



Guía del usuario de

AWS Health



AWS Health: Guía del usuario de

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 Health?	1
Conceptos para AWS Health	2
AWS Health evento	2
Evento específico de cuenta	3
Evento público	3
AWS Health Panel de control	3
AWS Health Panel de control: estado del servicio	4
Código de tipo de evento	4
Categorías de tipos de eventos	4
Estado del evento	6
Capacidad de acción	6
Personas	7
Entidades afectadas	7
AWS Health eventos en Amazon EventBridge	8
AWS Health API	8
Vista organizativa	8
AWS User Notifications	9
Introducción	10
Configuración	10
Inscríbase en una Cuenta de AWS	11
Creación de un usuario con acceso administrativo	11
Vea los eventos de la cuenta en AWS Health el panel de control	12
Problemas abiertos y recientes	13
Cambios programados	14
Otras notificaciones	15
Registro de eventos	15
Detalles del evento	16
Tipos de eventos	18
Vista del calendario	18
Vista de los recursos afectados	19
Configuración de la zona horaria	21
El estado de su organización	21
Alertas de AWS Health eventos	22
Configuración de Amazon EventBridge	22

Administra las notificaciones en AWS User Notifications	23
Configure su suscripción a notificaciones AWS gestionadas para eventos AWS Health	24
AWS Preguntas frecuentes sobre las notificaciones gestionadas	24
AWS Health Tablero	27
Eventos del ciclo de vida planificados para AWS Health	30
¿Qué son los eventos del ciclo de vida planificado?	30
¿Qué debo esperar cuando recibo una notificación de un evento de ciclo de vida planificado?	31
Modelo de responsabilidad compartida para resiliencia	34
Acceder a los eventos planificados del ciclo de vida	34
Integración con otros sistemas mediante la AWS Health API	36
Firmar solicitudes AWS Health de API	37
Elegir puntos de enlace para las solicitudes de AWS Health API	37
Demostraciones: recuperación de los últimos siete días de datos de eventos mediante programación	39
Demostración: recuperación de los últimos siete días de datos de eventos de AWS Health mediante Java	39
Demostración: recuperación de los últimos siete días de datos de eventos de AWS Health mediante Python	43
Tutorial: Uso de la AWS Health API con ejemplos de Java	45
Paso 1: Inicializar las credenciales	46
Paso 2: inicializar un AWS Health cliente de API	46
Paso 3: Usa las operaciones de AWS Health la API para obtener información sobre los eventos	46
Seguridad	50
Protección de datos	51
Cifrado de datos	52
Identity and Access Management	52
Público	53
Autenticación con identidades	53
Administración del acceso con políticas	54
¿Cómo AWS Health funciona con IAM	57
Ejemplos de políticas basadas en identidades	62
Resolución de problemas	75
Cómo utilizar roles vinculados a servicios	79
AWS políticas gestionadas para AWS Health	80

Inicio de sesión y supervisión AWS Health	86
Validación de conformidad	87
Resiliencia	87
Seguridad de la infraestructura	88
Configuración y análisis de vulnerabilidades	88
Prácticas recomendadas de seguridad	88
Otorgue AWS Health a los usuarios los permisos mínimos posibles	88
Vea el AWS Health Dashboard	89
Intégrelo AWS Health con Amazon Chime o Slack	89
Supervise los AWS Health eventos	89
Aregar eventos AWS Health	90
Requisitos previos	90
Habilitación de la vista organizativa	91
Visualización de una vista organizativa	95
Deshabilitación de la vista organizativa	100
Administración de vistas de administrador delegado para una organización	101
Registro de un administrador delegado	102
Eliminación de una cuenta de administrador delegado	102
Monitorización de eventos de Salud con EventBridge	104
Crear EventBridge reglas de Región de AWS cobertura	105
Configuración de alta disponibilidad (opcional)	106
Integración simplificada	106
Eventos globales	106
Monitoreo de eventos públicos y específicos de cuenta para AWS Health	106
Reglas de Backup para AWS Health eventos	108
Visualización de listas paginadas de eventos en AWS Health EventBridge	108
Aregar AWS Health eventos mediante la vista organizativa y el acceso de administrador delegado	109
Integrar la supervisión y las notificaciones de AWS Health eventos con JIRA y ServiceNow	109
Configurar una EventBridge regla para enviar notificaciones sobre eventos	110
Cómo crear una regla para varios servicios y categorías	114
Configuración de Amazon Q Developer en aplicaciones de chat para enviar notificaciones sobre eventos	116
Requisitos previos	116
Ejecutar operaciones en EC2 las instancias automáticamente en respuesta a eventos	118
Requisitos previos	119

Crea una regla para EventBridge	123
Referencia: Amazon EventBridge esquema de AWS Health eventos	126
AWS Health esquema de eventos	126
Public Health Event: problema EC2 operativo de Amazon	141
AWS Health Evento específico de la cuenta: problema con la API de Elastic Load	
Balancing	142
AWS Health Evento específico de la cuenta: disminución del rendimiento de Amazon EC2	
Instance Store Drive	143
Supervisión AWS Health	145
Registrar las llamadas a la AWS Health API con AWS CloudTrail	145
AWS Health información en CloudTrail	146
Ejemplo: entradas de archivos de AWS Health registro	147
Historial de revisión	149
Actualizaciones anteriores	160
	clxi

¿Qué es AWS Health?

AWS Health proporciona una visibilidad continua del rendimiento de sus recursos y de la disponibilidad de sus Servicios de AWS cuentas. Puede utilizar AWS Health los eventos para saber cómo los cambios en los servicios y los recursos pueden afectar a las aplicaciones en las que se estén ejecutando AWS. AWS Health proporciona información relevante y oportuna para ayudarle a gestionar los eventos en curso. AWS Health también le ayuda a conocer las actividades planificadas y a prepararse para ellas. El servicio proporciona alertas y notificaciones que se activan cuando se produce un cambio en el estado de AWS los recursos, de forma que puede obtener una visibilidad casi instantánea de los eventos y una orientación que le ayudará a acelerar la resolución de problemas.

Todos los clientes pueden usar el [AWS Health Panel de Control AWS](#), que funciona con la AWS Health API. El panel no requiere configuración y está listo para que lo usen [AWS los usuarios autenticados](#). Para ver más aspectos destacados del servicio, consulta la [AWS Health página de detalles del de control](#).

AWS Health proporciona una consola, denominada AWS Health panel de control, para todos los clientes. No es necesario escribir código ni realizar ninguna operación para instalar el panel.

Para conocer los conceptos básicos AWS Health y los términos que encontrará al utilizar el servicio, para comprender los conceptos básicos del servicio, AWS Health consulte [Conceptos para AWS Health](#).

Notas

- El AWS Health panel de control está disponible para todos AWS los clientes sin coste adicional.
- Todos AWS los clientes pueden recibir AWS Health eventos a través de Amazon EventBridge sin coste adicional.
- Si tiene un plan Business, Enterprise On-Ramp o Enterprise Support, puede usar la AWS Health API para integrarse con sistemas internos y de terceros. Para obtener más información, consulte la [Referencia de la API de AWS Health](#).
- Para obtener más información sobre AWS Support los planes disponibles, consulte [AWS Support](#).

Conceptos para AWS Health

Conozca AWS Health los conceptos y comprenda cómo puede utilizar el servicio para mantener el buen estado de sus aplicaciones, servicios y recursos en su entorno Cuenta de AWS.

Temas

- [AWS Health evento](#)
- [AWS Health Panel de control](#)
- [Código de tipo de evento](#)
- [Categorías de tipos de eventos](#)
- [Estado del evento](#)
- [Capacidad de acción](#)
- [Personas](#)
- [Entidades afectadas](#)
- [AWS Health eventos en Amazon EventBridge](#)
- [AWS Health API](#)
- [Vista organizativa](#)
- [AWS User Notifications](#)

AWS Health evento

AWS Health Los eventos, también conocidos como eventos de Salud, son notificaciones que se AWS Health envían en nombre de otros AWS servicios. Puede usar estos eventos para obtener información sobre los cambios futuros o programados que podrían afectar su cuenta. Por ejemplo, AWS Health puede enviar un evento si AWS Identity and Access Management (IAM) planea dejar de usar una política administrada o AWS Config planea dejar de usar una regla administrada. AWS Health también envía eventos cuando hay problemas de disponibilidad del servicio en un. Región de AWS Puede revisar la descripción del evento para comprender el problema, identificar los recursos afectados y adoptar las medidas recomendadas.

Existen dos tipos de eventos de estado:

Contenido

- [Evento específico de cuenta](#)
- [Evento público](#)

Evento específico de cuenta

Los eventos específicos de la cuenta son locales para su cuenta Cuenta de AWS o para una cuenta de su AWS organización. Por ejemplo, si hay un problema con un tipo de instancia de Amazon Elastic Compute Cloud (Amazon EC2) en una región que utilices, AWS Health proporciona información sobre el evento y el nombre de los recursos afectados.

Puedes encontrar eventos específicos de la cuenta en tu [AWS Health panel de control](#), la [AWS Health API](#) o usar [Amazon EventBridge](#) o [AWS User Notifications para recibir notificaciones](#).

Evento público

Los eventos públicos son eventos de servicio notificados que no son específicos de una cuenta. Por ejemplo, si hay un problema con el servicio de Amazon Simple Storage Service (Amazon S3) en la región Este de EE. UU. (Ohio), AWS Health proporciona información sobre el evento, incluso si no utiliza ese servicio o no tiene buckets S3 en esa región. Le recomendamos que revise las notificaciones públicas antes de tomar medidas al respecto.

Puedes encontrar los eventos públicos en tu AWS Health panel de control y en el AWS Health panel de control: estado del servicio.

Si tiene una cuenta, consulte [Introducción al Panel de AWS Health](#).

Si no tiene una cuenta, consulte [AWS Health Tablero](#).

AWS Health Panel de control

Si tienes una Cuenta de AWS, tu AWS Health panel de control muestra tanto los eventos públicos como los eventos específicos de la cuenta.

Te recomendamos que utilices tu AWS Health panel de control para obtener información sobre los eventos que generen notoriedad, como un próximo problema de mantenimiento de un servicio en una región. También puedes usar el AWS Health panel de control para obtener información sobre los eventos que podrían afectarte directamente, como un recurso obsoleto en tu cuenta.

Puedes iniciar sesión en la Consola de administración de AWS para ver tu AWS Health panel de control desde <https://health.aws.com/health/casa>.

Para obtener más información, consulte [Introducción al Panel de AWS Health](#).

AWS Health Panel de control: estado del servicio

Si no tienes una cuenta, puedes usar el AWS Health panel de control: estado del servicio en <https://health.aws.com/health/estado> para ver los eventos públicos. Los eventos públicos son problemas de servicio notificados para AWS que proporcionan información sobre la disponibilidad del servicio. Este sitio web solo muestra eventos públicos, que no son específicos de cualquier cuenta. No necesita iniciar sesión o tener una cuenta para ver esta página.

Para obtener más información, consulte [AWS Health Tablero](#).

Código de tipo de evento

Los códigos de tipo de evento que se muestran en un evento de estado incluyen el servicio afectado y el tipo de evento. Por ejemplo, si recibe un evento de estado que tiene el código de tipo de evento de AWS_EC2_SYSTEM_MAINTENANCE_EVENT, significa que el servicio está programando un evento de mantenimiento que podría afectarle. Use esta información para planificar con antelación o tomar medidas para su cuenta.

Categorías de tipos de eventos

Todos los eventos de estado tienen una categoría de tipo de evento asociada. En el caso de algunos eventos, la categoría del tipo de evento puede aparecer en el código del tipo de evento, como el código AWS_RDS_MAINTENANCE_SCHEDULED. En este ejemplo, la categoría está programada. Puede utilizar esta información para comprender las categorías de eventos a un alto nivel.

Se recomienda supervisar todas las categorías de tipos de eventos. Tenga en cuenta que cada categoría aparece para diferentes tipos de eventos. También puedes usar la operación de la [DescribeEventTypes](#) API para buscar la categoría del tipo de evento.

Notificación de cuenta

Estos eventos proporcionan información sobre la administración o la seguridad de sus cuentas y servicios. Estos eventos pueden ser informativos o requerir que tome medidas urgentes.

Le recomendamos que preste atención a este tipo de eventos y revise todas las acciones recomendadas.

A continuación, se muestran ejemplos de códigos de tipo de evento para las notificaciones de cuentas:

- AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION: tiene un bucket de Amazon S3 que podría permitir el acceso público.
- AWS_BILLING_SUSPENSION_NOTICE: su cuenta tiene cargos pendientes y ha sido suspendida o la ha desactivado.
- AWS_WORKSPACES_OPERATIONAL_NOTIFICATION— Hay un problema con el servicio de Amazon WorkSpaces.

Problema

Estos eventos son eventos inesperados que afectan a AWS los servicios o recursos. Entre los eventos habituales de esta categoría se incluyen las comunicaciones sobre problemas operativos que están provocando la degradación del servicio o problemas localizados a nivel de recursos, para su información.

A continuación se presentan casos problemáticos de tipos de evento de ejemplo:

- AWS_EC2_OPERATIONAL_ISSUE: un problema operativo de un servicio, como retrasos en el uso de un servicio.
- AWS_EC2_API_ISSUE: un problema operativo de la API de un servicio, como el aumento de la latencia de una operación de API.
- AWS_EBS_VOLUME_ATTACHMENT_ISSUE: un problema a nivel de recurso localizado que podría afectar a sus recursos de Amazon Elastic Block Store (Amazon EBS).
- AWS_ABUSE_PII_CONTENT_REMOVAL_REPORT: este evento significa que su cuenta podría suspenderse si no toma ninguna medida.

Cambio programado

Estos eventos proporcionan información sobre los próximos cambios en sus servicios y recursos. Estos eventos incluyen eventos del ciclo de vida planificados, como end-of-support notificaciones y actualizaciones automáticas para diferentes versiones. Algunos eventos pueden recomendarle que tome medidas para evitar interrupciones en el servicio, mientras que otros se producirán automáticamente, sin que usted tome alguna medida. Es posible que un recurso no esté disponible temporalmente durante la actividad de cambio programada. Todos los eventos de esta categoría son eventos específicos de la cuenta.

A continuación, se muestran ejemplos de códigos de tipo de evento para los cambios programados:

- AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED— Una EC2 instancia de Amazon requiere un reinicio.
- AWS_SAGEMAKER_SCHEDULED_MAINTENANCE— La SageMaker IA requiere un evento de mantenimiento, como solucionar un problema de servicio.
- AWS_RDS_PLANNED_LIFECYCLE_EVENT— Amazon RDS está programando un evento del ciclo de vida planificado, como un end-of-support evento para una de sus versiones, que requiere la acción del cliente.

 Tip

Si utiliza la AWS Health API o AWS Command Line Interface (AWS CLI) para devolver los detalles del evento, el Event objeto contiene el eventScopeCode campo con el ACCOUNT_SPECIFIC valor. Para obtener más información, consulte la [Referencia de la API de AWS Health](#).

Estado del evento

El estado del evento le indica si el evento de estado está abierto, cerrado o próximo. Puedes ver los eventos de Health en el AWS Health panel de control o en la AWS Health API durante un máximo de 90 días.

Capacidad de acción

La capacidad de acción es un campo que le ayuda a priorizar los eventos de Salud en función de si se requiere una acción por su parte. Los eventos de salud incluyen un estado de capacidad de acción que indica si es necesario tomar medidas para mitigar los riesgos para sus AWS recursos o si el evento es de naturaleza informativa.

El campo de accionabilidad puede contener uno de los siguientes valores:

- ACTION_REQUIRED: Los eventos con este estado requieren que tomes medidas para mitigar el posible impacto relacionado con la disponibilidad, la facturación o la seguridad de tus AWS recursos.

