confirme que la información del recurso, como el ARN o el tipo, es correcta y existe y, a continuación, vuelva a intentar la solicitud.

message

La solicitud hace referencia a un recurso que no existe.

resourceId

Identificador hipotético del recurso afectado.

resourceType

Tipo hipotético del recurso afectado.

Código de estado HTTP: 404

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

message

La solicitud ha dado error debido a la limitación de la solicitud.

quotaCode

Este es el código unívoco del servicio de origen con la cuota.

retryAfterSeconds

Vuelva a intentar la llamada pasados varios segundos.

serviceCode

Este es el código unívoco del servicio de origen.

Código de estado HTTP: 429

ValidationException

La entrada no satisface las limitaciones que especifica un servicio.

message

La entrada no satisface las limitaciones que especifica un servicio de Amazon.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)

- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)
- [AWS SDK para Ruby V3](#)

UntagResource

Servicio: AWS Backup

Esta operación elimina etiquetas del recurso especificado.

Sintaxis de la solicitud

```
DELETE /tags/ResourceArn?tagKeys=TagKeys HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[ResourceArn](#)

Es el nombre de recurso de Amazon (ARN) que identifica el recurso de forma unívoca para el que desea eliminar las etiquetas.

Obligatorio: sí

[TagKeys](#)

Este parámetro obligatorio contiene las claves de etiqueta que desea eliminar del origen.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

No tiene acceso suficiente para realizar esta acción.

message

El usuario no tiene acceso suficiente para realizar esta acción.

Código de estado HTTP: 403

InternalServerError

Se ha producido un error interno del servidor. Vuelva a enviar la solicitud.

message

Error inesperado durante el procesamiento de la solicitud.

retryAfterSeconds

Vuelva a intentar la llamada pasados varios segundos.

Código de estado HTTP: 500

ResourceNotFoundException

No se ha encontrado el recurso para esta solicitud.

Confirme que la información del recurso, como el ARN o el tipo, es correcta y existe y, a continuación, vuelva a intentar la solicitud.

message

La solicitud hace referencia a un recurso que no existe.

resourceId

Identificador hipotético del recurso afectado.

resourceType

Tipo hipotético del recurso afectado.

Código de estado HTTP: 404

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

message

La solicitud ha dado error debido a la limitación de la solicitud.

quotaCode

Este es el código unívoco del servicio de origen con la cuota.

retryAfterSeconds

Vuelva a intentar la llamada pasados varios segundos.

serviceCode

Este es el código unívoco del servicio de origen.

Código de estado HTTP: 429

ValidationException

La entrada no satisface las limitaciones que especifica un servicio.

message

La entrada no satisface las limitaciones que especifica un servicio de Amazon.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [Interfaz de la línea de comandos de AWS versión 2](#)
- [AWS SDK de para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK de para Kotlin](#)
- [AWS SDK de para PHP V3](#)
- [AWS SDK de para Python](#)

- [AWS SDK para Ruby V3](#)

Data Types

Los siguientes tipos de datos son compatibles con AWS Backup:

- [AdvancedBackupSetting](#)
- [AggregatedScanResult](#)
- [BackupJob](#)
- [BackupJobSummary](#)
- [BackupPlan](#)
- [BackupPlanInput](#)
- [BackupPlansListMember](#)
- [BackupPlanTemplatesListMember](#)
- [BackupRule](#)
- [BackupRuleInput](#)
- [BackupSelection](#)
- [BackupSelectionsListMember](#)
- [BackupVaultListMember](#)
- [CalculatedLifecycle](#)
- [Condition](#)
- [ConditionParameter](#)
- [Conditions](#)
- [ControlInputParameter](#)
- [ControlScope](#)
- [CopyAction](#)
- [CopyJob](#)
- [CopyJobSummary](#)
- [DateRange](#)
- [Framework](#)
- [FrameworkControl](#)

- [IndexAction](#)
- [IndexedRecoveryPoint](#)
- [KeyValue](#)
- [LatestMpaApprovalTeamUpdate](#)
- [LatestRevokeRequest](#)
- [LegalHold](#)
- [Lifecycle](#)
- [ProtectedResource](#)
- [ProtectedResourceConditions](#)
- [RecoveryPointByBackupVault](#)
- [RecoveryPointByResource](#)
- [RecoveryPointCreator](#)
- [RecoveryPointMember](#)
- [RecoveryPointSelection](#)
- [ReportDeliveryChannel](#)
- [ReportDestination](#)
- [ReportJob](#)
- [ReportPlan](#)
- [ReportSetting](#)
- [ResourceSelection](#)
- [RestoreAccessBackupVaultListMember](#)
- [RestoreJobCreator](#)
- [RestoreJobsListMember](#)
- [RestoreJobSummary](#)
- [RestoreTestingPlanForCreate](#)
- [RestoreTestingPlanForGet](#)
- [RestoreTestingPlanForList](#)
- [RestoreTestingPlanForUpdate](#)
- [RestoreTestingRecoveryPointSelection](#)
- [RestoreTestingSelectionForCreate](#)

- [RestoreTestingSelectionForGet](#)
- [RestoreTestingSelectionForList](#)
- [RestoreTestingSelectionForUpdate](#)
- [ScanAction](#)
- [ScanJob](#)
- [ScanJobCreator](#)
- [ScanJobSummary](#)
- [ScanResult](#)
- [ScanResultInfo](#)
- [ScanSetting](#)
- [ScheduledPlanExecutionMember](#)
- [TieringConfiguration](#)
- [TieringConfigurationInputForCreate](#)
- [TieringConfigurationInputForUpdate](#)
- [TieringConfigurationsListMember](#)

Los siguientes tipos de datos son compatibles con AWS Backup gateway:

- [BandwidthRateLimitInterval](#)
- [Gateway](#)
- [GatewayDetails](#)
- [Hypervisor](#)
- [HypervisorDetails](#)
- [MaintenanceStartTime](#)
- [Tag](#)
- [VirtualMachine](#)
- [VirtualMachineDetails](#)
- [VmwareTag](#)
- [VmwareToAwsTagMapping](#)

Los siguientes tipos de datos son compatibles con AWS Backup:

- [BackupCreationTimeFilter](#)
- [CurrentSearchProgress](#)
- [EBSItemFilter](#)
- [EBSResultItem](#)
- [ExportJobSummary](#)
- [ExportSpecification](#)
- [ItemFilters](#)
- [LongCondition](#)
- [ResultItem](#)
- [S3ExportSpecification](#)
- [S3ItemFilter](#)
- [S3ResultItem](#)
- [SearchJobBackupsResult](#)
- [SearchJobSummary](#)
- [SearchScope](#)
- [SearchScopeSummary](#)
- [StringCondition](#)
- [TimeCondition](#)

AWS Backup

Los siguientes tipos de datos son compatibles con AWS Backup:

- [AdvancedBackupSetting](#)
- [AggregatedScanResult](#)
- [BackupJob](#)
- [BackupJobSummary](#)
- [BackupPlan](#)
- [BackupPlanInput](#)
- [BackupPlansListMember](#)
- [BackupPlanTemplatesListMember](#)
- [BackupRule](#)

- [BackupRuleInput](#)
- [BackupSelection](#)
- [BackupSelectionsListMember](#)
- [BackupVaultListMember](#)
- [CalculatedLifecycle](#)
- [Condition](#)
- [ConditionParameter](#)
- [Conditions](#)
- [ControlInputParameter](#)
- [ControlScope](#)
- [CopyAction](#)
- [CopyJob](#)
- [CopyJobSummary](#)
- [DateRange](#)
- [Framework](#)
- [FrameworkControl](#)
- [IndexAction](#)
- [IndexedRecoveryPoint](#)
- [KeyValue](#)
- [LatestMpaApprovalTeamUpdate](#)
- [LatestRevokeRequest](#)
- [LegalHold](#)
- [Lifecycle](#)
- [ProtectedResource](#)
- [ProtectedResourceConditions](#)
- [RecoveryPointByBackupVault](#)
- [RecoveryPointByResource](#)
- [RecoveryPointCreator](#)
- [RecoveryPointMember](#)
- [RecoveryPointSelection](#)

- [ReportDeliveryChannel](#)
- [ReportDestination](#)
- [ReportJob](#)
- [ReportPlan](#)
- [ReportSetting](#)
- [ResourceSelection](#)
- [RestoreAccessBackupVaultListMember](#)
- [RestoreJobCreator](#)
- [RestoreJobsListMember](#)
- [RestoreJobSummary](#)
- [RestoreTestingPlanForCreate](#)
- [RestoreTestingPlanForGet](#)
- [RestoreTestingPlanForList](#)
- [RestoreTestingPlanForUpdate](#)
- [RestoreTestingRecoveryPointSelection](#)
- [RestoreTestingSelectionForCreate](#)
- [RestoreTestingSelectionForGet](#)
- [RestoreTestingSelectionForList](#)
- [RestoreTestingSelectionForUpdate](#)
- [ScanAction](#)
- [ScanJob](#)
- [ScanJobCreator](#)
- [ScanJobSummary](#)
- [ScanResult](#)
- [ScanResultInfo](#)
- [ScanSetting](#)
- [ScheduledPlanExecutionMember](#)
- [TieringConfiguration](#)
- [TieringConfigurationInputForCreate](#)
- [TieringConfigurationInputForUpdate](#)

- [TieringConfigurationsListMember](#)

AdvancedBackupSetting

Servicio: AWS Backup

Las opciones de copia de seguridad para cada tipo de recurso.

Contenido

BackupOptions

Especifica la opción de copia de seguridad para un recurso seleccionado. Esta opción está disponible para los trabajos de copia de seguridad de Windows VSS y las copias de seguridad de S3.

Valores válidos:

Configure "WindowsVSS": "enabled" para habilitar la opción de copia de seguridad de WindowsVSS y crear una copia de seguridad de Windows VSS.

Configure "WindowsVSS": "disabled" para crear una copia de seguridad normal. La opción WindowsVSS no está habilitada de forma predeterminada.

Para las copias de seguridad de S3, configure "S3BackupACLs": "disabled" para excluir las ACL de la copia de seguridad o "S3BackupObjectTags": "disabled" para excluir las etiquetas de objetos de la copia de seguridad. De forma predeterminada, las ACL y las etiquetas de objetos se incluyen en las copias de seguridad de S3.

Si especifica una opción no válida, obtendrá una excepción `InvalidParameterValueException`.

Para obtener más información acerca de las copias de seguridad de Windows VSS, consulte [Creación de una copia de seguridad de Windows habilitada para VSS](#).

Tipo: mapa de cadena a cadena

Patrón de clave: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Patrón de valores: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatorio: no

ResourceType

Especifica un objeto que contiene diferentes opciones de tipos de recursos y copias de seguridad. El único tipo de recurso compatible son las instancias de Amazon EC2 con Windows Volume

Shadow Copy Service (VSS). Para ver un ejemplo de CloudFormation, consulte el [ejemplo de plantilla de CloudFormation para habilitar Windows VSS](#) en la Guía del usuario de AWS Backup.

Valores válidos: -.: EC2.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

AggregatedScanResult

Servicio: AWS Backup

Contiene resultados de escaneo agregados en múltiples operaciones de escaneo, proporcionando un resumen del estado del escaneo y los hallazgos.

Contenido

FailedScan

Un valor booleano que indica si alguno de los escaneos agregados ha fallado.

Tipo: Booleano

Obligatorio: no

Findings

Conjunto de hallazgos descubiertos en todos los escaneos agregados.

Tipo: matriz de cadenas

Valores válidos: MALWARE

Obligatorio: no

LastComputed

La marca temporal en la que se calculó por última vez el resultado agregado del escaneo, en formato Unix y en hora universal coordinada (UTC).

Tipo: marca temporal

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

BackupJob

Servicio: AWS Backup

Contiene información detallada acerca de un trabajo de copia de seguridad.

Contenido

AccountId

El ID de la cuenta a la que pertenece el trabajo de copia de seguridad.

Tipo: cadena

Patrón: `^[0-9]{12}$`

Obligatorio: no

BackupJobId

Identifica de forma exclusiva una solicitud de AWS Backup para hacer una copia de seguridad de un recurso.

Tipo: cadena

Requerido: no

BackupOptions

Especifica la opción de copia de seguridad para un recurso seleccionado. Esta opción solo está disponible para los trabajos de copia de seguridad de Windows Volume Shadow Copy Service (VSS).

Valores válidos: configure `"WindowsVSS": "enabled"` para habilitar la opción de copia de seguridad de WindowsVSS y crear una copia de seguridad de Windows VSS. Configure `"WindowsVSS": "disabled"` para crear una copia de seguridad normal. Si especifica una opción no válida, obtendrá una excepción `InvalidParameterValueException`.

Tipo: mapa de cadena a cadena

Patrón de clave: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Patrón de valores: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatorio: no

BackupSizeInBytes

Es el tamaño de una copia de seguridad (punto de recuperación) en bytes.

Este valor puede representarse de forma diferente según el tipo de recurso, ya que AWS Backup extrae información de los datos de otros servicios de AWS. Por ejemplo, el valor devuelto puede mostrar un valor 0, que puede ser distinto al valor previsto.

A continuación se describe el comportamiento esperado de los valores por tipo de recurso:

- En Amazon Aurora, Amazon DocumentDB y Amazon Neptune, este valor no se rellena con la operación `GetBackupJobStatus`.
- En el caso de Amazon DynamoDB con características avanzadas, este valor es el tamaño del punto de recuperación (copia de seguridad).
- Amazon EC2 y Amazon EBS muestran el tamaño del volumen (almacenamiento aprovisionado) que se devuelve con este valor. Amazon EBS no devuelve información sobre el tamaño de la copia de seguridad; el tamaño de la instantánea tendrá el mismo valor que el recurso original a partir del cual se realizó la copia de seguridad.
- En Amazon EFS, este valor hace referencia a los bytes delta transferidos durante una copia de seguridad.
- Amazon FSx no rellena este valor de la operación `GetBackupJobStatus` para los sistemas de archivo de FSx.
- Una instancia de Amazon RDS se mostrará como 0.
- En el caso de las máquinas virtuales que ejecutan VMware, este valor se transfiere a AWS Backup través de un flujo de trabajo asíncrono, lo que puede significar que el valor mostrado puede representar de forma insuficiente el tamaño real de la copia de seguridad.

Tipo: Long

Obligatorio: no

BackupType

Representa el tipo de copia de seguridad de un trabajo de copia de seguridad.

Tipo: cadena

Requerido: no

BackupVaultArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un almacén de copia de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

Requerido: no

BackupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: no

BytesTransferred

El tamaño en bytes transferido a un almacén de copias de seguridad en el momento en que se consultó el estado del trabajo.

Tipo: Long

Obligatorio: no

CompletionDate

La fecha y la hora en que se completó un trabajo para crear un trabajo de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de `CompletionDate` tiene una precisión de milisegundos. Por ejemplo, el valor `1516925490.087` representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

CreatedBy

Contiene información de identificación sobre la creación de un trabajo de copia de seguridad, que incluye los valores de `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion` y `BackupRuleId` del plan de copia de seguridad utilizado para crearlo.

Tipo: objeto [RecoveryPointCreator](#)

Obligatorio: no

CreationDate

La fecha y la hora en que se creó el trabajo de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

EncryptionKeyArn

Es el nombre de recurso de Amazon (ARN) de la clave de KMS que se utiliza para cifrar la copia de seguridad. Puede ser una clave administrada por el cliente o una clave administrada de AWS, en función de la configuración del almacén.

Tipo: cadena

Requerido: no

ExpectedCompletionDate

La fecha y la hora en que se espera completar un trabajo de copia de seguridad de recursos, en formato Unix y horario universal coordinado (UTC). El valor de `ExpectedCompletionDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

IamRoleArn

Especifica el ARN del rol de IAM utilizado para crear el punto de recuperación de destino. Los roles de IAM distintos del rol predeterminado deben incluir `AWSBackup` o `AwsBackup` en el

nombre del rol. Por ejemplo, `arn:aws:iam::123456789012:role/AWSBackupRDSAccess`. Los nombres de los roles sin esas cadenas carecen de permisos para realizar trabajos de copia de seguridad.

Tipo: cadena

Requerido: no

InitiationDate

La fecha en que se inició un trabajo de copia de seguridad.

Tipo: marca temporal

Obligatorio: no

IsEncrypted

Es un valor booleano que indica si la copia de seguridad está cifrada. Todas las copias de seguridad de AWS Backup están cifradas, pero este campo indica el estado de cifrado para garantizar la transparencia.

Tipo: Booleano

Obligatorio: no

IsParent

Se trata de un valor booleano que indica que es un trabajo de copia de seguridad principal (compuesto).

Tipo: Booleano

Obligatorio: no

MessageCategory

Este parámetro es el recuento de trabajos de la categoría de mensajes especificada.

Las cadenas de ejemplo pueden ser `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` y `INVALIDPARAMETERS`. Consulte en [Monitorización](#) una lista de cadenas de `MessageCategory`.

El valor `ANY` devuelve el recuento de todas las categorías de mensajes.

`AGGREGATE_ALL` suma los recuentos de trabajos de todas las categorías de mensajes y devuelve la suma.

Tipo: cadena

Requerido: no

ParentJobId

Identifica de forma exclusiva una solicitud de AWS Backup para hacer una copia de seguridad de un recurso. Se devolverá el ID del trabajo principal (compuesto).

Tipo: cadena

Requerido: no

PercentDone

Contiene el porcentaje estimado que se ha completado de un trabajo en el momento en que se consultó el estado del trabajo.

Tipo: cadena

Requerido: no

RecoveryPointArn

Un ARN que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

Requerido: no

RecoveryPointLifecycle

Especifica el período, en días, antes de que un punto de recuperación se transfiera al almacenamiento en frío o se elimine.

Las copias de seguridad que se han migrado al almacenamiento en frío deben permanecer en él durante un mínimo de 90 días. Por lo tanto, en la consola, el valor de retención debe tener 90 días más que el valor del número de días tras los cuales se transferirá al almacenamiento en frío. El valor de "transition to cold after days" (número de días tras los cuales migrará a almacenamiento en frío) no puede cambiarse una vez que se ha migrado una copia de seguridad al almacenamiento en frío.

Los tipos de recursos que se pueden transferir al almacenamiento en frío se enumeran en la tabla [Disponibilidad de características por recurso](#). AWS Backup omite esta expresión para otros tipos de recurso.

Para eliminar el ciclo de vida y los períodos de retención existentes y conservar los puntos de recuperación indefinidamente, especifique -1 para `MoveToColdStorageAfterDays` y `DeleteAfterDays`.

Tipo: objeto [Lifecycle](#)

Obligatorio: no

ResourceArn

Un ARN que identifica de forma única a un recurso. El formato del ARN depende del tipo de recurso.

Tipo: cadena

Requerido: no

ResourceName

El nombre no exclusivo del recurso que pertenece a la copia de seguridad especificada.

Tipo: cadena

Requerido: no

ResourceType

El tipo de recurso de AWS del que se va a hacer la copia de seguridad; por ejemplo, un volumen de Amazon Elastic Block Store (Amazon EBS) o una base de datos de Amazon Relational Database Service (Amazon RDS). Para las copias de seguridad de Windows Volume Shadow Copy Service (VSS), el único tipo de recurso admitido es Amazon EC2.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatorio: no

StartBy

Especifica la hora en formato Unix y horario universal coordinado (UTC) en la que se debe iniciar un trabajo de copia de seguridad antes de que se cancele. El valor se calcula agregando el

periodo de inicio a la hora programada. Por lo tanto, si la hora programada fueran las 18:00 h y el periodo de inicio fuera de 2 horas, la hora `StartBy` sería las 20:00 h en la fecha especificada. El valor de `StartBy` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

State

El estado actual de un trabajo de copia de seguridad.

Tipo: cadena

Valores válidos: `CREATED` | `PENDING` | `RUNNING` | `ABORTING` | `ABORTED` | `COMPLETED` | `FAILED` | `EXPIRED` | `PARTIAL`

Obligatorio: no

StatusMessage

Un mensaje detallado que explica el estado del trabajo de copia de seguridad de un recurso.

Tipo: cadena

Requerido: no

VaultLockState

Es el estado de bloqueo del almacén de copias de seguridad. En el caso de los almacenes aislados lógicamente, indica si el almacén está bloqueado en el modo de conformidad. Los valores válidos son `LOCKED` y `UNLOCKED`.

Tipo: cadena

Requerido: no

VaultType

Es el tipo de almacén de copias de seguridad en el que se guarda el punto de recuperación. Los valores válidos son `BACKUP_VAULT` para los almacenes de copias de seguridad estándar y `LOGICALLY_AIR_GAPPED_BACKUP_VAULT` para los almacenes aislados lógicamente.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

BackupJobSummary

Servicio: AWS Backup

Es un resumen de los trabajos creados o en ejecución en los 30 últimos días.

El resumen devuelto puede contener lo siguiente: Region, Account, State, ResourceType, MessageCategory, StartTime, EndTime y Count de trabajos incluidos.

Contenido

AccountId

El ID de la cuenta propietaria de los trabajos del resumen.

Tipo: cadena

Patrón: `^[0-9]{12}$`

Obligatorio: no

Count

El valor expresado como número de trabajos en un resumen de trabajos.

Tipo: entero

Obligatorio: no

EndTime

El valor de hora en formato numérico de la hora de finalización de un trabajo.

Este valor es la hora en formato Unix, Hora universal coordinada (UTC) y tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

MessageCategory

Este parámetro es el recuento de trabajos de la categoría de mensajes especificada.

Las cadenas de ejemplo pueden ser AccessDenied, Success y InvalidParameters. Consulte en [Monitorización](#) una lista de cadenas de MessageCategory.

El valor ANY devuelve el recuento de todas las categorías de mensajes.

AGGREGATE_ALL suma los recuentos de trabajos de todas las categorías de mensajes y devuelve la suma.

Tipo: cadena

Requerido: no

Region

Las regiones de AWS incluidas en el resumen del trabajo.

Tipo: cadena

Requerido: no

ResourceType

Este valor es el recuento de trabajos para el tipo de recurso especificado. La solicitud GetSupportedResourceTypes devuelve cadenas para los tipos de recursos compatibles.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatorio: no

StartTime

El valor de hora en formato numérico de la hora de inicio de un trabajo.

Este valor es la hora en formato Unix, Hora universal coordinada (UTC) y tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

State

Este valor es el recuento de trabajos con el estado especificado.

Tipo: cadena

Valores válidos: CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED
| FAILED | EXPIRED | PARTIAL | AGGREGATE_ALL | ANY

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

BackupPlan

Servicio: AWS Backup

Contiene un nombre de visualización de plan de copia de seguridad opcional y una matriz de objetos `BackupRule`, cada uno de los cuales especifica una regla de copia de seguridad. Cada regla de un plan de copia de seguridad es una tarea programada independiente y puede hacer una copia de seguridad de una selección diferente de recursos de AWS .

Contenido

BackupPlanName

El nombre de visualización del plan de copia de seguridad. Debe contener solo caracteres alfanuméricos o “-”. caracteres especiales.

Si se establece en la consola, puede contener de 1 a 50 caracteres; si se establece mediante CLI o API, puede contener de 1 a 200 caracteres.

Tipo: cadena

Obligatorio: sí

Rules

Una matriz de objetos `BackupRule`, cada uno de los cuales especifica una tarea programada que se utiliza para realizar una copia de seguridad de una selección de recursos.

Tipo: matriz de objetos [BackupRule](#)

Obligatorio: sí

AdvancedBackupSettings

Contiene una lista de `BackupOptions` para cada tipo de recurso.

Tipo: matriz de objetos [AdvancedBackupSetting](#)

Obligatorio: no

ScanSettings

Contiene la configuración de escaneo para el plan de respaldo e incluye el escáner de malware, los recursos seleccionados y la función del escáner.

Tipo: matriz de objetos [ScanSetting](#)

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

BackupPlanInput

Servicio: AWS Backup

Contiene un nombre de visualización de plan de copia de seguridad opcional y una matriz de objetos `BackupRule`, cada uno de los cuales especifica una regla de copia de seguridad. Cada regla de un plan de copia de seguridad es una tarea programada independiente.

Contenido

BackupPlanName

El nombre de visualización del plan de copia de seguridad. Debe contener de 1 a 50 caracteres alfanuméricos o “_”. caracteres.

Tipo: cadena

Obligatorio: sí

Rules

Una matriz de objetos `BackupRule`, cada uno de los cuales especifica una tarea programada que se utiliza para realizar una copia de seguridad de una selección de recursos.

Tipo: matriz de objetos [BackupRuleInput](#)

Obligatorio: sí

AdvancedBackupSettings

Especifica una lista de `BackupOptions` para cada tipo de recurso. Esta configuración solo está disponible para los trabajos de copia de seguridad de Windows Volume Shadow Copy Service (VSS).

Tipo: matriz de objetos [AdvancedBackupSetting](#)

Obligatorio: no

ScanSettings

Contiene la configuración de escaneo para la regla de respaldo e incluye el escáner de malware y el modo de escaneo completo o incremental.

Tipo: matriz de objetos [ScanSetting](#)

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

BackupPlansListMember

Servicio: AWS Backup

Contiene metadatos sobre un plan de copia de seguridad.

Contenido

AdvancedBackupSettings

Contiene una lista de BackupOptions para un tipo de recurso.

Tipo: matriz de objetos [AdvancedBackupSetting](#)

Obligatorio: no

BackupPlanArn

Un nombre de recurso de Amazon (ARN) que identifica de forma única un plan de copia de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Tipo: cadena

Requerido: no

BackupPlanId

Identifica de forma única un plan de copia de seguridad.

Tipo: cadena

Requerido: no

BackupPlanName

El nombre de visualización del plan de copia de seguridad guardado.

Tipo: cadena

Requerido: no

CreationDate

La fecha y la hora en que se creó el plan de copia de seguridad de un recurso, en formato Unix y horario universal coordinado (UTC). El valor de CreationDate tiene una precisión de

milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

CreatorRequestId

Una cadena única que identifica la solicitud y permite que se reintenten las solicitudes que han producido un error sin el riesgo de ejecutar la operación dos veces. Este parámetro es opcional.

Si se utiliza, este parámetro debe contener de 1 a 50 caracteres alfanuméricos o “-”. caracteres.

Tipo: cadena

Requerido: no

DeletionDate

La fecha y la hora en que se eliminó el plan de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de `DeletionDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

LastExecutionDate

La última vez que se ejecutó este plan de copia de seguridad. Una fecha y hora, en formato Unix y horario universal coordinado (UTC). El valor de `LastExecutionDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

VersionId

Cadenas cifradas en UTF-8, Unicode, únicas, generadas aleatoriamente que tienen como máximo una longitud de 1024 bytes. Los ID de versión no se pueden editar.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

BackupPlanTemplatesListMember

Servicio: AWS Backup

Un objeto que especifica los metadatos asociados a una plantilla de plan de copia de seguridad.

Contenido

BackupPlanTemplateId

Identifica de forma exclusiva una plantilla de plan de copia de seguridad almacenada.

Tipo: cadena

Requerido: no

BackupPlanTemplateName

El nombre de visualización opcional de la plantilla de copia de seguridad.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

BackupRule

Servicio: AWS Backup

Especifica una tarea programada utilizada para hacer una copia de seguridad de una selección de recursos.

Contenido

RuleName

Un nombre de visualización para una regla de copia de seguridad. Debe contener de 1 a 50 caracteres alfanuméricos o “-”. caracteres.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatorio: sí

TargetBackupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\.]{2,50}$`

Obligatorio: sí

CompletionWindowMinutes

Un valor en minutos después de que un trabajo de copia de seguridad se haya iniciado correctamente antes que AWS Backup deba completarlo o cancelarlo. Este valor es opcional.

Tipo: largo

Obligatorio: no

CopyActions

Una matriz de objetos `CopyAction`, que contiene los detalles de la operación de copia.

Tipo: matriz de objetos [CopyAction](#)

Obligatorio: no

EnableContinuousBackup

Especifica si AWS Backup crea copias de seguridad continuas. True hace AWS Backup que se creen copias de seguridad continuas con capacidad de point-in-time restauración (PITR). Si es falso (o no se ha especificado), AWS Backup se crean copias de seguridad instantáneas.

Tipo: Booleano

Obligatorio: no

IndexActions

IndexActions es una matriz que se utiliza para especificar cómo se deben indexar los datos de las copias de seguridad.

Cada una BackupRule puede tener 0 o 1 IndexAction, ya que cada copia de seguridad puede tener hasta un índice asociado.

Dentro de la matriz está ResourceType. Solo se aceptará uno para cada uno BackupRule.

Tipo: matriz de objetos [IndexAction](#)

Obligatorio: no

Lifecycle

El ciclo de vida define cuándo un recurso protegido pasa a almacenamiento en frío y cuándo caduca. AWS Backup cambia y vence las copias de seguridad automáticamente según el ciclo de vida que usted defina.

Las copias de seguridad que se transfieran al almacenamiento en frío deben almacenarse en un almacenamiento en frío durante un mínimo de 90 días. Por lo tanto, el valor de retención debe tener 90 días más que el valor del número de días tras los cuales se transferirá al almacenamiento en frío. El valor de “número de días tras los cuales migrará a almacenamiento en frío” no puede cambiarse una vez que se ha migrado una copia de seguridad al almacenamiento en frío.

Los tipos de recursos que pueden pasar al almacenamiento en frío se enumeran en la tabla [Disponibilidad de funciones por recurso](#). AWS Backup omite esta expresión para otros tipos de recursos.

Tipo: objeto [Lifecycle](#)

Obligatorio: no

RecoveryPointTags

Las etiquetas que se asignan a los recursos asociados a esta regla cuando se restauran desde una copia de seguridad.

Tipo: mapa de cadena a cadena

Obligatorio: no

RuleId

Identifica de forma exclusiva una regla que se utiliza para programar la copia de seguridad de una selección de recursos.

Tipo: cadena

Requerido: no

ScanActions

Contiene la configuración de escaneo para la regla de respaldo e incluye el escáner de malware y el modo de escaneo completo o incremental.

Tipo: matriz de objetos [ScanAction](#)

Obligatorio: no

ScheduleExpression

Expresión cron en UTC que especifica cuándo se AWS Backup inicia un trabajo de copia de seguridad. Si no se proporciona ninguna expresión CRON, AWS Backup utilizará la expresión por defecto. `cron(0 5 ? * * *)`

Para obtener más información sobre las expresiones AWS cron, consulte [Programar expresiones para reglas](#) en la Guía del usuario de Amazon CloudWatch Events.