- ACTION_MAY_BE_REQUIRED: Los eventos con este estado comunican los cambios que requieren una acción, en función de la implementación, las dependencias y los flujos de trabajo específicos. Estos eventos requieren su revisión para determinar si es necesario tomar medidas.
- INFORMATIONAL: Los eventos con este estado proporcionan una visibilidad continua de la información operativa sobre los AWS servicios que utiliza. No se espera ninguna acción inmediata.

 Note

Los eventos de salud relacionados con problemas de servicio no incluyen una etiqueta de capacidad de acción, ya que la necesidad de acciones de recuperación depende de la arquitectura de la aplicación específica.

Personas

El campo personas proporciona una lista de contactos que le ayuda a enviar la información relevante a los equipos correspondientes de su organización. Cada evento de Health puede incluir una o más de las siguientes personas:

- OPERATIONS: Para eventos relacionados con las actividades operativas y la disponibilidad de los servicios.
- SECURITY: Para eventos relacionados con consideraciones de seguridad.
- BILLING: Para eventos con posibles implicaciones financieras.

Por ejemplo, cuando se AWS envía un evento sobre la finalización del soporte estándar y se convierte en soporte extendido, el evento también se incluye BILLING OPERATIONS en la lista de personas para garantizar que la información llegue a los equipos responsables de la gestión de costes.

Entidades afectadas

Las entidades afectadas son AWS recursos que podrían verse afectados por el evento. Por ejemplo, si recibes un evento programado para el EC2 mantenimiento de Amazon para un tipo de instancia específico que estás usando en tu cuenta, puedes usar el evento Health para determinar el ID de las instancias afectadas. Utilice esta información para solucionar cualquier posible problema de servicio, como la creación o la desactivación de recursos.

AWS Health eventos en Amazon EventBridge

Puedes configurar EventBridge las reglas de Amazon para tus cuentas a fin de automatizar las acciones después de que una cuenta reciba el AWS Health evento correspondiente. Pueden ser acciones generales, como enviar todos los mensajes sobre los eventos de ciclo de vida planificados a una interfaz de chat. O bien, pueden ser acciones específicas, como activar un flujo de trabajo en una herramienta de administración de servicios de TI.

Para obtener más información, consulte [Monitorización de eventos AWS Health con Amazon EventBridge](#).

AWS Health API

Puede usar la AWS Health API para acceder mediante programación a la información que aparece en el [AWS Health panel de control](#), como la siguiente:

- Obtenga información sobre los eventos que podrían afectar a sus AWS servicios y recursos
- Habilite o deshabilite la función de vista organizacional de su AWS organización
- Filtrado de eventos por servicios específicos, categorías de tipos de eventos y códigos de tipos de eventos

Para obtener más información, consulte la [Referencia de la API de AWS Health](#).

 Note

Para usar la AWS Health API, debe tener un plan Business, Enterprise On-Ramp o Enterprise Support. [AWS Support](#) Si llamas a la AWS Health API desde una cuenta que no tiene un plan Business, Enterprise On-Ramp o Enterprise Support, recibirás un `SubscriptionRequiredException` error.

Vista organizativa

Puedes usar esta función para agregar todos los eventos de salud de tus AWS cuentas en una sola vista AWS Organizations en el AWS Health panel de control. A continuación, puede iniciar sesión en la cuenta de administración de su organización o utilizar la AWS Health API para ver todos los eventos que puedan afectar a las distintas cuentas y recursos. Puede habilitar esta función desde la

AWS Health consola o la API. Para obtener más información, consulte [Aregar AWS Health eventos en todas las cuentas](#).

AWS User Notifications

AWS Health se integra [AWS User Notifications](#) para que pueda recibir y controlar fácilmente las notificaciones sobre los eventos que afectan a sus servicios Cuentas de AWS y a los suyos. Notificaciones de usuario ofrece notificaciones gestionadas para AWS Health eventos de forma predeterminada. Puede configurar estas suscripciones para controlar la frecuencia con la que recibe mensajes mediante la agregación basada en el tiempo, los tipos de AWS Health eventos sobre los que recibe notificaciones y dónde se envían las notificaciones. Para empezar, abre Notificaciones de usuario en. [Consola de administración de AWS](#) Para obtener más información, consulte [Administra AWS Health las notificaciones en AWS User Notifications](#)

Introducción al Panel de AWS Health

Puedes usar tu AWS Health panel de control para obtener información sobre AWS Health los eventos. Estos eventos pueden afectar a su Servicios de AWS o Cuenta de AWS. Después de iniciar sesión en tu cuenta, el AWS Health panel de control muestra la información de las siguientes maneras:

- [Los eventos de su cuenta](#): en esta página se muestran los eventos específicos de su cuenta. Puede ver los cambios abiertos, recientes y programados. También puede ver las notificaciones y un registro de eventos que muestra todos los eventos de los últimos 90 días.
- [Los eventos de su organización](#): en esta página se muestran los eventos específicos de su organización AWS Organizations. Puede ver los cambios abiertos, recientes y programados de su organización. También puede ver las notificaciones, así como un registro de eventos que muestra todos los eventos de la organización de los últimos 90 días.

Note

Si no tienes una Cuenta de AWS, puedes utilizarla [AWS Health Tablero](#) para obtener información sobre la disponibilidad general de los servicios.

Si tienes una cuenta, te recomendamos que inicies sesión en tu AWS Health panel de control para obtener información más detallada sobre los eventos y los próximos cambios que podrían afectar a tus servicios y recursos.

Temas

- [Configurar tu AWS cuenta](#)
- [Ver los eventos de su cuenta en el panel de control de AWS Health](#)
- [Configuración de Amazon EventBridge](#)
- [Administra AWS Health las notificaciones en AWS User Notifications](#)

Configurar tu AWS cuenta

Antes de poder AWS Health activarla, debe tener una Cuenta de AWS. Si no tiene una AWS cuenta, complete los siguientes pasos para crear una.

Inscríbase en una Cuenta de AWS

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

Para suscribirte a una Cuenta de AWS

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

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

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

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

Creación de un usuario con acceso administrativo

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

Proteja su Usuario raíz de la cuenta de AWS

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

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

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

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

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

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

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

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

Inicio de sesión como usuario con acceso de administrador

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

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

Concesión de acceso a usuarios adicionales

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

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

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

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

Ver los eventos de su cuenta en el panel de control de AWS Health

Puede iniciar sesión en su cuenta para recibir eventos y recomendaciones personalizados.

Para ver los eventos de la cuenta en tu AWS Health panel

1. Abre tu AWS Health panel de control en <https://health.aws.com/health/casa>.
2. En el panel de navegación, en Estado de su cuenta, puede elegir las siguientes opciones:
 - a. Problemas abiertos y recientes: consulte los eventos abiertos y cerrados recientemente.
 - b. Cambios programados: consulte los próximos eventos que podrían afectar a sus servicios y recursos.
 - c. Otras notificaciones: consulte todas las demás notificaciones y eventos en curso de los últimos siete días que puedan afectar su cuenta.
 - d. Registro de eventos: vea todos los eventos de los últimos 90 días.

Problemas abiertos y recientes

Use la pestaña Problemas pendientes y recientes para ver todos los eventos en curso de los últimos siete días que puedan afectar su cuenta.

Cuando elige un evento del panel, aparece el panel Detalles con información sobre el evento y una lista de los recursos afectados. Para obtener más información, consulte [Detalles del evento](#).

Puede filtrar los eventos que aparecen en cualquier pestaña utilizando las opciones de la lista de filtros. Por ejemplo, puedes restringir los resultados por zona de disponibilidad, región, hora de finalización del evento o hora de la última actualización Servicio de AWS, etc.

Para ver todos los eventos, en lugar de los recientes que aparecen en el panel de control, seleccione la pestaña [Registro de eventos](#).

 Note

Actualmente, no puede eliminar notificaciones de eventos que aparecen en su panel de control de AWS Health . Una vez que se Servicio de AWS resuelve un evento, la notificación se elimina de la vista del panel.

Example : Evento sobre problemas operativos para Amazon Elastic Compute Cloud (Amazon EC2)

La siguiente imagen muestra un evento relacionado con errores de lanzamiento y problemas de conectividad en las EC2 instancias de Amazon.

Your account health

Stay informed of important events affecting your AWS resources.

Configure EventBridge

Get notifications for events that might affect your services and resources.

[Go to EventBridge](#)

[Open and recent issues \(16\)](#)

Scheduled changes (0)

Notifications (3)

Event log

Open and recent issues (16)

View events that might affect your AWS infrastructure. [35 issues](#) were resolved in the past 24 hours.

Add filter

Service: Elastic Compute Cloud [X](#)

[Clear filter](#)

< 1 >

Event summary

Operational issue - EC2 (Ohio)

Last update: February 20, 2022 at 11:16:34 PM UTC-8
us-east-2

Operational issue - EC2 (Ohio)

Last update: February 17, 2022 at 11:56:09 PM UTC-8
us-east-2

Operational issue - EC2 (N. Virginia)

Last update: February 16, 2022 at 1:36:29 AM UTC-8
us-east-1

Operational issue - EC2 (Ohio)

[Back to list view](#)

[Details](#)

Affected resources

Event data

Service

EC2

Start time

February 20, 2022 at 11:16:24 PM UTC-8

Status

Open

End time

-

Region / Availability Zone

us-east-1

Category

Issue

Account specific

No

Affected resources

1

Description

[04:35 AM PST] We are investigating increased EC2 launch failures and networking connectivity issues for some instances in a single Availability Zone (USE1-AZ4) in the US-EAST-1 Region. Other Availability Zones within the US-EAST-1 Region are not affected by this issue.

Cambios programados

Use la pestaña Cambios programados para ver los próximos eventos que podrían afectar su cuenta. Estos eventos pueden incluir actividades de mantenimiento programadas para los servicios y eventos de ciclo de vida planificados cuya resolución requiera la adopción de medidas. Para ayudarle a planificar estas actividades, se proporciona una vista del calendario para que pueda mapear estos cambios programados en un calendario mensual. Hay filtros disponibles. Para obtener más información sobre los eventos del ciclo de vida planificados, consulte [Eventos del ciclo de vida planificados para AWS Health](#).

Otras notificaciones

Use la pestaña Notificaciones para ver todas las demás notificaciones y eventos en curso de los últimos siete días que puedan afectar su cuenta. Esto puede incluir eventos, como la rotación de certificados, las notificaciones de facturación y las vulnerabilidades de seguridad.

Registro de eventos

Use la pestaña Registro de eventos para ver todos los AWS Health eventos. La tabla de registro incluye columnas adicionales para que pueda filtrar por estado y hora de inicio.

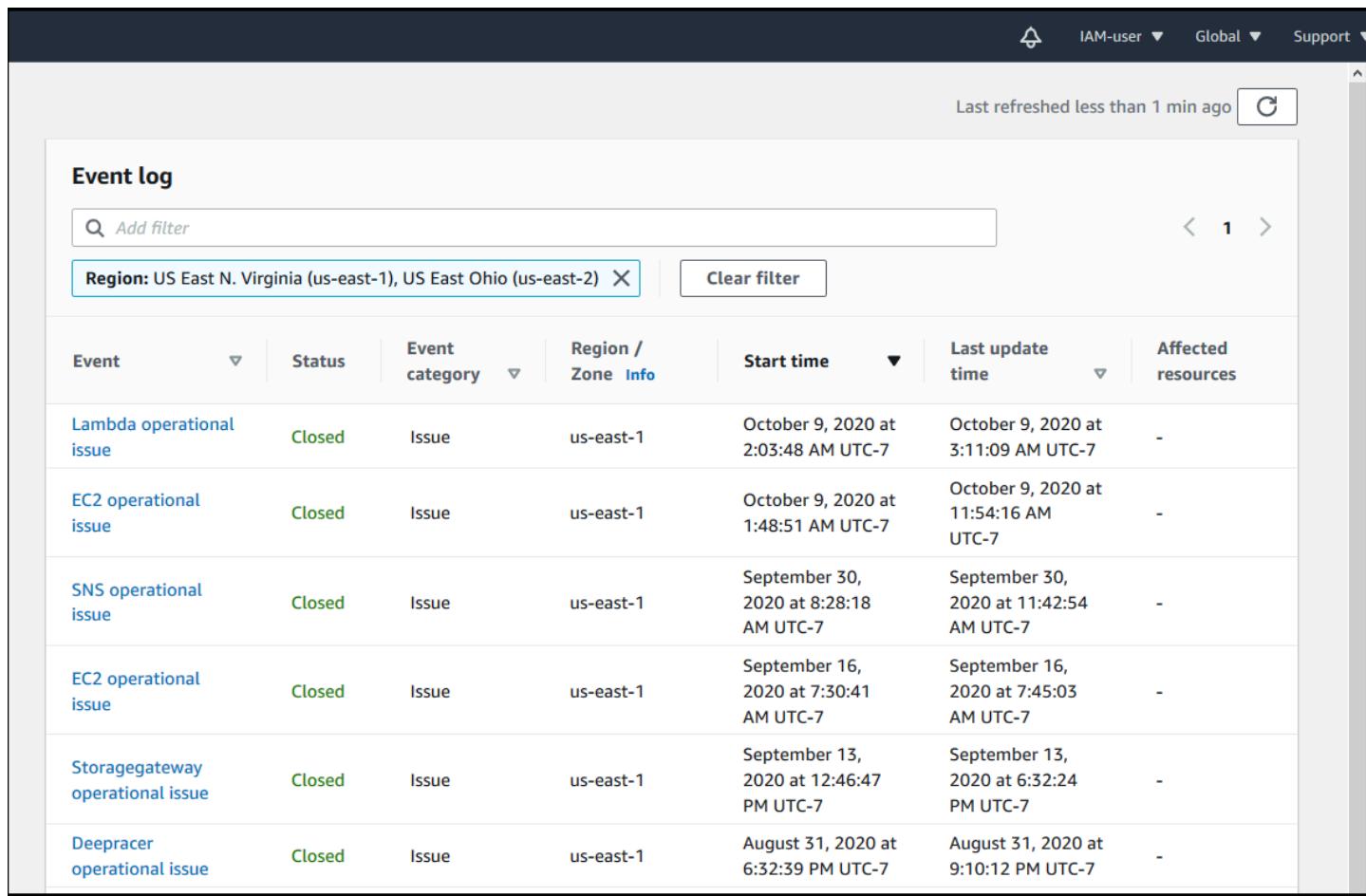
Cuando elige un evento en la tabla de Registro de eventos, aparece el panel Detalles con información sobre el evento y la lista de recursos afectados. Para obtener más información, consulte [Detalles del evento](#).

Puede elegir las siguientes opciones de filtro para afinar sus resultados:

- Zona de disponibilidad
- Hora de finalización
- Event
- ARN del evento
- Categoría de evento
- Hora de la última actualización
- Region
- ID de recurso/ARN
- Servicio
- Hora de inicio
- Status

Example : registro de eventos

La siguiente imagen muestra los eventos recientes de las regiones Este de EE. UU. (Norte de Virginia) y Este de EE. UU. (Ohio).



The screenshot shows the AWS Health Event log interface. At the top, there are navigation links for IAM-user, Global, and Support, along with a refresh button and a message indicating the data was last refreshed less than 1 minute ago. Below this is a search bar with the placeholder 'Add filter' and a 'Clear filter' button. A filter bar shows 'Region: US East N. Virginia (us-east-1), US East Ohio (us-east-2)' with an 'X' button to clear it. To the right of the filter bar are navigation arrows and a page number '1'. The main area is titled 'Event log' and contains a table of operational issues. The columns are: Event, Status, Event category, Region / Zone Info, Start time, Last update time, and Affected resources. The table lists six issues, all of which are 'Closed' and categorized as 'Issue'. All issues occurred in the 'us-east-1' region. The start times range from August 31, 2020, to October 9, 2020. The last update times are the same as the start times. The affected resources are listed as '-' for all issues.