Dos ejemplos de expresiones AWS cron son `15 * ? * * *` (realizar una copia de seguridad cada hora 15 minutos después de la hora) y `0 12 * * ? * *` (realizar una copia de seguridad todos los días a las 12 del mediodía UTC).

Para ver una tabla de ejemplos, haga clic en el enlace anterior y desplácese hacia abajo en la página.

Tipo: cadena

Requerido: no

`ScheduleExpressionTimezone`

La zona horaria en la que se establece la expresión de programación. De forma predeterminada, `ScheduleExpressions` están en UTC. Puede modificar esto para una zona horaria específica.

Tipo: cadena

Requerido: no

`StartWindowMinutes`

Un valor en minutos después del que una copia de seguridad está programada antes de que se cancele el trabajo si no se ha iniciado correctamente. Este valor es opcional. Si se incluye este valor, debe ser de al menos 60 minutos para evitar errores.

Durante el intervalo de inicio, el estado del trabajo de copia de seguridad permanece en ese estado `CREATED` hasta que comience correctamente o hasta que se agote el tiempo del intervalo de inicio. Si dentro de la ventana de inicio, Time AWS Backup recibe un error que permite volver a intentar el trabajo, AWS Backup volverá a intentarlo automáticamente al menos cada 10 minutos hasta que la copia de seguridad comience correctamente (el estado del trabajo cambia a `RUNNING`) o hasta que el estado del trabajo cambie a `EXPIRED` (lo que se espera que ocurra cuando finalice el tiempo de la ventana de inicio).

Tipo: largo

Obligatorio: no

`TargetLogicallyAirGappedBackupVaultArn`

El ARN de una bóveda con huecos de aire lógicos. El ARN debe estar en la misma cuenta y región. Si se proporcionan, los recursos compatibles totalmente gestionados realizan copias de seguridad directamente en un almacén aislado de forma lógica, mientras que otros recursos compatibles crean una instantánea temporal (facturable) en el almacén de respaldo y, a continuación, la copian en un almacén aislado de forma lógica. Los recursos no compatibles solo se respaldan en el almacén de respaldo especificado.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

BackupRuleInput

Servicio: AWS Backup

Especifica una tarea programada utilizada para hacer una copia de seguridad de una selección de recursos.

Contenido

RuleName

Un nombre de visualización para una regla de copia de seguridad. Debe contener de 1 a 50 caracteres alfanuméricos o “-”. caracteres.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatorio: sí

TargetBackupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\.]{2,50}$`

Obligatorio: sí

CompletionWindowMinutes

Un valor en minutos después de que un trabajo de copia de seguridad se haya iniciado correctamente antes que AWS Backup deba completarlo o cancelarlo. Este valor es opcional.

Tipo: largo

Obligatorio: no

CopyActions

Una matriz de objetos `CopyAction`, que contiene los detalles de la operación de copia.

Tipo: matriz de objetos [CopyAction](#)

Obligatorio: no

EnableContinuousBackup

Especifica si AWS Backup crea copias de seguridad continuas. True hace AWS Backup que se creen copias de seguridad continuas con capacidad de point-in-time restauración (PITR). Si es falso (o no se ha especificado), AWS Backup se crean copias de seguridad instantáneas.

Tipo: Booleano

Obligatorio: no

IndexActions

Puede haber hasta una IndexAction en cada una BackupRule, ya que cada copia de seguridad puede tener 0 o 1 índice de copia de seguridad asociado.

Dentro de la matriz está ResourceTypes. Solo se aceptará 1 tipo de recurso para cada uno BackupRule. Valores válidos:

- EBS para Amazon Elastic Block Store (EBS)
- S3 para Amazon Simple Storage Service (Amazon S3)

Tipo: matriz de objetos [IndexAction](#)

Obligatorio: no

Lifecycle

El ciclo de vida define cuándo un recurso protegido pasa a almacenamiento en frío y cuándo caduca. AWS Backup realizará la transición y caducará las copias de seguridad automáticamente según el ciclo de vida que usted defina.

Las copias de seguridad que se transfieran al almacenamiento en frío deben almacenarse en un almacenamiento en frío durante un mínimo de 90 días. Por lo tanto, el valor de retención debe tener 90 días más que el valor del número de días tras los cuales se transferirá al almacenamiento en frío. El valor de "transition to cold after days" (número de días tras los cuales migrará a almacenamiento en frío) no puede cambiarse una vez que se ha migrado una copia de seguridad al almacenamiento en frío.

Los tipos de recursos que pueden pasar al almacenamiento en frío se enumeran en la tabla [Disponibilidad de funciones por recurso](#). AWS Backup omite esta expresión para otros tipos de recursos.

Este parámetro tiene un valor máximo de 100 años (36 500 días).

Tipo: objeto [Lifecycle](#)

Obligatorio: no

RecoveryPointTags

Las etiquetas para asignar a los recursos.

Tipo: mapa de cadena a cadena

Obligatorio: no

ScanActions

Contiene la configuración de escaneo para la regla de respaldo e incluye el escáner de malware y el modo de escaneo completo o incremental.

Tipo: matriz de objetos [ScanAction](#)

Obligatorio: no

ScheduleExpression

Expresión CRON en UTC que especifica cuándo se AWS Backup inicia un trabajo de copia de seguridad. Si no se proporciona ninguna expresión CRON, AWS Backup utilizará la expresión por defecto. `cron(0 5 ? * * *)`

Tipo: cadena

Requerido: no

ScheduleExpressionTimezone

La zona horaria en la que se establece la expresión de programación. De forma predeterminada, ScheduleExpressions están en UTC. Puede modificar esto para una zona horaria específica.

Tipo: cadena

Requerido: no

StartWindowMinutes

Un valor en minutos después del que una copia de seguridad está programada antes de que se cancele el trabajo si no se ha iniciado correctamente. Este valor es opcional. Si se incluye este valor, debe ser de al menos 60 minutos para evitar errores.

Este parámetro tiene un valor máximo de 100 años (52 560 000 minutos).

Durante el intervalo de inicio, el estado del trabajo de copia de seguridad permanece en ese estado CREATED hasta que comience correctamente o hasta que se agote el tiempo del intervalo de inicio. Si dentro de la ventana de inicio, Time AWS Backup recibe un error que permite volver a intentar el trabajo, AWS Backup volverá a intentarlo automáticamente al menos cada 10 minutos hasta que la copia de seguridad comience correctamente (el estado del trabajo cambia a RUNNING) o hasta que el estado del trabajo cambie a EXPIRED (lo que se espera que ocurra cuando finalice el tiempo de la ventana de inicio).

Tipo: largo

Obligatorio: no

TargetLogicallyAirGappedBackupVaultArn

El ARN de una bóveda con huecos de aire lógicos. El ARN debe estar en la misma cuenta y región. Si se proporcionan, los recursos compatibles totalmente gestionados realizan copias de seguridad directamente en un almacén aislado de forma lógica, mientras que otros recursos compatibles crean una instantánea temporal (facturable) en el almacén de respaldo y, a continuación, la copian en un almacén aislado de forma lógica. Los recursos no compatibles solo se respaldan en el almacén de respaldo especificado.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

BackupSelection

Servicio: AWS Backup

Se usa para especificar un conjunto de recursos para un plan de copia de seguridad.

Le recomendamos que especifique las condiciones, etiquetas o recursos que desee incluir o excluir. De lo contrario, Backup intentará seleccionar todos los recursos de almacenamiento compatibles y opcionales, lo que podría tener implicaciones de costo imprevistas.

Para obtener más información, consulte [Asignación de recursos mediante programación](#).

Contenido

IamRoleArn

El ARN del rol de IAM que AWS Backup utiliza para autenticarse al crear copias de seguridad del recurso de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

Obligatorio: sí

SelectionName

El nombre de visualización de un documento de selección de recursos. Debe contener de 1 a 50 caracteres alfanuméricos o “-”. caracteres.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatorio: sí

Conditions

Las condiciones que defina para asignar recursos a sus planes de copia de seguridad mediante etiquetas. Por ejemplo, `"StringEquals": { "ConditionKey": "aws:ResourceTag/backup", "ConditionValue": "daily" }`.

Conditions admite `StringEquals`, `StringLike`, `StringNotEquals` y `StringNotLike`. Los operadores de condición distinguen entre mayúsculas y minúsculas.

Si especifica varias condiciones, los recursos deben coincidir con todas las condiciones (lógica AND).

Tipo: objeto [Conditions](#)

Obligatorio: no

ListOfTags

Le recomendamos que utilice el parámetro `Conditions` en lugar de este parámetro.

Las condiciones que defina para asignar recursos a sus planes de copia de seguridad mediante etiquetas. Por ejemplo, `"StringEquals": { "ConditionKey": "backup", "ConditionValue": "daily" }`.

`ListOfTags` solo es compatible con `StringEquals`. Los operadores de condición distinguen entre mayúsculas y minúsculas.

Si especifica varias condiciones, los recursos deben coincidir con cualquiera de las condiciones (lógica OR).

Tipo: matriz de objetos [Condition](#)

Obligatorio: no

NotResources

La lista de nombres de recursos de Amazon (ARN) de los recursos que se van a excluir de un plan de copia de seguridad. El número máximo de ARN es 500 sin caracteres comodín o 30 ARN con caracteres comodín.

Si necesita excluir muchos recursos de un plan de copia de seguridad, considere una estrategia de selección de recursos diferente, como asignar solo uno o unos pocos tipos de recursos o refinar su selección de recursos utilizando etiquetas.

Tipo: matriz de cadenas

Obligatorio: no

Resources

La lista de nombres de recursos de Amazon (ARN) de los recursos que se van a asignar a un plan de copia de seguridad. El número máximo de ARN es 500 sin caracteres comodín o 30 ARN con caracteres comodín.

Si necesita asignar muchos recursos a un plan de copia de seguridad, considere una estrategia de selección de recursos diferente, como asignar todos los recursos de un tipo de recurso o ajustar su selección de recursos mediante etiquetas.

Si especifica varios ARN, los recursos deben coincidir con cualquiera de los ARN (lógica OR).

Tipo: matriz de cadenas

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

BackupSelectionsListMember

Servicio: AWS Backup

Contiene metadatos sobre un objeto `BackupSelection`.

Contenido

`BackupPlanId`

Identifica de forma única un plan de copia de seguridad.

Tipo: cadena

Requerido: no

`CreationDate`

La fecha y la hora en que se creó el plan de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

`CreatorRequestId`

Una cadena única que identifica la solicitud y permite que se reintenten las solicitudes que han producido un error sin el riesgo de ejecutar la operación dos veces. Este parámetro es opcional.

Si se utiliza, este parámetro debe contener de 1 a 50 caracteres alfanuméricos o “-_”. caracteres.

Tipo: cadena

Requerido: no

`IamRoleArn`

Especifica el nombre de recurso de Amazon (ARN) del rol de IAM para crear el punto de recuperación de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

Requerido: no

SelectionId

Identifica de forma única una solicitud para asignar un conjunto de recursos a un plan de copia de seguridad.

Tipo: cadena

Requerido: no

SelectionName

El nombre de visualización de un documento de selección de recursos.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

BackupVaultListMember

Servicio: AWS Backup

Contiene metadatos sobre un almacén de copias de seguridad.

Contenido

BackupVaultArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un almacén de copia de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

Requerido: no

BackupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: no

CreationDate

La fecha y la hora en que se creó la copia de seguridad de un recurso, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor `1516925490.087` representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

CreatorRequestId

Una cadena única que identifica la solicitud y permite que se reintenten las solicitudes que han producido un error sin el riesgo de ejecutar la operación dos veces. Este parámetro es opcional.

Si se utiliza, este parámetro debe contener de 1 a 50 caracteres alfanuméricos o “-”. caracteres.

Tipo: cadena

Requerido: no

EncryptionKeyArn

Una clave de cifrado del lado del servidor que puede especificar para cifrar las copias de seguridad de los servicios que admiten la AWS Backup administración completa; por ejemplo, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab` Si especifica una clave, debe especificar su ARN, no su alias. Si no especifica ninguna clave, AWS Backup crea una clave de KMS para usted de forma predeterminada.

Para saber qué AWS Backup servicios admiten la AWS Backup administración completa y cómo se AWS Backup gestiona el cifrado de las copias de seguridad de los servicios que aún no lo son AWS Backup, consulte [Cifrado](#) de copias de seguridad en AWS Backup

Tipo: cadena

Requerido: no

EncryptionKeyType

El tipo de clave de cifrado utilizada para el almacén de copias de seguridad. Los valores válidos son `CUSTOMER_MANAGED_KMS_KEY` para las claves administradas por el cliente o `_OWNED_KMS_KEY` para las claves propiedad del cliente. AWS AWS

Tipo: cadena

Valores válidos: `AWS_OWNED_KMS_KEY` | `CUSTOMER_MANAGED_KMS_KEY`

Obligatorio: no

LockDate

La fecha y la hora en que la configuración de Vault Lock pasa a ser inmutable, lo que significa que no se puede cambiar ni eliminar. AWS Backup

Si ha aplicado el bloqueo de almacenes a su almacén sin especificar una fecha de bloqueo, puede cambiar la configuración del bloqueo de almacenes o eliminarlo del almacén por completo en cualquier momento.

Este valor está en formato Unix, horario universal coordinado (UTC) y tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

Locked

Un valor booleano que indica si AWS Backup Vault Lock se aplica al almacén de respaldo seleccionado. Si `true`, el bloqueo de almacenes impide las operaciones de eliminación y actualización en los puntos de recuperación del almacén seleccionado.

Tipo: Booleano

Obligatorio: no

MaxRetentionDays

La configuración de bloqueo del AWS Backup almacén que especifica el período máximo de retención durante el que el almacén conserva sus puntos de recuperación. Si no se especifica este parámetro, el bloqueo de almacenes no impone un periodo de retención máximo en los puntos de recuperación del almacén (lo que permite un almacenamiento indefinido).

Si se especifica, cualquier trabajo de copia de seguridad o copia en el almacén debe tener una política de ciclo de vida con un periodo de retención igual o inferior al periodo de retención máximo. Si el periodo de retención del trabajo es superior a ese periodo de retención máximo, el almacén falla el trabajo de copia de seguridad o de copia de seguridad, y deberá modificar la configuración del ciclo de vida o utilizar un almacén diferente. Los puntos de recuperación ya almacenados en el almacén antes del bloqueo del mismo no se ven afectados.

Tipo: largo

Obligatorio: no

MinRetentionDays

La configuración de bloqueo del AWS Backup almacén que especifica el período mínimo de retención durante el que el almacén conserva sus puntos de recuperación. Si no se especifica este parámetro, el bloqueo del almacén no impondrá un periodo mínimo de retención.

Si se especifica, cualquier trabajo de copia de seguridad o copia en el almacén debe tener una política de ciclo de vida con un periodo de retención igual o superior al periodo de retención

mínimo. Si el periodo de retención del trabajo es más breve que ese periodo de retención mínimo, el almacén dará error en el trabajo de copia de seguridad o copia, y deberá modificar la configuración del ciclo de vida o usar un almacén diferente. Los puntos de recuperación ya almacenados en el almacén antes del bloqueo del mismo no se ven afectados.

Tipo: largo

Obligatorio: no

NumberOfRecoveryPoints

El número de puntos de recuperación que se almacenan en un almacén de copias de seguridad.

Tipo: largo

Obligatorio: no

VaultState

El estado actual del almacén.

Tipo: cadena

Valores válidos: CREATING | AVAILABLE | FAILED

Obligatorio: no

VaultType

El tipo de almacén en el que se guarda el punto de recuperación descrito.

Tipo: cadena

Valores válidos: BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT |
RESTORE_ACCESS_BACKUP_VAULT

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)

- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

CalculatedLifecycle

Servicio: AWS Backup

Contiene las marcas de tiempo `MoveToColdStorageAt` y `DeleteAt`, que se utilizan para especificar el ciclo de vida de un punto de recuperación.

El ciclo de vida define el momento en que se migra un recurso protegido al almacenamiento en frío y cuándo dicho recurso vence. AWS Backup migra las copias de seguridad y las da por vencidas automáticamente en función del ciclo de vida que se defina.

Las copias de seguridad que se han migrado al almacenamiento en frío deben permanecer en él durante un mínimo de 90 días. Por lo tanto, el valor de retención debe tener 90 días más que el valor del número de días tras los cuales se transferirá al almacenamiento en frío. El valor de "transition to cold after days" (número de días tras los cuales migrará a almacenamiento en frío) no puede cambiarse una vez que se ha migrado una copia de seguridad al almacenamiento en frío.

Los tipos de recursos que se pueden transferir al almacenamiento en frío se enumeran en la tabla [Disponibilidad de características por recurso](#). AWS Backup omite esta expresión para otros tipos de recurso.

Contenido

DeleteAt

Una marca de tiempo que especifica cuándo se debe eliminar un punto de recuperación.

Tipo: marca temporal

Obligatorio: no

MoveToColdStorageAt

Una marca de tiempo que especifica cuándo se debe realizar la transferencia de un punto de recuperación al almacenamiento en frío.

Tipo: marca temporal

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

Condition

Servicio: AWS Backup

Contiene una matriz de triplos compuesta por un tipo de condición (como `StringEquals`), una clave y un valor. Se utiliza para filtrar los recursos mediante sus etiquetas y asignarlos a un plan de copia de seguridad. Distingue mayúsculas de minúsculas.

Contenido

ConditionKey

La clave en un par de clave-valor. Por ejemplo, en la etiqueta `Department: Accounting`, la clave es `Department`.

Tipo: cadena

Obligatorio: sí

ConditionType

Una operación que se aplica a un par clave-valor que se utiliza para asignar recursos a su plan de copia de seguridad. La condición solo es compatible con `StringEquals`. Si desea opciones de asignación más flexibles, incluida `StringLike` y la posibilidad de excluir recursos de su plan de copia de seguridad, utilice `Conditions` (con una "s" al final) para su plan [BackupSelection](#).

Tipo: cadena

Valores válidos: `STRINGEQUALS`

Obligatorio: sí

ConditionValue

El valor de un par clave-valor. Por ejemplo, en la etiqueta `Department: Accounting`, el valor es `Accounting`.

Tipo: cadena

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ConditionParameter

Servicio: AWS Backup

Incluye información sobre las etiquetas que se definen para asignar recursos etiquetados a un plan de copia de seguridad.

Incluya el prefijo `aws:ResourceTag` en sus etiquetas. Por ejemplo, `"aws:ResourceTag/TagKey1": "Value1"`.

Contenido

ConditionKey

La clave en un par de clave-valor. Por ejemplo, en la etiqueta `Department: Accounting`, la clave es `Department`.

Tipo: cadena

Requerido: no

ConditionValue

El valor de un par clave-valor. Por ejemplo, en la etiqueta `Department: Accounting`, el valor es `Accounting`.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

Conditions

Servicio: AWS Backup

Contiene información acerca de los recursos que se deben incluir o excluir de un plan de copias de seguridad mediante sus etiquetas. Las condiciones distinguen entre mayúsculas y minúsculas.

Contenido

StringEquals

Filtra los valores de los recursos etiquetados solo para aquellos recursos que se etiquetaron con el mismo valor. También se denomina “coincidencia exacta”.

Tipo: matriz de objetos [ConditionParameter](#)

Obligatorio: no

StringLike

Filtra los valores de los recursos etiquetados para que coincidan con los valores de etiqueta mediante el uso de un carácter comodín (*) en cualquier parte de la cadena. Por ejemplo, “prod*” o “*rod*” coinciden con el valor de etiqueta “production”.

Tipo: matriz de objetos [ConditionParameter](#)

Obligatorio: no

StringNotEquals

Filtra los valores de los recursos etiquetados solo para aquellos recursos que se etiquetaron y que no tienen el mismo valor. También se denomina “coincidencia negada”.

Tipo: matriz de objetos [ConditionParameter](#)

Obligatorio: no

StringNotLike

Filtra los valores de los recursos etiquetados para detectar valores de etiqueta no coincidentes mediante el uso de un carácter comodín (*) en cualquier parte de la cadena.

Tipo: matriz de objetos [ConditionParameter](#)

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ControlInputParameter

Servicio: AWS Backup

Los parámetros para un control. Un control puede tener cero, uno o más parámetros. Un ejemplo de un control con dos parámetros es: “La frecuencia del plan de copia de seguridad es de al menos `daily` y el período de retención es de al menos `1 year`”. El primer parámetro es `daily`. El segundo parámetro es `1 year`.

Contenido

ParameterName

El nombre de un parámetro, por ejemplo, `BackupPlanFrequency`.

Tipo: cadena

Requerido: no

ParameterValue

El valor del parámetro, por ejemplo, `hourly`.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ControlScope

Servicio: AWS Backup

Un marco consta de uno o varios controles. Cada control tiene su propio alcance de control. El alcance de control puede incluir uno o varios tipos de recursos, una combinación de un valor y una clave de etiqueta, o una combinación de un tipo de recurso y un ID de recurso. Si no se especifica ningún alcance, las evaluaciones de la regla se activan cuando cambia la configuración de cualquier recurso del grupo de registro.

Note

Para establecer un alcance de control que incluya todo un recurso en particular, deje `ControlScope` vacío o no lo pase cuando llame a `CreateFramework`.

Contenido

ComplianceResourceIds

El ID del único recurso de AWS que desea que contenga el alcance de control.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 100 artículos.

Obligatorio: no

ComplianceResourceTypes

Describe si el alcance de control incluye uno o más tipos de recursos, como EFS o RDS.

Tipo: matriz de cadenas

Obligatorio: no

Tags

El par de clave-valor de etiqueta que se aplica a los recursos de AWS en los que desea activar una evaluación de una regla. Se puede proporcionar un máximo de un par de clave-valor. El valor de la etiqueta es opcional, pero no puede ser una cadena vacía si está creando o editando un marco desde la consola (aunque el valor puede ser una cadena vacía cuando se incluye en una plantilla de CloudFormation).

La estructura para asignar una etiqueta es .: [{"Key": "string", "Value": "string"}].

Tipo: mapa de cadena a cadena

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

CopyAction

Servicio: AWS Backup

Los detalles de la operación de copia.

Contenido

DestinationBackupVaultArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva el almacén de copia de seguridad de destino para la copia de seguridad copiada. Por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

Obligatorio: sí

Lifecycle

Especifica el período, en días, antes de que un punto de recuperación se transfiera al almacenamiento en frío o se elimine.

Las copias de seguridad que se han migrado al almacenamiento en frío deben permanecer en él durante un mínimo de 90 días. Por lo tanto, en la consola, el valor de retención debe tener 90 días más que el valor del número de días tras los cuales se transferirá al almacenamiento en frío. El valor de "transition to cold after days" (número de días tras los cuales migrará a almacenamiento en frío) no puede cambiarse una vez que se ha migrado una copia de seguridad al almacenamiento en frío.

Los tipos de recursos que se pueden transferir al almacenamiento en frío se enumeran en la tabla [Disponibilidad de características por recurso](#). AWS Backup omite esta expresión para otros tipos de recurso.

Para eliminar el ciclo de vida y los períodos de retención existentes y conservar los puntos de recuperación indefinidamente, especifique -1 para `MoveToColdStorageAfterDays` y `DeleteAfterDays`.

Tipo: objeto [Lifecycle](#)

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

CopyJob

Servicio: AWS Backup

Contiene información detallada acerca de un trabajo de copia.

Contenido

AccountId

El ID de la cuenta a la que pertenece el trabajo de copia.

Tipo: cadena

Patrón: `^[0-9]{12}$`

Obligatorio: no

BackupSizeInBytes

El tamaño de un trabajo de copia, en bytes.

Tipo: largo

Obligatorio: no

ChildJobsInState

Devuelve las estadísticas de los trabajos de copia secundarios (anidados) incluidos.

Tipo: mapa de cadena a largo

Claves válidas: `CREATED` | `RUNNING` | `COMPLETED` | `FAILED` | `PARTIAL`

Obligatorio: no

CompletionDate

La fecha y la hora en que se completó el trabajo de copia, en formato Unix y horario universal coordinado (UTC). El valor de `CompletionDate` tiene una precisión de milisegundos. Por ejemplo, el valor `1516925490.087` representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

CompositeMemberIdentifier

El identificador de un recurso dentro de un grupo compuesto, como un punto de recuperación anidado (secundario) que pertenece a una pila compuesta (principal). El ID se transfiere desde el [ID lógico](#) de una pila.

Tipo: cadena

Requerido: no

CopyJobId

Identifica de forma exclusiva un trabajo de copia.

Tipo: cadena

Requerido: no

CreatedBy

Contiene información sobre el plan de respaldo y la regla que AWS Backup se usaron para iniciar la copia de seguridad del punto de recuperación.

Tipo: objeto [RecoveryPointCreator](#)

Obligatorio: no

CreatedByBackupJobId

El identificador del trabajo de copia de seguridad que inició este trabajo de copia. Solo se aplica a los trabajos de copia programados y a los trabajos de copia automática a un almacén con huecos lógicos.

Tipo: cadena

Requerido: no

CreationDate

La fecha y la hora en que se creó el trabajo de copia, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

DestinationBackupVaultArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un almacén de copias de seguridad de destino al que copiar; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

Requerido: no

DestinationEncryptionKeyArn

Es el nombre de recurso de Amazon (ARN) de la clave de KMS que se utiliza para cifrar la copia de seguridad copiada en el almacén de destino. Puede ser una clave gestionada por el cliente o una clave gestionada. AWS

Tipo: cadena

Requerido: no

DestinationRecoveryPointArn

Un ARN que identifica de forma exclusiva un punto de recuperación de destino; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

Requerido: no

DestinationRecoveryPointLifecycle

Especifica el período, en días, antes de que un punto de recuperación se transfiera al almacenamiento en frío o se elimine.

Las copias de seguridad que se transfieran al almacenamiento en frío deben almacenarse en un almacenamiento en frío durante un mínimo de 90 días. Por lo tanto, en la consola, el valor de retención debe tener 90 días más que el valor del número de días tras los cuales se transferirá al almacenamiento en frío. El valor de "transition to cold after days" (número de días tras los cuales migrará a almacenamiento en frío) no puede cambiarse una vez que se ha migrado una copia de seguridad al almacenamiento en frío.

Los tipos de recursos que pueden pasar al almacenamiento en frío se enumeran en la tabla [Disponibilidad de funciones por recurso](#). AWS Backup omite esta expresión para otros tipos de recursos.

Para eliminar el ciclo de vida y los períodos de retención existentes y conservar los puntos de recuperación indefinidamente, especifique -1 para `MoveToColdStorageAfterDays` y `DeleteAfterDays`.

Tipo: objeto [Lifecycle](#)

Obligatorio: no

`DestinationVaultLockState`

Es el estado de bloqueo del almacén de copias de seguridad de destino. En el caso de los almacenes aislados lógicamente, indica si el almacén está bloqueado en el modo de conformidad. Los valores válidos son `LOCKED` y `UNLOCKED`.

Tipo: cadena

Requerido: no

`DestinationVaultType`

Es el tipo de almacén de copias de seguridad de destino en el que se almacena el punto de recuperación copiado. Los valores válidos son `BACKUP_VAULT` para los almacenes de copias de seguridad estándar y `LOGICALLY_AIR_GAPPED_BACKUP_VAULT` para los almacenes aislados lógicamente.

Tipo: cadena

Requerido: no

`IamRoleArn`

Especifica el ARN del rol de IAM utilizado para copiar el punto de recuperación de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

Requerido: no

`IsParent`

Se trata de un valor booleano que indica que es un trabajo de copia principal (compuesto).

Tipo: Booleano

Obligatorio: no

MessageCategory

Este parámetro es el recuento de trabajos de la categoría de mensajes especificada.

Las cadenas de ejemplo pueden ser AccessDenied, SUCCESS, AGGREGATE_ALL y InvalidParameters. Consulte [Supervisión](#) para obtener una lista de MessageCategory cadenas.

El valor ANY devuelve el recuento de todas las categorías de mensajes.

AGGREGATE_ALL suma los recuentos de trabajos de todas las categorías de mensajes y devuelve la suma

Tipo: cadena

Requerido: no

NumberOfChildJobs

El número de trabajos de copia secundarios (anidados).

Tipo: largo

Obligatorio: no

ParentJobId

Identifica de forma exclusiva una solicitud de AWS Backup para hacer una copia de un recurso. Se devolverá el ID del trabajo principal (compuesto).

Tipo: cadena

Requerido: no

ResourceArn

El AWS recurso que se va a copiar; por ejemplo, un volumen de Amazon Elastic Block Store (Amazon EBS) o una base de datos de Amazon Relational Database Service (Amazon RDS).

Tipo: cadena

Requerido: no

ResourceName

El nombre no exclusivo del recurso que pertenece a la copia de seguridad especificada.

Tipo: cadena

Requerido: no

ResourceType