Event	Status	Event category	Region / Zone Info	Start time	Last update time	Affected resources
Lambda operational issue	Closed	Issue	us-east-1	October 9, 2020 at 2:03:48 AM UTC-7	October 9, 2020 at 3:11:09 AM UTC-7	-
EC2 operational issue	Closed	Issue	us-east-1	October 9, 2020 at 1:48:51 AM UTC-7	October 9, 2020 at 11:54:16 AM UTC-7	-
SNS operational issue	Closed	Issue	us-east-1	September 30, 2020 at 8:28:18 AM UTC-7	September 30, 2020 at 11:42:54 AM UTC-7	-
EC2 operational issue	Closed	Issue	us-east-1	September 16, 2020 at 7:30:41 AM UTC-7	September 16, 2020 at 7:45:03 AM UTC-7	-
Storagegateway operational issue	Closed	Issue	us-east-1	September 13, 2020 at 12:46:47 PM UTC-7	September 13, 2020 at 6:32:24 PM UTC-7	-
Deepracer operational issue	Closed	Issue	us-east-1	August 31, 2020 at 6:32:39 PM UTC-7	August 31, 2020 at 9:10:12 PM UTC-7	-

Detalles del evento

Al elegir un evento, aparecen dos pestañas sobre el evento. La pestaña Detalles muestra la siguiente información:

- Servicio
- Status
- Región / Zona de disponibilidad
- Si el evento es específico de la cuenta o no
- Hora de inicio y finalización
- Categoría
- La cantidad de recursos afectados
- Descripción y cronología de las actualizaciones sobre el evento

La pestaña Recursos afectados muestra la siguiente información sobre AWS los recursos afectados por el evento:

- El identificador del recurso (por ejemplo, el identificador de un volumen de Amazon EBS como `vol-a1b2c34f`) o el nombre de recurso de Amazon (ARN), si están disponible o si procede.
- En el caso de los eventos del ciclo de vida planificados, esta lista de recursos afectados también contiene el estado más reciente de los recursos (pendiente, desconocido o resuelto). Por lo general, esta lista se actualiza una vez cada 24 horas, pero puede tardar hasta 72 horas en reflejar el estado actual.

Puede filtrar los elementos que aparecen en los recursos. Puede filtrar sus resultados por identificador del recurso o ARN.

Example : AWS Health evento para AWS Lambda

En la siguiente captura de pantalla se muestra un ejemplo de evento para Lambda.

The screenshot shows the AWS Health interface. On the left, the 'Event log' sidebar lists several operational issues: Lambda operational issue (closed), EC2 operational issue (closed), SNS operational issue (closed), EC2 operational issue (closed), Storagegateway operational issue (closed), Deepracer operational issue (closed), Sagemaker operational issue (closed), and Batch operational issue (closed). The 'Region' filter is set to 'US East N. Virginia (us-east-1), US East Ohio (us-east-2)'. The main content area is titled 'Lambda operational issue' and shows the following details:

Event data	
Event	Start time
Lambda operational issue	October 9, 2020 at 2:03:48 AM UTC-7
Status	End time
Closed	October 9, 2020 at 3:11:08 AM UTC-7
Region / Availability Zone	Affected resources
us-east-1	-
Category	
Issue	
Description	
[RESOLVED] Increased Invoke Error Rate	
[02:03 AM PDT] We have identified an increase in invoke error rates in the US-EAST-1 Region and are working towards resolution.	
[03:11 AM PDT] Between October 8 10:35 PM and October 9 2:25 AM PDT we experienced increased Lambda invoke error rates in the US-EAST-1 Region. The issue has been resolved and the service is operating normally.	

Tipos de eventos

Hay dos tipos de AWS Health eventos:

- Los eventos públicos son eventos de servicio que no son específicos de una cuenta. Por ejemplo, si hay un problema con Amazon EC2 en una Región de AWS, AWS Health proporciona información sobre el evento, incluso si no utilizas los servicios o recursos de esa región.
- Los eventos específicos de cuenta son específicos de su cuenta o de una de su organización. Por ejemplo, si hay un problema con una EC2 instancia de Amazon en una de las Región de AWS que utilizas, AWS Health proporciona información sobre el evento y la lista de EC2 instancias de Amazon afectadas.

Puede utilizar las siguientes opciones para identificar si un evento es público o específico de una cuenta:

- En el AWS Health panel de control, selecciona la pestaña Recursos afectados para un evento. Los eventos con recursos son específicos de su cuenta. Los eventos sin recursos son públicos y no son específicos de su cuenta. Para obtener más información, consulta [Introducción al Panel de AWS Health](#).
- Usa la AWS Health API para devolver el eventScopeCode parámetro. Los eventos pueden tener el valor PUBLIC, ACCOUNT_SPECIFIC o NONE. Para obtener más información, consulta la [DescribeEventDetails](#) operación en la Referencia de la AWS Health API.

Vista del calendario

La vista del calendario está disponible en la pestaña de cambios programados para proyectar AWS Health los eventos en un calendario mensual. Esta vista le permite ver los cambios programados hasta 3 meses en el pasado y un año en el futuro.

AWS Health los eventos se muestran por fecha. Seleccione una fecha para mostrar un panel lateral con más detalles sobre el AWS Health evento. Los eventos próximos y en curso se muestran en negro. Los eventos completados se muestran en gris. Si hay más de dos eventos en una fecha, solo se muestra el número de eventos negros y grises. Seleccione una fecha para mostrar una lista de AWS Health eventos en el panel lateral. Puede seleccionar un evento en el panel lateral para mostrar información sobre el evento. El panel lateral tiene rutas de navegación para acceder a una vista anterior.

Scheduled changes

View upcoming events and ongoing events from the past seven days that might affect your AWS infrastructure, such as scheduled maintenance activities.

Q Add filter

Any event ▾

February 2024

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	
28	2 Upcoming	29	30 2 Upcoming 1 Completed	31	1	2

30 January 2024 ⚙️ X

Scheduled events starting on 30 January 2024 (Showing 3 of 3) [View all on the table view](#)

[EKS planned lifecycle event \(us-west-2\)](#)

Event status: **Upcoming**

[EKS planned lifecycle event \(us-east-1\)](#)

Event status: **Upcoming**

[EKS planned lifecycle event \(eu-west-1\)](#)

Event status: **Completed**

Vista de los recursos afectados

AWS Health los eventos pueden especificar los recursos precisos que se ven afectados. Puede ver los recursos afectados en la pestaña Recursos afectados del evento de AWS Health . Para ver el estado, seleccione el AWS Health evento. El estado se muestra en la pestaña de recursos afectados del panel lateral. En el caso de los eventos del ciclo de vida planificados, AWS Health los eventos proporcionan actualizaciones diarias del estado de los recursos afectados.

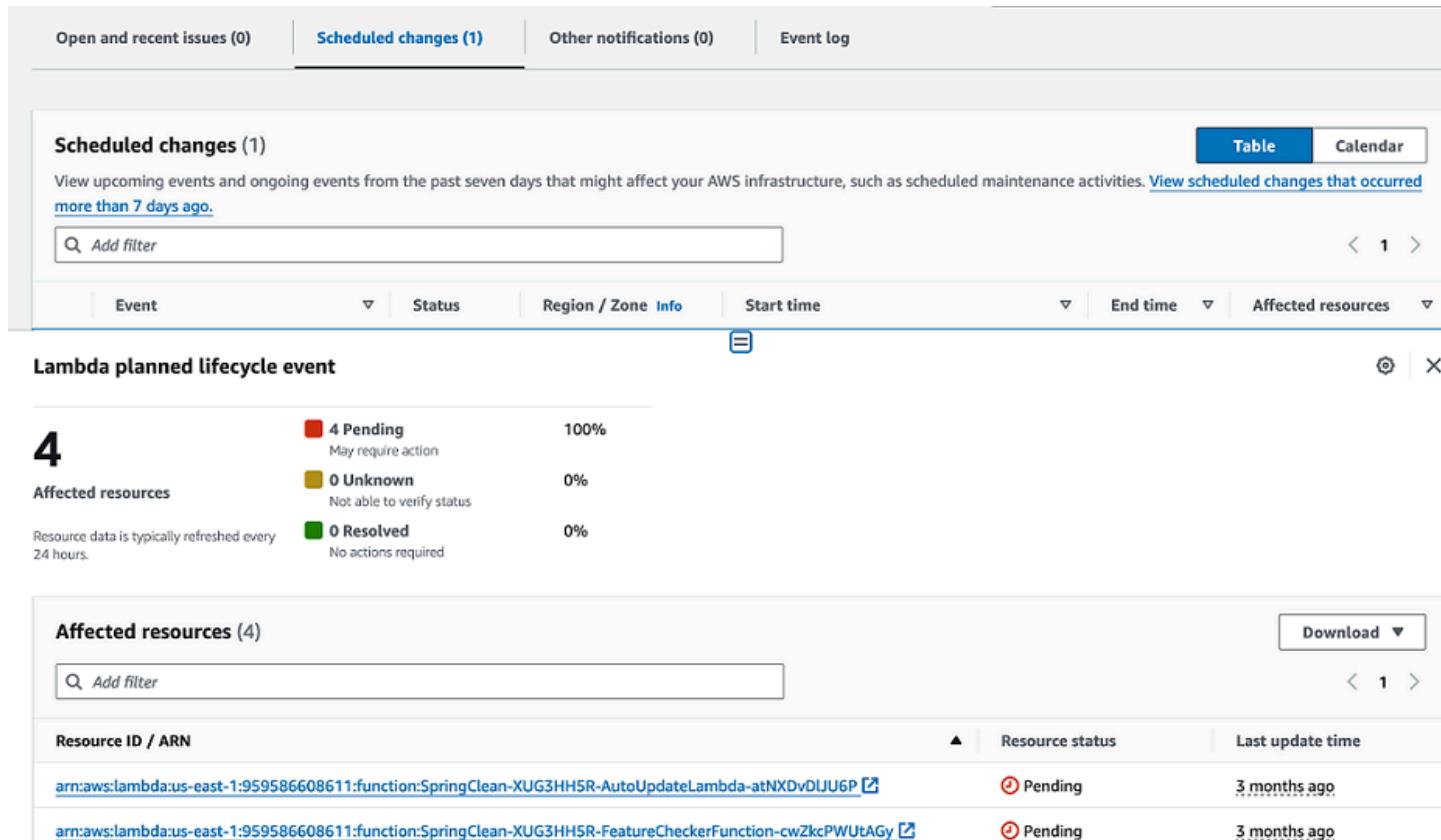
AWS Health Los eventos a nivel de cuenta muestran un resumen del estado de los recursos afectados en la parte superior de la pestaña Recursos afectados. Se muestra una lista de los recursos afectados en una tabla junto con el estado correspondiente. Los eventos de ciclo de vida planificados son un ejemplo de los tipos de eventos que utilizan el campo de estado del recurso. Para obtener más información sobre los eventos de ciclo de vida planificados, consulte [Eventos del ciclo de vida planificados para AWS Health](#).

Al acceder a la vista de la organización, AWS Health los eventos muestran un resumen del estado de todos los recursos afectados para todas las cuentas incluidas. Después del resumen aparece una

lista de las cuentas afectadas y el número de recursos pendientes correspondiente a esa cuenta. Seleccione el número de cuenta o el número de recursos pendientes para mostrar el resumen de la vista de la cuenta. El resumen de la vista de la cuenta tiene rutas de navegación para volver a la lista organizativa de las cuentas afectadas. Se muestra un resumen de los estados de los recursos afectados en la parte superior del panel dividido.

Puede descargar la lista de recursos afectados de la pestaña de recursos afectados en formato CSV o JSON. En la vista organizativa, el archivo descargado incluye todos los recursos de las cuentas enumeradas. Navegue hasta el nivel de la cuenta en la vista organizativa para incluir solo los recursos de esa cuenta en el archivo descargado. Cada recurso afectado del archivo descargado incluye el Cuenta de AWS ID, el eventARN, el nombre de la entidad, el entityARN, el estado y la hora de la última actualización del recurso. Si hay filtros activados, el archivo descargado solo incluye los resultados filtrados.

Solo se puede descargar un archivo a la vez. Los archivos se descargan automáticamente en la carpeta de descargas predeterminada del navegador y tienen un nombre de archivo preestablecido basado en el título del evento Región de AWS, la fecha de inicio del evento y la fecha de descarga.



The screenshot shows the AWS Health interface with the 'Scheduled changes' tab selected. At the top, there are four tabs: 'Open and recent issues (0)', 'Scheduled changes (1)', 'Other notifications (0)', and 'Event log'. Below the tabs, a heading 'Scheduled changes (1)' is displayed, with a sub-instruction: 'View upcoming events and ongoing events from the past seven days that might affect your AWS infrastructure, such as scheduled maintenance activities. [View scheduled changes that occurred more than 7 days ago.](#)' A search bar with 'Add filter' and navigation buttons ('< 1 >') are also present. The main content area has a table with columns: Event, Status, Region / Zone, Start time, End time, and Affected resources. A summary section for 'Lambda planned lifecycle event' shows 4 Pending resources (100% completion), 0 Unknown resources (0%), and 0 Resolved resources (0%). A note states: 'Resource data is typically refreshed every 24 hours.' At the bottom, a section titled 'Affected resources (4)' shows a table with columns: Resource ID / ARN, Resource status, and Last update time. Two entries are listed: 'arn:aws:lambda:us-east-1:959586608611:function:SpringClean-XUG3HH5R-AutoUpdateLambda-atNXDvDLJU6P' (Pending, 3 months ago) and 'arn:aws:lambda:us-east-1:959586608611:function:SpringClean-XUG3HH5R-FeatureCheckerFunction-cwZkcPWUtAGy' (Pending, 3 months ago). A 'Download' button is located in the top right of this section.

Event	Status	Region / Zone	Info	Start time	End time	Affected resources
Lambda planned lifecycle event						
4 Affected resources	4 Pending May require action	100%				
	0 Unknown Not able to verify status	0%				
	0 Resolved No actions required	0%				

Resource ID / ARN	Resource status	Last update time
arn:aws:lambda:us-east-1:959586608611:function:SpringClean-XUG3HH5R-AutoUpdateLambda-atNXDvDLJU6P	Pending	3 months ago
arn:aws:lambda:us-east-1:959586608611:function:SpringClean-XUG3HH5R-FeatureCheckerFunction-cwZkcPWUtAGy	Pending	3 months ago

Configuración de la zona horaria

Puedes ver los eventos en el AWS Health panel de control de tu zona horaria local o en UTC. Si cambias la zona horaria en tu AWS Health panel de control, todas las marcas horarias del panel y los eventos públicos se actualizarán a la zona horaria que especifiques.

Actualización de la configuración de la zona horaria

1. Abre tu AWS Health panel de control en casa. <https://health.aws.com/health/>
2. En la parte inferior de la página, elija Preferencias de cookies.
3. Seleccione Permitido para las cookies funcionales. Elija a continuación Guardar preferencias.
4. En el panel de navegación del panel de AWS Health control, selecciona la configuración de zona horaria.
5. Selecciona una zona horaria para tus sesiones AWS Health del panel de control. A continuación, elija Guardar cambios.

El estado de su organización

AWS Health se integra AWS Organizations para que pueda ver los eventos de todas las cuentas que forman parte de su organización. Esto le proporciona una vista centralizada de los eventos que aparecen en la organización. Puede utilizar estos eventos para monitorear los cambios en los recursos, servicios y aplicaciones.

Para obtener más información, consulte [Agregar AWS Health eventos en todas las cuentas](#).