El tipo de AWS recurso que se va a copiar; por ejemplo, un volumen de Amazon Elastic Block Store (Amazon EBS) o una base de datos de Amazon Relational Database Service (Amazon RDS).

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatorio: no

SourceBackupVaultArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un almacén de copias de origen; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

Requerido: no

SourceRecoveryPointArn

Un ARN que identifica de forma exclusiva un punto de recuperación de origen; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

Requerido: no

State

El estado actual de un trabajo de copia.

Tipo: cadena

Valores válidos: CREATED | RUNNING | COMPLETED | FAILED | PARTIAL

Obligatorio: no

StatusMessage

Un mensaje detallado que explica el estado del trabajo de copia de un recurso.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

CopyJobSummary

Servicio: AWS Backup

Es un resumen de los trabajos de copia creados o en ejecución en los 30 últimos días.

El resumen devuelto puede contener lo siguiente: Region, Account, State, ResourceType, MessageCategory, StartTime, EndTime y Count de trabajos incluidos.

Contenido

AccountId

El ID de la cuenta propietaria de los trabajos del resumen.

Tipo: cadena

Patrón: `^[0-9]{12}$`

Obligatorio: no

Count

El valor expresado como número de trabajos en un resumen de trabajos.

Tipo: entero

Obligatorio: no

EndTime

El valor de hora en formato numérico de la hora de finalización de un trabajo.

Este valor es la hora en formato Unix, Hora universal coordinada (UTC) y tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

MessageCategory

Este parámetro es el recuento de trabajos de la categoría de mensajes especificada.

Las cadenas de ejemplo pueden ser AccessDenied, Success y InvalidParameters. Consulte en [Monitorización](#) una lista de cadenas de MessageCategory.

El valor ANY devuelve el recuento de todas las categorías de mensajes.

AGGREGATE_ALL suma los recuentos de trabajos de todas las categorías de mensajes y devuelve la suma.

Tipo: cadena

Requerido: no

Region

Las regiones de AWS incluidas en el resumen del trabajo.

Tipo: cadena

Requerido: no

ResourceType

Este valor es el recuento de trabajos para el tipo de recurso especificado. La solicitud GetSupportedResourceTypes devuelve cadenas para los tipos de recursos compatibles

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatorio: no

StartTime

El valor de hora en formato numérico de la hora de inicio de un trabajo.

Este valor es la hora en formato Unix, Hora universal coordinada (UTC) y tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

State

Este valor es el recuento de trabajos con el estado especificado.

Tipo: cadena

Valores válidos: CREATED | RUNNING | ABORTING | ABORTED | COMPLETING |
COMPLETED | FAILING | FAILED | PARTIAL | AGGREGATE_ALL | ANY

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

DateRange

Servicio: AWS Backup

Este es un filtro de recursos que contiene FromDate: DateTime y ToDate: DateTime. Ambos valores son obligatorios. No se permiten valores de DateTime futuros.

La fecha y la hora están en formato Unix y horario universal coordinado (UTC) y tienen una precisión de milisegundos (los milisegundos son opcionales). Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Contenido

FromDate

Este valor es la fecha de inicio, inclusive.

La fecha y la hora están en formato Unix y horario universal coordinado (UTC) y tienen una precisión de milisegundos (los milisegundos son opcionales).

Tipo: marca temporal

Obligatorio: sí

ToDate

Este valor es la fecha de finalización, inclusive.

La fecha y la hora están en formato Unix y horario universal coordinado (UTC) y tienen una precisión de milisegundos (los milisegundos son opcionales).

Tipo: marca temporal

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

Framework

Servicio: AWS Backup

Contiene información detallada acerca de un marco. Los marcos contienen controles que evalúan e informan sobre sus eventos y recursos de copia de seguridad. Los marcos generan resultados de conformidad diarios.

Contenido

CreationTime

La fecha y la hora en que se creó un marco con la norma ISO 8601. El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, `2020-07-10T15:00:00.000-08:00` representa el 10 de julio de 2020 a las 15:00 h, 8 horas menos que UTC.

Tipo: marca temporal

Obligatorio: no

DeploymentStatus

El estado de implementación de un marco. Los estados son:

`CREATE_IN_PROGRESS` | `UPDATE_IN_PROGRESS` | `DELETE_IN_PROGRESS` | `COMPLETED`
| `FAILED`

Tipo: cadena

Requerido: no

FrameworkArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un recurso. El formato del ARN depende del tipo de recurso.

Tipo: cadena

Requerido: no

FrameworkDescription

Una descripción opcional del marco con un máximo de 1024 caracteres.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `.*\S.*`

Obligatorio: no

FrameworkName

El nombre único de un marco. Este nombre debe contener entre 1 y 256 caracteres, comenzando por una letra, y contar con letras (a-z, A-Z), números (0-9) y guiones bajos (_).

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `[a-zA-Z][_a-zA-Z0-9]*`

Obligatorio: no

NumberOfControls

El número de controles que contiene el marco.

Tipo: entero

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

FrameworkControl

Servicio: AWS Backup

Contiene información detallada acerca de todos los controles de un marco. Cada marco debe contener al menos un control.

Contenido

ControlName

El nombre de un control. Este nombre tiene entre 1 y 256 caracteres.

Tipo: cadena

Obligatorio: sí

ControlInputParameters

Los pares nombre-valor.

Tipo: matriz de objetos [ControlInputParameter](#)

Obligatorio: no

ControlScope

El alcance de un control. El alcance del control define lo que evaluará el control. Tres ejemplos de alcance de control son: un plan de copia de seguridad específico, todos los planes de copia de seguridad con una etiqueta específica o todos los planes de copia de seguridad.

Para obtener más información, consulte [ControlScope](#).

Tipo: objeto [ControlScope](#)

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)

- [AWS SDK para Ruby V3](#)

IndexAction

Servicio: AWS Backup

Esta es una matriz opcional dentro de una BackupRule.

IndexAction consta de un ResourceTypes.

Contenido

ResourceTypes

Se aceptará una o ninguna acción de indexación por cada BackupRule.

Valores válidos:

- EBS para Amazon Elastic Block Store (EBS)
- S3 para Amazon Simple Storage Service (Amazon S3)

Tipo: matriz de cadenas

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

IndexedRecoveryPoint

Servicio: AWS Backup

Se trata de un punto de recuperación que tiene un índice de copias de seguridad asociado.

En una búsqueda solo se pueden incluir puntos de recuperación con un índice de copias de seguridad.

Contenido

BackupCreationDate

Es la fecha y la hora de creación de una copia de seguridad, expresadas en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor `1516925490.087` representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

BackupVaultArn

Es un ARN que identifica de forma unívoca el almacén de copias de seguridad en el que se almacena el índice de puntos de recuperación.

Por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

Requerido: no

IamRoleArn

Especifica el ARN del rol de IAM utilizado para esta operación.

Por ejemplo, `arn:aws:iam::123456789012:role/S3Access`

Tipo: cadena

Requerido: no

IndexCreationDate

Es la fecha y la hora de creación de un índice de copias de seguridad, expresadas en formato Unix y en horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

IndexStatus

Este es el estado actual del índice de copias de seguridad asociado al punto de recuperación especificado.

Los estados son: PENDING | ACTIVE | FAILED | DELETING

En una búsqueda se puede incluir un punto de recuperación con un índice con el estado ACTIVE.

Tipo: cadena

Valores válidos: PENDING | ACTIVE | FAILED | DELETING

Obligatorio: no

IndexStatusMessage

Es una cadena en forma de mensaje detallado que explica el estado del índice de copias de seguridad asociado al punto de recuperación.

Tipo: cadena

Requerido: no

RecoveryPointArn

Un ARN que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

Requerido: no

ResourceType

Es el tipo de recurso del punto de recuperación indexado.

- EBS para Amazon Elastic Block Store (EBS)
- S3 para Amazon Simple Storage Service (Amazon S3)

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatorio: no

SourceResourceArn

Es una cadena de un Nombre de recurso de Amazon (ARN) que identifica de forma unívoca un recurso de origen.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

KeyValue

Servicio: AWS Backup

Par de dos cadenas relacionadas. Los caracteres permitidos son letras, espacios en blanco y números que se pueden representar en UTF-8, y los siguientes caracteres: + - = . _ : /.

Contenido

Key

La clave de la etiqueta (cadena). La clave no pueden comenzar por aws :.

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: `^(?![aA]{1}[wW]{1}[sS]{1}:)([\\p{L}\\p{Z}\\p{N}_.:/=+\\-@]+)$`

Tipo: cadena

Obligatorio: sí

Value

El valor de la clave.

Limitaciones de longitud: longitud máxima de 256.

Patrón: `^([\\p{L}\\p{Z}\\p{N}_.:/=+\\-@]*)$`

Tipo: cadena

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

LatestMpaApprovalTeamUpdate

Servicio: AWS Backup

Contiene información sobre la última actualización de la asociación del equipo de aprobación MPA.

Contenido

ExpiryDate

Fecha y hora en que caducará la actualización del equipo de aprobación MPA.

Tipo: marca temporal

Obligatorio: no

InitiationDate

Fecha y hora en que se inició la actualización del equipo de aprobación MPA.

Tipo: marca temporal

Obligatorio: no

MpaSessionArn

Es el ARN de la sesión de MPA asociada con esta actualización.

Tipo: cadena

Requerido: no

Status

Es el estado actual de la actualización del equipo de aprobación MPA.

Tipo: cadena

Valores válidos: PENDING | APPROVED | FAILED

Obligatorio: no

StatusMessage

Es un mensaje que describe el estado actual de la actualización del equipo de aprobación MPA.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

LatestRevokeRequest

Servicio: AWS Backup

Contiene información sobre la última solicitud para revocar el acceso a un almacén de copias de seguridad.

Contenido

ExpiryDate

Fecha y hora en que se caduca la solicitud de revocación.

Tipo: marca temporal

Obligatorio: no

InitiationDate

Fecha y hora en que se inició la solicitud de revocación.

Tipo: marca temporal

Obligatorio: no

MpaSessionArn

Es el ARN de la sesión de MPA asociada con esta solicitud de revocación.

Tipo: cadena

Requerido: no

Status

Es el estado actual de la solicitud de revocación.

Tipo: cadena

Valores válidos: PENDING | FAILED

Obligatorio: no

StatusMessage

Es un mensaje que describe el estado actual de la solicitud de revocación.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

LegalHold

Servicio: AWS Backup

Una retención legal es una herramienta administrativa que ayuda a evitar que las copias de seguridad se eliminen mientras están retenidas. Mientras la retención esté en vigor, las copias de seguridad retenidas no se pueden eliminar y las políticas de ciclo de vida que podrían alterar el estado de las copias de seguridad (como la transferencia al almacenamiento en frío) se retrasan hasta que se elimine la retención legal. Una copia de seguridad puede tener más de una retención legal. Las retenciones legales se aplican a una o más copias de seguridad (también se conocen como puntos de recuperación). Estas copias de seguridad se pueden filtrar por tipos de recursos y por ID de recursos.

Contenido

CancellationDate

Hora a la que se canceló la retención legal.

Tipo: marca temporal

Obligatorio: no

CreationDate

La hora en la que se creó la retención legal.

Tipo: marca temporal

Obligatorio: no

Description

La descripción de una cadena de la retención legal.

Tipo: cadena

Requerido: no

LegalHoldArn

El nombre de recurso de Amazon (ARN) de la retención legal; por ejemplo,
`arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

Requerido: no

LegalHoldId

El identificador de la retención legal.

Tipo: cadena

Requerido: no

Status

El estado de la retención legal.

Tipo: cadena

Valores válidos: CREATING | ACTIVE | CANCELING | CANCELED

Obligatorio: no

Title

El título de una retención legal.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

Lifecycle

Servicio: AWS Backup

Especifica el período, en días, antes de que un punto de recuperación se transfiera al almacenamiento en frío o se elimine.

Las copias de seguridad que se transfieran a cámaras frigoríficas deben almacenarse en cámaras frigoríficas durante un mínimo de 90 días. Por lo tanto, en la consola, el valor de retención debe tener 90 días más que el valor del número de días tras los cuales se transferirá al almacenamiento en frío. El valor de "transition to cold after days" (número de días tras los cuales migrará a almacenamiento en frío) no puede cambiarse una vez que se ha migrado una copia de seguridad al almacenamiento en frío.

Los tipos de recursos que pueden pasar al almacenamiento en frío se enumeran en la tabla [Disponibilidad de funciones por recurso](#). AWS Backup omite esta expresión para otros tipos de recursos.

Para eliminar el ciclo de vida y los períodos de retención existentes y conservar los puntos de recuperación indefinidamente, especifique -1 para `MoveToColdStorageAfterDays` y `DeleteAfterDays`.

Contenido

`DeleteAfterDays`

El número de días después de la creación cuando se elimina un punto de recuperación. Este valor debe ser al menos 90 días posterior al número de días especificado en `MoveToColdStorageAfterDays`.

Tipo: largo

Obligatorio: no

`DeleteAfterEvent`

El evento tras el cual se elimina un punto de recuperación. Un punto de recuperación con ambos `DeleteAfterDays` y `DeleteAfterEvent` se eliminará una vez que se cumpla primero la condición. No es válido como entrada.

Tipo: cadena

Valores válidos: `DELETE_AFTER_COPY`

Obligatorio: no

MoveToColdStorageAfterDays

El número de días después de la creación cuando un punto de recuperación pasa a almacenamiento en frío.

Tipo: largo

Obligatorio: no

OptInToArchiveForSupportedResources

Si el valor es true, su plan de copia de seguridad lleva a cabo la transición de los recursos compatibles al nivel de almacenamiento de archivo (en frío) de acuerdo con la configuración del ciclo de vida.

Tipo: Booleano

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ProtectedResource

Servicio: AWS Backup

Estructura que contiene información sobre un recurso del que se ha hecho una copia de seguridad.

Contenido

LastBackupTime

La fecha y la hora en que se realizó la última una copia de seguridad de un recurso, en formato Unix y horario universal coordinado (UTC). El valor de `LastBackupTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

LastBackupVaultArn

El ARN (nombre de recurso de Amazon) del almacén de copias de seguridad que contiene el punto de recuperación de copia de seguridad más reciente.

Tipo: cadena

Requerido: no

LastRecoveryPointArn

El ARN (nombre de recurso de Amazon) del punto de recuperación más reciente.

Tipo: cadena

Requerido: no

ResourceArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un recurso. El formato del ARN depende del tipo de recurso.

Tipo: cadena

Requerido: no

ResourceName

El nombre no exclusivo del recurso que pertenece a la copia de seguridad especificada.

Tipo: cadena

Requerido: no

ResourceType

El tipo de recurso de AWS; por ejemplo, un volumen de Amazon Elastic Block Store (Amazon EBS) o una base de datos de Amazon Relational Database Service (Amazon RDS). Para las copias de seguridad de Windows Volume Shadow Copy Service (VSS), el único tipo de recurso admitido es Amazon EC2.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ProtectedResourceConditions

Servicio: AWS Backup

La lista de condiciones que se define para los recursos del plan de prueba de restauración mediante etiquetas.

Contenido

StringEquals

Filtra los valores de los recursos etiquetados solo para aquellos recursos que se etiquetaron con el mismo valor. También se denomina “coincidencia exacta”.

Tipo: matriz de objetos [KeyValue](#)

Obligatorio: no

StringNotEquals

Filtra los valores de los recursos etiquetados solo para aquellos recursos que se etiquetaron y que no tienen el mismo valor. También se denomina “coincidencia negada”.

Tipo: matriz de objetos [KeyValue](#)

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

RecoveryPointByBackupVault

Servicio: AWS Backup

Contiene información detallada sobre los puntos de recuperación almacenados en un almacén de copias de seguridad.

Contenido

AggregatedScanResult

Contiene los resultados de escaneo más recientes contra el punto de recuperación y actualmente incluye `FailedScan`, `Findings`, `LastComputed`.

Tipo: objeto [AggregatedScanResult](#)

Obligatorio: no

BackupSizeInBytes

El tamaño de una copia de seguridad, en bytes.

Tipo: largo

Obligatorio: no

BackupVaultArn

Un ARN que identifica de forma exclusiva un almacén de copias de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

Requerido: no

BackupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: no

CalculatedLifecycle

Un objeto `CalculatedLifecycle` que contiene las marcas temporales `MoveToColdStorageAt` y `DeleteAt`.

Tipo: objeto [CalculatedLifecycle](#)

Obligatorio: no

CompletionDate

La fecha y la hora en que se completó un trabajo para restaurar un punto de recuperación, en formato Unix y horario universal coordinado (UTC). El valor de `CompletionDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

CompositeMemberIdentifier

El identificador de un recurso dentro de un grupo compuesto, como un punto de recuperación anidado (secundario) que pertenece a una pila compuesta (principal). El ID se transfiere desde el [ID lógico](#) de una pila.

Tipo: cadena

Requerido: no

CreatedBy

Contiene información de identificación sobre la creación de un punto de recuperación, que incluye los valores de `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion` y `BackupRuleId` del plan de copia de seguridad que se utilizó para crearlo.

Tipo: objeto [RecoveryPointCreator](#)

Obligatorio: no

CreationDate

La fecha y la hora en que se creó un punto de recuperación, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

EncryptionKeyArn

La clave de cifrado en el servidor que se utiliza para proteger sus copias de seguridad; por ejemplo, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Tipo: cadena

Requerido: no

EncryptionKeyType

El tipo de clave de cifrado utilizada para el punto de recuperación. Los valores válidos son `CUSTOMER_MANAGED_KMS_KEY` para las claves administradas por el cliente o `AWS_OWNED_KMS_KEY` para las claves propiedad del cliente. AWS

Tipo: cadena

Valores válidos: `AWS_OWNED_KMS_KEY` | `CUSTOMER_MANAGED_KMS_KEY`

Obligatorio: no

IamRoleArn

Especifica el ARN del rol de IAM utilizado para crear el punto de recuperación de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

Requerido: no

IndexStatus

Este es el estado actual del índice de copias de seguridad asociado al punto de recuperación especificado.

Los estados son: `PENDING` | `ACTIVE` | `FAILED` | `DELETING`

En una búsqueda se puede incluir un punto de recuperación con un índice con el estado `ACTIVE`.

Tipo: cadena

Valores válidos: PENDING | ACTIVE | FAILED | DELETING

Obligatorio: no

IndexStatusMessage

Es una cadena en forma de mensaje detallado que explica el estado del índice de copias de seguridad asociado al punto de recuperación.

Tipo: cadena

Requerido: no

InitiationDate

Fecha y hora en que se inició el trabajo de copia de seguridad que ha creado este punto de recuperación, expresadas en formato Unix y horario universal coordinado (UTC).

Tipo: marca temporal

Obligatorio: no

IsEncrypted

Un valor booleano que se devuelve como TRUE si el punto de recuperación especificado está cifrado o como FALSE si el punto de recuperación no está cifrado.

Tipo: Booleano

Obligatorio: no

IsParent

Se trata de un valor booleano que indica que es un punto de recuperación principal (compuesto).

Tipo: Booleano

Obligatorio: no

LastRestoreTime

La fecha y hora en que se restauró por última vez un punto de recuperación, en formato Unix y horario universal coordinado (UTC). El valor de LastRestoreTime tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

Lifecycle

El ciclo de vida define cuándo un recurso protegido pasa a almacenamiento en frío y cuándo caduca. AWS Backup cambia y vence las copias de seguridad automáticamente de acuerdo con el ciclo de vida que usted defina.

Las copias de seguridad que se transfieran al almacenamiento en frío deben almacenarse en un almacenamiento en frío durante un mínimo de 90 días. Por lo tanto, el valor de retención debe tener 90 días más que el valor del número de días tras los cuales se transferirá al almacenamiento en frío. El valor de “número de días tras los cuales migrará a almacenamiento en frío” no puede cambiarse una vez que se ha migrado una copia de seguridad al almacenamiento en frío.

Los tipos de recursos que pueden pasar al almacenamiento en frío se enumeran en la tabla [Disponibilidad de funciones por recurso](#). AWS Backup omite esta expresión para otros tipos de recursos.

Tipo: objeto [Lifecycle](#)

Obligatorio: no

ParentRecoveryPointArn

El nombre de recurso de Amazon (ARN) del punto de recuperación principal (compuesto).

Tipo: cadena

Requerido: no

RecoveryPointArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

Requerido: no

ResourceArn

Un ARN que identifica de forma única a un recurso. El formato del ARN depende del tipo de recurso.

Tipo: cadena

Requerido: no

ResourceName

El nombre no exclusivo del recurso que pertenece a la copia de seguridad especificada.

Tipo: cadena

Requerido: no

ResourceType

El tipo de AWS recurso guardado como punto de recuperación; por ejemplo, un volumen de Amazon Elastic Block Store (Amazon EBS) o una base de datos de Amazon Relational Database Service (Amazon RDS). Para las copias de seguridad de Windows Volume Shadow Copy Service (VSS), el único tipo de recurso compatible es Amazon EC2.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatorio: no

SourceBackupVaultArn

El almacén de copias de seguridad desde el que se copió originalmente el punto de recuperación. Si el punto de recuperación se restaura en la misma cuenta, este valor será `null`.

Tipo: cadena

Requerido: no

Status

Un código de estado que especifica el estado del punto de recuperación.

Tipo: cadena

Valores válidos: `COMPLETED | PARTIAL | DELETING | EXPIRED | AVAILABLE | STOPPED | CREATING`

Obligatorio: no

StatusMessage

Un mensaje que explica el estado actual del punto de recuperación.

Tipo: cadena

Requerido: no

VaultType

El tipo de almacén en el que se guarda el punto de recuperación descrito.

Tipo: cadena

Valores válidos: `BACKUP_VAULT` | `LOGICALLY_AIR_GAPPED_BACKUP_VAULT` | `RESTORE_ACCESS_BACKUP_VAULT`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

RecoveryPointByResource

Servicio: AWS Backup

Contiene información detallada sobre un punto de recuperación guardado.

Contenido

AggregatedScanResult

Contiene los resultados de escaneo más recientes contra el punto de recuperación y actualmente incluye `FailedScan`, `Findings`, `LastComputed`.

Tipo: objeto [AggregatedScanResult](#)

Obligatorio: no

BackupSizeBytes

El tamaño de una copia de seguridad, en bytes.

Tipo: largo

Obligatorio: no

BackupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: no

CreationDate

La fecha y la hora en que se creó un punto de recuperación, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

EncryptionKeyArn

La clave de cifrado en el servidor que se utiliza para proteger sus copias de seguridad; por ejemplo, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Tipo: cadena

Requerido: no

EncryptionKeyType

El tipo de clave de cifrado utilizada para el punto de recuperación. Los valores válidos son `CUSTOMER_MANAGED_KMS_KEY` para las claves administradas por el cliente o `_OWNED_KMS_KEY` para las claves propiedad del cliente. AWS AWS

Tipo: cadena

Valores válidos: `AWS_OWNED_KMS_KEY` | `CUSTOMER_MANAGED_KMS_KEY`

Obligatorio: no

IndexStatus

Este es el estado actual del índice de copias de seguridad asociado al punto de recuperación especificado.

Los estados son: `PENDING` | `ACTIVE` | `FAILED` | `DELETING`

En una búsqueda se puede incluir un punto de recuperación con un índice con el estado `ACTIVE`.

Tipo: cadena

Valores válidos: `PENDING` | `ACTIVE` | `FAILED` | `DELETING`

Obligatorio: no

IndexStatusMessage

Es una cadena en forma de mensaje detallado que explica el estado del índice de copias de seguridad asociado al punto de recuperación.

Tipo: cadena

Requerido: no

IsParent

Se trata de un valor booleano que indica que es un punto de recuperación principal (compuesto).

Tipo: Booleano

Obligatorio: no

ParentRecoveryPointArn

El nombre de recurso de Amazon (ARN) del punto de recuperación principal (compuesto).

Tipo: cadena

Requerido: no

RecoveryPointArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

Requerido: no

ResourceName

El nombre no exclusivo del recurso que pertenece a la copia de seguridad especificada.

Tipo: cadena

Requerido: no

Status

Un código de estado que especifica el estado del punto de recuperación.

Tipo: cadena

Valores válidos: COMPLETED | PARTIAL | DELETING | EXPIRED | AVAILABLE | STOPPED | CREATING

Obligatorio: no

StatusMessage

Un mensaje que explica el estado actual del punto de recuperación.

Tipo: cadena

Requerido: no

VaultType

El tipo de almacén en el que se guarda el punto de recuperación descrito.

Tipo: cadena

Valores válidos: `BACKUP_VAULT` | `LOGICALLY_AIR_GAPPED_BACKUP_VAULT` | `RESTORE_ACCESS_BACKUP_VAULT`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos, consulta lo siguiente AWS SDKs:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

RecoveryPointCreator

Servicio: AWS Backup

Contiene información sobre el plan de copia de seguridad y la regla que AWS Backup utilizó para iniciar la copia de seguridad del punto de recuperación.

Contenido

BackupPlanArn

Un nombre de recurso de Amazon (ARN) que identifica de forma única un plan de copia de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Tipo: cadena

Requerido: no

BackupPlanId

Identifica de forma única un plan de copia de seguridad.

Tipo: cadena

Requerido: no

BackupPlanName

Nombre del plan de copia de seguridad que ha creado este punto de recuperación. Proporciona un contexto legible para las personas sobre qué plan de copia de seguridad ha sido responsable del trabajo de copia de seguridad.

Tipo: cadena

Requerido: no

BackupPlanVersion

Los ID de versión son cadenas cifradas en UTF-8, Unicode, únicas, generadas aleatoriamente que tienen como máximo una longitud de 1024 bytes. No es posible editarlos.

Tipo: cadena

Requerido: no

BackupRuleCron

Es la expresión cron que define la programación de la regla de copia de seguridad. Muestra la frecuencia y el momento en que las copias de seguridad se activan de forma automática.

Tipo: cadena

Requerido: no

BackupRuleId

Identifica de forma exclusiva una regla utilizada para programar la copia de seguridad de una selección de recursos.

Tipo: cadena

Requerido: no

BackupRuleName

Nombre de la regla de copia de seguridad en el plan de copia de seguridad que ha creado este punto de recuperación. Esto ayuda a identificar qué regla específica ha activado el trabajo de copia de seguridad.

Tipo: cadena

Requerido: no

BackupRuleTimezone

Es la zona horaria utilizada para la programación de las reglas de copia de seguridad. Esto proporciona un contexto para determinar cuándo se programa la ejecución de las copias de seguridad en la zona horaria especificada.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)

- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

RecoveryPointMember

Servicio: AWS Backup

Se trata de un punto de recuperación que es un punto de recuperación secundario (anidado) de un punto de recuperación principal (compuesto). Estos puntos de recuperación se pueden disociar de su punto de recuperación principal (compuesto), en cuyo caso dejarán de ser miembros.

Contenido

BackupVaultName

El nombre del almacén de copias de seguridad (el contenedor lógico en el que se almacenan las copias de seguridad).

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatorio: no

RecoveryPointArn

El nombre de recurso de Amazon (ARN) del punto de recuperación principal (compuesto).

Tipo: cadena

Requerido: no

ResourceArn

El nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un recurso guardado.

Tipo: cadena

Requerido: no

ResourceType

El tipo de recurso de AWS que se guarda como punto de recuperación.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

RecoveryPointSelection

Servicio: AWS Backup

Esto especifica criterios para asignar un conjunto de recursos, como los tipos de recursos o los almacenes de copias de seguridad.

Contenido

DateRange

Este es un filtro de recursos que contiene FromDate: DateTime y ToDate: DateTime. Ambos valores son obligatorios. No se permiten valores de DateTime futuros.

La fecha y la hora están en formato Unix y horario universal coordinado (UTC) y tienen una precisión de milisegundos (los milisegundos son opcionales). Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: objeto [DateRange](#)

Obligatorio: no

ResourceIdentifiers

Estos son los recursos incluidos en la selección de recursos (incluidos los tipos de recursos y los almacenes).

Tipo: matriz de cadenas

Obligatorio: no

VaultNames

Estos son los nombres de los almacenes en los que se encuentran los puntos de recuperación seleccionados.

Tipo: matriz de cadenas

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ReportDeliveryChannel

Servicio: AWS Backup

Contiene información del plan de informe sobre dónde entregar los informes, específicamente el nombre del bucket de Amazon S3, el prefijo de clave de S3 y los formatos de los informes.

Contenido

S3BucketName

El nombre único del bucket de S3 que recibe los informes.

Tipo: cadena

Obligatorio: sí

Formats

El formato de los informes: CSV, JSON o ambos. Si no se especifica, el formato predeterminado es CSV.

Tipo: matriz de cadenas

Obligatorio: no

S3KeyPrefix