Enable organizational view

Key benefits

 Organization-wide visibility Aggregate your Health events from all member AWS accounts in your AWS organization. This provides a centralized view for all events, such as operational issues, scheduled maintenance, and account notifications.	 API access If you have a Business or Enterprise Support plan, you can integrate with the AWS Health API to programmatically use organizational view and look up details for events that occur in your organization. Learn more	 Chat integration Using the AWS Health API, you can ingest events into your Amazon Chime or Slack channel to get notified when an event occurs. Filter events to get the ones that matter most to your organization. Learn more
--	---	---

Get started

1. Set up AWS Organizations You must have an AWS organization with all features enabled.  Success Manage AWS Organizations  View documentation	2. Enable organizational view for AWS Health After you set up AWS Organizations and sign in to the management account, you can enable AWS Health to aggregate all events. These events appear in the Personal Health Dashboard. Enable organizational view View documentation
--	--

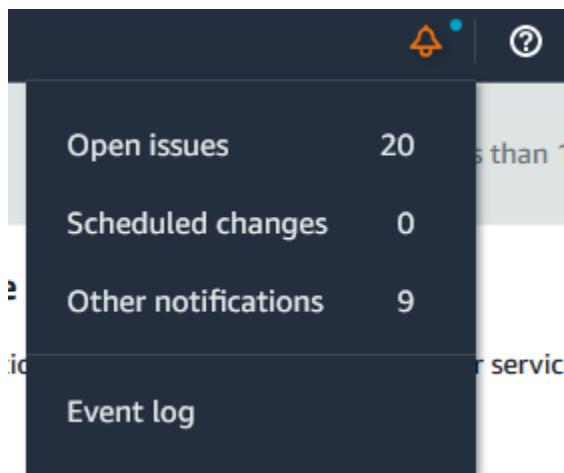
Alertas de AWS Health eventos

El AWS Health panel de control tiene un ícono de campana en la barra de navegación de la consola con un menú de alertas. Esta función muestra el número de AWS Health eventos recientes que aparecen en el panel de control de cada categoría. Este ícono de campana aparece en varias AWS consolas, como las de Amazon EC2, Amazon Relational Database Service (Amazon RDS) AWS Identity and Access Management , (IAM) y. AWS Trusted Advisor

Elija el ícono de campana para ver si eventos recientes afectan su cuenta. A continuación, puede elegir un evento para acceder a su AWS Health panel de control y obtener más información.

Example : eventos abiertos

La siguiente imagen muestra los eventos abiertos y de notificación de una cuenta.



Configuración de Amazon EventBridge

Se utiliza EventBridge para detectar los cambios de los AWS Health eventos y reaccionar ante ellos. Puedes monitorear AWS Health eventos específicos que ocurren en tu cuenta y, luego, configurar reglas para que te AWS Health notifiquen o tomes medidas cuando cambien los eventos.

EventBridge Úsalo con AWS Health

1. Abre tu AWS Health panel de control en <https://health.aws.com/health/casa>.
2. Para ir a la EventBridge consola y crear una regla, realiza una de las siguientes acciones:
 - En el panel de navegación, en Health Integrations, selecciona Amazon EventBridge.
 - En Configurar EventBridge, elija Ir a EventBridge.

3. Siga este procedimiento para crear reglas y monitorizar eventos. Consulte [Monitorización de eventos AWS Health con Amazon EventBridge](#).

Administra AWS Health las notificaciones en AWS User Notifications

AWS las notificaciones gestionadas te AWS User Notifications permiten recibir y gestionar notificaciones sobre eventos que afectan a ti Cuentas de AWS y a tus servicios. Al utilizar las notificaciones AWS gestionadas en AWS User Notifications, puede especificar qué categorías de AWS Health eventos desea recibir, configurar una vista organizativa de los correos electrónicos y obtener notificaciones consolidadas en lugar de varios correos electrónicos similares. Para obtener información sobre cómo habilitar este servicio, consulte [Habilitar o deshabilitar las notificaciones AWS administradas AWS Health en AWS User Notifications](#).

Puedes elegir los siguientes canales adicionales para recibir tus AWS Health eventos: AWS User Notifications

- Correo electrónico
- Chat
- Envía notificaciones al AWS Console Mobile Application

Si bien estas notificaciones no son tan detalladas como AWS Health las herramientas directas, proporcionan una forma eficaz de notificar a las partes interesadas los problemas y los cambios.

Note

Para obtener una visibilidad completa de los detalles del AWS Health evento IDs, incluidos el recurso afectado, el estado actual (abierto o cerrado) y el estado del recurso, se recomienda utilizar una de las siguientes AWS Health herramientas:

- La AWS Health API
- La fuente de `aws.health` en Amazon EventBridge
- El AWS Health Dashboard

Estas herramientas proporcionan la información más detallada y en tiempo real sobre los eventos y cambios en curso que podrían afectar a sus cargas de trabajo.

Configure su suscripción a notificaciones AWS gestionadas para eventos AWS Health

Para configurar tu suscripción a las notificaciones AWS gestionadas, sigue estos pasos:

1. Abre Notificaciones de usuario en [Consola de administración de AWS](#).
2. En el panel de navegación, selecciona suscripciones a notificaciones AWS gestionadas.
3. Puedes gestionar las notificaciones de tus AWS Health eventos por categoría. Para obtener más información, consulta [Añadir y eliminar contactos de la cuenta para las notificaciones AWS gestionadas en AWS User Notifications](#).

Note

AWS Health migró la entrega de correo electrónico a las notificaciones AWS gestionadas en AWS User Notifications. Desde el 15 de diciembre de 2025, recibes correos electrónicos de notificaciones AWS gestionadas. Para obtener más información, consulta [¿Qué ha cambiado en la migración a las notificaciones AWS gestionadas?](#) en el [AWS notificaciones gestionadas en las preguntas frecuentes sobre notificaciones de AWS usuario](#).

AWS notificaciones gestionadas en las preguntas frecuentes sobre notificaciones de AWS usuario

¿Qué ha cambiado en la migración a las notificaciones AWS gestionadas?

De forma predeterminada, los correos electrónicos relacionados con las notificaciones gestionadas se envían a los contactos de tu cuenta existentes (direcciones de correo raíz, de operaciones, de facturación y de seguridad). Los correos electrónicos que recibes de las notificaciones AWS gestionadas provienen de, `health@aws.com` en lugar de `no-reply-aws@amazon.com`, y el formato de los correos electrónicos cambia. Si anteriormente configuraste reglas de correo

electrónico para las AWS Health notificaciones, como enrutar un correo electrónico por ID de remitente o eliminar el contenido del correo electrónico, debes actualizar esta configuración para que coincida con el nuevo formato de correo electrónico. Si necesitas la automatización mediante notificaciones push, te recomendamos que evalúes AWS Health los eventos enviados a través de Amazon EventBridge como alternativa a las notificaciones gestionadas.

¿Cómo funciona la agregación de correos electrónicos y cómo activo esta función?

AWS la notificación gestionada agrega los AWS Health eventos que afectan a varias cuentas de la misma AWS Organizations organización en una única notificación agregada. Puedes ver la organización agregada en el centro de notificaciones de la cuenta de administración. Las notificaciones administradas envían por correo electrónico la notificación agregada a los contactos de la cuenta de administración. Para reducir la duplicación de correos electrónicos, las notificaciones AWS gestionadas envían una notificación cuando los contactos de la cuenta se comparten entre la administración y las cuentas de los miembros.

Para habilitar la agregación, debes haber AWS Organizations configurado y conceder un acceso confiable entre tu cuenta de administración y el AWS User Notifications servicio.

Para obtener más información, consulte [Agregación de notificaciones AWS administradas en AWS User Notifications](#).

¿Tengo que habilitar el acceso AWS Organizations confiable AWS User Notifications para recibir correos electrónicos agregados de las notificaciones AWS administradas?

Sí, se requiere un acceso confiable AWS User Notifications desde AWS Organizations .

¿Cuál es la diferencia entre permitir un acceso confiable AWS Organizations con AWS Health y con AWS User Notifications?

La confianza organizacional y los privilegios de administrador delegado asociados se asignan por servicio y actúan como barreras contra la sobreextensión de los permisos. El acceso confiable AWS Health permite ver organizativamente los AWS Health Dashboard AWS Health eventos enviados a través de Amazon EventBridge y las configuraciones de notificaciones en Notificaciones de usuario. AWS Health APIs El acceso confiable AWS User Notifications permite agregar notificaciones dentro de las notificaciones AWS administradas. Como el acceso de confianza no se comparte, es necesario añadir la configuración de administradores delegados por separado para cada servicio.

¿Hay alguna forma de conservar los correos electrónicos de texto sin formato para mi caso de uso específico?

No. Los AWS Health correos electrónicos de texto sin formato actuales se deshabilitan una vez finalizada la migración. Si utilizas reglas de correo electrónico para impulsar diferentes flujos de trabajo, te recomendamos que evalúes AWS Health los eventos enviados a través de Amazon EventBridge como alternativa.

¿A qué corresponden las categorías de notificaciones AWS gestionadas del AWS Health esquema?

Las notificaciones de operaciones de salud, seguridad y facturación corresponden a las notificaciones de AWS Health cuenta y los cambios programados que tienen la personalidad de operaciones, seguridad y facturación, respectivamente. AWS Health los eventos con más de una etiqueta personal se envían a través de las categorías Seguridad y Facturación. Los problemas específicos de la cuenta incluyen la categoría de problemas de salud que son específicos de un. Cuenta de AWS

Los eventos de servicio público no están disponibles a través de las notificaciones AWS gestionadas.

AWS Health Tablero

Puede utilizar el AWS Health panel de control: estado del servicio para ver el estado de salud de todos Servicios de AWS. En esta página se muestran los eventos de servicio notificados en todos los servicios de Regiones de AWS. No necesita iniciar sesión ni tener uno para acceder Cuenta de AWS a la página AWS Health Panel de control: estado del servicio.

Tip

Este sitio web solo muestra eventos públicos, que no son específicos de un Cuenta de AWS. Si ya tiene una cuenta, le recomendamos que inicie sesión para ver su AWS Health panel de control y mantenerse informado sobre los eventos que puedan afectar a su cuenta y sus servicios. Para obtener más información, consulte [Introducción al Panel de AWS Health](#).

Para ver el AWS Health panel de control: estado del servicio

1. Navegue a la página https://health.aws.com/health/de_estado.

Note

Si ya has iniciado sesión en tu página Cuenta de AWS, se te redirigirá al AWS Health Panel de control, la página de estado de tu cuenta.

2. En Estado del servicio, seleccione Problemas abiertos y recientes para ver los eventos notificados recientemente. Puede ver la siguiente información sobre el evento:

- El nombre del evento y la región afectada. Por ejemplo, Operational issue – Amazon Elastic Compute Cloud
- El nombre del servicio
- La gravedad del evento, por ejemplo, si se ha visto afectado o degradado
- Cronología de las actualizaciones recientes del evento
- Una lista de los Servicios de AWS que también se ven afectadas por este evento

Note

Puede ver los eventos en su zona horaria local o en UTC. Para obtener más información, consulte la [Configuración de zona horaria](#).

3. Seleccione Service history para ver la tabla de Service history. En esta tabla se muestran todas las interrupciones de los últimos 12 meses.

Tip

Puede filtrar por Service, Región de AWS y fecha.

4. Junto a un evento de servicio en curso, seleccione el ícono de estado () para ver más información sobre el evento.
5. (Opcional) Para ver esto como una lista de eventos históricos, utilice el botón de lista de eventos. Seleccione cualquier evento en la columna de eventos para ver más información sobre ese evento concreto en el panel lateral emergente.

Service history

[List of services](#)[List of events](#)

The following table is a running log of AWS service interruptions for the past 12 months. Choose a status icon to see status updates for that service. All dates and times are reported in Pacific Standard Time (PST). To update your time zone, see [Time zone settings](#).

[Add filter](#)**Note**

Al seleccionar cualquier evento público después de septiembre de 2023, se rellenará la URL en el navegador con un enlace a ese evento público de AWS Health . Después de seleccionar este enlace, accederá a la vista de lista de eventos con la ventana emergente de ese evento.

6. (Opcional) Puede ver los eventos en su zona horaria local o en UTC. Para obtener más información, consulte [Configuración de la zona horaria](#).
7. (Opcional) Si tiene una cuenta, seleccione Open your account health para iniciar sesión. Después de iniciar sesión, podrá ver los eventos específicos de su cuenta. Para obtener más información, consulte [Introducción al Panel de AWS Health](#).

 Note

Aunque hay una fuente RSS disponible para eventos de salud, el formato está sujeto a cambios. Por lo tanto, es posible que al eliminar la fuente RSS no se proporcionen todos los datos relevantes. Para ingerir datos de eventos de salud de forma programática, te recomendamos integrarlos con Amazon EventBridge. Para obtener más información, consulte [Monitorización de eventos AWS Health con Amazon EventBridge](#).

Eventos del ciclo de vida planificados para AWS Health

Obtenga información sobre los eventos del ciclo de vida planificados para AWS Health.

Temas

- [¿Qué son los eventos del ciclo de vida planificado?](#)
- [¿Qué debo esperar cuando recibo una notificación de un evento de ciclo de vida planificado?](#)
- [Modelo de responsabilidad compartida para resiliencia](#)
- [Acceder a los eventos planificados del ciclo de vida](#)

¿Qué son los eventos del ciclo de vida planificado?

AWS Health comunica los cambios importantes que pueden afectar a la disponibilidad de sus aplicaciones. En el modelo de responsabilidad AWS compartida, AWS toma medidas para mantener el hardware y la infraestructura subyacentes que respaldan sus recursos actualizados y seguros. Sin embargo, algunos cambios requieren la acción o la coordinación del cliente para evitar que sus aplicaciones se vean afectadas. AWS Health le notifica con antelación los cambios importantes, tales como:

- Fin del soporte del software de código abierto: algunos Servicios de AWS utilizan versiones de software de código abierto. Si la comunidad de código abierto deja de dar soporte a las versiones de software, le AWS informa de cuándo debe tomar medidas para actualizar y evitar que sus aplicaciones se vean afectadas.
 - [Fin del soporte de la versión del motor Amazon RDS para MySQL](#)
 - [Fin del soporte para la versión Amazon EKS Kubernetes](#)
- Cambios que afecten a los recursos AWS propios y que puedan requerir tu acción.
 - [Vencimiento de los certificados de autoridad de certificación de Amazon RDS.](#)

 Note

Todas las notificaciones que se ajusten a este criterio se registrarán AWS Health como eventos del ciclo de vida planificado.

- Distribución dinámica de los recursos y mejora de los metadatos: desde el momento en que recibes la notificación hasta que finaliza el AWS Health evento, los recursos afectados se asocian

al AWS Health evento como entidades afectadas con un estado de entidad específico. Los recursos afectados se especifican en formato ARN, cuando proceda. Si los recursos afectados requieren que el cliente tome medidas, aparecerán en la lista con el estado “PENDIENTE”. Si a los recursos afectados se les realizó la acción requerida o se eliminaron los recursos, el estado se actualizará a “RESUELTO”.

 Note

- Las actualizaciones del estado de los recursos se realizan de forma asíncrona y periódica y, en raras ocasiones, pueden demorarse hasta 72 horas.
- En las excepciones en las que no se proporcionen actualizaciones dinámicas, en lugar de que los recursos tengan el estado “PENDIENTE” o “RESUELTO”, no se asignará ningún estado a los recursos.
- Las actualizaciones del estado de los recursos no se admiten en AWS GovCloud (US) las regiones ni en China.

¿Qué debo esperar cuando recibo una notificación de un evento de ciclo de vida planificado?

La AWS Health experiencia de planificar los eventos del ciclo de vida ayuda a sus equipos a conocer los próximos cambios en el ciclo de vida y a hacer un seguimiento de la finalización de las acciones.

Categoría de tipo: cambio programado

Código de tipo de evento: AWS_{SERVICE}_PLANNED_LIFECYCLE_EVENT

Hora de inicio del evento: la hora de inicio del evento es la fecha más temprana en la que sus recursos se ven afectados por el cambio.

Hora de finalización del evento: la hora de finalización del evento es la fecha en la que finaliza el cambio en todos los AWS recursos. Tenga en cuenta que la hora de finalización no siempre se especifica. Es importante tratar la hora de inicio como la fecha de cambio.

 Note

Las organizaciones pueden esperar recibir un único ARN de evento por cada evento del ciclo de vida planificado agrupado por región en el que haya recursos afectados. Sin embargo,

es posible que reciban varios ARNs si la organización tiene un gran número de recursos Cuentas de AWS o afectados.

Visibilidad temprana de los eventos del ciclo de vida planificado: los eventos del ciclo de vida planificado están diseñados para tener un plazo mínimo de 180 días para los principales versions/ changes and 90 days for minor versions/changes, siempre que sea posible.

Distribución dinámica de los recursos y mejora de los metadatos: desde el momento en que recibes la notificación y hasta que AWS Health finaliza el evento, los recursos afectados se asocian al AWS Health evento como [entidades afectadas](#) con un estado de entidad específico. Los recursos afectados se especifican en formato ARN, cuando proceda. Si los recursos afectados requieren que el cliente tome medidas, aparecerán en la lista con el estado “PENDIENTE”. Si a los recursos afectados se les realizó la acción requerida o se eliminaron los recursos, el estado se actualizará a “RESUELTO”.

 Note

- AWS Health las notificaciones proporcionan actualizaciones de estado a lo largo del tiempo siempre que es posible, excepto en las regiones AWS GovCloud (US) y China.
- Las actualizaciones del estado de los recursos se realizan de forma asíncrona y periódica y, en raras ocasiones, pueden demorarse hasta 72 horas.

Open and recent issues | **Scheduled changes** | Other notifications | Event log

Scheduled changes

View upcoming events and ongoing events from the past seven days that might affect your AWS infrastructure, such as scheduled maintenance activities.

Add filter | < 1 >

Event	Status	Region / Zone	Info	Start time	End time	Affected resources
<input checked="" type="radio"/> EKS planned lifecycle event	Upcoming	us-west-2		January 30, 2024 at 6:00:00 PM UTC-8		9 pending
<input type="radio"/> DMS planned lifecycle event	Upcoming	us-east-1		January 29, 2024 at 6:00:00 PM UTC-8		1 pending
<input type="radio"/> DMS planned lifecycle event	Upcoming	eu-west-1		January 29, 2024 at 6:00:00 PM UTC-8		10 pending
<input type="radio"/> EKS planned lifecycle event	Completed	eu-west-1		January 30, 2024 at 6:00:00 PM UTC-8		-

EKS planned lifecycle event | = | X

Resource data is typically refreshed every 24 hours. 0 Resolved 0% No actions required

Affected resources in account 745485236264 (5)

Add filter | < 1 >

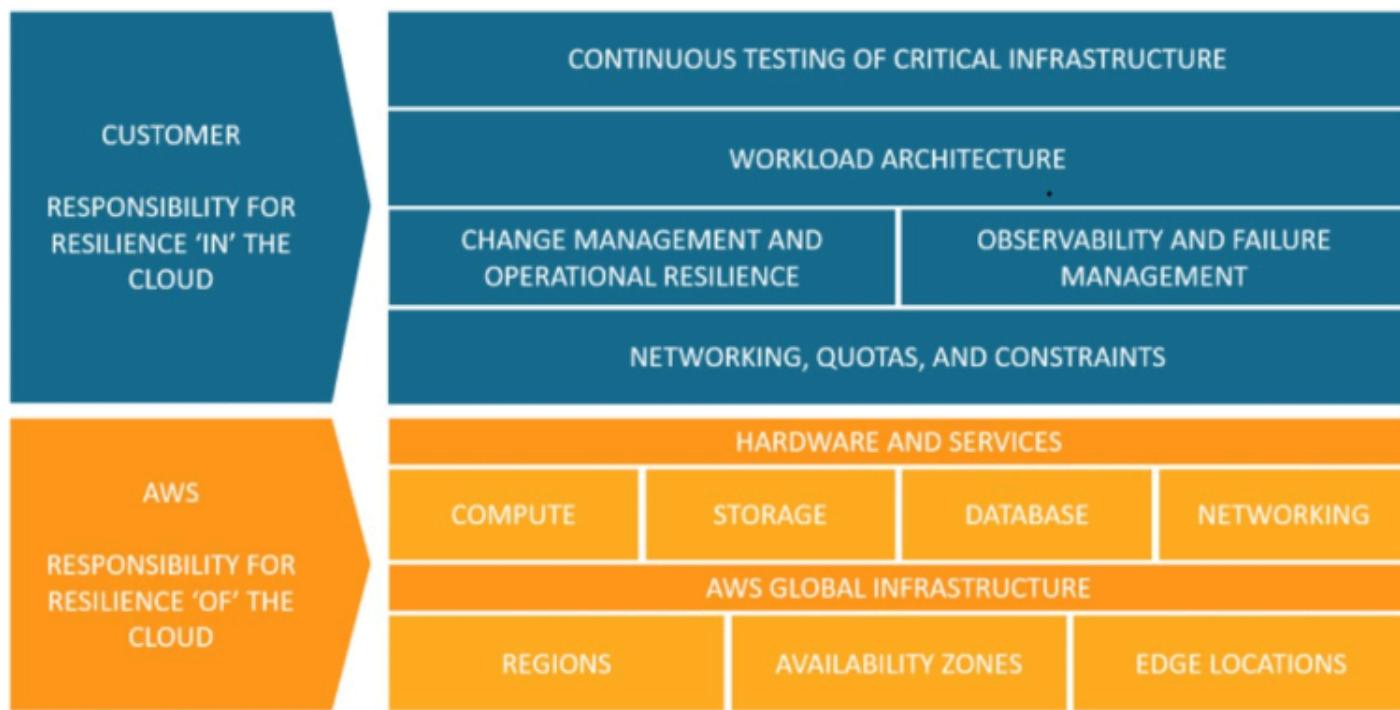
Resource ID / ARN	Resource status	Last update time
arn:aws:eks:us-west-2:745485236264:cluster/prod-ops-cluster	⌚ Pending	15 days ago
arn:aws:eks:us-west-2:745485236264:cluster/nonprod-dev5	⌚ Pending	15 days ago
arn:aws:eks:us-west-2:745485236264:cluster/n-preprd-eks	⌚ Pending	15 days ago
arn:aws:eks:us-west-2:745485236264:cluster/argoworkflows-refactor51	⌚ Pending	15 days ago
arn:aws:eks:us-west-1:745485236264:cluster/prod-refactor	⌚ Pending	15 days ago

Una vez pasada la fecha del evento planificado:

1. Si corresponde, el servicio podría implementar el cambio descrito en su recurso en cualquier momento después de la fecha de inicio del evento.
2. Si resuelve todos los recursos antes de la fecha de finalización del soporte, el AWS Health evento cambiará al estado **Closed**.
3. Si tienes recursos pendientes después de la fecha de cambio y no se han resuelto, el AWS Health evento permanecerá abierto durante 4 años a partir de la fecha de inicio o finalización del evento (si esta fecha es posterior). Transcurrido este tiempo, el AWS Health evento se eliminará.

Modelo de responsabilidad compartida para resiliencia

La seguridad y el cumplimiento son responsabilidades compartidas entre el cliente AWS y el cliente. Según los servicios implementados, este modelo compartido puede ayudar a aliviar la carga operativa del cliente. Esto se debe a AWS que opera, administra y controla los componentes desde el sistema operativo anfitrión y la capa de virtualización hasta la seguridad física de las instalaciones en las que opera el servicio. El cliente asume la responsabilidad y la administración del sistema operativo huésped (incluidas las actualizaciones y los parches de seguridad) y demás software de aplicación asociado, además de la configuración del firewall del grupo de seguridad que proporciona AWS. Para obtener más información, consulte el [Modelo de responsabilidad compartida](#).



Acceder a los eventos planificados del ciclo de vida

Se puede acceder a los eventos del ciclo de vida planificados y supervisarlos mediante varios canales:

- [Usa Amazon EventBridge](#)
- [Usa el AWS Health panel de control](#)
 - [Vista del calendario](#)
 - [Vista de los recursos afectados](#)

- [Uso de la API de AWS Health](#)

Integración AWS Health con otros sistemas mediante la AWS Health API

AWS Health es un servicio RESTful web que utiliza HTTPS como transporte y JSON como formato de serialización de mensajes. Su código de aplicación puede realizar solicitudes directamente a la API de AWS Health . Cuando utiliza directamente la API de REST, es necesario escribir el código necesario para firmar y autenticar sus solicitudes. Para obtener más información sobre las AWS Health operaciones y los parámetros, consulta la [referencia de la AWS Health API](#).

Note

Para usar la AWS Health API, debe tener un plan Business, Enterprise On-Ramp o Enterprise Support. [AWS Support](#) Si llamas a la AWS Health API desde una AWS cuenta que no tiene un plan Business, Enterprise On-Ramp o Enterprise Support, recibirás un `SubscriptionRequiredException` error.

Puedes usarlo AWS SDKs para empaquetar las llamadas a la API AWS Health REST, lo que puede simplificar el desarrollo de tu aplicación. Usted especifica sus AWS credenciales y estas bibliotecas se encargan de autenticar y firmar las solicitudes por usted.

AWS Health también incluye un AWS Health panel de control Consola de administración de AWS que puede utilizar para ver y buscar eventos y entidades afectadas. Consulte [Introducción al Panel de AWS Health](#).

Temas

- [Firmar solicitudes AWS Health de API](#)
- [Elegir puntos de enlace para las solicitudes de AWS Health API](#)
- [Demostraciones: recuperación de los últimos siete días de datos de eventos de AWS Health mediante programación](#)
- [Tutorial: Uso de la AWS Health API con ejemplos de Java](#)

Firmar solicitudes AWS Health de API

Cuando utilizas AWS SDKs o AWS Command Line Interface (AWS CLI) para realizar solicitudes AWS, estas herramientas firman automáticamente las solicitudes por ti con la clave de acceso que especifiques al configurar las herramientas. Por ejemplo, si las utiliza AWS SDK para Java para la anterior demostración de terminales de alta disponibilidad, no es necesario que firme las solicitudes usted mismo.

Ejemplos de código Java

Para ver más ejemplos sobre cómo usar la AWS Health API con AWS SDK para Java, consulta este [código de ejemplo](#).

Cuando realices solicitudes, te recomendamos encarecidamente que no utilices las credenciales de tu cuenta AWS raíz para acceder habitualmente a ella AWS Health. Puede utilizar las credenciales de un usuario de IAM. Para obtener más información, consulte [Bloquear las claves de acceso de los usuarios raíz de su AWS cuenta](#) en la Guía del usuario de IAM.

Si no utiliza las AWS SDKs o las AWS CLI, debe firmar las solicitudes usted mismo. Le recomendamos que utilice la versión 4 de AWS Signature. Para obtener más información, consulte [Firmar solicitudes de AWS API](#) en Referencia general de AWS.

Elegir puntos de enlace para las solicitudes de AWS Health API

La AWS Health API sigue una arquitectura de aplicaciones multirregional, una arquitectura de y tiene dos puntos finales regionales en una configuración activo-pasiva. Para admitir la conmutación por error de DNS activa-pasiva, AWS Health proporciona un único punto de conexión global. Puede realizar una búsqueda de DNS en el punto final global para determinar el punto final activo y la región de firma correspondiente. AWS Esto le ayuda a saber qué punto final debe utilizar en su código, de modo que pueda obtener la información más reciente AWS Health.

Al realizar una solicitud al punto final global, debe especificar sus credenciales de AWS acceso al punto final regional al que se dirige y configurar la firma para su región. De lo contrario, es posible que se produzca un error en la autenticación. Para obtener más información, consulte [Firmar solicitudes AWS Health de API](#).

Para las solicitudes IPv6 exclusivas, te recomendamos realizar una búsqueda de DNS en el punto de conexión global para determinar el punto de conexión activo Región de AWS y, a continuación, llamar al punto de conexión de doble pila IPv6 compatible para esa región.

En la siguiente tabla, se representa la configuración por defecto.

Descripción	Región de firma	Punto de conexión	Protocolo
Activo	us-east-1	health.us-east-1.a mazonaws.com (solo) IPv4 health.us-east-1.a pi.aws (y compatibles) IPv4 IPv6	HTTPS
Pasivo	us-east-2	health.us-east-2.a mazonaws.com (solo) IPv4 health.us-east-2.a pi.aws (y compatibles) IPv4 IPv6	HTTPS
Global	us-east-1	global.health.amazonaws.com	HTTPS

 Note

Esta es la
región de
firma del
punto de
conexión
activo actual.

Para determinar si un punto final es el punto final activo, realice una búsqueda de DNS en el CNAME del punto final global y, a continuación, extraiga la región del nombre resuelto. AWS

Example : búsqueda de DNS en el punto de conexión global

El siguiente comando completa una búsqueda de DNS en el punto de conexión global.health.amazonaws.com A continuación, el devuelve el punto de conexión de la región us-east-1. Este resultado indica para qué punto final debe utilizarse. AWS Health

```
dig global.health.amazonaws.com | grep CNAME
global.health.amazonaws.com. 10 IN CNAME health.us-east-1.amazonaws.com
```

Tip

Tanto los puntos finales activos como los pasivos devuelven AWS Health datos. Sin embargo, los datos de AWS Health más recientes solo están disponibles en el punto de conexión activo. Los datos del punto de conexión pasivo serán coherentes con el punto de conexión activo. Le recomendamos que reinicie todos los flujos de trabajo cuando cambie el punto de conexión activo.

Demostraciones: recuperación de los últimos siete días de datos de eventos de AWS Health mediante programación

En los siguientes ejemplos de código, AWS Health utiliza una búsqueda de DNS en el punto final global para determinar el punto final regional activo y la región de firma. AWS Health utiliza esta información para recuperar un informe de los datos del evento de los últimos siete días. El código reinicia el flujo de trabajo si cambia el punto de conexión activo.

Temas

- [Demostración: recuperación de los últimos siete días de datos de eventos de AWS Health mediante Java](#)
- [Demostración: recuperación de los últimos siete días de datos de eventos de AWS Health mediante Python](#)

Demostración: recuperación de los últimos siete días de datos de eventos de AWS Health mediante Java

Requisito previo

Debe instalar [Gradle](#).

Para usar el ejemplo de Java

1. Descargue la [demostración de terminales de AWS Health alta disponibilidad](#) desde GitHub.
2. Desplácese hasta el directorio del proyecto `high-availability-endpoint/java` de demostración.
3. En una ventana con una línea de comandos, escriba el siguiente comando:

```
gradle build
```

4. Introduzca los siguientes comandos para especificar sus AWS credenciales.

```
export AWS_ACCESS_KEY_ID="AKIAIOSFODNN7EXAMPLE"
export AWS_SECRET_ACCESS_KEY="wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
export AWS_SESSION_TOKEN="your-aws-token"
```

5. Ingrese el comando siguiente para ejecutar la demostración.

```
gradle run
```

Example : salida AWS Health del evento

El ejemplo de código devuelve el AWS Health evento reciente de los últimos siete días en tu AWS cuenta. En el siguiente ejemplo, el resultado incluye un AWS Health evento para el AWS Config servicio.

```
> Task :run
[main] INFO aws.health.high.availability.endpoint.demo.HighAvailabilityV2Workflow
- EventDetails(Event=Event(Arn=arn:aws:health:global::event/CONFIG/
AWS_CONFIG_OPERATIONAL_NOTIFICATION/AWS_CONFIG_OPERATIONAL_NOTIFICATION_88a43e8a-
e419-4ca7-9baa-56bcde4dba3,
Service=CONFIG, EventTypeCode=AWS_CONFIG_OPERATIONAL_NOTIFICATION,
EventTypeCategory=accountNotification, Region=global,
StartTime=2020-09-11T02:55:49.899Z, LastUpdatedTime=2020-09-11T03:46:31.764Z,
StatusCode=open, EventScopeCode=ACCOUNT_SPECIFIC),
EventDescription=EventDescription(LatestDescription=As part of our ongoing efforts
to optimize costs associated with recording changes related to certain ephemeral
workloads,
AWS Config is scheduled to release an update to relationships modeled within
ConfigurationItems (CI) for 7 EC2 resource types on August 1, 2021.
```

Examples of ephemeral workloads include changes to Amazon Elastic Compute Cloud (Amazon EC2) Spot Instances, Amazon Elastic MapReduce jobs, and Amazon EC2 AutoScaling.