El prefijo del lugar donde AWS Backup Audit Manager entrega los informes a Amazon S3. El prefijo es la parte que se indica en la siguiente ruta: `s3://your-bucket-name/prefix/Backup/us-west-2/year/month/day/report-name`. Si no se especifica, no hay prefijo.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)

- [AWS SDK para Ruby V3](#)

ReportDestination

Servicio: AWS Backup

Contiene información de su trabajo de informe sobre el destino de su informe.

Contenido

S3BucketName

El nombre único del bucket de Amazon S3 que recibe los informes.

Tipo: cadena

Requerido: no

S3Keys

El nombre clave que identifica de forma exclusiva sus informes en el bucket de S3.

Tipo: matriz de cadenas

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ReportJob

Servicio: AWS Backup

Contiene información detallada acerca de un trabajo de informe. Un trabajo de informe compila un informe en función de un plan de informes y lo publica en Amazon S3.

Contenido

CompletionTime

La fecha y la hora en que se completó el trabajo de informe, en formato Unix y horario universal coordinado (UTC). El valor de `CompletionTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

CreationTime

La fecha y la hora en que se creó un trabajo de informe, en formato Unix y horario universal coordinado (UTC). El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

ReportDestination

El nombre del bucket de S3 y las claves S3 del destino en el que el trabajo de informe publica el informe.

Tipo: objeto [ReportDestination](#)

Obligatorio: no

ReportJobId

El identificador de un trabajo de informe. Una única cadena cifrada en UTF-8, Unicode, generada aleatoriamente que tiene como máximo una longitud de 1024 bytes. El ID del trabajo de informe no se puede editar.

Tipo: cadena

Requerido: no

ReportPlanArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un recurso. El formato del ARN depende del tipo de recurso.

Tipo: cadena

Requerido: no

ReportTemplate

Identifica la plantilla para el informe. Los informes se crean mediante una plantilla. Las plantillas de informes son:

RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT |
BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT

Tipo: cadena

Requerido: no

Status

El estado de un trabajo de informe. Los estados son:

CREATED | RUNNING | COMPLETED | FAILED

COMPLETED significa que el informe está disponible para su revisión en el destino designado. Si el estado es FAILED, revise el motivo en el StatusMessage.

Tipo: cadena

Requerido: no

StatusMessage

Un mensaje que explica el estado del trabajo de informe.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ReportPlan

Servicio: AWS Backup

Contiene información detallada acerca de un plan de informes.

Contenido

CreationTime

La fecha y la hora en que se creó el plan de informes, en formato Unix y horario universal coordinado (UTC). El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

DeploymentStatus

Devuelve el estado de una implementación de un plan de informes. Los estados son:

`CREATE_IN_PROGRESS` | `UPDATE_IN_PROGRESS` | `DELETE_IN_PROGRESS` | `COMPLETED`

Tipo: cadena

Requerido: no

LastAttemptedExecutionTime

La fecha y la hora en que se intentó ejecutar por última vez un trabajo de informe asociado a este plan de informes, en formato Unix y horario universal coordinado (UTC). El valor de `LastAttemptedExecutionTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

LastSuccessfulExecutionTime

La fecha y la hora en que se ejecutó por última vez con éxito un trabajo de informe asociado con este plan de informes, en formato Unix y horario universal coordinado (UTC). El valor de `LastSuccessfulExecutionTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

ReportDeliveryChannel

Contiene información sobre dónde y cómo entregar sus informes, específicamente el nombre del bucket de Amazon S3, el prefijo de clave de S3 y los formatos de sus informes.

Tipo: objeto [ReportDeliveryChannel](#)

Obligatorio: no

ReportPlanArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un recurso. El formato del ARN depende del tipo de recurso.

Tipo: cadena

Requerido: no

ReportPlanDescription

Una descripción opcional del plan de informes con un máximo de 1024 caracteres.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `.*\S.*`

Obligatorio: no

ReportPlanName

El nombre único del plan de informes. Este nombre debe contener entre 1 y 256 caracteres, comenzando por una letra, y contar con letras (a-z, A-Z), números (0-9) y guiones bajos (_).

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `[a-zA-Z][_a-zA-Z0-9]*`

Obligatorio: no

ReportSetting

Identifica la plantilla para el informe. Los informes se crean mediante una plantilla. Las plantillas de informes son:

RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT |
BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT

Si la plantilla de informe es RESOURCE_COMPLIANCE_REPORT o CONTROL_COMPLIANCE_REPORT, este recurso de la API también describe la cobertura de informes por Regiones de AWS y marcos.

Tipo: objeto [ReportSetting](#)

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ReportSetting

Servicio: AWS Backup

Contiene información detallada acerca de la configuración de un informe.

Contenido

ReportTemplate

Identifica la plantilla para el informe. Los informes se crean mediante una plantilla. Las plantillas de informes son:

RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT |
BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT |
SCAN_JOB_REPORT

Tipo: cadena

Obligatorio: sí

Accounts

Estas son las cuentas que se incluirán en el informe.

Usa el valor de cadena de ROOT para incluir todas las unidades organizativas.

Tipo: matriz de cadenas

Obligatorio: no

FrameworkArns

Los nombres de los recursos de Amazon (ARNs) de los marcos que cubre un informe.

Tipo: matriz de cadenas

Obligatorio: no

NumberOfFrameworks

El número de marcos que cubre un informe.

Tipo: entero

Obligatorio: no

OrganizationUnits

Estas son las unidades organizativas que se incluirán en el informe.

Tipo: matriz de cadenas

Obligatorio: no

Regions

Estas son las regiones que se incluirán en el informe.

Usa el comodín como valor de cadena para incluir todas las regiones.

Tipo: matriz de cadenas

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ResourceSelection

Servicio: AWS Backup

Contiene metadatos sobre la selección de recursos para las configuraciones de estratificación.

Puede especificar hasta 5 selecciones de recursos diferentes por configuración de organización en niveles. Los datos trasladados a un nivel de menor coste permanecen allí hasta que se eliminen (transición unidireccional).

Contenido

Resources

Matriz de cadenas que contiene uno ARNs de los recursos asociados o un comodín * para especificar todos los recursos. Puede especificar hasta 100 recursos específicos por configuración de estratificación.

Tipo: matriz de cadenas

Obligatorio: sí

ResourceType

El tipo de AWS recurso; por ejemplo, S3 para Amazon S3. En el caso de las configuraciones por niveles, actualmente se limita a S3.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatorio: sí

TieringDownSettingsInDays

El número de días transcurridos desde su creación en una bóveda de respaldo durante los cuales un objeto puede pasar a la capa de almacenamiento en caliente de bajo coste. Debe ser un número entero positivo comprendido entre 60 y 36500 días.

Tipo: entero

Rango válido: valor mínimo de 60. Valor máximo de 36500.

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

RestoreAccessBackupVaultListMember

Servicio: AWS Backup

Contiene información sobre un almacén de copias de seguridad con acceso a la restauración.

Contenido

ApprovalDate

Fecha y hora en que se aprobó el almacén de copias de seguridad con acceso a la restauración.

Tipo: marca temporal

Obligatorio: no

CreationDate

Fecha y hora en que se creó el almacén de copias de seguridad con acceso a la restauración.

Tipo: marca temporal

Obligatorio: no

LatestRevokeRequest

Información sobre la última solicitud para revocar el acceso a este almacén de copias de seguridad.

Tipo: objeto [LatestRevokeRequest](#)

Obligatorio: no

RestoreAccessBackupVaultArn

Es el ARN del almacén de copias de seguridad con acceso a la restauración.

Tipo: cadena

Requerido: no

VaultState

Es el estado actual del almacén de copias de seguridad con acceso a la restauración.

Tipo: cadena

Valores válidos: CREATING | AVAILABLE | FAILED

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

RestoreJobCreator

Servicio: AWS Backup

Contiene información sobre el plan de prueba de restauración que utilizó AWS Backup para iniciar el trabajo de restauración.

Contenido

RestoreTestingPlanArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un plan de prueba de restauración.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

RestoreJobsListMember

Servicio: AWS Backup

Contiene metadatos sobre un trabajo de restauración.

Contenido

AccountId

El ID de la cuenta a la que pertenece el trabajo de restauración.

Tipo: cadena

Patrón: `^[0-9]{12}$`

Obligatorio: no

BackupSizeInBytes

El tamaño del recurso restaurado, en bytes.

Tipo: largo

Obligatorio: no

BackupVaultArn

Es el Nombre de recurso de Amazon (ARN) del almacén de copias de seguridad que contiene el punto de recuperación que se va a restaurar. Esto ayuda a identificar las políticas y los permisos de acceso al almacén.

Tipo: cadena

Requerido: no

CompletionDate

La fecha y la hora en que se completó un trabajo para restaurar un punto de recuperación, en formato Unix y horario universal coordinado (UTC). El valor de `CompletionDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

CreatedBy

Contiene información de identificación sobre la creación de un trabajo de restauración.

Tipo: objeto [RestoreJobCreator](#)

Obligatorio: no

CreatedResourceArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un recurso. El formato del ARN depende del tipo de recurso.

Tipo: cadena

Requerido: no

CreationDate

La fecha y la hora en que se creó un trabajo de restauración, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

DeletionStatus

Indica el estado de los datos generados por la prueba de restauración. El estado puede ser `Deleting`, `Failed` o `Successful`.

Tipo: cadena

Valores válidos: `DELETING` | `FAILED` | `SUCCESSFUL`

Obligatorio: no

DeletionStatusMessage

Describe el estado de eliminación del trabajo de restauración.

Tipo: cadena

Requerido: no

ExpectedCompletionTimeMinutes

La cantidad de tiempo en minutos que se espera que tarde un trabajo de restauración de un punto de recuperación.

Tipo: largo

Obligatorio: no

IamRoleArn

El ARN del rol de IAM utilizado para crear el punto de recuperación de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

Requerido: no

IsParent

Se trata de un valor booleano que indica si el trabajo de restauración es un trabajo de restauración principal (compuesto).

Tipo: Booleano

Obligatorio: no

ParentJobId

Es el identificador único del trabajo de restauración principal del trabajo de restauración seleccionado.

Tipo: cadena

Requerido: no

PercentDone

Contiene el porcentaje estimado que se ha completado de un trabajo en el momento en que se consultó el estado del trabajo.

Tipo: cadena

Requerido: no

RecoveryPointArn

Un ARN que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

Requerido: no

RecoveryPointCreationDate

La fecha en la que se creó un punto de recuperación.

Tipo: marca temporal

Obligatorio: no

ResourceType

El tipo de recurso de los trabajos de restauración enumerados; por ejemplo, un volumen de Amazon Elastic Block Store (Amazon EBS) o una base de datos de Amazon Relational Database Service (Amazon RDS). Para las copias de seguridad de Windows Volume Shadow Copy Service (VSS), el único tipo de recurso compatible es Amazon EC2.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatorio: no

RestoreJobId

Identifica de forma exclusiva el trabajo que restaura un punto de recuperación.

Tipo: cadena

Requerido: no

SourceResourceArn

Es el Nombre de recurso de Amazon (ARN) del recurso original del que se ha realizado la copia de seguridad. Proporciona un contexto sobre el recurso que se está restaurando.

Tipo: cadena

Requerido: no

Status

Un código de estado que especifica el estado del trabajo iniciado AWS Backup para restaurar un punto de recuperación.

Tipo: cadena

Valores válidos: PENDING | RUNNING | COMPLETED | ABORTED | FAILED

Obligatorio: no

StatusMessage

Un mensaje detallado que explica el estado del trabajo de restauración de un punto de recuperación.

Tipo: cadena

Requerido: no

ValidationStatus

El estado de la validación ejecutada en el trabajo de restauración indicado.

Tipo: cadena

Valores válidos: FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING

Obligatorio: no

ValidationStatusMessage

Describe el estado de la validación ejecutada en el trabajo de restauración indicado.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

RestoreJobSummary

Servicio: AWS Backup

Es un resumen de los trabajos de restauración creados o en ejecución en los 30 últimos días.

El resumen devuelto puede contener lo siguiente: Region, Account, State, ResourceType, MessageCategory, StartTime, EndTime y Count de trabajos incluidos.

Contenido

AccountId

El ID de la cuenta propietaria de los trabajos del resumen.

Tipo: cadena

Patrón: `^[0-9]{12}$`

Obligatorio: no

Count

El valor expresado como número de trabajos en un resumen de trabajos.

Tipo: entero

Obligatorio: no

EndTime

El valor de hora en formato numérico de la hora de finalización de un trabajo.

Este valor es la hora en formato Unix, Hora universal coordinada (UTC) y tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

Region

Las regiones de AWS incluidas en el resumen del trabajo.

Tipo: cadena

Requerido: no

ResourceType

Este valor es el recuento de trabajos para el tipo de recurso especificado. La solicitud `GetSupportedResourceTypes` devuelve cadenas para los tipos de recursos compatibles.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatorio: no

StartTime

El valor de hora en formato numérico de la hora de inicio de un trabajo.

Este valor es la hora en formato Unix, Hora universal coordinada (UTC) y tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

State

Este valor es el recuento de trabajos con el estado especificado.

Tipo: cadena

Valores válidos: `CREATED | PENDING | RUNNING | ABORTED | COMPLETED | FAILED | AGGREGATE_ALL | ANY`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)

- [AWS SDK para Ruby V3](#)

RestoreTestingPlanForCreate

Servicio: AWS Backup

Contiene metadatos sobre un plan de prueba de restauración.

Contenido

RecoveryPointSelection

`RecoveryPointSelection` tiene cinco parámetros (tres obligatorios y dos opcionales). Los valores que especifique determinan qué punto de recuperación se incluye en la prueba de restauración. Debe indicar `Algorithm` si desea incluir el último punto de recuperación dentro del suyo `SelectionWindowDays` o si desea un punto de recuperación aleatorio, y debe indicar a través de `IncludeVaults` de qué bóvedas se pueden elegir los puntos de recuperación.

`Algorithm` (obligatorio) Valores válidos: "LATEST_WITHIN_WINDOW" o "RANDOM_WITHIN_WINDOW".

`Recovery point types` (obligatorio) Valores válidos: "SNAPSHOT" y/o "CONTINUOUS". Incluir SNAPSHOT para restaurar únicamente los puntos de recuperación de instantáneas; incluir CONTINUOUS para restaurar puntos de recuperación continua (restauración puntual o PITR); utilizar ambos para restaurar una instantánea o un punto de recuperación continua. El punto de recuperación vendrá determinado por el valor de `Algorithm`.

`IncludeVaults` (obligatorio). Debe incluir uno o más almacenes de copia de seguridad. Utilice el comodín ["*"] o ARN específicos.

`SelectionWindowDays` (opcional) El valor debe ser un número entero (en días) comprendido entre 1 y 365. Si no se incluye, el valor se establece de forma predeterminada en 30.

`ExcludeVaults` (opcional). Puede optar por introducir uno o más ARN de almacenes de copia de seguridad específicos para impedir que el contenido de esos almacenes pueda restaurarse. O puede incluir una lista de selectores. Si este parámetro y su valor no están incluidos, el valor predeterminado es una lista vacía.

Tipo: objeto [RestoreTestingRecoveryPointSelection](#)

Obligatorio: sí

RestoreTestingPlanName

RestoreTestingPlanName es una cadena única que es el nombre del plan de prueba de restauración. No se puede cambiar después de la creación y debe constar únicamente de caracteres alfanuméricos y guiones bajos.

Tipo: cadena

Obligatorio: sí

ScheduleExpression

Una expresión CRON en la zona horaria especificada cuando se ejecuta un plan de prueba de restauración. Si no se proporciona ninguna expresión CRON, AWS Backup utilizará la expresión `cron(0 5 ? * * *)` predeterminada.

Tipo: cadena

Obligatorio: sí

ScheduleExpressionTimezone

Opcional. La zona horaria en la que se establece la expresión de programación. De forma predeterminada, las ScheduleExpressions están en UTC. Puede modificar esto para una zona horaria específica.

Tipo: cadena

Requerido: no

StartWindowHours

El valor predeterminado es 24 horas.

Un valor en horas después de una prueba de restauración programada para que se cancele el trabajo si no se ha iniciado correctamente. Este valor es opcional. Si se incluye este valor, este parámetro tiene un valor máximo de 168 horas (una semana).

Tipo: entero

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

RestoreTestingPlanForGet

Servicio: AWS Backup

Contiene metadatos sobre un plan de prueba de restauración.

Contenido

CreationTime

La fecha y la hora en que se creó un plan de prueba de restauración, en formato Unix y Hora universal coordinada (UTC). El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: sí

RecoveryPointSelection

Los criterios especificados para asignar un conjunto de recursos, como tipos de punto de recuperación o almacenes de copias de seguridad.

Tipo: objeto [RestoreTestingRecoveryPointSelection](#)

Obligatorio: sí

RestoreTestingPlanArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un plan de prueba de restauración.

Tipo: cadena

Obligatorio: sí

RestoreTestingPlanName

El nombre del plan de prueba de restauración.

Tipo: cadena

Obligatorio: sí

ScheduleExpression

Una expresión CRON en la zona horaria especificada cuando se ejecuta un plan de prueba de restauración. Si no se proporciona ninguna expresión CRON, AWS Backup utilizará la expresión `cron(0 5 ? * * *)` predeterminada.

Tipo: cadena

Obligatorio: sí

CreatorRequestId

Identifica la solicitud y permite que se reintenten las solicitudes que han producido un error sin el riesgo de ejecutar la operación dos veces. Si la solicitud incluye un `CreatorRequestId` que coincide con un plan de copia de seguridad existente, se devuelve ese plan. Este parámetro es opcional.

Si se utiliza, este parámetro debe contener de 1 a 50 caracteres alfanuméricos o “-”. caracteres.

Tipo: cadena

Requerido: no

LastExecutionTime

La última vez que se ejecutó una prueba de restauración con el plan de prueba de restauración especificado. Una fecha y hora, en formato Unix y horario universal coordinado (UTC). El valor de `LastExecutionDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

LastUpdateTime

La fecha y hora en que se actualizó el plan de prueba de restauración. Esta actualización está en formato Unix y horario universal coordinado (UTC). El valor de `LastUpdateTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

ScheduleExpressionTimezone

Opcional. La zona horaria en la que se establece la expresión de programación. De forma predeterminada, las ScheduleExpressions están en UTC. Puede modificar esto para una zona horaria específica.

Tipo: cadena

Requerido: no

StartWindowHours

El valor predeterminado es 24 horas.

Un valor en horas después de una prueba de restauración programada para que se cancele el trabajo si no se ha iniciado correctamente. Este valor es opcional. Si se incluye este valor, este parámetro tiene un valor máximo de 168 horas (una semana).

Tipo: entero

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

RestoreTestingPlanForList

Servicio: AWS Backup

Contiene metadatos sobre un plan de prueba de restauración.

Contenido

CreationTime

La fecha y la hora en que se creó un plan de prueba de restauración, en formato Unix y Hora universal coordinada (UTC). El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: sí

RestoreTestingPlanArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un plan de prueba de restauración.

Tipo: cadena

Obligatorio: sí

RestoreTestingPlanName

El nombre del plan de prueba de restauración.

Tipo: cadena

Obligatorio: sí

ScheduleExpression

Una expresión CRON en la zona horaria especificada cuando se ejecuta un plan de prueba de restauración. Si no se proporciona ninguna expresión CRON, AWS Backup utilizará la expresión `cron(0 5 ? * * *)` predeterminada.

Tipo: cadena

Obligatorio: sí

LastExecutionTime

La última vez que se ejecutó una prueba de restauración con el plan de prueba de restauración especificado. Una fecha y hora, en formato Unix y horario universal coordinado (UTC). El valor de LastExecutionDate tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

LastUpdateTime

La fecha y hora en que se actualizó el plan de prueba de restauración. Esta actualización está en formato Unix y horario universal coordinado (UTC). El valor de LastUpdateTime tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

ScheduleExpressionTimezone

Opcional. La zona horaria en la que se establece la expresión de programación. De forma predeterminada, las ScheduleExpressions están en UTC. Puede modificar esto para una zona horaria específica.

Tipo: cadena

Requerido: no

StartWindowHours

El valor predeterminado es 24 horas.

Un valor en horas después de una prueba de restauración programada para que se cancele el trabajo si no se ha iniciado correctamente. Este valor es opcional. Si se incluye este valor, este parámetro tiene un valor máximo de 168 horas (una semana).

Tipo: entero

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

RestoreTestingPlanForUpdate

Servicio: AWS Backup

Contiene metadatos sobre un plan de prueba de restauración.

Contenido

RecoveryPointSelection

Obligatorio: `Algorithm`; `RecoveryPointTypes`; `IncludeVaults` (uno o varios).

Opcional: `SelectionWindowDays` ('30' si no se especifica); `ExcludeVaults` (si no se incluye ninguno, aparece una lista vacía de forma predeterminada).

Tipo: objeto [RestoreTestingRecoveryPointSelection](#)

Obligatorio: no

ScheduleExpression

Una expresión CRON en la zona horaria especificada cuando se ejecuta un plan de prueba de restauración. Si no se proporciona ninguna expresión CRON, AWS Backup utilizará la expresión `cron(0 5 ? * * *)` predeterminada.

Tipo: cadena

Requerido: no

ScheduleExpressionTimezone

Opcional. La zona horaria en la que se establece la expresión de programación. De forma predeterminada, las `ScheduleExpressions` están en UTC. Puede modificar esto para una zona horaria específica.

Tipo: cadena

Requerido: no

StartWindowHours

El valor predeterminado es 24 horas.

Un valor en horas después de una prueba de restauración programada para que se cancele el trabajo si no se ha iniciado correctamente. Este valor es opcional. Si se incluye este valor, este parámetro tiene un valor máximo de 168 horas (una semana).

Tipo: entero

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

RestoreTestingRecoveryPointSelection

Servicio: AWS Backup

`RecoveryPointSelection` tiene cinco parámetros (tres obligatorios y dos opcionales). Los valores que especifique determinan qué punto de recuperación se incluye en la prueba de restauración. Debe indicar `Algorithm` si desea incluir el último punto de recuperación dentro del suyo `SelectionWindowDays` o si desea un punto de recuperación aleatorio, y debe indicar a través de `IncludeVaults` de qué bóvedas se pueden elegir los puntos de recuperación.

`Algorithm` (obligatorio) Valores válidos: "LATEST_WITHIN_WINDOW" o "RANDOM_WITHIN_WINDOW".

`Recovery point types` (obligatorio) Valores válidos: "SNAPSHOT" y/o "CONTINUOUS". Incluir `SNAPSHOT` para restaurar únicamente los puntos de recuperación de instantáneas; incluir `CONTINUOUS` para restaurar puntos de recuperación continua (restauración puntual o PITR); utilizar ambos para restaurar una instantánea o un punto de recuperación continua. El punto de recuperación vendrá determinado por el valor de `Algorithm`.

`IncludeVaults` (obligatorio) Debe incluir uno o más almacenes de copia de seguridad. Utilice el comodín ["*"] o ARN específicos.

`SelectionWindowDays` (opcional) El valor debe ser un número entero (en días) comprendido entre 1 y 365. Si no se incluye, el valor se establece de forma predeterminada en 30.

`ExcludeVaults` (opcional). Puede optar por introducir uno o más ARN de almacenes de copia de seguridad específicos para impedir que el contenido de esos almacenes pueda restaurarse. O puede incluir una lista de selectores. Si este parámetro y su valor no están incluidos, el valor predeterminado es una lista vacía.

Contenido

Algorithm

Los valores aceptables son "LATEST_WITHIN_WINDOW" o "RANDOM_WITHIN_WINDOW"

Tipo: cadena

Valores válidos: LATEST_WITHIN_WINDOW | RANDOM_WITHIN_WINDOW

Obligatorio: no

ExcludeVaults

Los valores aceptados son ARN específicos o una lista de selectores. Si no se incluye ninguno, aparece una lista vacía de forma predeterminada.

Tipo: matriz de cadenas

Obligatorio: no

IncludeVaults

Los valores aceptados son el comodín ["*"] o ARN específicos o sustitución de comodín ARN ["arn:aws:backup:us-west-2:123456789012:backup-vault:asdf", ...] ["arn:aws:backup:*:*:backup-vault:asdf-*", ...]

Tipo: matriz de cadenas

Obligatorio: no

RecoveryPointTypes

Son los tipos de puntos de recuperación.

Incluir SNAPSHOT para restaurar únicamente los puntos de recuperación de instantáneas; incluir CONTINUOUS para restaurar puntos de recuperación continua (restauración puntual o PITR); utilizar ambos para restaurar una instantánea o un punto de recuperación continua. El punto de recuperación vendrá determinado por el valor de `Algorithm`.

Tipo: matriz de cadenas

Valores válidos: CONTINUOUS | SNAPSHOT

Obligatorio: no

SelectionWindowDays

Los valores aceptados son números enteros de 1 a 365.

Tipo: entero

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

RestoreTestingSelectionForCreate

Servicio: AWS Backup

Contiene metadatos sobre una selección de pruebas de restauración específica.

ProtectedResourceType es obligatorio, como Amazon EBS o Amazon EC2.

Consta de RestoreTestingSelectionName, ProtectedResourceType y uno de los siguientes elementos:

- ProtectedResourceArns
- ProtectedResourceConditions

Cada tipo de recurso protegido puede tener un único valor.

Una selección de pruebas de restauración puede incluir un valor comodín ("*") como ProtectedResourceArns junto con ProtectedResourceConditions. Como alternativa, puede incluir hasta 30 recursos ARNs protegidos específicos. ProtectedResourceArns

StringEquals y StringNotEquals son ejemplos de ProtectedResourceConditions.

Contenido

IamRoleArn

El nombre de recurso de Amazon (ARN) del rol de IAM que AWS Backup utiliza para crear el recurso de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

Obligatorio: sí

ProtectedResourceType

El tipo de AWS recurso incluido en una selección de pruebas de restauración; por ejemplo, un volumen de Amazon EBS o una base de datos de Amazon RDS.

Los tipos de recursos admitidos son:

- Aurora para Amazon Aurora
- DocumentDB para Amazon DocumentDB (con compatibilidad con MongoDB)
- DynamoDB para Amazon DynamoDB

- EBS para Amazon Elastic Block Store (EBS)
- EC2 para Amazon Elastic Compute Cloud
- EFS para Amazon Elastic File System
- FSx para Amazon FSx
- Neptune para Amazon Neptune
- RDS para Amazon Relational Database Service
- S3 para Amazon S3

Tipo: cadena

Obligatorio: sí

RestoreTestingSelectionName

El nombre único de la selección de pruebas de restauración que pertenece al plan de prueba de restauración.

El nombre consta de únicamente de caracteres alfanuméricos y guiones bajos. La longitud máxima es 50.

Tipo: cadena

Obligatorio: sí

ProtectedResourceArns

Cada recurso protegido se puede filtrar por su valor específico ARNs, como `ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]` por ejemplo un comodín: `ProtectedResourceArns: ["*"]`, pero no por ambos.

Tipo: matriz de cadenas

Obligatorio: no

ProtectedResourceConditions

Si ha incluido el comodín `ProtectedResourceArns`, puede incluir las condiciones del recurso, por ejemplo. `ProtectedResourceConditions: { StringEquals: [{ key: "XXXX", value: "YYYY" }] }`

Tipo: objeto [ProtectedResourceConditions](#)

Obligatorio: no

RestoreMetadataOverrides

Puede anular determinadas claves de metadatos de restauración incluyendo el parámetro `RestoreMetadataOverrides` en el cuerpo de `RestoreTestingSelection`. Los valores de clave no distinguen mayúsculas y minúsculas.

Consulte la lista completa de [metadatos inferidos de pruebas de restauración](#).

Tipo: mapa de cadena a cadena

Obligatorio: no

ValidationWindowHours

Es la cantidad de horas (de 0 a 168) disponibles para ejecutar un script de validación de los datos. Los datos se eliminarán al finalizar el script de validación o al final del periodo de retención especificado, lo que ocurra primero.

Tipo: entero

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

RestoreTestingSelectionForGet

Servicio: AWS Backup

Contiene metadatos sobre una selección de pruebas de restauración.

Contenido

CreationTime

La fecha y la hora en que se creó una selección de pruebas de restauración, en formato Unix y Hora universal coordinada (UTC). El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: sí

IamRoleArn

El nombre de recurso de Amazon (ARN) del rol de IAM que AWS Backup utiliza para crear el recurso de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

Obligatorio: sí

ProtectedResourceType

El tipo de AWS recurso incluido en una selección de pruebas de recursos; por ejemplo, un volumen de Amazon EBS o una base de datos de Amazon RDS.

Tipo: cadena

Obligatorio: sí

RestoreTestingPlanName

`RestoreTestingPlanName` Es una cadena única que es el nombre del plan de pruebas de restauración.

Tipo: cadena

Obligatorio: sí

RestoreTestingSelectionName

El nombre único de la selección de pruebas de restauración que pertenece al plan de prueba de restauración.

El nombre consta de únicamente de caracteres alfanuméricos y guiones bajos. La longitud máxima es 50.

Tipo: cadena

Obligatorio: sí

CreatorRequestId

Identifica la solicitud y permite que se reintenten las solicitudes que han producido un error sin el riesgo de ejecutar la operación dos veces. Si la solicitud incluye un `CreatorRequestId` que coincide con un plan de copia de seguridad existente, se devuelve ese plan. Este parámetro es opcional.

Si se utiliza, este parámetro debe contener de 1 a 50 caracteres alfanuméricos o “-”. caracteres.

Tipo: cadena

Requerido: no

ProtectedResourceArns

Puede incluir un carácter específico ARNs, como por ejemplo, `ProtectedResourceArns: ["arn:aws:...","arn:aws:..."]` o puede incluir un comodín: `ProtectedResourceArns: ["*"]`, pero no ambos.

Tipo: matriz de cadenas

Obligatorio: no

ProtectedResourceConditions

En una selección de pruebas de recursos, este parámetro filtra por condiciones específicas, como `StringEquals` o `StringNotEquals`.

Tipo: objeto [ProtectedResourceConditions](#)

Obligatorio: no

RestoreMetadataOverrides

Puede anular determinadas claves de metadatos de restauración incluyendo el parámetro `RestoreMetadataOverrides` en el cuerpo de `RestoreTestingSelection`. Los valores de clave no distinguen mayúsculas y minúsculas.

Consulte la lista completa de [metadatos inferidos de pruebas de restauración](#).

Tipo: mapa de cadena a cadena

Obligatorio: no

ValidationWindowHours

Es el número de horas (de 1 a 168) disponibles para ejecutar un script de validación de los datos. Los datos se eliminarán al finalizar el script de validación o al final del periodo de retención especificado, lo que ocurra primero.

Tipo: entero

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

RestoreTestingSelectionForList

Servicio: AWS Backup

Contiene metadatos sobre una selección de pruebas de restauración.

Contenido

CreationTime

La fecha y la hora en que se creó una selección de pruebas de restauración, en formato Unix y Hora universal coordinada (UTC). El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: sí

IamRoleArn

El nombre de recurso de Amazon (ARN) del rol de IAM que AWS Backup utiliza para crear el recurso de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

Obligatorio: sí

ProtectedResourceType

El tipo de AWS recurso incluido en una selección de pruebas de restauración; por ejemplo, un volumen de Amazon EBS o una base de datos de Amazon RDS.

Tipo: cadena

Obligatorio: sí

RestoreTestingPlanName

Cadena única que es el nombre del plan de prueba de restauración.

El nombre no se puede cambiar después de crear el plan. El nombre consta de únicamente de caracteres alfanuméricos y guiones bajos. La longitud máxima es 50.

Tipo: cadena

Obligatorio: sí

RestoreTestingSelectionName

Nombre único de la selección de pruebas de restauración.

El nombre consta de únicamente de caracteres alfanuméricos y guiones bajos. La longitud máxima es 50.

Tipo: cadena

Obligatorio: sí

ValidationWindowHours

Este valor representa el tiempo, en horas, que se retienen los datos después de una prueba de restauración para poder completar la validación opcional.

El valor aceptado es un entero entre 0 y 168 (el equivalente en horas a siete días).

Tipo: entero

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

RestoreTestingSelectionForUpdate

Servicio: AWS Backup

Contiene metadatos sobre una selección de pruebas de restauración.

Contenido

IamRoleArn

El nombre de recurso de Amazon (ARN) del rol de IAM que AWS Backup utiliza para crear el recurso de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

Requerido: no

ProtectedResourceArns

Puede incluir una lista de ARN específicos, por ejemplo, `ProtectedResourceArns: ["arn:aws:...","arn:aws:..."]`, o incluir un comodín: `ProtectedResourceArns: ["*"]`, pero no ambos.

Tipo: matriz de cadenas

Obligatorio: no

ProtectedResourceConditions

La lista de condiciones que se define para los recursos del plan de prueba de restauración mediante etiquetas.

Tipo: objeto [ProtectedResourceConditions](#)

Obligatorio: no

RestoreMetadataOverrides

Puede anular determinadas claves de metadatos de restauración incluyendo el parámetro `RestoreMetadataOverrides` en el cuerpo de `RestoreTestingSelection`. Los valores de clave no distinguen mayúsculas y minúsculas.

Consulte la lista completa de [metadatos inferidos de pruebas de restauración](#).

Tipo: mapa de cadena a cadena

Obligatorio: no

ValidationWindowHours

Este valor representa el tiempo, en horas, que se retienen los datos después de una prueba de restauración para poder completar la validación opcional.

El valor aceptado es un entero entre 0 y 168 (el equivalente en horas a siete días).

Tipo: entero

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ScanAction

Servicio: AWS Backup

Define una acción de análisis que especifica el escáner de malware y el modo de análisis que se van a utilizar.

Contenido

MalwareScanner

El escáner de malware que se utilizará para la acción de escaneo. En la actualidad, solo se admite GUARDDUTY.

Tipo: cadena

Valores válidos: GUARDDUTY

Obligatorio: no

ScanMode

El modo de escaneo que se utilizará para la acción de escaneo.

Valores válidos: FULL_SCAN | INCREMENTAL_SCAN.

Tipo: cadena

Valores válidos: FULL_SCAN | INCREMENTAL_SCAN

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ScanJob

Servicio: AWS Backup

Contiene metadatos sobre un trabajo de digitalización, incluida información sobre el proceso de digitalización, los resultados y los recursos asociados.

Contenido

AccountId

El ID de cuenta propietario del trabajo de escaneo.

Tipo: cadena

Obligatorio: sí

BackupVaultArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un almacén de copia de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

Obligatorio: sí

BackupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copias de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Tipo: cadena

Obligatorio: sí

CreatedBy

Contiene información de identificación sobre la creación de un trabajo de escaneo.

Tipo: objeto [ScanJobCreator](#)

Obligatorio: sí

CreationDate

La fecha y la hora en que se crea un trabajo de escaneo, en formato Unix y en hora universal coordinada (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: sí

IamRoleArn

Especifica el ARN del rol de IAM utilizado para crear el trabajo de escaneo; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`

Tipo: cadena

Obligatorio: sí

MalwareScanner

El motor de escaneo utilizado para el trabajo de escaneo. En la actualidad, solo se admite GUARDDUTY.

Tipo: cadena

Valores válidos: GUARDDUTY

Obligatorio: sí

RecoveryPointArn

Un ARN que identifica de forma exclusiva el punto de recuperación que se está escaneando; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

Tipo: cadena

Obligatorio: sí

ResourceArn

Un ARN que identifica de forma exclusiva el recurso de origen del punto de recuperación que se está escaneando.

Tipo: cadena

Obligatorio: sí

ResourceName

El nombre no exclusivo del recurso que pertenece a la copia de seguridad especificada.

Tipo: cadena

Obligatorio: sí

ResourceType

El tipo de AWS recurso que se está escaneando; por ejemplo, un volumen de Amazon Elastic Block Store (Amazon EBS) o una base de datos del Amazon Relational Database Service (Amazon RDS).

Tipo: cadena

Valores válidos: EBS | EC2 | S3

Obligatorio: sí

ScanJobId

El identificador único con el que se identifica la solicitud de trabajo de escaneo. AWS Backup

Tipo: cadena

Obligatorio: sí

ScanMode

Especifica el tipo de escaneo que se utilizará para el trabajo de escaneo.

Incluye:

FULL_SCAN Escaneará todo el linaje de datos de la copia de seguridad.

INCREMENTAL_SCAN Escaneará la diferencia de datos entre el punto de recuperación objetivo y el ARN del punto de recuperación base.

Tipo: cadena

Valores válidos: FULL_SCAN | INCREMENTAL_SCAN

Obligatorio: sí

ScannerRoleArn

Especifica el ARN del rol de IAM del escáner que se utiliza para el trabajo de escaneo.

Tipo: cadena

Obligatorio: sí

CompletionDate

La fecha y la hora en que se completa un trabajo de escaneo, en formato Unix y en hora universal coordinada (UTC). El valor de `CompletionDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

ScanBaseRecoveryPointArn

Un ARN que identifica de forma exclusiva el punto de recuperación base para el escaneo. Este campo se rellena cuando se realiza un trabajo de escaneo incremental.

Tipo: cadena

Requerido: no

ScanId

El ID de escaneo generado por el escáner de malware para el trabajo de escaneo correspondiente.

Tipo: cadena

Requerido: no

ScanResult

Contiene la información de los resultados del análisis, incluido el estado de las amenazas detectadas durante el análisis.

Tipo: objeto [ScanResultInfo](#)

Obligatorio: no

State

El estado actual del trabajo de escaneo.

Valores válidos: CREATED | RUNNING | COMPLETED | COMPLETED_WITH_ISSUES | FAILED | CANCELED.

Tipo: cadena

Valores válidos: CANCELED | COMPLETED | COMPLETED_WITH_ISSUES | CREATED | FAILED | RUNNING

Obligatorio: no

StatusMessage

Un mensaje detallado que explica el estado del trabajo de escaneo.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ScanJobCreator

Servicio: AWS Backup

Contiene información de identificación sobre la creación de un trabajo de escaneo, incluido el plan de respaldo y la regla que inició el escaneo.

Contenido

BackupPlanArn

Un nombre de recurso de Amazon (ARN) que identifica de forma única un plan de copia de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Tipo: cadena

Obligatorio: sí

BackupPlanId

El ID del plan de copia de seguridad.

Tipo: cadena

Obligatorio: sí

BackupPlanVersion

Cadenas cifradas en UTF-8, Unicode, únicas, generadas aleatoriamente que tienen como máximo una longitud de 1024 bytes. La versión IDs no se puede editar.

Tipo: cadena

Obligatorio: sí

BackupRuleId

Identifica de forma exclusiva la regla de copia de seguridad que inició el trabajo de escaneo.

Tipo: cadena

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ScanJobSummary

Servicio: AWS Backup

Contiene información resumida sobre los trabajos de escaneo, incluidos los recuentos y los metadatos para un período de tiempo y criterios específicos.

Contenido

AccountId

El ID de cuenta propietario de los trabajos de digitalización incluidos en este resumen.

Tipo: cadena

Patrón: `^[0-9]{12}$`

Obligatorio: no

Count

El número de trabajos de escaneo que cumplen los criterios especificados.

Tipo: entero

Obligatorio: no

EndTime

El valor de hora en formato numérico de la hora de finalización de un trabajo.

Este valor es la hora en formato Unix, Hora universal coordinada (UTC) y tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

MalwareScanner

Especifica el escáner de malware utilizado durante el trabajo de escaneo. Actualmente solo es compatible GUARDDUTY.

Tipo: cadena

Valores válidos: GUARDDUTY

Obligatorio: no

Region

La AWS región en la que se ejecutaron los trabajos de escaneo.

Tipo: cadena

Requerido: no

ResourceType

El tipo de AWS recurso para los trabajos de escaneo incluidos en este resumen.

Tipo: cadena

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatorio: no

ScanResultStatus

El estado de los resultados del escaneo para los trabajos de escaneo incluidos en este resumen.

Valores válidos: THREATS_FOUND | NO_THREATS_FOUND.

Tipo: cadena

Valores válidos: NO_THREATS_FOUND | THREATS_FOUND

Obligatorio: no

StartTime

El valor de hora en formato numérico de la hora de inicio de un trabajo.

Este valor es la hora en formato Unix, Hora universal coordinada (UTC) y tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

State

El estado de los trabajos de escaneo incluidos en este resumen.

Valores válidos: CREATED | RUNNING | COMPLETED | COMPLETED_WITH_ISSUES | FAILED | CANCELED.

Tipo: cadena

Valores válidos: CREATED | COMPLETED | COMPLETED_WITH_ISSUES | RUNNING | FAILED | CANCELED | AGGREGATE_ALL | ANY

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ScanResult

Servicio: AWS Backup

Contiene los resultados de un análisis de seguridad, incluida la información del escáner, el estado del análisis y cualquier hallazgo descubierto.

Contenido

Findings

Conjunto de hallazgos descubiertos durante el escaneo.

Tipo: matriz de cadenas

Valores válidos: MALWARE

Obligatorio: no

LastScanTimestamp

La marca de tiempo en la que se realizó el último escaneo, en formato Unix y en hora universal coordinada (UTC).

Tipo: marca temporal

Obligatorio: no

MalwareScanner

El escáner de malware utilizado para realizar el análisis. En la actualidad, solo se admite GUARDDUTY.

Tipo: cadena

Valores válidos: GUARDDUTY

Obligatorio: no

ScanJobState

El estado final del trabajo de escaneo.

Valores válidos: COMPLETED | FAILED | CANCELED.

Tipo: cadena

Valores válidos: COMPLETED | COMPLETED_WITH_ISSUES | FAILED | CANCELED

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ScanResultInfo

Servicio: AWS Backup

Contiene información sobre los resultados de un trabajo de escaneo.

Contenido

ScanResultStatus

El estado de los resultados del escaneo.

Valores válidos: THREATS_FOUND | NO_THREATS_FOUND.

Tipo: cadena

Valores válidos: NO_THREATS_FOUND | THREATS_FOUND

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ScanSetting

Servicio: AWS Backup

Contiene los ajustes de configuración para el análisis de malware, incluidos el tipo de escáner, los tipos de recursos de destino y la función del escáner.

Contenido

MalwareScanner

El escáner de malware que se utilizará para escanear. En la actualidad, solo se admite GUARDDUTY.

Tipo: cadena

Valores válidos: GUARDDUTY

Obligatorio: no

ResourceTypes

Una variedad de tipos de recursos para analizar en busca de malware.

Tipo: matriz de cadenas

Patrón: `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatorio: no

ScannerRoleArn

El nombre de recurso de Amazon (ARN) de la función de IAM que utiliza el escáner para acceder a los recursos; por ejemplo, `arn:aws:iam::123456789012:role/ScannerRole`

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)

- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ScheduledPlanExecutionMember

Servicio: AWS Backup

Contiene información sobre la ejecución programada de un plan de copia de seguridad, incluida la hora de ejecución, el tipo de regla y el identificador de la regla asociado.

Contenido

ExecutionTime

Fecha y hora en que se ha programado la ejecución de la copia de seguridad, expresadas en formato Unix y horario universal coordinado (UTC). El valor tiene una precisión de milisegundos.

Tipo: marca temporal

Obligatorio: no

RuleExecutionType

Es el tipo de ejecución de la regla de copia de seguridad. Los valores válidos son CONTINUOUS (recuperación en un momento dado), SNAPSHOTs (copias de seguridad de instantáneas) o CONTINUOUS_AND_SNAPSHOTs (ambos tipos combinados).

Tipo: cadena

Valores válidos: CONTINUOUS | SNAPSHOTs | CONTINUOUS_AND_SNAPSHOTs

Obligatorio: no

RuleId

Es el identificador unívoco de la regla de copia de seguridad que se ejecutará a la hora programada.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

TieringConfiguration

Servicio: AWS Backup

Contiene metadatos sobre una configuración de estratificación.

Contenido

BackupVaultName

El nombre del almacén de respaldo al que se aplica la configuración de estratificación. Se usa * para aplicarlo a todos los almacenes de respaldo.

Tipo: cadena

Patrón: `^(\\*|[a-zA-Z0-9\\-\\_]{2,50})$`

Obligatorio: sí

ResourceSelection

Conjunto de objetos de selección de recursos que especifican qué recursos se incluyen en la configuración de organización por niveles y sus ajustes de organización por niveles.

Tipo: matriz de objetos [ResourceSelection](#)

Obligatorio: sí

TieringConfigurationName

El nombre exclusivo de la configuración de organización por niveles. No se puede cambiar después de la creación y debe constar únicamente de caracteres alfanuméricos y guiones bajos.

Tipo: cadena

Patrón: `^[a-zA-Z0-9_]{1,200}$`

Obligatorio: sí

CreationTime

La fecha y la hora en que se creó una configuración de organización por niveles, en formato Unix y en hora universal coordinada (UTC). El valor de CreationTime tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

CreatorRequestId

Se trata de una cadena única que identifica la solicitud y permite volver a intentar las solicitudes fallidas sin correr el riesgo de ejecutar la operación dos veces.

Tipo: cadena

Requerido: no

LastUpdatedTime

Fecha y hora en que se actualizó una configuración de organización por niveles, en formato Unix y en hora universal coordinada (UTC). El valor de LastUpdatedTime tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

TieringConfigurationArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva la configuración de organización en niveles.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

TieringConfigurationInputForCreate

Servicio: AWS Backup

Contiene metadatos sobre una configuración de organización por niveles para las operaciones de creación.

Contenido

BackupVaultName

El nombre del almacén de respaldo en el que se aplica la configuración de organización por niveles. Se usa * para aplicarlo a todos los almacenes de respaldo.

Tipo: cadena

Patrón: `^(\\*|[a-zA-Z0-9\\-\\_]){2,50}$`

Obligatorio: sí

ResourceSelection

Conjunto de objetos de selección de recursos que especifican qué recursos se incluyen en la configuración de organización por niveles y sus ajustes de organización por niveles.

Tipo: matriz de objetos [ResourceSelection](#)

Obligatorio: sí

TieringConfigurationName

El nombre exclusivo de la configuración de organización por niveles. No se puede cambiar después de la creación y debe constar únicamente de caracteres alfanuméricos y guiones bajos.

Tipo: cadena

Patrón: `^[a-zA-Z0-9_]{1,200}$`

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

TieringConfigurationInputForUpdate

Servicio: AWS Backup

Contiene metadatos sobre una configuración por niveles para las operaciones de actualización.

Contenido

BackupVaultName

El nombre del almacén de respaldo en el que se aplica la configuración de organización por niveles. Se usa * para aplicarlo a todos los almacenes de respaldo.

Tipo: cadena

Patrón: `^(\*|[a-zA-Z0-9\-\_\]){2,50}$`

Obligatorio: sí

ResourceSelection

Conjunto de objetos de selección de recursos que especifican qué recursos se incluyen en la configuración de organización por niveles y sus ajustes de organización por niveles.

Tipo: matriz de objetos [ResourceSelection](#)

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

TieringConfigurationsListMember

Servicio: AWS Backup

Contiene metadatos sobre una configuración de estratificación devuelta en una lista.

Contenido

BackupVaultName

El nombre del almacén de respaldo en el que se aplica la configuración de organización por niveles. Se usa * para aplicarlo a todos los almacenes de respaldo.

Tipo: cadena

Patrón: `^(\\*|[a-zA-Z0-9\\-\\_]{2,50})$`

Obligatorio: no

CreationTime

Fecha y hora en que se creó una configuración de organización por niveles, en formato Unix y en hora universal coordinada (UTC). El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

LastUpdatedTime

Fecha y hora en que se actualizó la configuración de organización por niveles, en formato Unix y en hora universal coordinada (UTC). El valor de `LastUpdatedTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

TieringConfigurationArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva la configuración de organización en niveles.

Tipo: cadena

Requerido: no

TieringConfigurationName

El nombre exclusivo de la configuración de estratificación.

Tipo: cadena

Patrón: `^[a-zA-Z0-9_]{1,200}$`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

AWS Backup gateway

AWS Backup gateway admite los siguientes tipos de datos:

- [BandwidthRateLimitInterval](#)
- [Gateway](#)
- [GatewayDetails](#)
- [Hypervisor](#)
- [HypervisorDetails](#)
- [MaintenanceStartTime](#)
- [Tag](#)
- [VirtualMachine](#)
- [VirtualMachineDetails](#)
- [VmwareTag](#)

- [VmwareToAwsTagMapping](#)

BandwidthRateLimitInterval

Servicio: AWS Backup gateway

Describe un intervalo de límite de velocidad de ancho de banda para una puerta de enlace. Un programa de límite de velocidad de ancho de banda consta de uno o más intervalos de límite de velocidad de ancho de banda. Un intervalo de límite de velocidad de ancho de banda define un periodo de tiempo en uno o más días de la semana, durante el cual se especifican los límites de velocidad de ancho de banda para la carga, la descarga o ambas.

Contenido

DaysOfWeek

El componente de días de la semana del intervalo límite de velocidad de ancho de banda, se representa como números ordinales del 0 al 6, donde 0 representa el domingo y 6 representa el sábado.

Tipo: Matriz de números enteros

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 7 elementos.

Rango válido: valor mínimo de 0. Valor máximo de 6.

Obligatorio: sí

EndHourOfDay

La hora del día en que finaliza el intervalo de límite de velocidad de ancho de banda.

Tipo: número entero

Rango válido: valor mínimo de 0. Valor máximo de 23.

Obligatorio: sí

EndMinuteOfHour

El minuto de la hora en que finaliza el intervalo de límite de velocidad de ancho de banda.

Important

El intervalo de límite de velocidad de ancho de banda finaliza al final del minuto. Para finalizar un intervalo al final de una hora, utilice el valor 59.

Tipo: número entero

Rango válido: valor mínimo de 0. Valor máximo de 59.

Obligatorio: sí

StartHourOfDay

La hora del día en que comienza el intervalo de límite de velocidad de ancho de banda.

Tipo: número entero

Rango válido: valor mínimo de 0. Valor máximo de 23.

Obligatorio: sí

StartMinuteOfHour

El minuto de la hora en que comienza el intervalo de límite de velocidad de ancho de banda. El intervalo comienza al principio de ese minuto. Para comenzar un intervalo exactamente al principio de la hora, utilice el valor 0.

Tipo: número entero

Rango válido: valor mínimo de 0. Valor máximo de 59.

Obligatorio: sí

AverageUploadRateLimitInBitsPerSec

El componente de límite de velocidad de carga promedio del intervalo de límite de velocidad de ancho de banda, en bits por segundo. Este campo no aparece en la respuesta si no se ha establecido el límite de velocidad de carga.

Tipo: Long

Rango válido: valor mínimo de 51 200. Valor máximo de 8 000 000 000 000

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

Gateway

Servicio: AWS Backup gateway

Una puerta de enlace es un dispositivo de AWS Backup Gateway que se ejecuta en la red del cliente para proporcionar una conectividad perfecta al almacenamiento de copias de seguridad en la nube de AWS.

Contenido

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace. Utilice la operación `ListGateways` para devolver una lista de puertas de enlace para su cuenta y Región de AWS.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 180 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Obligatorio: no

GatewayDisplayName

El nombre de visualización de la puerta de enlace.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `[a-zA-Z0-9-]*`

Obligatorio: no

GatewayType

El tipo de puerta de enlace.

Tipo: cadena

Valores válidos: `BACKUP_VM`

Obligatorio: no

HypervisorId

El ID de hipervisor de la puerta de enlace.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Obligatorio: no

LastSeenTime

La última vez que la puerta de enlace de AWS Backup se comunicó con la puerta de enlace, en formato Unix y en hora UTC.

Tipo: marca temporal

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

GatewayDetails

Servicio: AWS Backup gateway

Los detalles de la puerta de enlace.

Contenido

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace. Utilice la operación `ListGateways` para devolver una lista de puertas de enlace para su cuenta y Región de AWS.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 180 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\[/code>`

Obligatorio: no

GatewayDisplayName

El nombre de visualización de la puerta de enlace.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `[a-zA-Z0-9-]*`

Obligatorio: no

GatewayType

El tipo de puerta de enlace.

Tipo: cadena

Valores válidos: `BACKUP_VM`

Obligatorio: no

HypervisorId

El ID de hipervisor de la puerta de enlace.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Obligatorio: no

LastSeenTime

Detalles que muestran la última vez que la puerta de enlace de AWS Backup se comunicó con la nube, en formato Unix y en hora UTC.

Tipo: marca temporal

Obligatorio: no

MaintenanceStartTime

Devuelve la hora de inicio del mantenimiento semanal de la puerta de enlace, incluido el día y la hora de la semana. Tenga en cuenta que los valores están expresados en términos de la zona horaria de la puerta de enlace. Puede ser semanal o mensual.

Tipo: objeto [MaintenanceStartTime](#)

Obligatorio: no

NextUpdateAvailabilityTime

Detalles que muestran la hora de disponibilidad de la próxima actualización de la puerta de enlace.

Tipo: marca temporal

Obligatorio: no

VpcEndpoint

El nombre de DNS del punto de conexión de la nube privada virtual (VPC) que utiliza la puerta de enlace para conectarse a la nube como puerta de enlace de copia de seguridad.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 255 caracteres.

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

Hypervisor

Servicio: AWS Backup gateway

Representa los permisos del hipervisor a los que se conectará la puerta de enlace.

Un hipervisor es un hardware, software o firmware que crea y administra máquinas virtuales y les asigna recursos.

Contenido

Host

El host del servidor del hipervisor. Puede ser una dirección IP o un nombre de dominio completo (FQDN).

Tipo: cadena

Limitaciones de longitud: longitud mínima de 3. Longitud máxima de 128.

Patrón: . +

Obligatorio: no

HypervisorArn

El nombre de recurso de Amazon (ARN) del hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\[/a-zA-Z-0-9]+

Obligatorio: no

KmsKeyArn

El nombre de recurso de Amazon (ARN) de la clave de AWS Key Management Service (KMS) que se utiliza para cifrar el hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: (^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)\$)|(^alias/(\S+)\$)

Obligatorio: no

Name

El nombre del hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: [a-zA-Z0-9-]*

Obligatorio: no

State

El estado del hipervisor.

Tipo: cadena

Valores válidos: PENDING | ONLINE | OFFLINE | ERROR

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

HypervisorDetails

Servicio: AWS Backup gateway

Estos son los detalles del hipervisor especificado. Un hipervisor es un hardware, software o firmware que crea y administra máquinas virtuales y les asigna recursos.

Contenido

Host

El host del servidor del hipervisor. Puede ser una dirección IP o un nombre de dominio completo (FQDN).

Tipo: cadena

Limitaciones de longitud: longitud mínima de 3. Longitud máxima de 128.

Patrón: . +

Obligatorio: no

HypervisorArn

El nombre de recurso de Amazon (ARN) del hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\[/code>`

Obligatorio: no

KmsKeyArn

El nombre de recurso de Amazon (ARN) de la clave de AWS KMS (KMS) que se utiliza para cifrar el hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias))/(\S+)$)|(^alias/(\S+)$)`

Obligatorio: no

LastSuccessfulMetadataSyncTime

Este es el momento en que se produjo la última sincronización correcta de los metadatos.

Tipo: marca temporal

Obligatorio: no

LatestMetadataSyncStatus

Este es el estado más reciente de la sincronización de metadatos indicada.

Tipo: cadena

Valores válidos: CREATED | RUNNING | FAILED | PARTIALLY_FAILED | SUCCEEDED

Obligatorio: no

LatestMetadataSyncStatusMessage

Este es el estado más reciente de la sincronización de metadatos indicada.

Tipo: cadena

Requerido: no

LogGroupArn

El nombre de recurso de Amazon (ARN) de grupo de puertas de enlace dentro del registro solicitado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0 caracteres. La longitud máxima es de 2048 caracteres.

Patrón: `$|^arn:(aws|aws-cn|aws-us-gov):logs:([a-zA-Z0-9-]+):([0-9]+):log-group:[a-zA-Z0-9_-\./\.\.]+:\*`

Obligatorio: no

Name

Este es el nombre del hipervisor especificado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `[a-zA-Z0-9-]*`

Obligatorio: no

State

Este es el estado actual del hipervisor especificado.

Los estados posibles son PENDING, ONLINE, OFFLINE o ERROR.

Tipo: cadena

Valores válidos: PENDING | ONLINE | OFFLINE | ERROR

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

MaintenanceStartTime

Servicio: AWS Backup gateway

Es la hora de inicio del mantenimiento semanal de la puerta de enlace, incluido el día y la hora de la semana. Tenga en cuenta que los valores están expresados en términos de la zona horaria de la puerta de enlace. Puede ser semanal o mensual.

Contenido

HourOfDay

El componente de horas de la hora de inicio del mantenimiento se representa como hh, donde hh es la hora (de 0 a 23). La hora del día corresponde a la zona horaria de la puerta de enlace.

Tipo: número entero

Rango válido: valor mínimo de 0. Valor máximo de 23.

Obligatorio: sí

MinuteOfHour

El componente de minutos de la hora de inicio del mantenimiento se representa como mm, donde mm es el minuto (de 0 a 59). El minuto de la hora corresponde a la zona horaria de la puerta de enlace.

Tipo: número entero

Rango válido: valor mínimo de 0. Valor máximo de 59.

Obligatorio: sí

DayOfMonth

El componente del día del mes de la hora de inicio del mantenimiento representado como un número ordinal de 1 a 28, donde 1 representa el primer día del mes y 28 representa el último día del mes.

Tipo: número entero

Rango válido: valor mínimo de 1. Valor máximo de 31.

Obligatorio: no

DayOfWeek

Número ordinal entre 0 y 6 que representa el día de la semana, donde 0 representa el domingo y 6 representa el sábado. El día de la semana corresponde a la zona horaria de la puerta de enlace.

Tipo: número entero

Rango válido: valor mínimo de 0. Valor máximo de 6.

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

Tag

Servicio: AWS Backup gateway

Un par clave-valor que puede utilizar para administrar, filtrar y buscar sus recursos. Los caracteres permitidos son los números y letras en UTF-8, además de los siguientes caracteres especiales: + - = . Los caracteres de espaciado _ : / . no se permiten en los valores de las etiquetas.

Contenido

Key

La parte de clave del par clave-valor de la etiqueta. La clave no pueden comenzar por aws : .