This update will optimize CI models for EC2 Instance, SecurityGroup, Network Interface, Subnet, VPC, VPN Gateway, and Customer Gateway resource types to record direct relationships and deprecate indirect relationships.

A direct relationship is defined as a one-way relationship (A->B) between a resource (A) and another resource (B), and is typically derived from the Describe API response of resource (A).

An indirect relationship, on the other hand, is a relationship that AWS Config infers (B->A), in order to create a bidirectional relationship.

For example, EC2 instance -> Security Group is a direct relationship, since security groups are returned as part of the describe API response for an EC2 instance.

But Security Group -> EC2 instance is an indirect relationship, since EC2 instances are not returned when describing an EC2 Security group.

Until now, AWS Config has recorded both direct and indirect relationships. With the launch of Advanced queries in March 2019, indirect relationships can easily be answered by running Structured Query Language (SQL) queries such as:

```
SELECT
  resourceId,
  resourceType
WHERE
  resourceType ='AWS::EC2::Instance'
AND
  relationships.resourceId = 'sg-234213'
```

By deprecating indirect relationships, we can optimize the information contained within a

Configuration Item while reducing AWS Config costs related to relationship changes.

This is especially useful in case of ephemeral workloads where there is a high volume of configuration changes for EC2 resource types.

Which resource relationships are being removed?

Resource Type: Related Resource Type

- 1 AWS::EC2::CustomerGateway: AWS::VPN::Connection
- 2 AWS::EC2::Instance: AWS::EC2::EIP, AWS::EC2::RouteTable
- 3 AWS::EC2::NetworkInterface: AWS::EC2::EIP, AWS::EC2::RouteTable
- 4 AWS::EC2::SecurityGroup: AWS::EC2::Instance, AWS::EC2::NetworkInterface

```
5 AWS::EC2::Subnet: AWS::EC2::Instance, AWS::EC2::NetworkACL,  
AWS::EC2::NetworkInterface, AWS::EC2::RouteTable  
6 AWS::EC2::VPC: AWS::EC2::Instance, AWS::EC2::InternetGateway,  
AWS::EC2::NetworkACL, AWS::EC2::NetworkInterface, AWS::EC2::RouteTable,  
AWS::EC2::Subnet, AWS::EC2::VPNGateway, AWS::EC2::SecurityGroup  
7 AWS::EC2::VPNGateway: AWS::EC2::RouteTable, AWS::EC2::VPNConnection
```

Alternate mechanism to retrieve this relationship information:

The `SelectResourceConfig` API accepts a SQL SELECT command, performs the corresponding search, and returns resource configurations matching the properties. You can use this API to retrieve the same relationship information.

For example, to retrieve the list of all EC2 Instances related to a particular VPC `vpc-1234abc`, you can use the following query:

```
SELECT  
  resourceId,  
  resourceType  
WHERE  
  resourceType = 'AWS::EC2::Instance'  
AND  
  relationships.resourceId = 'vpc-1234abc'
```

If you have any questions regarding this deprecation plan, please contact AWS Support [1]. Additional sample queries to retrieve the relationship information for the resources listed above is provided in [2].

[1] <https://aws.amazon.com/support>
[2] <https://docs.aws.amazon.com/config/latest/developerguide/examplerelationshipqueries.html>,
EventMetadata={})

Recursos de Java

- Para obtener más información, consulta la [interfaz HealthClient](#) en la referencia de la AWS SDK para Java API y el [código fuente](#).
- Para obtener más información sobre la biblioteca utilizada en esta demostración para las búsquedas de DNS, consulte [dnsjava](#) en GitHub

Demostración: recuperación de los últimos siete días de datos de eventos de AWS Health mediante Python

Requisito previo

Debe instalar [Python 3](#).

Para usar el ejemplo de Python

1. Descargue la demostración de terminales de [AWS Health alta disponibilidad desde GitHub](#).
2. Desplácese hasta el directorio del proyecto `high-availability-endpoint/python` de demostración.
3. En una ventana con una línea de comandos, escriba los siguientes comandos:

```
pip3 install virtualenv
virtualenv -p python3 v-aws-health-env
```

Note

En Python 3.3 y posteriores, puede utilizar el módulo `venv` integrado para crear un entorno virtual, en lugar de instalar `virtualenv`. Para obtener más información, consulte [venv - Creation of virtual environments](#) en el sitio web de Python.

```
python3 -m venv v-aws-health-env
```

4. Especifique el siguiente comando para activar el entorno virtual.

```
source v-aws-health-env/bin/activate
```

5. Ingrese el siguiente comando para instalar las dependencias.

```
pip install -r requirements.txt
```

6. Introduzca los siguientes comandos para especificar sus AWS credenciales.

```
export AWS_ACCESS_KEY_ID="AKIAIOSFODNN7EXAMPLE"
export AWS_SECRET_ACCESS_KEY="wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
export AWS_SESSION_TOKEN="your-aws-token"
```

7. Ingrese el comando siguiente para ejecutar la demostración.

```
python3 main.py
```

Example : salida AWS Health del evento

El ejemplo de código devuelve el AWS Health evento reciente de los últimos siete días en tu AWS cuenta. El siguiente resultado devuelve un AWS Health evento para una notificación AWS de seguridad.

```
INFO:botocore.credentials:Found credentials in environment variables.
INFO:root:Details: {'arn': 'arn:aws:health:global::event/SECURITY/
AWS_SECURITY_NOTIFICATION/AWS_SECURITY_NOTIFICATION_0e35e47e-2247-47c4-
a9a5-876544042721',
'service': 'SECURITY', 'eventTypeCode': 'AWS_SECURITY_NOTIFICATION',
'eventTypeCategory': 'accountNotification', 'region': 'global', 'startTime':
datetime.datetime(2020, 8, 19, 23, 30, 42, 476000,
tzinfo=tzlocal()), 'lastUpdatedTime': datetime.datetime(2020, 8, 20, 20, 44, 9,
547000, tzinfo=tzlocal()), 'statusCode': 'open', 'eventScopeCode': 'PUBLIC'},
description:
{'latestDescription': 'This is the second notice regarding TLS requirements on FIPS
endpoints.\n\nWe
are in the process of updating all AWS Federal Information Processing Standard
(FIPS) endpoints across all AWS regions
to Transport Layer Security (TLS) version 1.2 by March 31, 2021 . In order to avoid
an interruption in service, we encourage you to act now, by ensuring that you
connect to AWS FIPS endpoints at a TLS version of 1.2.
If your client applications fail to support TLS 1.2 it will result in connection
failures when TLS versions below 1.2 are no longer supported.\n\nBetween now and
March 31, 2021 AWS will remove TLS 1.0 and TLS 1.1 support from each FIPS endpoint
where no connections below TLS 1.2 are detected over a 30-day period.
After March 31, 2021 we may deploy this change to all AWS FIPS endpoints, even if
there continue
to be customer connections detected at TLS versions below 1.2. \n\nWe will provide
additional updates and reminders on the AWS Security Blog, with a 'TLS' tag [1].
If you need further guidance or assistance, please contact AWS Support [2] or your
Technical Account Manager (TAM).
Additional information is below.\n\nHow can I identify clients that are connecting
with TLS
1.0/1.1?\nFor customers using S3 [3], Cloudfront [4] or Application Load Balancer
[5] you can use
```

your access logs to view the TLS connection information for these services, and identify client connections that are not at TLS 1.2. If you are using the AWS Developer Tools on your clients, you can find information on how to properly configure your client's TLS versions by visiting Tools to Build on AWS [7] or our associated AWS Security Blog has a link for each unique code language [7].\n\nWhat is Transport Layer Security (TLS)?\nTransport Layer Security (TLS Protocols) are cryptographic protocols designed to provide secure communication across a computer network [6].\n\nWhat are AWS FIPS endpoints? All AWS services offer Transport Layer Security (TLS) 1.2 encrypted endpoints that can be used for all API calls. Some AWS services also offer FIPS 140-2 endpoints [9] for customers that require use of FIPS validated cryptographic libraries. \n\n[1] <https://aws.amazon.com/blogs/security/tag/tls/>\n[2] <https://aws.amazon.com/support/>\n[3] <https://docs.aws.amazon.com/AmazonS3/latest/dev/LogFormat.html>\n[4] <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html>\n[5] <https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html>\n[6] <https://aws.amazon.com/tools/>\n[7] <https://aws.amazon.com/blogs/security/tls-1-2-to-become-the-minimum-for-all-aws-fips-endpoints>\n[8] https://en.wikipedia.org/wiki/Transport_Layer_Security\n[9] <https://aws.amazon.com/compliance/fips/>

8. Una vez que haya terminado, ingrese el siguiente comando para desactivar la máquina virtual.

deactivate

Recursos de Python

- Para obtener más información sobre el Health. Client, consulte la [Referencia de la API de AWS SDK para Python \(Boto3\)](#).
- [Para obtener más información sobre la biblioteca utilizada en esta demostración para las búsquedas de DNS, consulte el kit de herramientas dnspython y el código fuente en él. GitHub](#)

Tutorial: Uso de la AWS Health API con ejemplos de Java

Los siguientes ejemplos de código de Java muestran cómo inicializar un AWS Health cliente y recuperar información sobre eventos y entidades.

Paso 1: Inicializar las credenciales

Se requieren credenciales válidas para comunicarse con la AWS Health API. Puede utilizar el par de claves de cualquier usuario de IAM asociado a la AWS cuenta.

Crea e inicializa una [AWSCredentials](#) instancia:

```
AWSCredentials credentials = null;
try {
    credentials = new ProfileCredentialsProvider("default").getCredentials();
} catch (Exception e) {
    throw new AmazonClientException(
        "Cannot load the credentials from the credential profiles file. "
        + "Please make sure that your credentials file is at the correct "
        + "location (/home/username/.aws/credentials), and is in valid format.", e);
}
```

Paso 2: inicializar un AWS Health cliente de API

Utilice el objeto credentials inicializado en el paso anterior para crear un cliente de AWS Health :

```
import com.amazonaws.services.health.AWSHealthClient;
AWSHealth awsHealthClient = new AWSHealthClient(credentials);
```

Paso 3: Usa las operaciones de AWS Health la API para obtener información sobre los eventos

DescribeEvents

```
import com.amazonaws.services.health.model.DescribeEventsRequest;
import com.amazonaws.services.health.model.DescribeEventsResult;
import com.amazonaws.services.health.model.Event;
import com.amazonaws.services.health.model.EventFilter;

DescribeEventsRequest request = new DescribeEventsRequest();

EventFilter filter = new EventFilter();
// Filter on any field from the supported AWS Health EventFilter model.
// Here is an example for Region us-east-1 events from the EC2 service.
filter.setServices(singletonList("EC2"));
```

```
filter.setRegions(singletonList("us-east-1"));
request.setFilter(filter);

DescribeEventsResult response = awsHealthClient.describeEvents(request);
List<Event> resultEvents = response.getEvents();

Event currentEvent = null;
for (Event event : resultEvents) {
    // Display result event data; here is a subset.
    System.out.println(event.getArn());
    System.out.println(event.getService());
    System.out.println(event.getRegion());
    System.out.println(event.getAvailabilityZone());
    System.out.println(event.getStartTime());
    System.out.println(event.getEndTime());
}
}
```

DescribeEventAggregates

```
import com.amazonaws.services.health.model.DescribeEventAggregatesRequest;
import com.amazonaws.services.health.model.DescribeEventAggregatesResult;
import com.amazonaws.services.health.model.EventAggregate;
import com.amazonaws.services.health.model.EventFilter;

DescribeEventAggregatesRequest request = new DescribeEventAggregatesRequest();
// set the aggregation field
request.setAggregateField("eventTypeCategory");

// filter more on result if needed
EventFilter filter = new EventFilter();
filter.setRegions(singleton("us-east-1"));
request.setFilter(filter);

DescribeEventAggregatesResult response =
awsHealthClient.describeEventAggregates(request);

// print event count for each eventTypeCategory
for (EventAggregate aggregate: response.getEventAggregates()) {
    System.out.println("Event Category:" + aggregate.getAggregateValue());
    System.out.println("Event Count:" + aggregate.getCount());
}
```

DescribeEventDetails

```
import com.amazonaws.services.health.model.DescribeEventDetailsRequest;
import com.amazonaws.services.health.model.DescribeEventDetailsResult;
import com.amazonaws.services.health.model.Event;
import com.amazonaws.services.health.model.EventDetails;

DescribeEventDetailsRequest describeEventDetailsRequest = new
DescribeEventDetailsRequest();
// set event ARN and local value

describeEventDetailsRequest.setEventArns(singletonList("arn:aws:health:us-
east-1::event/service/eventTypeCode/eventId"));
describeEventDetailsRequest.setLocale("en-US");
filter.setEventArns
DescribeEventDetailsResult describeEventDetailsResult =
awsHealthClient.describeEventDetails(request);
EventDetails eventDetail = describeEventDetailsResult.getSuccessfulSet().get(0);

// check event-related fields
Event event = eventDetail.getEvent();
System.out.println(event.getService());
System.out.println(event.getRegion());
System.out.println(event.getAvailabilityZone());
System.out.println(event.getStartTime());
System.out.println(event.getEndTime());

// print out event description
System.out.println(eventDetail.getEventDescription().getLatestDescription());
```

DescribeAffectedEntities

```
import com.amazonaws.services.health.model.AffectedEntity;
import com.amazonaws.services.health.model.DateTimeRange;
import com.amazonaws.services.health.model.DescribeAffectedEntitiesRequest;
import
com.amazonaws.services.health.model.DescribeAffectedEntitiesResult;

DescribeAffectedEntitiesRequest request = new DescribeAffectedEntitiesRequest();
EntityFilter filter = new EntityFilter();

filter.setEventArns(singletonList("arn:aws:health:us-
east-1::event/service/eventTypeCode/eventId"));
```

```
DescribeAffectedEntitiesResult response =
awsHealthClient.describeAffectedEntities(request);

for (AffectedEntity affectedEntity: response.getEntities()) {
    System.out.println(affectedEntity.getEntityValue());
    System.out.println(affectedEntity.getAwsAccountId());
    System.out.println(affectedEntity.getEntityArn());
}
```

DescribeEntityAggregates

```
import com.amazonaws.services.health.model.DescribeEntityAggregatesRequest;
import com.amazonaws.services.health.model.DescribeEntityAggregatesResult;
import com.amazonaws.services.health.model.EntityAggregate;

DescribeEntityAggregatesRequest request = new DescribeEntityAggregatesRequest();

request.setEventArns(singletonList("arn:aws:health:us-
east-1::event/service/eventTypeCode/eventId"));

DescribeEntityAggregatesResult response =
awsHealthClient.describeEntityAggregates(request);

for (EntityAggregate entityAggregate : response.getEntityAggregates()) {
    System.out.println(entityAggregate.getEventArn());
    System.out.println(entityAggregate.getCount());
}
```

Seguridad en AWS Health

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre AWS usted y usted. El [modelo de responsabilidad compartida](#) describe esto como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los [AWS programas](#) de de . Para obtener más información sobre los programas de cumplimiento aplicables AWS Health, consulte [AWS Servicios incluidos en el ámbito de aplicación por programa de conformidad y AWS servicios incluidos](#) .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza AWS Health. Los siguientes temas muestran cómo configurarlo AWS Health para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus AWS Health recursos.