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: ([\p{L}\p{Z}\p{N}_ . : / = + \ - @] *)

Obligatorio: sí

Value

La parte de valor del par clave-valor de la etiqueta.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Patrón: [^ \ x 0 0] *

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

VirtualMachine

Servicio: AWS Backup gateway

Una máquina virtual que se encuentra en un hipervisor.

Contenido

HostName

El nombre del host de la máquina virtual.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: [a-zA-Z0-9-]*

Obligatorio: no

HypervisorId

El ID del hipervisor de la máquina virtual.

Tipo: cadena

Requerido: no

LastBackupDate

La fecha más reciente en la que se realizó una copia de seguridad de una máquina virtual, en formato Unix y en hora UTC.

Tipo: marca temporal

Obligatorio: no

Name

Nombre de la máquina virtual.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: [a-zA-Z0-9-]*

Obligatorio: no

Path

La ruta de la máquina virtual.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 4096 caracteres.

Patrón: `[^\x00]+`

Obligatorio: no

ResourceArn

El nombre de recurso de Amazon (ARN) de la máquina virtual. Por ejemplo, `arn:aws:backup-gateway:us-west-1:0000000000000000:vm/vm-0000ABCDEFGHIJKL`.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

VirtualMachineDetails

Servicio: AWS Backup gateway

Sus objetos `VirtualMachine`, ordenados por sus nombres de recurso de Amazon (ARN).

Contenido

HostName

El nombre del host de la máquina virtual.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `[a-zA-Z0-9-]*`

Obligatorio: no

HypervisorId

El ID del hipervisor de la máquina virtual.

Tipo: cadena

Requerido: no

LastBackupDate

La fecha más reciente en la que se realizó una copia de seguridad de una máquina virtual, en formato Unix y en hora UTC.

Tipo: marca temporal

Obligatorio: no

Name

Nombre de la máquina virtual.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `[a-zA-Z0-9-]*`

Obligatorio: no

Path

La ruta de la máquina virtual.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 4096 caracteres.

Patrón: `[^\x00]+`

Obligatorio: no

ResourceArn

El nombre de recurso de Amazon (ARN) de la máquina virtual. Por ejemplo, `arn:aws:backup-gateway:us-west-1:0000000000000000:vm/vm-0000ABCDEFGHIJKL`.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Obligatorio: no

VmwareTags

Estos son los detalles de las etiquetas de VMware asociadas a la máquina virtual especificada.

Tipo: matriz de objetos [VmwareTag](#)

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

VmwareTag

Servicio: AWS Backup gateway

Una etiqueta de VMware es una etiqueta asociada a una máquina virtual específica. Una [etiqueta](#) es un par clave-valor que puede utilizar para administrar, filtrar y buscar sus recursos.

El contenido de las etiquetas de VMware puede corresponderse con las etiquetas de AWS.

Contenido

VmwareCategory

Esta es la categoría de VMware.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 80.

Obligatorio: no

VmwareTagDescription

Es una descripción definida por el usuario de una etiqueta de VMware.

Tipo: cadena

Requerido: no

VmwareTagName

Es el nombre definido por el usuario de una etiqueta de VMware.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 80.

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)

- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

VmwareToAwsTagMapping

Servicio: AWS Backup gateway

Muestra las asignaciones de las etiquetas de VMware a las etiquetas de AWS correspondientes.

Contenido

AwsTagKey

La parte de clave del par clave-valor de la etiqueta de AWS.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: `(?!aws:)[\p{L}\p{Z}\p{N}_.: /+=\ -@]+`

Obligatorio: sí

AwsTagValue

La parte de valor del par clave-valor de la etiqueta de AWS.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Patrón: `[^\x00]*`

Obligatorio: sí

VmwareCategory

Esta es la categoría de VMware.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 80.

Obligatorio: sí

VmwareTagName

Es el nombre definido por el usuario de una etiqueta de VMware.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 80.

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

AWS Backup

AWS Backup admite los siguientes tipos de datos:

- [BackupCreationTimeFilter](#)
- [CurrentSearchProgress](#)
- [EBSItemFilter](#)
- [EBSResultItem](#)
- [ExportJobSummary](#)
- [ExportSpecification](#)
- [ItemFilters](#)
- [LongCondition](#)
- [ResultItem](#)
- [S3ExportSpecification](#)
- [S3ItemFilter](#)
- [S3ResultItem](#)
- [SearchJobBackupsResult](#)
- [SearchJobSummary](#)
- [SearchScope](#)
- [SearchScopeSummary](#)
- [StringCondition](#)

- [TimeCondition](#)

BackupCreationTimeFilter

Servicio: AWS Backup

Este servicio filtra por puntos de recuperación dentro de las marcas temporales CreatedAfter y CreatedBefore.

Contenido

CreatedAfter

Esta marca temporal solo incluye los puntos de recuperación que se crean después del tiempo especificado.

Tipo: marca temporal

Obligatorio: no

CreatedBefore

Esta marca temporal solo incluye los puntos de recuperación que se crean antes del tiempo especificado.

Tipo: marca temporal

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

CurrentSearchProgress

Servicio: AWS Backup

Contiene los resultados de información obtenidos de un trabajo de búsqueda que puede que no se haya completado.

Contenido

ItemsMatchedCount

Este número es la suma de todos los elementos que coinciden con los filtros de elementos de un trabajo de búsqueda en curso.

Tipo: Long

Obligatorio: no

ItemsScannedCount

Este número es la suma de todos los elementos que se han escaneado hasta ahora durante un trabajo de búsqueda.

Tipo: Long

Obligatorio: no

RecoveryPointsScannedCount

Este número es la suma de todas las copias de seguridad que se han escaneado hasta ahora durante un trabajo de búsqueda.

Tipo: entero

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)

- [AWS SDK para Ruby V3](#)

EBSItemFilter

Servicio: AWS Backup

Contiene matrices de objetos, que pueden incluir objetos de condición de tiempo CreationTimes, objetos de cadena de FilePaths y objetos de condición de tiempo LastModificationTimes.

Contenido

CreationTimes

Puede incluir entre uno y diez valores.

Si se incluye uno, los resultados devolverán solo los elementos que coincidan.

Si se incluye más de uno, los resultados devolverán todos los elementos que coincidan con alguno de los valores incluidos.

Tipo: Matriz de [TimeCondition](#) objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 10 artículos.

Obligatorio: no

FilePaths

Puede incluir entre uno y diez valores.

Si se incluye una ruta de archivo, los resultados devolverán solo los elementos que coincidan con la ruta de archivo.

Si se incluye más de una ruta de archivo, los resultados devolverán todos los elementos que coincidan con alguna ruta de archivo.

Tipo: Matriz de [StringCondition](#) objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 10 artículos.

Obligatorio: no

LastModificationTimes

Puede incluir entre uno y diez valores.

Si se incluye uno, los resultados devolverán solo los elementos que coincidan.

Si se incluye más de uno, los resultados devolverán todos los elementos que coincidan con alguno de los valores incluidos.

Tipo: Matriz de [TimeCondition](#) objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 10 artículos.

Obligatorio: no

Sizes

Puede incluir entre uno y diez valores.

Si se incluye uno, los resultados devolverán solo los elementos que coincidan.

Si se incluye más de uno, los resultados devolverán todos los elementos que coincidan con alguno de los valores incluidos.

Tipo: Matriz de [LongCondition](#) objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 10 artículos.

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

EBSResultItem

Servicio: AWS Backup

Estos son los elementos devueltos en los resultados de una búsqueda en los metadatos de las copias de seguridad de Amazon EBS.

Contenido

BackupResourceArn

Se trata de uno o más elementos de los resultados que coinciden con los valores del nombre de recurso de Amazon (ARN) de los puntos de recuperación devueltos por una búsqueda en los metadatos de las copias de seguridad de Amazon EBS.

Tipo: cadena

Requerido: no

BackupVaultName

Es el nombre del almacén de copias de seguridad.

Tipo: cadena

Requerido: no

CreationTime

Se trata de uno o más elementos de los resultados que coinciden con los valores de los tiempos de creación devueltos por una búsqueda en los metadatos de las copias de seguridad de Amazon EBS.

Tipo: marca temporal

Obligatorio: no

FilePath

Se trata de uno o más elementos de los resultados que coinciden con las rutas de archivo devueltas por una búsqueda en los metadatos de las copias de seguridad de Amazon EBS.

Tipo: cadena

Requerido: no

FileSize

Se trata de uno o más elementos de los resultados que coinciden con los valores de los tamaños de archivo devueltos por una búsqueda en los metadatos de las copias de seguridad de Amazon EBS.

Tipo: Long

Obligatorio: no

FileSystemIdentifier

Se trata de uno o más elementos de los resultados que coinciden con los valores de los sistemas de archivo devueltos por una búsqueda en los metadatos de las copias de seguridad de Amazon EBS.

Tipo: cadena

Requerido: no

LastModifiedTime

Se trata de uno o más elementos de los resultados que coinciden con los valores de Hora de la última modificación devueltos por una búsqueda en los metadatos de las copias de seguridad de Amazon EBS.

Tipo: marca temporal

Obligatorio: no

SourceResourceArn

Se trata de uno o más elementos de los resultados que coinciden con los valores del nombre de recurso de Amazon (ARN) de los recursos de origen devueltos por una búsqueda en los metadatos de las copias de seguridad de Amazon EBS.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ExportJobSummary

Servicio: AWS Backup

Es el resumen de un trabajo de exportación.

Contenido

ExportJobIdentifier

Esta es la cadena unívoca que identifica un trabajo de exportación específico.

Tipo: cadena

Obligatorio: sí

CompletionTime

Es una marca temporal de la hora en que se completó el trabajo de exportación.

Tipo: marca temporal

Obligatorio: no

CreationTime

Es una marca temporal de la hora en que se creó el trabajo de exportación.

Tipo: marca temporal

Obligatorio: no

ExportJobArn

Este es el ARN (nombre de recurso de Amazon) exclusivo que pertenece al nuevo trabajo de exportación.

Tipo: cadena

Requerido: no

SearchJobArn

Cadena única que identifica el nombre de recurso de Amazon (ARN) del trabajo de búsqueda especificado.

Tipo: cadena

Requerido: no

Status

El estado del trabajo de exportación puede ser uno de los siguientes:

CREATED; RUNNING; FAILED; o bien COMPLETED.

Tipo: cadena

Valores válidos: RUNNING | FAILED | COMPLETED

Obligatorio: no

StatusMessage

Un mensaje de estado es una cadena que se devuelve para un trabajo de exportación.

El mensaje de estado se incluye para cualquier estado que no sea COMPLETED sin problemas.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ExportSpecification

Servicio: AWS Backup

Contiene el objeto de especificación de exportación.

Contenido

Important

Este tipo de datos es una unión, por lo que solo se puede especificar uno de los siguientes miembros cuando se usa o se devuelve.

s3ExportSpecification

Especifica el bucket de Amazon S3 de destino para el trabajo de exportación. Y, si se incluye, también especifica el prefijo de destino.

Tipo: objeto [S3ExportSpecification](#)

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ItemFilters

Servicio: AWS Backup

Son los filtros de elementos que representan todas las propiedades de los elementos de entrada especificados al crear la búsqueda.

Contiene EBSItemFilters o S3ItemFilters.

Contenido

EBSItemFilters

Esta matriz puede contener los objetos CreationTimes, FilePaths, LastModificationTimes o Sizes.

Tipo: matriz de objetos [EBSItemFilter](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 10 artículos.

Obligatorio: no

S3ItemFilters

Esta matriz puede contener los objetos CreationTimes, ETags, ObjectKeys, Sizes o VersionIds.

Tipo: matriz de objetos [S3ItemFilter](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 10 artículos.

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

LongCondition

Servicio: AWS Backup

La condición larga contiene un `Value` y, opcionalmente, puede contener un `Operator`.

Contenido

Value

Es el valor de un elemento incluido en uno de los filtros de elementos de búsqueda.

Tipo: Long

Obligatorio: sí

Operator

Es una cadena que define los valores que se devolverán.

Si se incluye, evite las combinaciones de operadores que devuelvan todos los valores posibles. Por ejemplo, si se incluyen `EQUALS_TO` y `NOT_EQUALS_TO` con el valor 4, se devolverán todos los valores.

Tipo: cadena

Valores válidos: `EQUALS_TO` | `NOT_EQUALS_TO` | `LESS_THAN_EQUAL_TO` | `GREATER_THAN_EQUAL_TO`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ResultItem

Servicio: AWS Backup

Se trata de un objeto que representa el elemento devuelto en los resultados de la búsqueda de un tipo de recurso específico.

Contenido

Important

Este tipo de datos es una unión, por lo que solo se puede especificar uno de los siguientes miembros cuando se usa o se devuelve.

EBSResultItem

Estos son los elementos devueltos en los resultados de una búsqueda en Amazon EBS.

Tipo: objeto [EBSResultItem](#)

Obligatorio: no

S3ResultItem

Estos son los elementos devueltos en los resultados de una búsqueda en Amazon S3.

Tipo: objeto [S3ResultItem](#)

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

S3ExportSpecification

Servicio: AWS Backup

Esta especificación contiene una cadena obligatoria del bucket de destino; si lo desea, puede incluir el prefijo de destino.

Contenido

DestinationBucket

Especifica el bucket de Amazon S3 de destino para el trabajo de exportación.

Tipo: cadena

Obligatorio: sí

DestinationPrefix

Especifica el prefijo del bucket de Amazon S3 de destino para el trabajo de exportación.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

S3ItemFilter

Servicio: AWS Backup

Contiene matrices de objetos como ObjectKeys, Sizes, CreationTimes, VersionIds o Etags.

Contenido

CreationTimes

Puede incluir entre uno y diez valores.

Si se incluye uno, los resultados solo devolverán los elementos que coincidan con el valor.

Si se incluye más de un valor, los resultados devolverán todos los elementos que coincidan con alguno de los valores.

Tipo: Matriz de [TimeCondition](#) objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 10 artículos.

Obligatorio: no

ETags

Puede incluir entre uno y diez valores.

Si se incluye uno, los resultados solo devolverán los elementos que coincidan con el valor.

Si se incluye más de un valor, los resultados devolverán todos los elementos que coincidan con alguno de los valores.

Tipo: Matriz de [StringCondition](#) objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 10 artículos.

Obligatorio: no

ObjectKeys

Puede incluir entre uno y diez valores.

Si se incluye uno, los resultados solo devolverán los elementos que coincidan con el valor.

Si se incluye más de un valor, los resultados devolverán todos los elementos que coincidan con alguno de los valores.

Tipo: Matriz de [StringCondition](#) objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 10 artículos.

Obligatorio: no

Sizes

Puede incluir entre uno y diez valores.

Si se incluye uno, los resultados solo devolverán los elementos que coincidan con el valor.

Si se incluye más de un valor, los resultados devolverán todos los elementos que coincidan con alguno de los valores.

Tipo: Matriz de [LongCondition](#) objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 10 artículos.

Obligatorio: no

VersionIds

Puede incluir entre uno y diez valores.

Si se incluye uno, los resultados solo devolverán los elementos que coincidan con el valor.

Si se incluye más de un valor, los resultados devolverán todos los elementos que coincidan con alguno de los valores.

Tipo: Matriz de [StringCondition](#) objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 10 artículos.

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)

- [AWS SDK para Ruby V3](#)

S3ResultItem

Servicio: AWS Backup

Estos son los elementos devueltos en los resultados de una búsqueda en los metadatos de las copias de seguridad de Amazon S3.

Contenido

BackupResourceArn

Se trata de elementos de los resultados que coinciden con la entrada del nombre de recurso de Amazon (ARN) de los puntos de recuperación devueltos por una búsqueda en los metadatos de las copias de seguridad de Amazon S3.

Tipo: cadena

Requerido: no

BackupVaultName

Es el nombre del almacén de copias de seguridad.

Tipo: cadena

Requerido: no

CreationTime

Se trata de uno o más elementos de los resultados devueltos que coinciden con los valores de la entrada del tiempo de creación de los elementos en una búsqueda en los metadatos de las copias de seguridad de Amazon S3.

Tipo: marca temporal

Obligatorio: no

ETag

Se trata de uno o más elementos de los resultados devueltos que coinciden con los valores de la entrada de ETags en una búsqueda en los metadatos de las copias de seguridad de Amazon S3.

Tipo: cadena

Requerido: no

ObjectKey

Se trata de uno o más elementos devueltos en los resultados de una búsqueda en los metadatos de las copias de seguridad de Amazon S3 que coinciden con los valores indicados en la clave del objeto.

Tipo: cadena

Requerido: no

ObjectSize

Se trata de los elementos de los resultados devueltos que coinciden con los valores de la entrada del tamaño de un objeto en una búsqueda en los metadatos de las copias de seguridad de Amazon S3.

Tipo: Long

Obligatorio: no

SourceResourceArn

Se trata de los elementos de los resultados devueltos que coinciden con la entrada del nombre de recurso de Amazon (ARN) de origen en una búsqueda en los metadatos de las copias de seguridad de Amazon S3.

Tipo: cadena

Requerido: no

VersionId

Se trata de uno o más elementos de los resultados devueltos que coinciden con los valores de la entrada de los ID de versión en una búsqueda en los metadatos de las copias de seguridad de Amazon S3.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

SearchJobBackupsResult

Servicio: AWS Backup

Contiene la información sobre los puntos de recuperación devueltos en los resultados de un trabajo de búsqueda.

Contenido

BackupCreationTime

Es la hora de creación de la copia de seguridad (punto de recuperación).

Tipo: marca temporal

Obligatorio: no

BackupResourceArn

Es el nombre de recurso de Amazon (ARN) que identifica de forma unívoca los recursos de copia de seguridad.

Tipo: cadena

Requerido: no

IndexCreationTime

Es la hora de creación del índice de copias de seguridad.

Tipo: marca temporal

Obligatorio: no

ResourceType

Este es el tipo de recurso de la búsqueda.

Tipo: cadena

Valores válidos: S3 | EBS

Obligatorio: no

SourceResourceArn

Es el nombre de recurso de Amazon (ARN) que identifica de forma unívoca los recursos de origen.

Tipo: cadena

Requerido: no

Status

Este es el estado del resultado de la copia de seguridad del trabajo de búsqueda.

Tipo: cadena

Valores válidos: RUNNING | COMPLETED | STOPPING | STOPPED | FAILED

Obligatorio: no

StatusMessage

Este es el mensaje de estado que se incluye con los resultados.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

SearchJobSummary

Servicio: AWS Backup

Esta es la información relacionada con un trabajo de búsqueda.

Contenido

CompletionTime

Este es el tiempo de finalización del trabajo de búsqueda.

Tipo: marca temporal

Obligatorio: no

CreationTime

Este es el tiempo de creación del trabajo de búsqueda.

Tipo: marca temporal

Obligatorio: no

Name

Este es el nombre del trabajo de búsqueda.

Tipo: cadena

Requerido: no

SearchJobArn

Cadena única que identifica el nombre de recurso de Amazon (ARN) del trabajo de búsqueda especificado.

Tipo: cadena

Requerido: no

SearchJobIdentifier

Cadena unívoca que especifica el trabajo de búsqueda.

Tipo: cadena

Requerido: no

SearchScopeSummary

Devuelve un resumen del ámbito del trabajo de búsqueda especificado, que incluye:

- `TotalBackupsToScanCount`, que es el número de puntos de recuperación que devuelve la búsqueda.
- `TotalItemsToScanCount`, que es el número de elementos que devuelve la búsqueda.

Tipo: objeto [SearchScopeSummary](#)

Obligatorio: no

Status

Este es el estado del trabajo de búsqueda.

Tipo: cadena

Valores válidos: `RUNNING` | `COMPLETED` | `STOPPING` | `STOPPED` | `FAILED`

Obligatorio: no

StatusMessage

Se devolverá un mensaje de estado para cada trabajo de búsqueda con un estado `ERRORRED` o un estado de trabajos `COMPLETED` con problemas.

Por ejemplo, un mensaje puede indicar que una búsqueda contiene puntos de recuperación que no se han podido analizar debido a un problema con permisos.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

SearchScope

Servicio: AWS Backup

Ámbito de búsqueda que incluye todas las propiedades de copia de seguridad introducidas en una búsqueda.

Contenido

BackupResourceTypes

Tipos de recursos incluidos en una búsqueda.

Los tipos de recursos elegibles son S3 y EBS.

Tipo: matriz de cadenas

Miembros de la matriz: número fijo de 1 elemento.

Valores válidos: S3 | EBS

Obligatorio: sí

BackupResourceArns

Es el nombre de recurso de Amazon (ARN) que identifica de forma unívoca los recursos de copia de seguridad.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 50 artículos.

Obligatorio: no

BackupResourceCreationTime

Es el momento en que se creó el recurso de copia de seguridad.

Tipo: objeto [BackupCreationTimeFilter](#)

Obligatorio: no

BackupResourceTags

Se trata de una o más etiquetas en la copia de seguridad (punto de recuperación).

Tipo: mapa de cadena a cadena

Obligatorio: no

SourceResourceArns

Es el nombre de recurso de Amazon (ARN) que identifica de forma unívoca los recursos de origen.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 50 artículos.

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

SearchScopeSummary

Servicio: AWS Backup

Resumen del ámbito del trabajo de búsqueda especificado, que incluye:

- `TotalBackupsToScanCount`, que es el número de puntos de recuperación que devuelve la búsqueda.
- `TotalItemsToScanCount`, que es el número de elementos que devuelve la búsqueda.

Contenido

`TotalItemsToScanCount`

Es el recuento del número total de elementos que se escaneará en una búsqueda.

Tipo: Long

Obligatorio: no

`TotalRecoveryPointsToScanCount`

Es el recuento del número total de copias de seguridad que se escaneará en una búsqueda.

Tipo: entero

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

StringCondition

Servicio: AWS Backup

Contiene el valor de la cadena y puede incluir uno o más operadores.

Contenido

Value

Es el valor de la cadena.

Tipo: cadena

Obligatorio: sí

Operator

Es una cadena que define los valores que se devolverán.

Si se incluye, evite las combinaciones de operadores que devuelvan todos los valores posibles. Por ejemplo, si se incluyen EQUALS_TO y NOT_EQUALS_TO con el valor 4, se devolverán todos los valores.

Tipo: cadena

Valores válidos: EQUALS_TO | NOT_EQUALS_TO | CONTAINS | DOES_NOT_CONTAIN | BEGINS_WITH | ENDS_WITH | DOES_NOT_BEGIN_WITH | DOES_NOT_END_WITH

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

TimeCondition

Servicio: AWS Backup

Una condición de tiempo indica la hora de creación, la hora de la última modificación u otra hora.

Contenido

Value

Es el valor de la marca temporal de la condición de tiempo.

Tipo: marca temporal

Obligatorio: sí

Operator

Es una cadena que define los valores que se devolverán.

Si se incluye, evite las combinaciones de operadores que devuelvan todos los valores posibles. Por ejemplo, si se incluyen EQUALS_TO y NOT_EQUALS_TO con el valor 4, se devolverán todos los valores.

Tipo: cadena

Valores válidos: EQUALS_TO | NOT_EQUALS_TO | LESS_THAN_EQUAL_TO | GREATER_THAN_EQUAL_TO

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

Parámetros comunes

La siguiente lista contiene los parámetros que utilizan todas las acciones para firmar solicitudes de Signature Version 4 con una cadena de consulta. Los parámetros específicos de acción se enumeran en el tema correspondiente a la acción. Para obtener más información sobre Signature Version 4, consulte [Firma de solicitudes API de AWS](#) en la Guía del usuario de IAM.

Action

Las acciones que se van a realizar.

Tipo: cadena

Obligatorio: sí

Version

La versión de la API para la que está escrita la solicitud, expresada en el formato AAAA-MM-DD.

Tipo: cadena

Obligatorio: sí

X-Amz-Algorithm

El algoritmo de hash que utilizó para crear la solicitud de firma.

Condición: especifique este parámetro cuando incluya información de autenticación en una cadena de consulta en lugar de en el encabezado de autorización HTTP.

Tipo: cadena

Valores válidos: AWS4-HMAC-SHA256

Obligatorio: condicional

X-Amz-Credential

El valor del ámbito de la credencial, que es una cadena que incluye la clave de acceso, la fecha, la región a la que se dirige, el servicio que solicita y una cadena de terminación ("aws4_request"). El valor se expresa en el siguiente formato: access_key/AAAAMMDD/region/service/aws4_request.

Para obtener más información, consulte [Crear una solicitud API de AWS firmada](#) en la Guía del usuario de IAM.

Condición: especifique este parámetro cuando incluya información de autenticación en una cadena de consulta en lugar de en el encabezado de autorización HTTP.

Tipo: cadena

Obligatorio: condicional

X-Amz-Date

La fecha utilizada para crear la firma. El formato debe ser ISO 8601 formato básico (AAAAMMDD'T'HHMMSS'Z'). Por ejemplo, la siguiente fecha y hora es un valor válido de X-Amz-Date para 20120325T120000Z.

Condición: X-Amz-Date es opcional en todas las solicitudes; se puede utilizar para anular la fecha empleada a fin de firmar las solicitudes. Si el encabezado Date se especifica en el formato básico ISO 8601, no se requiere X-Amz-Date. Cuando se usa X-Amz-Date, siempre anula el valor del encabezado Date. Para obtener más información, consulte [Elementos de una firma de solicitud API de AWS](#) en la Guía del usuario de IAM.

Tipo: cadena

Obligatorio: condicional

X-Amz-Security-Token

El token de seguridad temporal que se obtuvo mediante una llamada a AWS Security Token Service (AWS STS). Para obtener una lista de servicios compatibles con las credenciales de seguridad temporales de AWS STS, consulte [Servicios de AWS que funcionan con IAM](#) en la Guía del usuario de IAM.

Condición: si utiliza credenciales de seguridad temporales de AWS STS, debe incluir el token de seguridad.

Tipo: cadena

Obligatorio: condicional

X-Amz-Signature

Especifica la firma codificada hexadecimal que se calculó a partir de la cadena que se va a firmar y la clave de firma derivada.

Condición: especifique este parámetro cuando incluya información de autenticación en una cadena de consulta en lugar de en el encabezado de autorización HTTP.

Tipo: cadena

Obligatorio: condicional

X-Amz-SignedHeaders

Especifica todos los encabezados HTTP que se incluyeron como parte de la solicitud canónica. Para obtener más información acerca de especificar encabezados firmados, consulte [Crear una solicitud API de AWS firmada](#) en la Guía del usuario de IAM.

Condición: especifique este parámetro cuando incluya información de autenticación en una cadena de consulta en lugar de en el encabezado de autorización HTTP.

Tipo: cadena

Obligatorio: condicional

Errores comunes

En esta sección, se enumeran los errores comunes a las acciones de la API de todos los servicios de AWS. En el caso de los errores específicos de una acción de la API de este servicio, consulte el tema de dicha acción de la API.

AccessDeniedException

No tiene acceso suficiente para realizar esta acción.

Código de estado HTTP: 400

IncompleteSignature

La firma de solicitud no se ajusta a los estándares de AWS.

Código de estado HTTP: 400

InternalFailure

El procesamiento de la solicitud ha devuelto un error debido a un error o una excepción desconocidos.

Código de estado HTTP: 500

InvalidAction

La acción u operación solicitada no es válida. Compruebe que la acción se ha escrito correctamente.

Código de estado HTTP: 400

InvalidClientTokenId

El certificado X.509 o el ID de clave de acceso de AWS proporcionado no existen en nuestros registros.

Código de estado HTTP: 403

NotAuthorized

No tiene permiso para realizar esta acción.

Código de estado HTTP: 400

OptInRequired

El ID de clave de acceso de AWS necesita una suscripción al servicio.

Código de estado HTTP: 403

RequestExpired

La solicitud llegó al servicio más de 15 minutos después de la marca de fecha en la solicitud o más de 15 minutos después de la fecha de vencimiento de la solicitud (por ejemplo, para las URL prefirmadas) o la marca de fecha de la solicitud corresponde a una hora futura en más de 15 minutos.

Código de estado HTTP: 400

ServiceUnavailable

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 503

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

Código de estado HTTP: 400

ValidationError

La entrada no satisface las limitaciones que especifica un servicio de AWS.

Código de estado HTTP: 400

Historial de documentos para AWS Backup

- Versión de la API: 19 de noviembre de 2025
- Última actualización de la documentación: 19 de noviembre de 2025

En la siguiente tabla se enumeran todos los AWS Backup lanzamientos desde el lanzamiento del servicio en enero de 2019 hasta la fecha. Para recibir notificaciones sobre las actualizaciones de esta documentación, puede suscribirse al canal RSS que aparece más arriba.

Cambio	Descripción	Fecha
Protección contra GuardDuty malware de Amazon para AWS Backup	Amazon GuardDuty Malware Protection ahora es compatible con AWS Backup las copias de seguridad de EBS y S3 y amplía las capacidades de detección de malware. EC2 Para obtener más información, consulte la página de detalles del producto de .	19 de noviembre de 2025
Se ha añadido una nueva política administrada de AWS .	AWS Backup agregó la política AWSBackupGuardDutyRolePolicyForScans AWS gestionada. Para obtener más información, consulte Políticas administradas de AWS Backup.	19 de noviembre de 2025
Se ha añadido una nueva política administrada de AWS .	AWS Backup agregó la política AWSBackupServiceRolePolicyForScans AWS gestionada.	19 de noviembre de 2025