Temas

- [Protección de datos en AWS Health](#)
- [Administración de identidades y accesos para AWS Health](#)
- [Inicio de sesión y supervisión AWS Health](#)
- [Validación de conformidad para AWS Health](#)
- [Resiliencia en AWS Health](#)
- [Seguridad de la infraestructura en AWS Health](#)
- [Análisis de configuración y vulnerabilidad en AWS Health](#)
- [Prácticas recomendadas de seguridad para AWS Health](#)

Protección de datos en AWS Health

El modelo de [responsabilidad AWS compartida modelo](#) se aplica a la protección de datos en AWS Health. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos los Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las [Preguntas frecuentes sobre la privacidad de datos](#). Para obtener información sobre la protección de datos en Europa, consulta la publicación de blog sobre el [Modelo de responsabilidad compartida de AWS y RGPD](#) en el [Blog de seguridad de AWS](#).

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Se utiliza SSL/TLS para comunicarse con AWS los recursos. Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte [Cómo trabajar con CloudTrail senderos](#) en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados que contienen Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulta [Estándar de procesamiento de la información federal \(FIPS\) 140-3](#).

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con AWS Health o Servicios de AWS utiliza la consola, la API o AWS CLI AWS SDKs. Cualquier dato que introduzca en etiquetas o campos

de formato libre utilizados para los nombres se pueden emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Cifrado de datos

Consulte la siguiente información sobre cómo se AWS Health cifran los datos.

El cifrado de datos se refiere a la protección de los datos mientras están en tránsito (mientras viajan del servicio a su AWS cuenta) y en reposo (mientras están almacenados en AWS los servicios). Puede proteger los datos en tránsito mediante seguridad de la capa de transporte (TLS) o en reposo mediante el cifrado del cliente.

AWS Health no registra la información de identificación personal (PII), como las direcciones de correo electrónico o los nombres de los clientes, en los eventos.

Cifrado en reposo

Todos los datos almacenados por AWS Health están cifrados en reposo.

Cifrado en tránsito

Todos los datos enviados y recibidos AWS Health se cifran en tránsito.

Administración de claves

AWS Health no admite claves de cifrado administradas por el cliente para los datos cifrados en la AWS nube.

Administración de identidades y accesos para AWS Health

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos. AWS Health La IAM es una Servicio de AWS opción que puede utilizar sin coste adicional.

Temas

- [Público](#)
- [Autenticación con identidades](#)
- [Administración del acceso con políticas](#)
- [¿Cómo AWS Health funciona con IAM](#)
- [AWS Health ejemplos de políticas basadas en la identidad](#)
- [Solución de problemas AWS Health de identidad y acceso](#)
- [Cómo utilizar roles vinculados a servicios de AWS Health](#)
- [AWS políticas gestionadas para AWS Health](#)

Público

La forma de usar AWS Identity and Access Management (IAM) varía según la función que desempeñas:

- Usuario del servicio: solicita permisos al administrador si no se puede acceder a las características (consulte [Solución de problemas AWS Health de identidad y acceso](#)).
- Administrador del servicio: determina el acceso de los usuarios y envía las solicitudes de permiso (consulte [¿Cómo AWS Health funciona con IAM](#)).
- Administrador de IAM: escribe las políticas para administrar el acceso (consulte [AWS Health ejemplos de políticas basadas en la identidad](#)).

Autenticación con identidades

La autenticación es la forma en que inicias sesión AWS con tus credenciales de identidad. Debe autenticarse como usuario de Usuario raíz de la cuenta de AWS IAM o asumir una función de IAM.

Puede iniciar sesión como una identidad federada con las credenciales de una fuente de identidad, como AWS IAM Identity Center (IAM Identity Center), la autenticación de inicio de sesión único o las credenciales Google/Facebook. Para obtener más información sobre el inicio de sesión, consulte [Cómo iniciar sesión en la Cuenta de AWS](#) en la Guía del usuario de AWS Sign-In .

Para el acceso programático, AWS proporciona un SDK y una CLI para firmar criptográficamente las solicitudes. Para obtener más información, consulte [AWS Signature Version 4 para solicitudes de API](#) en la Guía del usuario de IAM.

AWS usuario raíz de la cuenta

Al crear una Cuenta de AWS, se comienza con una identidad de inicio de sesión denominada usuario Cuenta de AWS raíz, que tiene acceso completo a todos Servicios de AWS los recursos. Recomendamos encarecidamente que no utilice el usuario raíz para las tareas cotidianas. Para ver la lista completa de las tareas que requieren credenciales de usuario raíz, consulte [Tareas que requieren credenciales de usuario raíz](#) en la Guía del usuario de IAM.

Usuarios y grupos de IAM

Un [usuario de IAM](#) es una identidad con permisos específicos para una sola persona o aplicación. Recomendamos utilizar credenciales temporales en lugar de usuarios de IAM con credenciales a largo plazo. Para obtener más información, consulte [Exigir a los usuarios humanos que utilicen la federación con un proveedor de identidad para acceder AWS mediante credenciales temporales](#) en la Guía del usuario de IAM.

Un [grupo de IAM](#) especifica un conjunto de usuarios de IAM y facilita la administración de los permisos para grupos grandes de usuarios. Para obtener más información, consulte [Casos de uso para usuarios de IAM](#) en la Guía del usuario de IAM.

Roles de IAM

Un [rol de IAM](#) es una identidad con permisos específicos que proporciona credenciales temporales. Puede asumir un rol [cambiando de un rol de usuario a uno de IAM \(consola\)](#) o llamando a una AWS CLI operación de AWS API. Para obtener más información, consulte [Métodos para asumir un rol](#) en la Guía del usuario de IAM.

Las funciones de IAM son útiles para el acceso de usuarios federados, los permisos de usuario de IAM temporales, el acceso entre cuentas, el acceso entre servicios y las aplicaciones que se ejecutan en Amazon. EC2 Para obtener más información, consulte [Acceso a recursos entre cuentas en IAM](#) en la Guía del usuario de IAM.

Administración del acceso con políticas

El acceso se controla creando políticas y AWS adjuntándolas a identidades o recursos. Una política define los permisos cuando están asociados a una identidad o un recurso. AWS evalúa estas políticas cuando un director hace una solicitud. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre los documentos de políticas de JSON, consulte [Información general de políticas de JSON](#) en la Guía del usuario de IAM.

Mediante las políticas, los administradores especifican quién tiene acceso a qué, definiendo qué entidad principal puede realizar acciones sobre qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM crea políticas de IAM y las agrega a roles, que los usuarios pueden asumir posteriormente. Las políticas de IAM definen permisos independientemente del método que se utilice para realizar la operación.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de política de permisos JSON que asocia a una identidad (usuario, grupo o rol). Estas políticas controlan qué acciones pueden realizar las identidades, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte [Definición de permisos de IAM personalizados con políticas administradas por el cliente](#) en la Guía del usuario de IAM.

Las políticas basadas en identidad pueden ser políticas insertadas (incrustadas directamente en una sola identidad) o políticas administradas (políticas independientes asociadas a varias identidades). Para obtener información sobre cómo elegir entre políticas administradas e insertadas, consulte [Elegir entre políticas administradas y políticas insertadas](#) en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de políticas JSON que se asocian a un recurso. Son ejemplos las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Debe [especificar una entidad principal](#) en una política basada en recursos.

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

AWS Health apoya las condiciones basadas en los recursos. Puede especificar qué eventos de AWS Health pueden ver los usuarios. Por ejemplo, puedes crear una política que solo permita a un usuario de IAM acceder a EC2 eventos específicos de Amazon en AWS Health Dashboard.

Para obtener más información, consulte [Recursos](#).

Listas de control de acceso

Las listas de control de acceso (ACLs) controlan qué responsables (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios compatibles. AWS WAF ACLs Para obtener más información ACLs, consulte la [descripción general de la lista de control de acceso \(ACL\)](#) en la Guía para desarrolladores de Amazon Simple Storage Service.

AWS Health no es compatible ACLs.

Otros tipos de políticas

AWS admite tipos de políticas adicionales que pueden establecer los permisos máximos que conceden los tipos de políticas más comunes:

- Límites de permisos: establecen los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM. Para obtener más información, consulte [Límites de permisos para las entidades de IAM](#) en la Guía del usuario de IAM.
- Políticas de control de servicios (SCPs): especifican los permisos máximos para una organización o unidad organizativa en AWS Organizations. Para obtener más información, consulte [Políticas de control de servicios](#) en la Guía del usuario de AWS Organizations .
- Políticas de control de recursos (RCPs): establece los permisos máximos disponibles para los recursos de tus cuentas. Para obtener más información, consulte [Políticas de control de recursos \(RCPs\)](#) en la Guía del AWS Organizations usuario.
- Políticas de sesión: políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal para un rol o un usuario federado. Para obtener más información, consulte [Políticas de sesión](#) en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la [Lógica de evaluación de políticas](#) en la Guía del usuario de IAM.

¿Cómo AWS Health funciona con IAM

Antes de usar IAM para administrar el acceso AWS Health, debe comprender qué funciones de IAM están disponibles para su uso. AWS HealthPara obtener una visión general de cómo funcionan con IAM AWS Health y otros AWS servicios, consulte [AWS Servicios que funcionan con IAM en la Guía del usuario de IAM](#).

Temas

- [Políticas de AWS Health basadas en identidades](#)
- [Políticas de AWS Health basadas en recursos](#)
- [Autorización basada en etiquetas de AWS Health](#)
- [AWS Health Funciones de IAM](#)

Políticas de AWS Health basadas en identidades

Con las políticas basadas en identidad de IAM, puede especificar las acciones permitidas o denegadas y los recursos, además de las condiciones en las que se permiten o deniegan las acciones. AWS Health admite acciones, recursos y claves de condiciones específicos. Para obtener información sobre todos los elementos que utiliza en una política JSON, consulte [Referencia de los elementos de las políticas JSON de IAM](#) en la Guía del usuario de IAM.

Acciones

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Las acciones políticas AWS Health utilizan el siguiente prefijo antes de la acción:`health:`. Por ejemplo, para conceder a alguien permiso para ver información detallada sobre eventos específicos con la operación de la [DescribeEventDetails](#)API, debes incluir la `health:DescribeEventDetails` acción en la política.

Las declaraciones de política deben incluir un `NotAction` elemento `Action` o AWS Health define su propio conjunto de acciones que describen las tareas que puede realizar con este servicio.

Para especificar varias acciones de en una única instrucción, sepárelas con comas del siguiente modo.

```
"Action": [  
    "health:action1",  
    "health:action2"]
```

Puede utilizar caracteres comodín (*) para especificar varias acciones . Por ejemplo, para especificar todas las acciones que comiencen con la palabra **Describe**, incluya la siguiente acción.

```
"Action": "health:Describe*"
```

Para ver una lista de AWS Health acciones, consulte las [acciones definidas por AWS Health](#) en la Guía del usuario de IAM.

Recursos

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento **Resource** de la política JSON especifica el objeto u objetos a los que se aplica la acción. Como práctica recomendada, especifique un recurso utilizando el [Nombre de recurso de Amazon \(ARN\)](#). En el caso de las acciones que no admiten permisos por recurso, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Un AWS Health evento tiene el siguiente formato de nombre de recurso de Amazon (ARN).

```
arn:${Partition}:health:*::event/service/event-type-code/event-ID
```

Por ejemplo, para especificar el evento EC2_INSTANCE_RETIREMENT_SCHEDULED_ABC123-DEF456 en la instrucción, utilice el siguiente ARN.

```
"Resource": "arn:aws:health:*::event/EC2/EC2_INSTANCE_RETIREMENT_SCHEDULED/  
EC2_INSTANCE_RETIREMENT_SCHEDULED_ABC123-DEF456"
```

Para especificar todos los AWS Health eventos de Amazon EC2 que pertenecen a una cuenta específica, usa el comodín (*).

```
"Resource": "arn:aws:health:*::event/EC2/*/*"
```

Para obtener más información sobre el formato de ARNs, consulte [Amazon Resource Names \(ARNs\)](#) y [AWS Service Namespaces](#).

Algunas AWS Health acciones no se pueden realizar en un recurso específico. En dichos casos, debe utilizar el carácter comodín (*).

```
"Resource": "*"
```

AWS Health Las operaciones de la API pueden implicar varios recursos. Por ejemplo, la [DescribeEvents](#) operación devuelve información sobre los eventos que cumplen un criterio de filtro específico. Esto significa que un usuario de IAM debe tener permisos para ver este evento.

Para especificar varios recursos en una sola sentencia, sepárelos ARNs con comas.

```
"Resource": [  
    "resource1",  
    "resource2"
```

AWS Health solo admite permisos a nivel de recurso para eventos de estado y solo para las operaciones de la API [DescribeAffectedEntities](#) y [DescribeEventDetails](#) la API. Para obtener más información, consulte [Condiciones basadas en recursos y en acciones](#).

Para ver una lista de los tipos de AWS Health recursos y sus correspondientes ARNs, consulte [los recursos definidos por AWS Health](#) en la Guía del usuario de IAM. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte [Acciones definidas por AWS Health](#).

Claves de condición

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento Condition especifica cuándo se ejecutan las instrucciones en función de criterios definidos. Puede crear expresiones condicionales que utilizan [operadores de condición](#), tales como

igual o menor que, para que la condición de la política coincida con los valores de la solicitud. Para ver todas las claves de condición AWS globales, consulte las claves de [contexto de condición AWS globales](#) en la Guía del usuario de IAM.

AWS Health define su propio conjunto de claves de condición y también admite el uso de algunas claves de condición globales. Para ver todas las claves de condición AWS globales, consulte las claves de [contexto de condición AWS globales](#) en la Guía del usuario de IAM.

Las operaciones [DescribeAffectedEntities](#) y la [DescribeEventDetails](#) API admiten las claves de `health:service` condición `health:eventTypeCode` y.

Para ver una lista de claves de AWS Health condición, consulta las [claves de condición AWS Health](#) en la Guía del usuario de IAM. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte [Acciones definidas por AWS Health](#).

Ejemplos

Para ver ejemplos de políticas AWS Health basadas en la identidad, consulte. [AWS Health ejemplos de políticas basadas en la identidad](#)

Políticas de AWS Health basadas en recursos

Las políticas basadas en recursos son documentos de políticas de JSON que especifican qué acciones puede realizar un director específico en el AWS Health recurso y en qué condiciones. AWS Health admite políticas de permisos basadas en recursos para eventos de salud. Las políticas basadas en recursos le permiten otorgar permiso de uso a otras cuentas por recurso. También puede utilizar una política basada en recursos para permitir que un AWS servicio acceda a sus eventos.

AWS Health

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la [entidad principal de una política basada en recursos](#). Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso están en AWS cuentas diferentes, también debes conceder permiso a la entidad principal para acceder al recurso. Conceda permiso asociando a la entidad una política basada en identidades. Sin embargo, si la política basada en recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte [Cómo los roles de IAM difieren de las políticas basadas en recursos](#) en la Guía del usuario de IAM.

AWS Health solo admite políticas basadas en recursos para las operaciones de la [DescribeEventDetails](#) API [DescribeAffectedEntities](#) y de la API. Puede especificar estas acciones en una política para definir qué entidades principales (cuentas, usuarios, roles y usuarios federados) pueden realizar acciones en el evento. AWS Health

Ejemplos

Para ver ejemplos de políticas AWS Health basadas en recursos, consulte. [Condiciones basadas en recursos y en acciones](#)

Autorización basada en etiquetas de AWS Health

AWS Health no admite el etiquetado de los recursos ni el control del acceso en función de las etiquetas.