Cambio	Descripción	Fecha
	Para obtener más información, consulte Políticas administradas de AWS Backup .	
Actualizaciones de políticas administradas	AWS Backup se agregaron permisos adicionales a las siguientes políticas AWS administradas: • AWSBackupFullAccess • AWSBackupOperatorAccess Para obtener más información, consulte Actualizaciones de las políticas administradas de AWS Backup.	19 de noviembre de 2025
Backup por niveles	AWS Backup presenta un nivel de almacenamiento en caliente de bajo coste para los datos de backup de Amazon S3. Para obtener más información, consulte Organización de copias de seguridad en niveles.	18 de noviembre de 2025

Cambio	Descripción	Fecha
Copias de seguridad principales en almacenes aislados lógicamente	Lógicamente, ahora se admiten bóvedas aisladas como objetivo de respaldo principal. Esta mejora permite a los clientes aprovechar los beneficios de seguridad y recuperación que ofrecen las bóvedas herméticas de forma lógica y, al mismo tiempo, mantener una sola copia de respaldo, lo que reduce los costos operativos y de almacenamiento. Anteriormente, las bóvedas con huecos lógicos solo podían almacenar copias de las copias de seguridad existentes. Para obtener más información, consulte Copias de seguridad principales en bóvedas aisladas de forma lógica.	17 de noviembre de 2025

Cambio	Descripción	Fecha
AWS Backup soporte para clústeres de Amazon Elastic Kubernetes Service	AWS Backup ahora es compatible con los clústeres de Amazon EKS. Los clientes pueden crear copias de seguridad y restaurar puntos de recuperación para los clústeres de Amazon EKS y sus recursos asociados. Para obtener más información, consulte Disponibilidad de funciones por recurso y Actualizaciones de políticas administradas para AWS Backup.	10 de noviembre de 2025

Cambio	Descripción	Fecha
Actualizaciones de políticas administradas	AWS Backup agregó permisos adicionales a las siguientes políticas AWS administradas: • AWSBackupFullAccess • AWSBackupOperatorAccess • AWSBackupServiceRolePolicyForBackup • AWSBackupServiceLinkedRolePolicyForBackup • AWSBackupServiceRolePolicyForRestores Para obtener más información, consulte Actualizaciones de las políticas administradas de AWS Backup.	10 de noviembre de 2025
Soporte de bóveda agrupado de forma lógica para claves administradas por el cliente AWS KMS	Las bóvedas herméticas lógicas ahora admiten el cifrado con claves administradas por el cliente. AWS KMS Para obtener más información, consulte Logically air-gapped vault.	6 de noviembre de 2025

Cambio	Descripción	Fecha
Soporte de copia de instantáneas entre regiones y cuentas	Amazon RDS, Aurora, DocumentDB y Neptune ahora admiten la copia de instantáneas entre regiones y cuentas en una sola acción. Para obtener más información, consulte Disponibilidad de funciones por recurso.	23 de octubre de 2025
AWS Backup Expansión del soporte regional para Aurora DSQL	Ya se pueden realizar copias de seguridad y restauraciones de Amazon Aurora DSQL en Europa (Fráncfort). Para obtener más información, consulte Servicios compatibles por región y Copias de seguridad de Aurora DSQL.	22 de octubre de 2025
AWS Backup Expansión regional	AWS Backup, junto con gran cantidad de sus características, ya está disponible en Asia-Pacífico (Nueva Zelanda). Para obtener más información, consulte Disponibilidad de características por región.	29 de septiembre de 2025

Cambio	Descripción	Fecha
Compatibilidad opcional con Amazon S3 ACLs y copias de seguridad de etiquetas de objetos	AWS Backup ahora admite la exclusión opcional de Amazon S3 ACLs y de las etiquetas de objetos, lo que permite a los clientes reducir los costes de backup. Para obtener más información, consulte Copias de seguridad Amazon S3.	9 de septiembre de 2025
Actualizaciones de políticas administradas	AWS Backup agregó permisos adicionales a las siguientes políticas AWS administradas: • AWSBackupServiceLinkedRolePolicyForBackup Para obtener más información, consulte Actualizaciones de las políticas administradas de AWS Backup.	9 de septiembre de 2025

Cambio	Descripción	Fecha
AWS Backup Expansión regional de Audit Manager	AWS Backup Audit Manager Los informes interregionales y multicuentas ya están disponibles en otros idiomas Regiones de AWS, incluidos Asia Pacífico (Hyderabad), Asia Pacífico (Yakarta), Asia Pacífico (Melbourne), Europa (España), Europa (Zúrich) y Oriente Medio (Emiratos Árabes Unidos). Para obtener más información, consulte Disponibilidad de características por Región de AWS y Creación de planes de informes.	5 de septiembre de 2025
Mayor AWS Backup compatibilidad con la restauración multirregional de Amazon Aurora DSQL	AWS Backup los usuarios ahora pueden restaurar los clústeres multirregionales de Aurora DSQL a través de la AWS Backup consola o mediante la CLI AWS Backup . Para obtener más información, consulte Restauración de un clúster de varias regiones de Aurora DSQL.	29 de julio de 2025

Cambio	Descripción	Fecha
Actualizaciones de políticas administradas	AWS Backup agregó permisos adicionales a las siguientes políticas AWS administradas: • AWSBackupServiceRolePolicyForRestore Para obtener más información, consulte Actualizaciones de las políticas administradas de AWS Backup.	29 de julio de 2025
AWS Backup soporte adicional para la restauración multirregional de Amazon Aurora DSQL Regiones de AWS	AWS Backup ahora es compatible con la restauración multirregional Aurora DSQL, además. Regiones de AWS Para obtener más información, consulte Restauración de un clúster de varias regiones de Aurora DSQL y Servicios compatibles por región.	3 de julio de 2025

Cambio	Descripción	Fecha
AWS Backup característica Expansión regional	AWS Backup añade compatibilidad con la copia multicuenta y entre regiones de las copias de seguridad de Amazon S3 en AWS GovCloud (EE. UU. Este) y AWS GovCloud (EE. UU. Oeste). Regiones de AWS Para obtener más información, consulte Copias de seguridad de Amazon S3 y Copia de seguridad y copia de etiquetas.	26 de junio de 2025
AWS Backup soporte para Amazon Aurora DSQL en Asia Pacífico (Seúl)	AWS Backup ahora es compatible con Aurora DSQL en Asia Pacífico (Seúl). Para obtener más información, consulte Servicios compatibles por región.	26 de junio de 2025

Cambio	Descripción	Fecha
AWS Backup soporte para la aprobación multipartita	AWS Backup ahora admite la integración opcional para que las bóvedas con huecos lógicos utilicen la aprobación de varias partes. Esta funcionalidad ya está disponible para las cuentas en la región del Este de EE. UU. (Norte de Virginia). Para obtener más información, consulte lo siguiente: • Aprobación de varias partes para almacenes aislados lógicamente Guía de usuario de la aprobación de varias partes	17 de junio de 2025
AWS actualización de política gestionada	AWS Backup se han añadido nuevos permisos a la política AWS gestionada AWSBackupFullAccess. Para obtener más información sobre los permisos específicos, consulte Actualizaciones de políticas.	17 de junio de 2025

Cambio	Descripción	Fecha
AWS Backup Expansión regional de Audit Manager	AWS Backup Audit Manager ahora está disponible en versiones adicionales Regiones de AWS, que incluyen: • Asia-Pacífico (Hyderabad) • Asia-Pacífico (Yakarta) • Asia-Pacífico (Melbourne) • Europa (España) • Europa (Zúrich) • Medio Oriente (EAU) Para obtener más información, consulte Disponibilidad de características por región y Administrador de auditoría de Backup.	16 de junio de 2025
AWS Backup Expansión regional	AWS Backup, junto con muchas de sus funciones, ya está disponible en Asia Pacífico (Taipéi) Región de AWS. Para obtener más información, consulte Disponibilidad de características por región y Servicios compatibles por región.	6 de junio de 2025

Cambio	Descripción	Fecha
Compatibilidad con las notificaciones y eventos del índice de copias de seguridad	AWS Backup lanza la compatibilidad con las notificaciones de Amazon Simple Notification Service y EventBridge los eventos de Amazon para los índices de respaldo. AWS Backup La compatibilidad con los índices de copias de seguridad de notificaciones está disponible en todos los establecimientos AWS comerciales y en GovCloud las regiones en las que se admiten los índices de copia de seguridad y las redes sociales. EventBridge Para obtener más información, consulte la Notificaciones de usuario consola, la consola y la EventBridge búsqueda e índice de copias de seguridad.	3 de junio de 2025

Cambio	Descripción	Fecha
Funciones adicionales de Amazon EC2 Restore	Las configuraciones de volumen se pueden personalizar durante un trabajo de restauración. Puede especificar una configuración personalizada para los volúmenes de Amazon EBS adjuntos a una EC2 AMI de Amazon, incluidos los metadatos de restauración para las asignaciones de dispositivos de bloques. Para obtener información adicional, consulte Restore Amazon EC2 with AWS CLI y la Guía del usuario de Amazon Elastic Compute Cloud.	28 de mayo de 2025

Cambio	Descripción	Fecha
AWS Backup compatibilidad con clústeres DSQL de Amazon Aurora	AWS Backup ahora ofrece integración con Aurora DSQL en varias Regiones de AWS. Los clientes pueden crear copias de seguridad y restaurar puntos de recuperación para los clústeres de Aurora DSQL de una única región o de múltiples regiones. Para obtener más información, consulte Restauración de Amazon Aurora DSQL, Disponibilidad de funciones por recurso y Administración de clústeres en Aurora DSQL con AWS CLI.	27 de mayo de 2025

Cambio	Descripción	Fecha
Actualizaciones de políticas administradas	AWS Backup agregó permisos adicionales a las siguientes políticas AWS administradas: AWSBackupFullAccess, AWSBackupOperatorAccess, AWSBackupServiceLinkedRolePolicyForBackup, AWSBackupServiceRolePolicyForBackup, y AWSBackupServiceRolePolicyForRestores. Para obtener más información, consulte Actualizaciones de las políticas administradas de AWS Backup.	27 de mayo de 2025
AWS Backup cuentan con expansión regional	AWS Backup La búsqueda ya está disponible en Asia Pacífico (Tailandia), México (Central), (EEUU-Este) AWS GovCloud y (Regiones de AWS EEUU-Oeste). AWS GovCloud Para obtener más información, consulte Disponibilidad de las funciones por Región de AWS y Búsqueda de copias de seguridad.	22 de abril de 2025

Cambio	Descripción	Fecha
AWS Backup compatibilidad con los espacios de nombres de Amazon Redshift Serverless	Los clientes ahora pueden utilizarlas AWS Backup para crear copias de seguridad manuales de instantáneas de Redshift Serverless y restaurarlas en los espacios de nombres de Redshift Serverless. Para obtener más información, consulte Copias de seguridad de Amazon Redshift sin servidor.	31 de marzo de 2025

Cambio	Descripción	Fecha
Actualizaciones de políticas administradas	AWS Backup se agregaron permisos adicionales a las siguientes políticas administradas: AWS • AWSBackupFullAccess • AWSBackupOperatorAccess • AWSBackupServiceLinkedRolePolicyForBackup • AWSBackupServiceRolePolicyForBackup • AWSBackupServiceRolePolicyForRestores Para obtener más información, consulte Actualizaciones de las políticas administradas de AWS Backup.	31 de marzo de 2025

Cambio	Descripción	Fecha
AWS Backup servicio compatible: expansión regional	AWS Backup El soporte FSx para OpenZFS ya está disponible en las siguientes direcciones: Regiones de AWS • Oeste de EE. UU. (Norte de California) • África (Ciudad del Cabo) • Asia-Pacífico (Hyderabad) • Asia-Pacífico (Yakarta) • Asia-Pacífico (Osaka) • Europa (Milán) • Europa (París) • Europa (España) • Europa (Zúrich) • Israel (Tel Aviv) • Middle East (Bahrain) • Medio Oriente (EAU) • América del Sur (São Paulo) Para obtener más información, consulte Servicios compatibles con. Regiones de AWS	12 de marzo de 2025

Cambio	Descripción	Fecha
Expansión de los recursos en un almacén aislado lógicamente	Los puntos de recuperación (copias de seguridad) FSx de los recursos FSx de Lustre, Windows File Server y FSx OpenZFS ahora se pueden copiar en un almacén cerrado de forma lógica. Para obtener más información, consulte lo siguiente: • Tener un almacén aislado lógicamente • Disponibilidad de funciones por recurso	12 de marzo de 2025
Nueva política AWS gestionada	AWS Backup se agregó una nueva política AWS administrada: AWSBackupSearchOperatorAccess. Para obtener más información, consulte AWSBackupSearchOperatorAccess la Guía de políticas AWS administradas.	27 de febrero de 2025
AWS Backup Expansión regional	AWS Backup, junto con muchas de sus funciones, ya está disponible en México (Central) Región de AWS. Para obtener más información, consulte Disponibilidad de características por región.	21 de enero de 2025

Cambio	Descripción	Fecha
AWS Backup Expansión regional	AWS Backup, junto con numerosas características, ya está disponible en Asia-Pacífico (Tailandia). Para obtener más información, consulte Disponibilidad de características por región.	14 de enero de 2025
Se actualizaron las políticas administradas de AWS	AWS Backup agregó el permiso <code>rds:AddTagsToResource</code> a la política gestionada <code>AWSBackupServiceLinkedRolePolicyForBackup</code>. AWS Backup agregó los permisos <code>rds:CreateTenantDatabase</code> y <code>rds:DeleteTenantDatabase</code> a la política <code>AWSBackupServiceRolePolicyForRestores</code>. Para obtener más información, consulte Actualizaciones de políticas.	8 de enero de 2025

Cambio	Descripción	Fecha
Support para IPv6	AWS Backup ahora es compatible con los protocolos de Internet, versión 6 (IPv6) y IPv4. Para obtener más información sobre las capacidades y los puntos de conexión de doble pila, consulte Red de AWS Backup.	18 de diciembre de 2024
AWS Backup servicio compatible: expansión regional	AWS Backup La compatibilidad con Amazon Timestream ya está disponible AWS GovCloud en (EE. UU.-Oeste). Para obtener más información, consulte Servicios compatibles por Regiones de AWS y Copias de seguridad de Amazon Timestream.	18 de diciembre de 2024
Se ha añadido la característica de búsqueda	AWS Backup presenta la opción de buscar propiedades a nivel de elemento en los metadatos de las copias de seguridad para ayudarle a encontrar puntos de recuperación y otros archivos u objetos que desee restaurar. Consulte Búsqueda de copias de seguridad para obtener más detalles.	17 de diciembre de 2024

Cambio	Descripción	Fecha
Se ha añadido una nueva política administrada de AWS .	AWS Backup agregó la política AWSBackupServiceRolePolicyForItemRestores AWS gestionada. Para obtener más información, consulte Políticas administradas de AWS Backup.	17 de diciembre de 2024
Se ha añadido una nueva política administrada de AWS .	AWS Backup agregó la política AWSBackupServiceRolePolicyForIndexing AWS gestionada. Para obtener más información, consulte Políticas administradas de AWS Backup.	17 de diciembre de 2024
AWS Backup característica: Expansión regional	La administración multicuenta para monitorear los trabajos de respaldo, copia y restauración mediante la AWS Organizations integración AWS Backup y ahora está disponible Regiones de AWS cuando se requiere la suscripción. Para obtener más información, consulte Disponibilidad de características por región.	12 de diciembre de 2024

Cambio	Descripción	Fecha
AWS Backup servicio compatible: expansión regional	AWS Backup La compatibilidad con Amazon Timestream ya está disponible en Asia Pacífico (Bombay). Para obtener más información, consulte Servicios compatibles por Regiones de AWS y Copias de seguridad de Amazon Timestream.	22 de noviembre de 2024
Características adicionales de la restauración de Amazon S3	AWS Backup añade flexibilidad adicional al restaurar las copias de seguridad de S3. Ahora puede restaurar versiones adicionales de objetos, incluida la restauración de todas las versiones. Para obtener más información, consulte Restaurar datos de S3 mediante AWS Backup.	21 de noviembre de 2024

Cambio	Descripción	Fecha
AWS Backup función Expansión regional	AWS Backup los clientes ahora pueden crear copias entre regiones de las copias de seguridad de Amazon Neptune en más regiones, incluidas África (Ciudad del Cabo), Asia Pacífico (Yakarta) y Asia Pacífico (Osaka). Para obtener más información, consulte Disponibilidad de características por región y Creación de copias de seguridad entre Regiones de AWS.	13 de noviembre de 2024
Expansión de la copia entre regiones	Ahora se admite la copia entre regiones de las copias de seguridad de Amazon S3 en los Regiones de AWS casos en los que se requiere la suscripción. Para obtener más información, consulte Disponibilidad de características por Región de AWS.	13 de noviembre de 2024

Cambio	Descripción	Fecha
AWS Backup Expansión regional de Audit Manager	AWS Backup Audit Manager ya está disponible en Región de AWS Asia Pacífico (Osaka). Para obtener más información, consulte Disponibilidad de características por región y Administrador de auditoría de Backup.	29 de octubre de 2024
AWS Backup ahora disponible en la región Asia Pacífico (Malasia)	La copia de seguridad restauración para muchos tipos de recursos ya están disponibles en Región de AWS Asia-Pacífico (Malasia). Para ver las características de copia de seguridad compatibles, consulte Feature availability by Región de AWS. Para ver los tipos de recursos compatibles, consulte Servicios compatibles de Región de AWS.	10 de octubre de 2024

Cambio	Descripción	Fecha
AWS Backup Control Audit Manager para bóvedas con huecos de aire lógicos	AWS Backup Audit Manager ahora ofrece los recursos de control en una bóveda con huecos lógicos para ayudar a supervisar si los recursos se han copiado a una bóveda con huecos lógicos dentro del plazo especificado. Para obtener más información, consulte Controles y corrección y Auditoría de pruebas de restauración.	12 de septiembre de 2024
AWS Backup cuentan con expansión regional	AWS Backup los clientes ahora pueden crear copias entre regiones de las copias de seguridad de Amazon Neptune en más regiones, incluidas Asia Pacífico (Hong Kong), Israel (Tel Aviv), Oriente Medio (Baréin) y Oriente Medio (Emiratos Árabes Unidos). Para obtener más información, consulte la disponibilidad de la característica por región y la creación de copias de seguridad entre Regiones de AWS.	29 de agosto. 2024

Cambio	Descripción	Fecha
AWS Backup admite copias entre regiones y cuentas para bases de datos de SAP HANA	Los usuarios que han realizado copias de seguridad de las bases de datos de SAP HANA en EC2 las instancias de Amazon ahora pueden copiar instantáneas de las copias de seguridad completas a otras regiones y otras cuentas. Para obtener más información, consulte Bases de datos de SAP HANA en EC2 instancias de Amazon.	20 de agosto de 2024
AWS Backup ahora ofrece un nuevo tipo de bóveda segura	AWS Backup ha introducido un tipo secundario de bóveda para almacenar copias de las copias de seguridad . Los almacenes aislados lógicamente ofrecen características de seguridad mejoradas , así como la posibilidad de compartir el acceso al almacén con las cuentas a través de AWS RAM. Para obtener más información, consulte Logically air-gapped vault.	7 de agosto de 2024

Cambio	Descripción	Fecha
AWS Backup función: expansión regional	AWS Backup La compatibilidad con Amazon Simple Storage Service (Amazon S3) ya está disponible en el oeste de Canadá (Calgary). Los clientes ya pueden hacer copias de seguridad y restaurar los recursos en la región Oeste de Canadá (Calgary). Para obtener más información sobre la disponibilidad en la región AWS Backup Amazon S3, consulte Servicios compatibles de Región de AWS.	27 de junio de 2024
Cierre de la versión preliminar del Almacén aislado lógicamente	Ha finalizado la versión preliminar del Almacén aislado lógicamente .	27 de junio de 2024
AWS Backup cuentan con expansión regional	AWS Backup La compatibilidad con el nivel de archivado de instantáneas de Amazon EBS ya está disponible en las siguientes regiones: • China (Pekín) • China (Ningxia) • AWS GovCloud (EE. UU.- Oeste) • AWS GovCloud (Estados Unidos-Este)	3 de junio de 2024

Cambio	Descripción	Fecha
Se actualizaron las políticas administradas de AWS	AWS Backup se agregó permiso backup : TagResource a las siguientes políticas administradas: • AWSBackupServiceRolePolicyForBackup • AWSBackupServiceRolePolicyForS3 Backup • AWSBackupServiceLinkedRolePolicyForBackup Para obtener más información, consulte Actualizaciones de políticas.	17 de mayo de 2024
AWS Backup ahora disponible en la región Canadá Oeste (Calgary)	La copia de seguridad y restauración para muchos tipos de recursos ya están disponibles en la región Región de AWS Oeste de Canadá (Calgary). Para ver las características de copia de seguridad compatibles, consulte Feature availability by Región de AWS. Para ver los tipos de recursos compatibles, consulte Servicios compatibles Región de AWS de.	14 de marzo de 2024

Cambio	Descripción	Fecha
Permisos añadidos a la política administrada	AWS Backup actualizó la política AWSServiceRolePolicyForBackupRestoreTesting añadiendo permisos para admitir tipos de recursos adicionales dentro de la función de pruebas de restauración. Para obtener más información sobre los permisos específicos agregados, consulte Policy updates.	14 de febrero de 2024
Soporte de backup y restauración FSx para volúmenes ONTAP FlexGroup	AWS Backup ahora admite la copia de seguridad y la restauración de los FlexGroup volúmenes FSx de ONTAP en la mayoría de los casos. Regiones de AWS Para obtener más información, consulta Restauración de un sistema de FSx archivos de Amazon.	10 de enero de 2024

Cambio	Descripción	Fecha
Compatibilidad con copia de seguridad y restauración de SAP HANA HA	AWS Backup ahora ofrece soporte para bases de datos de alta disponibilidad de SAP HANA en Amazon EC2 backup y restore. Para obtener más información, consulte EC2 Respaldos de SAP HANA en Amazon y restauración de un sistema de alta disponibilidad de SAP HANA	21 de diciembre de 2023
AWS Backup Control Audit Manager para pruebas de restauración	AWS Backup Audit Manager ahora ofrece el control del tiempo de restauración para que los recursos cumplan con el objetivo para ayudar a monitorear los tiempos de restauración. Este control comprueba si el tiempo de restauración de un recurso cumple la duración objetivo. Para obtener más información, consulte Controles y corrección y Auditoría de pruebas de restauración.	18 de diciembre de 2023

Cambio	Descripción	Fecha
Compatibilidad con almacenamiento en frío de Amazon EBS	AWS Backup ahora admite la transición de copias de seguridad de EBS del almacenamiento en caliente al almacenamiento en frío. Para obtener más información, consulte Amazon EBS Archive Tier para almacenamiento en frío y Creación de plan de copia de seguridad. Ciclo de vida y niveles de almacenamiento	27 de noviembre de 2023
Presentación de las políticas de restauración	AWS Backup presenta las pruebas de restauración, que permiten una evaluación automática y periódica de la viabilidad de la restauración, así como la capacidad de supervisar los tiempos de duración de las tareas de restauración. Para obtener más información, consulte Pruebas de restauración.	27 de noviembre de 2023

Cambio	Descripción	Fecha
Se actualizaron las políticas administradas de AWS	AWS Backup agregó los permisos <code>ec2:DescribeSnapshotTierStatus</code> y <code>ec2:ModifySnapshotTier</code> a las políticas administradas <code>AWSBackupServiceRolePolicyForBackups</code> y <code>AWSBackupServiceLinkedRolePolicyForBackup</code>. AWS Backup también agregó los permisos <code>ec2:DescribeSnapshotTierStatus</code> y <code>ec2:RestoreSnapshotTier</code> a la política administrada <code>AWSBackupServiceRolePolicyForRestores</code>. Estos permisos son necesarios para que los usuarios tengan la opción de realizar la transición de los recursos de Amazon EBS almacenados en AWS Backup al almacenamiento de archivos y de restaurar los recursos del nivel de almacenamiento de archivos. Para obtener más información, consulte Actualizaciones de políticas.	27 de noviembre de 2023

Cambio	Descripción	Fecha
Se agregó el permiso para transmitir roles para facilitar pruebas de restauración.	AWS Backup agregado <code>restore-testing.backup.amazonaws.com</code> a <code>IamPassRolePermissions</code> y <code>IamCreateServiceLinkedRolePermissions</code> Esta adición es necesaria para AWS Backup realizar pruebas de restauración en nombre de los clientes.	27 de noviembre de 2023

Cambio	Descripción	Fecha
Se ha agregado una nueva política de roles vinculados a servicios	AWS Backup ha agregado el nuevo rol vinculado al servicio denominado AWSServiceRoleForBackupRestoreTesting, que proporciona permisos de respaldo para realizar pruebas de restauración. Esta nueva función vinculada al servicio proporciona los permisos necesarios para realizar AWS Backup las pruebas de restauración. Los permisos incluyen las acciones <code>list</code>, <code>read</code>, and <code>write</code> para que los siguientes servicios se incluyan en las pruebas de restauración: Aurora, DocumentDB, DynamoDB, Amazon EBS, Amazon EC2, Amazon EFS, para Lustre, para Windows File Server FSx, para ONTAP FSx, para FSx OpenZFS FSx, Amazon Neptune, Amazon RDS y Amazon S3.	27 de noviembre de 2023

Cambio	Descripción	Fecha
Nuevo panel de métricas de tareas en la consola AWS Backup	La AWS Backup consola ahora muestra un panel de tareas, lo que simplifica la supervisión del estado de las copias de seguridad a gran escala con una nueva interfaz visual de usuario y métricas agregadas de respaldo, copia y restauración de los servicios compatibles AWS Backup. El panel de empleos está disponible en todas las regiones en las que está disponible AWS Backup Audit Manager. Las regiones que no figuran en la lista podrán seguir accediendo al CloudWatch panel. Para obtener más información, consulte paneles de la consola de AWS Backup.	15 de noviembre de 2023

Cambio	Descripción	Fecha
Compatibilidad con copias de seguridad de pilas anidadas	AWS Backup ha ampliado su compatibilidad con las copias de seguridad de CloudFormation los recursos. Las pilas de CloudFormation aplicaciones que contienen pilas anidadas se pueden incluir en las copias de seguridad. Para obtener más información, consulte CloudFormation stack backups.	8 de noviembre de 2023
Compatibilidad con Amazon S3 en China (Pekín) y China (Ningxia).	AWS Backup El soporte para Amazon S3 ya está disponible en las regiones de China (Pekín) y China (Ningxia). Para obtener más información, consulte Disponibilidad de características por región.	26 de octubre de 2023
Support para copias de seguridad y Point-in-time restauración continuas de Amazon Aurora	AWS Backup ahora admite copias de seguridad y point-in-time restauración continuas (PITR) para los recursos de Aurora. Para obtener más información, consulte Respaldos y Point-in-time recuperación continuos.	7 de septiembre de 2023

Cambio	Descripción	Fecha
CloudFormation las pilas admiten la exclusión de recursos	AWS Backup ahora admite la opción de excluir los recursos elegidos de la CloudFormation pila. Para obtener más información, consulte CloudFormation stack backups.	6 de septiembre de 2023
Las reglas del plan de copia de seguridad introducen flexibilidad en las zonas horarias	AWS Backup las reglas del plan ahora pueden tener una zona horaria específica para las ventanas de respaldo. Para obtener más información, consulte Administración de planes de copia de seguridad.	28 de agosto de 2023
AWS Backup ahora disponible en la región de Israel (Tel Aviv)	Muchas AWS Backup funciones ya están disponibles en la nueva región de Israel (Tel Aviv). Para ver qué recursos son compatibles, visite Disponibilidad de características por Región de AWS.	22 de agosto de 2023

Cambio	Descripción	Fecha
AWS Backup Audit Manager ahora admite cuentas de administrador delegado	AWS Backup Las cuentas de administrador delegado ahora pueden acceder a la generación de informes de Audit Manager. Para obtener más información, consulte Auditar copias de seguridad y crear informes con AWS Backup Audit Manager , Trabajar con informes de auditoría y Delegated Administrator .	16 de agosto de 2023
AWS Backup mejora las copias de seguridad de Amazon S3	AWS Backup ha aumentado las capacidades de rendimiento, tamaño y velocidad para las copias de seguridad en cubos de S3. Para obtener más información, consulte Copias de seguridad Amazon S3 .	1 de agosto de 2023
La característica de etiquetar las restauraciones ahora está disponible en regiones de China	Ahora puede copiar las etiquetas que forman parte de una copia de seguridad al crear un trabajo de restauración en las regiones de China (Pekín) o China (Ningxia). Para obtener más información, consulte Copia de etiquetas durante una restauración .	17 de julio de 2023

Cambio	Descripción	Fecha
AWS Backup ahora es compatible con Amazon S3 en regiones adicionales	AWS Backup El soporte para Amazon S3 ya está disponible en las regiones de Europa (España), Europa (Zúrich), Asia Pacífico (Hyderabad) y Asia Pacífico (Melbourne). Para obtener más información, consulte Disponibilidad de características por región.	6 de julio de 2023
La copia entre cuentas se ha ampliado a más regiones	AWS Backup ahora admite copias de seguridad multicuenta de la mayoría de los recursos en las siguientes regiones: Asia Pacífico (Yakarta), Oriente Medio (Baréin), Asia Pacífico (Hong Kong), África (Ciudad del Cabo), Europa (Milán), Asia Pacífico (Osaka), Oriente Medio (Emiratos Árabes Unidos), Europa (España), Europa (Zúrich), Asia Pacífico (Hyderabad) y Asia Pacífico (Melbourne). Para obtener más información, consulte Disponibilidad de características por región.	5 de julio de 2023

Cambio	Descripción	Fecha
Backup Audit Manager disponible en GovCloud las regiones	AWS Backup ha ampliado AWS Backup Audit Manager a AWS GovCloud (EE. UU. Este) y AWS GovCloud (EE. UU. Oeste). Para obtener más información, consulte Disponibilidad de características por región.	29 de junio de 2023
La administración de cuentas cruzadas ahora está disponible en las regiones GovCloud	AWS Backup ahora admite la gestión multicuenta de los recursos en AWS GovCloud (EE. UU. este) y AWS GovCloud (EE. UU., oeste). Para obtener más información, consulte Administración de recursos de AWS Backup en varias cuentas de AWS.	29 de junio de 2023
Compatibilidad con copias entre regiones de Amazon Aurora en más regiones	AWS Backup ahora admite copias de seguridad entre regiones para los clústeres de Aurora desde y hacia las siguientes regiones: Asia Pacífico (Yakarta), Oriente Medio (Baréin), Asia Pacífico (Hong Kong), África (Ciudad del Cabo), Europa (Milán), Oriente Medio (Emiratos Árabes Unidos), Europa (España), Europa (Zúrich), Asia Pacífico (Hyderabad) y Asia Pacífico (Melbourne).	5 de junio de 2023

Cambio	Descripción	Fecha
Copia de etiquetas al restaurar	Las etiquetas que forman parte de una copia de seguridad ahora se pueden copiar al crear un trabajo de restauración. Para obtener más información, consulte Copia de etiquetas durante una restauración.	22 de mayo de 2023
AWS Backup se integra con las notificaciones de usuario AWS	Ahora puede optar por recibir notificaciones relacionadas con los eventos de copia de seguridad, copia y restauración a través de la Consola de AWS User Notifications. Para obtener más información, consulte Introducción a las notificaciones AWS de usuario.	10 de mayo de 2023
Copias de seguridad entre regiones disponibles en cuatro regiones nuevas	AWS Backup ahora admite copias de seguridad entre regiones en la región de Oriente Medio (EAU), la región de Europa (España), la región de Europa (Zúrich) y la región de Asia Pacífico (Hyderabad).	28 de abril de 2023

Cambio	Descripción	Fecha
Soporte ampliado de copias entre regiones AWS Backup	Las copias de seguridad entre regiones de los recursos de Amazon EFS y DynamoDB ahora se pueden realizar en las siguientes regiones: Asia Pacífico (Yakarta), Oriente Medio (Baréin), Asia Pacífico (Hong Kong), África (Ciudad del Cabo) y Europa (Milán). VMware	28 de abril de 2023
Copia de seguridad y restauración de Amazon S3 en la región de América del Sur (São Paulo)	AWS Backup El soporte para Amazon S3 (Amazon Simple Storage Service) ya está disponible en la región de Sudamérica (São Paulo). Para obtener más información, consulte Copias de seguridad Amazon S3.	20 de abril de 2023
AWS Backup se expande a la región de Asia Pacífico (Melbourne)	AWS Backup ahora está disponible en la región Asia Pacífico (Melbourne). Para obtener más información, consulte Disponibilidad de funciones por AWS región.	20 de abril de 2023

Cambio	Descripción	Fecha
Ampliación de la compatibilidad regional para Amazon S3	AWS Backup La compatibilidad con Amazon S3 (Amazon Simple Storage Service) ya está disponible en las regiones AWS GovCloud (EE. UU. Este) y AWS GovCloud (EE. UU. Oeste) Para obtener más información, consulte Copias de seguridad Amazon S3.	19 de abril de 2023
Backup y restauración de bases de datos de SAP HANA en EC2 instancias de Amazon	AWS Backup ahora ofrece la posibilidad de realizar copias de seguridad y restaurar las bases de datos de SAP HANA que se ejecutan en EC2 instancias de Amazon en la mayoría de las regiones. Para obtener más información, consulte la copia de seguridad de bases de datos de SAP HANA en EC2 instancias de Amazon.	17 de abril de 2023

Cambio	Descripción	Fecha
AWS Backup ahora disponible en las regiones de Europa (España), Europa (Zúrich) y Asia Pacífico (Hyderabad)	AWS Backup el apoyo se ha extendido a nuevas regiones, incluidas Europa (España), Europa (Zúrich) y Asia Pacífico (Hyderabad). En estas regiones se pueden realizar copias de seguridad y restauraciones de los recursos compatibles. Para obtener más información, consulte Disponibilidad de funciones por AWS región.	13 de abril de 2023
Política AWS gestionada actualizada AWSBackup AuditAccess	Política AWS gestionada actualizada AWSBackup AuditAccess. AWS Backup sustituyó la selección de recursos de la API <code>config:DescribeComplianceByConfigRule</code> por un recurso comodín. Para obtener más información, consulte Actualizaciones de políticas para AWS Backup.	11 de abril de 2023

Cambio	Descripción	Fecha
Hipervisores con Amazon Logs CloudWatch	AWS Backup Los usuarios de gateway ahora pueden integrar los hipervisores con los registros para mantener los CloudWatch registros. Para obtener más información, consulte Edición de la configuración de un hipervisor y de los registros. CloudWatch	29 de marzo de 2023
Compatibilidad regional ampliada para Amazon S3	AWS Backup El soporte para Amazon S3 ya está disponible en las regiones de Asia Pacífico (Yakarta) y Oriente Medio (Emiratos Árabes Unidos).	22 de marzo de 2023
Mejora de la copia de seguridad incremental de máquinas virtuales	VMware Las copias de seguridad de las máquinas virtuales (máquinas virtuales) que presentan problemas con los datos de CBT (Changed Block Tracking) ahora contienen información adicional para ayudar a solucionar problemas y solucionar problemas. Para obtener más información, consulte Copias de seguridad incrementales de máquinas virtuales y Solucionar problemas de máquinas virtuales .	15 de marzo de 2023

Cambio	Descripción	Fecha
AWS Backup soporte para varios adaptadores de red	AWS Backup la puerta de enlace ahora admite la configuración de varios adaptadores de red Para obtener más información sobre la configuración de los adaptadores de red, consulte <u>Configurar la puerta de enlace para múltiples NICs entradas VMware</u> en la Guía para AWS Backup desarrolladores.	8 de marzo de 2023
AWS Backup compatibilidad con vSphere 8	AWS Backup ahora admite la copia de seguridad y la restauración de máquinas virtuales que se ejecutan en VMware vSphere 8. Para obtener más información sobre VMware las opciones compatibles, consulte las opciones compatibles VMs en la Guía para AWS Backup desarrolladores.	8 de marzo de 2023

Cambio	Descripción	Fecha
AWS Backup Audit Manager es compatible con las copias de seguridad Multi-AZ de Amazon RDS	Backup Audit Manager ofrece ahora compatibilidad con copias de seguridad en varias zonas de disponibilidad de Amazon Relational Database Service Para obtener más información, consulte cómo auditar las copias de seguridad y crear informes con AWS Backup Audit Manager.	1 de febrero de 2023
AWS Backup ofrece copias de seguridad incrementales para las tablas de Amazon Timestream	AWS Backup ahora ofrece capacidades de respaldo ampliadas para las copias de seguridad de Timestream. Los planes de copia de seguridad ahora pueden realizar copias de seguridad incrementales para reducir el tiempo necesario para realizar copias de seguridad de los recursos de Timestream y reducir los costos de almacenamiento. Para obtener más información, consulte Copias de seguridad de Amazon Timestream.	23 de enero de 2023

Cambio	Descripción	Fecha
AWS Backup ahora disponible en Dubái	AWS Backup se ha expandido a la región de Oriente Medio (EAU). En esta región se pueden realizar copias de seguridad y restauraciones de los recursos compatibles.	17 de enero de 2023
Copia entre regiones disponible en más regiones	AWS Backup ahora ofrece copias de seguridad entre regiones en la región de Asia Pacífico (Yakarta), la región de Medio Oriente (Baréin), la región de Asia Pacífico (Hong Kong), la región de África (Ciudad del Cabo) y la región de Europa (Milán) para la mayoría de los recursos. Para obtener más información, consulte Creación de copias de las copias de seguridad entre Regiones de AWS.	21 de diciembre de 2022

Cambio	Descripción	Fecha
Limitación y regulación del ancho de banda de Backup Gateway	AWS Backup La puerta de enlace ahora permite limitar el rendimiento de carga desde las puertas de enlace AWS Backup para controlar la cantidad de ancho de banda de red que utiliza la puerta de enlace. Para respaldar esta función, AWS Backup ha creado y actualizado políticas administradas, que incluyen AWSBackupFullAccess y AWSBackupOperatorAccess Para obtener más información, consulte Limitación del ancho de banda de Backup Gateway.	15 de diciembre de 2022

Cambio	Descripción	Fecha
Compatibilidad con VMware etiquetas de Backup Gateway	AWS Backup Gateway ahora admite VMware etiquetas. Los usuarios tienen la flexibilidad adicional de crear AWS etiquetas que coincidan con las etiquetas utilizadas en las máquinas virtuales. Para respaldar esta función, AWS Backup ha creado y actualizado políticas administradas, que incluyen <code>AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync</code>, <code>AWSBackupFullAccess</code>, y <code>AWSBackupOperatorAccess</code>. Para obtener más información, consulte las VMware etiquetas.	15 de diciembre de 2022
AWS Backup soporte para Amazon Timestream	AWS Backup ahora admite la creación de copias de seguridad y la restauración de las tablas de Amazon Timestream. Para obtener más información, consulte Copias de seguridad de Amazon Timestream.	13 de diciembre de 2022

Cambio	Descripción	Fecha
AWS Backup ofrece retención legal	AWS Backup presenta una nueva herramienta para ayudar a proteger los puntos de recuperación en caso de retención legal. Para obtener más información, consulte Retención legal .	27 de noviembre de 2022
AWS Backup Audit Manager Informes entre regiones y cuentas	AWS Backup Audit Manager aporta funciones adicionales a los informes de cumplimiento y de trabajo. Los usuarios pueden generar informes que incorporen varias regiones y varias cuentas. Para obtener más información, consulte Uso de informes de auditoría .	27 de noviembre de 2022
AWS Backup es compatible con Amazon Redshift	AWS Backup ahora ofrece soporte para realizar copias de seguridad de clústeres de Amazon Redshift y restaurar clústeres y tablas de Amazon Redshift. Para obtener más información, consulte Copias de seguridad Amazon Redshift .	27 de noviembre de 2022

Cambio	Descripción	Fecha
AWS Backup ofrece soporte para hacer copias de seguridad de pilas de aplicaciones AWS CloudFormation	AWS Backup proporciona la capacidad de realizar copias de seguridad CloudFormation y restaurar aplicaciones que contienen varios recursos mediante la creación de copias de seguridad de una pila y la restauración de los recursos que contiene. Para obtener más información, consulte Copias de seguridad de pilas de aplicaciones.	27 de noviembre de 2022
AWS Backup ofrece cuentas de administrador delegadas y delegación de políticas de respaldo	AWS Backup las cuentas inscritas AWS Organizations pueden designar las cuentas de los miembros como cuentas de administrador delegado. Para obtener más información, consulte Administrar varias cuentas con AWS Organizations.	27 de noviembre de 2022

Cambio	Descripción	Fecha
Vista previa pública de la copia de seguridad y restauración de SAP HANA en Amazon EC2 Instances	AWS Backup y AWS Backup ofrecen una vista previa pública integrada de la funcionalidad para hacer copias de seguridad y restaurar las bases de datos de SAP HANA en las EC2 instancias. Para obtener más información, consulte nuestra versión preliminar pública de las EC2 instancias de SAP HANA en Amazon. Para respaldar esta versión preliminar, AWS Backup hemos incluido actualizaciones de políticas y nuevas políticas AWS gestionadas para estas funciones.	20 de noviembre de 2022

Cambio	Descripción	Fecha
Restaurar VMware en EC2 instancias de Amazon	AWS Backup ahora ofrece la posibilidad de restaurar máquinas virtuales en EC2 instancias de Amazon, además de la capacidad de restaurar máquinas en EBS VMware, VMware Cloud on AWS y VMware Cloud on AWS Outposts. Para obtener más información, consulte la documentación sobre cómo usar la AWS Backup consola para restaurar los puntos de recuperación de máquinas virtuales.	9 de noviembre de 2022
Funcionalidad ampliada de AWS Backup Vault Lock	AWS Backup Ahora, Vault Lock se puede crear en modo de gobierno para ofrecer protecciones adicionales de IAM o en modo de conformidad para garantizar la inmutabilidad. Obtenga más información en Bloqueo de almacenes de AWS Backup.	4 de octubre de 2022

Cambio	Descripción	Fecha
AWS Backup Audit Manager ya está disponible en la región de África (Ciudad del Cabo) y en la región de Europa (Milán)	AWS Backup Audit Manager se ha expandido a la región de África (Ciudad del Cabo) y a la región de Europa (Milán). Para obtener más información sobre Backup Audit Manager, consulte Auditar copias de seguridad y crear informes con AWS Backup Audit Manager .	14 de septiembre de 2022
AWS Backup lleva CloudWatch las métricas de Amazon al panel de control de la consola de Backup	AWS Backup mejora el panel de control de la consola Backup para mostrar CloudWatch las métricas integradas de Amazon para las tareas de backup y restauración, con el fin de aumentar la flexibilidad y la capacidad de supervisión.	8 de septiembre de 2022
Compatibilidad con una mayor flexibilidad de cifrado de Amazon EBS durante la restauración	AWS Backup ahora ofrece opciones adicionales de cifrado durante la restauración de las instantáneas de Amazon EBS.	1 de septiembre de 2022

Cambio	Descripción	Fecha
AWS Backup admite copias de seguridad entre cuentas y regiones de Amazon S3	AWS Backup ahora ofrece copias de seguridad entre regiones y cuentas para copias de seguridad de Amazon S3. Para obtener más información, consulte Copias de seguridad Amazon S3.	28 de julio de 2022
AWS Backup Audit Manager ofrece soporte de control adicional FSx para ONTAP	AWS Backup Audit Manager ahora ofrece controles adicionales para respaldar la supervisión y la auditoría FSx de los volúmenes de ONTAP, incluidos los recursos de Backup incluidos en al menos un plan de respaldo y la creación del último punto de recuperación. Para obtener más información, consulte Controles y correcciones de AWS Backup Audit Manager.	22 de julio de 2022

Cambio	Descripción	Fecha
AWS Backup añade soporte para realizar copias de seguridad y restaurar clústeres Multi-AZ de Amazon RDS para clústeres PostgreSQL y MySQL	AWS Backup ha agregado una opción de copia de seguridad y restauración de clústeres en zonas de disponibilidad múltiple con una instancia de base de datos principal y dos en espera legibles. Para obtener más información, consulte Copias de seguridad de Amazon RDS Multi-AZ.	20 de julio de 2022
AWS Backup Audit Manager añade un nuevo control para la creación de puntos de recuperación	AWS Backup Audit Manager ofrece un nuevo control de auditoría para aumentar el apoyo al cumplimiento. Last recovery point created es un control adicional opcional para garantizar que los puntos de recuperación se creen dentro de los plazos especificados. Para obtener más información, consulte Último punto de recuperación creado.	29 de junio de 2022
Se agregó un ejemplo AWS Backup de punto final Gateway	AWS Backup Gateway proporcionó un ejemplo de punto final para ayudar a los usuarios a conectarse a VPNs (redes privadas virtuales).	14 de junio de 2022

Cambio	Descripción	Fecha
AWS Backup ahora ofrece puntos de enlace de Amazon VPC para VMware	AWS Backup ahora es compatible con los puntos de enlace de Amazon VPC VMware, lo que le permite utilizar una red privada virtual entre sus VMware entornos y el uso. AWS PrivateLink Para obtener más información, consulte Creación de una puerta de enlace y AWS Backup y AWS PrivateLink.	1 de junio de 2022
AWS Backup Audit Manager ofrece soporte de control adicional para Amazon S3	Backup Audit Manager ahora admite el control de conformidad Recursos de copias de seguridad protegidos por planes de copia de seguridad para los tipos de recursos de S3. Para obtener más información, consulte Controles y correcciones de AWS Backup Audit Manager.	25 de mayo de 2022

Cambio	Descripción	Fecha
AWS Backup Audit Manager ofrece soporte de control adicional para Storage Gateway	Backup Audit Manager ahora admite el control de conformidad Recursos de copias de seguridad protegidos por planes de copia de seguridad para los tipos de recursos de Storage Gateway. Para obtener más información, consulte Controles y correcciones de AWS Backup Audit Manager.	25 de mayo de 2022
Support de Amazon FSx para OpenZFS	AWS Backup ahora ofrece una gestión adicional de la protección de datos para realizar copias de seguridad y restaurar archivos en los sistemas FSx de archivos OpenZFS.	18 de mayo de 2022
AWS Backup Soporte de Audit Manager para VMware	AWS Backup ahora ofrece soporte para máquinas virtuales en los controles y la corrección de Backup Audit Manager. Para obtener más información, consulte Controles y correcciones de AWS Backup Audit Manager .	11 de mayo de 2022

Cambio	Descripción	Fecha
Amazon FSx ahora es compatible con la región de Asia Pacífico (Osaka)	AWS Backup ahora ofrece copias de seguridad de Amazon FSx en la región de Asia Pacífico (Osaka) y copias entre regiones desde y hacia dicha región.	26 de abril de 2022
Support de Amazon FSx para Lustre Persistent_2	AWS Backup ahora ofrece compatibilidad general con Amazon FSx for Lustre, que admite niveles más altos de rendimiento por unidad de almacenamiento en comparación con los sistemas de archivos Persistent_1.	5 de abril de 2022
VMware Mejoras	AWS Backup ahora ofrece restauración a Amazon EBS Volume, restauración a nivel de disco y compatibilidad con VMware on AWS Outposts. Para obtener más información, consulte Restauración de una máquina virtual .	31 de marzo de 2022
AWS Backup Disponibilidad para Asia Pacífico (Yakarta)	AWS Backup ya está disponible para los clientes de la región de Asia Pacífico (Yakarta).	17 de marzo de 2022

Cambio	Descripción	Fecha
Nuevos controles para AWS Backup Audit Manager	AWS Backup Audit Manager presenta tres nuevos controles de auditoría: copia entre regiones, copia entre cuentas y Backup Vault Lock. Para obtener más información, consulte Controles y correcciones de AWS Backup Audit Manager .	17 de marzo de 2022
Support para AWS PrivateLink	Con AWS PrivateLink for AWS Backup, puede conectarse directamente AWS Backup mediante un punto final de interfaz en su VPC en lugar de conectarse a través de la Internet pública. Se puede acceder directamente a los puntos finales de la interfaz desde las aplicaciones que se encuentran en las instalaciones o en una región diferente AWS . Para obtener más información, consulte AWS Backup y AWS PrivateLink .	28 de febrero de 2022

Cambio	Descripción	Fecha
Compatibilidad con Amazon Simple Storage Service (Amazon S3)	La disponibilidad general AWS Backup de Amazon S3 Regiones de AWS está disponible en todas las regiones, excepto en las regiones China (Pekín), China (Ningxia), AWS GovCloud EE. UU. oeste y AWS GovCloud EE. UU. Este. Para obtener más información, consulte Uso de objetos de Amazon S3 .	14 de febrero de 2022
Support para copias de seguridad avanzadas de DynamoDB en las regiones de China AWS	La copia de seguridad avanzada de DynamoDB ya está disponible en las regiones de China (Pekín) y China (Ningxia). Para obtener más información, consulte Copia de seguridad avanzada de DynamoDB .	18 de enero de 2022
Versión preliminar pública de la compatibilidad con Amazon S3	AWS Backup ofrece una vista previa pública de las copias de seguridad de Amazon S3. Para obtener más información, consulte Uso de datos de Amazon S3 .	30 de noviembre de 2021
Support para máquinas VMware virtuales (VMs)	Ahora puede utilizarla AWS Backup para realizar copias de seguridad automáticamente VMware VMs. Para obtener más información, consulte Copias de seguridad de máquinas virtuales .	30 de noviembre de 2021

Cambio	Descripción	Fecha
Compatibilidad con copias de seguridad avanzadas de DynamoDB	Ahora puede utilizar AWS Backup las siguientes funciones para todas las nuevas copias de seguridad de tablas de DynamoDB que cree: almacenamiento en frío por niveles, etiquetado de asignación de costes, copia entre regiones, copia entre cuentas, cifrado independiente y copia de etiquetas de tablas de DynamoDB de origen. Para obtener más información, consulte Copia de seguridad avanzada de DynamoDB la Guía para desarrolladores de Amazon DynamoDB y su uso con AWS Backup DynamoDB.	23 de noviembre de 2021
Support para mejorar la asignación de AWS Backup recursos en las regiones de AWS China	AWS Backup La mejora de la asignación de recursos ahora está disponible en la región de China (Beijing) y en la región de China (Ningxia) . Para obtener más información, consulte Asignación de recursos a un plan de copia de seguridad .	16 de noviembre de 2021

Cambio	Descripción	Fecha
Lanzamiento de la mejora de la asignación AWS Backup de recursos	La mejora de la asignación de recursos de backup le proporciona controles adicionales y detallados y nuevos procesos simplificados para implementar planes de respaldo que protegen cientos de miles de recursos. AWS Utilice esta característica para aumentar la velocidad, la flexibilidad y la precisión a la hora de proteger los datos que AWS Backup utiliza. Para obtener más información, consulte Asignación de recursos a un plan de copia de seguridad .	10 de noviembre de 2021
Compatibilidad con Amazon Neptune	Ahora puede utilizarla AWS Backup para hacer copias de seguridad de los clústeres de Amazon Neptune. Para obtener más información, consulte ¿Qué es AWS Backup?	5 de noviembre de 2021
Compatibilidad con Amazon DocumentDB	Ahora puede utilizarlo AWS Backup para hacer copias de seguridad de los clústeres de Amazon DocumentDB. Para obtener más información, consulte ¿Qué es AWS Backup?	5 de noviembre de 2021

Cambio	Descripción	Fecha
Support para AWS Backup Vault Lock en las regiones de AWS China	AWS Backup Vault Lock ya está disponible en las regiones China (Pekín) y China (Ningxia). Para obtener más información, consulte Bloqueo de almacenes de AWS Backup .	3 de noviembre de 2021
Lanzamiento de AWS Backup Vault Lock	Con AWS Backup Vault Lock, puede evitar que se eliminen las copias de seguridad almacenadas en una bóveda AWS Backup de copias de seguridad. Para obtener más información, consulte Bloqueo de almacenes de AWS Backup .	7 de octubre de 2021
Lanzamiento de los informes de conformidad de AWS Backup Audit Manager	Con los informes de conformidad, puede generar informes diarios sobre la conformidad de su actividad y sus recursos de backup con respecto a los controles que definió en sus marcos de trabajo de AWS Backup Audit Manager. Para obtener más información, consulte Plantillas de informes de conformidad .	5 de octubre de 2021

Cambio	Descripción	Fecha
CloudFormation soporte para AWS Backup Audit Manager	Con CloudFormation, ahora puede implementar marcos, controles y planes de informes de AWS Backup Audit Manager de manera segura y repetible a escala. Para obtener más información, consulte Auditoría e informes de Backup con AWS Backup Audit Manager .	4 de octubre de 2021
Lanzamiento de AWS Backup Audit Manager	Con AWS Backup Audit Manager, ahora puede definir los controles para la actividad y los recursos de backup e identificar las actividades y los recursos que no cumplen con sus controles. También puede usar AWS Backup Audit Manager para generar informes diarios y bajo demanda que sirvan como evidencia del cumplimiento de los controles definidos a lo largo del tiempo. Para obtener más información, consulte Auditoría e informes de Backup con AWS Backup Audit Manager .	24 de agosto de 2021

Cambio	Descripción	Fecha
Compatibilidad con nuevas operaciones asíncronas de puntos de recuperación	AWS Backup ahora asume una función vinculada al servicio para administrar las reglas del ciclo de vida de las copias de seguridad en caso de que modifique o elimine su función de IAM original. Para obtener más información, consulte Eliminación de copias de seguridad .	23 de agosto de 2021
Compatibilidad con copias de seguridad de varios volúmenes y coherentes ante bloqueos de Amazon EBS	Ahora, cuando lo utiliza AWS Backup para proteger sus EC2 instancias de Amazon, AWS Backup realiza copias de seguridad de varios volúmenes y coherentes con los bloqueos de todos los volúmenes de Amazon EBS adjuntos a cada instancia de Amazon de forma predeterminada. EC2 Para obtener más información, consulte Creación de copias de seguridad de varios volúmenes y coherentes ante bloqueos de Amazon EBS .	14 de junio de 2021

Cambio	Descripción	Fecha
Support for Amazon FSx en forma adicional Regiones de AWS	Ahora puede utilizarlos AWS Backup para proteger sus sistemas de FSx archivos de Amazon en las siguientes regiones: AWS GovCloud (US) región de Europa (Milán), región de África (Ciudad del Cabo) y región de Oriente Medio (Baréin). Para obtener más información, consulte Puntos de conexión y cuotas de AWS Backup en la Referencia general de AWS .	15 de abril de 2021

Cambio	Descripción	Fecha
Support para copias de FSx seguridad entre regiones y cuentas de Amazon	Ahora puedes usarlo AWS Backup para copiar FSx copias de seguridad de Amazon entre cuentas Regiones de AWS y cuentas. Para obtener más información, consulte Creación de una copia de la copia de seguridad. Si utiliza políticas administradas por el cliente, debe agregar el nuevo permiso <code>fsx:CopyBackup</code> para evitar que se produzcan errores en los trabajos de copia de seguridad existentes. Para obtener ese permiso, consulta la última declaración de la política de FSx copias de seguridad de Amazon en las políticas gestionadas por el cliente.	12 de abril de 2021
Compatibilidad con etiquetas de asignación de costos para copias de seguridad de Amazon EFS	Ahora puede utilizar etiquetas de asignación de costes para realizar un seguimiento detallado de los costes de sus copias de seguridad de Amazon EFS, así como ver y filtrar esas etiquetas mediante ellas AWS Cost Explorer. Para obtener más información, consulte Uso de etiquetas de asignación de costes .	7 de abril de 2021

Cambio	Descripción	Fecha
Autorización FedRAMP High	AWS Backup ahora está autorizado para soportar cargas de trabajo de FedRAMP High. Para obtener más información, consulte Servicios de AWS en el ámbito del programa de conformidad .	25 de marzo de 2021
¿Nuevo Región de AWS	AWS Backup ya está disponible en la región de Asia Pacífico (Osaka). En esta región, AWS Backup actualmente no admite Storage Gateway FSx, Amazon ni la copia de seguridad multicuenta en esta región. Para obtener más información, consulte Puntos de conexión y cuotas de AWS Backup en la Referencia general de AWS .	25 de marzo de 2021
Compatibilidad con operaciones por lotes en puntos de recuperación	Ahora puede usar la AWS Backup consola para automatizar las operaciones por lotes y limpiar los puntos de recuperación de sus almacenes de respaldo. Para obtener más información, consulte Eliminación de copias de seguridad .	23 de marzo de 2021

Cambio	Descripción	Fecha
Compatibilidad con restauraciones a la clase de almacenamiento Amazon EFS One Zone	Ahora puede restaurar sus copias de seguridad de Amazon EFS en la clase de almacenamiento Amazon EFS One Zone. Para obtener más información, consulte Restauración de un sistema de archivos de Amazon EFS .	12 de marzo de 2021
Support para la restauración y el backup continuo de Amazon Relational Database point-in-time Service	Ahora puede utilizarlos AWS Backup para automatizar las copias de seguridad continuas y realizar point-in-time restauraciones (PITR) de Amazon RDS, además de organizar las copias de seguridad de las instantáneas. Para obtener más información, consulte Restaurar a un tiempo específico mediante la recuperación. point-in-time	10 de marzo de 2021
Support para Amazon CloudWatch	Ahora puedes usarlo CloudWatch para monitorear AWS Backup las métricas. Para obtener más información, consulta Monitorización de eventos y métricas con Amazon CloudWatch y Amazon EventBridge .	3 de febrero de 2021

Cambio	Descripción	Fecha
Support para Amazon EventBridge	Ahora puede usarlo EventBridge para monitorear AWS Backup eventos. Para obtener más información, consulta Monitorización de eventos y métricas con Amazon CloudWatch y Amazon EventBridge .	3 de febrero de 2021
Compatibilidad con copias de seguridad entre cuentas	Ahora puede utilizarlos AWS Backup para hacer copias de seguridad de sus recursos en varios Cuentas de AWS. Para obtener más información, consulta Cómo crear copias de seguridad en todas AWS las cuentas .	18 de noviembre de 2020
Support para realizar copias de seguridad y restaurar los sistemas de FSx archivos de Amazon	Ahora puedes usarlo AWS Backup para hacer copias de seguridad de los sistemas de FSx archivos de Amazon. Para obtener más información, consulte Trabajar con los sistemas de FSx archivos de Amazon .	9 de noviembre de 2020
¿Nuevo Regiones de AWS	AWS Backup ya está disponible en África (Ciudad del Cabo) y Europa (Milán) Regiones de AWS. Para obtener más información, consulte Puntos de conexión y cuotas de AWS Backup en la Referencia general de AWS .	21 de octubre de 2020

Cambio	Descripción	Fecha
Compatibilidad con copias de seguridad de Windows habilitadas para VSS	Ahora puede realizar copias de seguridad y restaurar aplicaciones Windows habilitadas para VSS (Volume Shadow Copy Service) que se ejecuten en instancias de Amazon EC2 . Para obtener más información, consulte Creación de copias de seguridad de Windows VSS .	22 de septiembre de 2020
Compatibilidad con copias de seguridad automáticas de Amazon EFS	Ahora puede utilizarla AWS Backup para realizar copias de seguridad automáticas de los sistemas de archivos de Amazon EFS. Para obtener más información, consulte Primeros pasos 4: creación de copias de seguridad automáticas de Amazon EFS .	16 de julio de 2020
¿Nuevo Región de AWS	AWS Backup ya está disponible en AWS GovCloud (US) Region. Para obtener más información, consulte Puntos de conexión y cuotas de AWS Backup en la Referencia general de AWS .	24 de junio de 2020

Cambio	Descripción	Fecha
Support para administrar copias de seguridad en múltiples Cuentas de AWS	Ahora puede administrar las copias de seguridad en varias Cuentas de AWS mediante AWS Organizations . Para obtener más información, consulte Cómo funciona la administración entre cuentas .	24 de junio de 2020
Support para Amazon Aurora se agregó a AWS Backup	Ahora puede configurarlo AWS Backup para hacer copias de seguridad de los recursos de Amazon Aurora. Para obtener información, consulte Información general de copias de seguridad y restauración de un clúster de base de datos Aurora en la Guía del usuario de Amazon Aurora.	10 de junio de 2020
Support para configurar los servicios con los que trabajar AWS Backup	Ahora puede configurarlo AWS Backup para hacer copias de seguridad de los recursos de AWS servicios específicos. Para obtener más información, consulte Aceptar la administración de servicios con AWS Backup .	20 de mayo de 2020

Cambio	Descripción	Fecha
Soporte para realizar copias de seguridad de EC2 instancias de Amazon y también añade soporte para copias de seguridad entre regiones	Ahora puedes hacer copias de seguridad de EC2 instancias completas de Amazon y también copiar recursos entre ellas Regiones de AWS. Para obtener más información, consulte Creación de copias de las copias de seguridad entre Regiones de AWS .	13 de enero de 2020
Nueva guía	AWS lanzamientos AWS Backup y la guía para AWS Backup desarrolladores.	15 de enero de 2019

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.