AWS Health Funciones de IAM

Un [rol de IAM](#) es una entidad de tu AWS cuenta que tiene permisos específicos.

Usar credenciales temporales con AWS Health

Puede utilizar credenciales temporales para iniciar sesión con federación, asumir un rol de IAM o asumir un rol de acceso entre cuentas. Las credenciales de seguridad temporales se obtienen llamando a operaciones de AWS STS API como [AssumeRole](#) o [GetFederationToken](#).

AWS Health admite el uso de credenciales temporales.

Roles vinculados a servicios

Los [roles vinculados a un servicio](#) permiten a AWS los servicios acceder a los recursos de otros servicios para completar una acción en tu nombre. Los roles vinculados a servicios aparecen en la cuenta de IAM y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

AWS Health admite la integración de roles vinculados al servicio. AWS Organizations El rol vinculado a servicio se denomina `AWSServiceRoleForHealth_Organizations`. Esta función incluye la política gestionada por [Health_OrganizationsServiceRolePolicy](#) AWS . La política AWS gestionada permite acceder AWS Health a los eventos de salud desde otras AWS cuentas de la organización.

Puede usar la [EnableHealthServiceAccessForOrganization](#) operación para crear el rol vinculado al servicio en la cuenta. Sin embargo, si desea deshabilitar esta función, primero debe llamar a la [DisableHealthServiceAccessForOrganization](#) operación. A continuación, puede eliminar el rol a través

de la consola de IAM, la API de IAM o AWS Command Line Interface (AWS CLI). Para obtener más información, consulte [Uso de roles vinculados a servicios](#) en la Guía del usuario de IAM.

Para obtener más información, consulte [Aregar AWS Health eventos en todas las cuentas](#).

Roles de servicio

Esta característica permite que un servicio asuma un [rol de servicio](#) en su nombre. Este rol permite que el servicio obtenga acceso a los recursos de otros servicios para completar una acción en su nombre. Los roles de servicio aparecen en su cuenta de IAM y son propiedad de la cuenta. Esto significa que un administrador de IAM puede cambiar los permisos de este rol. Sin embargo, hacerlo podría deteriorar la funcionalidad del servicio.

AWS Health no admite funciones de servicio.

AWS Health ejemplos de políticas basadas en la identidad

De forma predeterminada, los usuarios y los roles de IAM no tienen permiso para crear, ver ni modificar recursos de AWS Health. Tampoco pueden realizar tareas con la API Consola de administración de AWS AWS CLI, o AWS . Un administrador de IAM debe crear políticas de IAM que concedan permisos a los usuarios y a los roles para realizar operaciones de la API concretas en los recursos especificados que necesiten. El administrador debe adjuntar esas políticas a los usuarios o grupos de IAM que necesiten esos permisos.

Para obtener información acerca de cómo crear una política basada en identidad de IAM con estos documentos de políticas JSON de ejemplo, consulte [Creación de políticas en la pestaña JSON](#) en la Guía del usuario de IAM.

Temas

- [Prácticas recomendadas relativas a políticas](#)
- [Mediante la consola de AWS Health](#)
- [Cómo permitir a los usuarios consultar sus propios permisos](#)
- [Acceder a la API AWS Health Dashboard y a la API AWS Health](#)
- [Condiciones basadas en recursos y en acciones](#)

Prácticas recomendadas relativas a políticas

Las políticas basadas en la identidad determinan si alguien puede crear AWS Health recursos de tu cuenta, acceder a ellos o eliminarlos. Estas acciones pueden generar costos adicionales para su

Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su Cuenta de AWS. Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las [políticas administradas por AWS](#) o las [políticas administradas por AWS para funciones de tarea](#) en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte [Políticas y permisos en IAM](#) en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo CloudFormation. Para obtener más información, consulte [Elementos de la política de JSON de IAM: Condición](#) en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte [Validación de políticas con el Analizador de acceso de IAM](#) en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte [Acceso seguro a la API con MFA](#) en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte [Prácticas recomendadas de seguridad en IAM](#) en la Guía del usuario de IAM.

Mediante la consola de AWS Health

Para acceder a la AWS Health consola, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los AWS Health recursos de su AWS cuenta. Si crea una política basada en identidad que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles de IAM) que tengan esa política.

Para garantizar que esas entidades puedan seguir utilizando la AWS Health consola, puede adjuntar la siguiente política AWS gestionada: [AWSHealthFullAccess](#).

La política de AWSHealthFullAccess concede a una entidad acceso completo a lo siguiente:

- Activa o desactiva la función de visualización de la AWS Health organización para todas las cuentas de una AWS organización
- El AWS Health Dashboard de la AWS Health consola
- AWS Health Operaciones y notificaciones de la API
- Consulta la información sobre las cuentas que forman parte de tu AWS organización
- Consulte las unidades organizativas (OU) de la cuenta de administración

Example : AWSHealthFullAccess

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "organizations:EnableAWSServiceAccess",  
        "organizations:DisableAWSServiceAccess"  
      ],  
      "Resource": "*",  
      "Condition": {  
        "StringEquals": {  
          "organizations:ServicePrincipal": "health.amazonaws.com"  
        }  
      }  
    }  
  ]  
}
```

```
},
{
  "Effect": "Allow",
  "Action": [
    "health:*",
    "organizations:DescribeAccount",
    "organizations>ListAccounts",
    "organizations>ListDelegatedAdministrators",
    "organizations>ListParents"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": "iam>CreateServiceLinkedRole",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "iam:AWSServiceName": "health.amazonaws.com"
    }
  }
}
]
```

 Note

También puede usar la política `Health_OrganizationsServiceRolePolicy` AWS administrada para ver los eventos de otras cuentas de su organización. AWS Health Para obtener más información, consulte [Cómo utilizar roles vinculados a servicios de AWS Health](#).

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realizan llamadas a la API AWS CLI o a la AWS API. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intenta realizar.

Para obtener más información, consulte [Adición de permisos a un usuario](#) en la Guía del usuario de IAM.

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o AWS .

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "ViewOwnUserInfo",  
      "Effect": "Allow",  
      "Action": [  
        "iam:GetUserPolicy",  
        "iam>ListGroupsForUser",  
        "iam>ListAttachedUserPolicies",  
        "iam>ListUserPolicies",  
        "iam GetUser"  
      ],  
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]  
    },  
    {  
      "Sid": "NavigateInConsole",  
      "Effect": "Allow",  
      "Action": [  
        "iam:GetGroupPolicy",  
        "iam:GetPolicyVersion",  
        "iam GetPolicy",  
        "iam>ListAttachedGroupPolicies",  
        "iam>ListGroupPolicies",  
        "iam>ListPolicyVersions",  
        "iam>ListPolicies",  
        "iam>ListUsers"  
      ],  
      "Resource": "*"  
    }  
  ]  
}
```

Acceder a la API AWS Health Dashboard y a la API AWS Health

AWS Health Dashboard Está disponible para todas las AWS cuentas. La AWS Health API solo está disponible para cuentas con un plan Business, Enterprise On-Ramp o Enterprise Support. Para obtener más información, consulte [Soporte](#).

Puede usar IAM para crear entidades (usuarios, grupos o roles) y, a continuación, conceder a esas entidades permisos de acceso a la API AWS Health Dashboard y a la AWS Health misma.

De forma predeterminada, los usuarios de IAM no tienen acceso a la API AWS Health Dashboard ni a la AWS Health misma. Para dar acceso a los usuarios a la AWS Health información de su cuenta, debe adjuntar las políticas de IAM a un único usuario, un grupo de usuarios o un rol. Para obtener más información, consulte [Identidades \(usuarios, grupos y roles\)](#) e [Información general sobre las políticas de IAM](#).

Después de crear los usuarios de IAM, puede asignarles contraseñas. Luego, pueden iniciar sesión en tu cuenta y ver la AWS Health información mediante una página de inicio de sesión específica de la cuenta. Para obtener más información, consulte [Cómo inician sesión los usuarios en la cuenta](#).

Note

Un usuario de IAM con permisos de visualización AWS Health Dashboard tiene acceso de solo lectura a la información de salud en todos los AWS servicios de la cuenta, que pueden incluir, entre otros, AWS recursos IDs como la EC2 instancia IDs de Amazon, las direcciones IP de las EC2 instancias y las notificaciones de seguridad generales.

Por ejemplo, si una política de IAM concede acceso únicamente a AWS Health Dashboard la AWS Health API, el usuario o rol al que se aplica la política puede acceder a toda la información publicada sobre los AWS servicios y los recursos relacionados, incluso si otras políticas de IAM no permiten ese acceso.

Puedes usar dos grupos de APIs for. AWS Health

- Cuentas individuales: puede utilizar operaciones como [DescribeEvents](#), por ejemplo, [DescribeEventDetails](#) obtener información sobre AWS Health los eventos de su cuenta.
- Cuenta de organización: puede utilizar operaciones como [DescribeEventsForOrganization](#), por ejemplo, [DescribeEventDetailsForOrganization](#) obtener información sobre AWS Health eventos para las cuentas que forman parte de su organización.

Para obtener más información sobre las operaciones de la API disponibles, consulte la [Referencia de la API de AWS Health](#).

Acciones individuales

Puede establecer el elemento `Action` de una política de IAM en `health:Describe*`. Esto permite el acceso a AWS Health Dashboard y AWS Health. AWS Health admite el control de acceso a los eventos en función del servicio `eventTypeCode` and.

Describir el acceso

Esta declaración de política otorga acceso a cualquiera de las operaciones de la `Describe*` AWS Health API AWS Health Dashboard y a cualquiera de ellas. Por ejemplo, un usuario de IAM con esta política puede acceder a la operación AWS Health Dashboard de AWS Health `DescribeEvents` API Consola de administración de AWS y llamar a ella.

Example : describir el acceso

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "health:Describe*"  
      ],  
      "Resource": "*"  
    }]  
}
```

Denegar el acceso

Esta declaración de política deniega el acceso a la AWS Health API AWS Health Dashboard y a la misma. Un usuario de IAM con esta política no puede ver ni llamar a ninguna de las operaciones de la AWS Health API. AWS Health Dashboard Consola de administración de AWS

Example : denegar el acceso

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Deny",  
      "Action": [  
        "health:*"  
      ],  
      "Resource": "*"  
    }]  
}
```

Vista organizativa

Si quieras habilitar la vista organizacional para AWS Health, debes permitir el acceso a las AWS Organizations acciones AWS Health y.

El elemento Action de una política de IAM debe incluir los siguientes permisos:

- `iam:CreateServiceLinkedRole`
- `organizations:EnableAWSServiceAccess`
- `organizations:DescribeAccount`
- `organizations:DisableAWSServiceAccess`
- `organizations>ListAccounts`
- `organizations>ListDelegatedAdministrators`
- `organizations>ListParents`

Para conocer los permisos exactos necesarios para cada una de ellas APIs, consulte [las acciones definidas por AWS Health APIs y las notificaciones](#) en la Guía del usuario de IAM.

Note

Debe utilizar las credenciales de la cuenta de administración para que una organización pueda acceder a la AWS Health APIs . AWS Organizations Para obtener más información, consulte [Aregar AWS Health eventos en todas las cuentas](#).

Cómo permitir el acceso a la vista organizativa de AWS Health

Esta declaración de política otorga acceso a todas AWS Health las AWS Organizations acciones que necesite para la función de visualización de la organización.

Example : Permitir el acceso a la vista de la AWS Health organización

JSON

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "organizations:EnableAWSServiceAccess",  
                "organizations:DisableAWSServiceAccess"  
            ],  
            "Resource": "*",  
            "Condition": {  
                "StringEquals": {  
                    "organizations:ServicePrincipal": "health.amazonaws.com"  
                }  
            }  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "health:*",  
                "organizations:DescribeAccount",  
                "organizations>ListAccounts",  
                "organizations>ListDelegatedAdministrators",  
                "organizations>ListParents"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

```
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": "iam:CreateServiceLinkedRole",
        "Resource": "arn:aws:iam::*:role/aws-service-role/
health.amazonaws.com/AWSServiceRoleForHealth*"
    }
]
```

Cómo restringir el acceso a la vista organizativa de AWS Health

Esta declaración de política deniega el acceso a AWS Organizations las acciones, pero permite el acceso a AWS Health las acciones de una cuenta individual.

Example : Denegar el acceso a la vista de la AWS Health organización

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "health:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "health.amazonaws.com"
                }
            }
        }
    ]
}
```

```
  },
  {
    "Effect": "Deny",
    "Action": [
      "organizations:DescribeAccount",
      "organizations>ListAccounts",
      "organizations>ListDelegatedAdministrators",
      "organizations>ListParents"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Deny",
    "Action": "iam>CreateServiceLinkedRole",
    "Resource": "arn:aws:iam::*:role/aws-service-role/
health.amazonaws.com/AWSServiceRoleForHealth*"
  }
]
```

 Note

Si el usuario o el grupo al que quieras conceder permisos ya tiene una política de IAM, puedes añadir la declaración AWS Health de política específica a esa política.

Condiciones basadas en recursos y en acciones

AWS Health admite [las condiciones de IAM para las operaciones](#) de API [DescribeAffectedEntities](#) [DescribeEventDetails](#) de IAM. Puede usar condiciones basadas en recursos y acciones para restringir los eventos que la AWS Health API envía a un usuario, grupo o rol.

Para ello, actualice el bloque `Condition` de la política de IAM o establezca el elemento `Resource`. Puedes usar [las condiciones de cadena](#) para restringir el acceso en función de determinados campos de AWS Health eventos.

Puedes usar los siguientes campos al especificar un AWS Health evento en tu política:

- `eventTypeCode`
- `service`

Notas

- Las operaciones [DescribeAffectedEntities](#) y la [DescribeEventDetails](#) API admiten permisos a nivel de recursos. Por ejemplo, puede crear una política para permitir o rechazar eventos específicos de AWS Health .
- Las operaciones [DescribeAffectedEntitiesForOrganization](#) y la [DescribeEventDetailsForOrganization](#) API no admiten permisos a nivel de recursos.
- Para obtener más información, consulta [las acciones, los recursos y las claves de condición y las AWS Health APIs notificaciones](#) en la Referencia de autorización de servicios.

Example : condición basada en acciones

Esta declaración de política concede el acceso a AWS Health Dashboard las operaciones de la AWS Health `Describe*` API, pero deniega el acceso a cualquier AWS Health evento relacionado con Amazon EC2.

JSON

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "health:Describe*",  
            "Resource": "*"  
        },  
        {  
            "Effect": "Deny",  
            "Action": [  
                "health:DescribeAffectedEntities",  
                "health:DescribeEventDetails"  
            ],  
            "Resource": "*",  
            "Condition": {  
                "StringEquals": {  
                    "health:service": "EC2"  
                }  
            }  
        }  
    ]  
}
```

```
        }
    }
]
```

Example : condición basada en recursos

La política siguiente tiene el mismo efecto, pero utiliza el elemento **Resource** en su lugar.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "health:Describe*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": [
        "health:DescribeEventDetails",
        "health:DescribeAffectedEntities"
      ],
      "Resource": "arn:aws:health:*::event/EC2/*/*"
    }
  ]
}
```

Example : eventTypeCode condición

Esta declaración de política concede el acceso a AWS Health Dashboard las operaciones de la AWS Health **Describe*** API, pero deniega el acceso a cualquier AWS Health evento **eventTypeCode** que coincida **AWS_EC2_***.

JSON

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "health:Describe*",  
            "Resource": "*"  
        },  
        {  
            "Effect": "Deny",  
            "Action": [  
                "health:DescribeAffectedEntities",  
                "health:DescribeEventDetails"  
            ],  
            "Resource": "*",  
            "Condition": {  
                "StringLike": {  
                    "health:eventTypeCode": "AWS_EC2_**"  
                }  
            }  
        }  
    ]  
}
```

⚠ Important

Si llamas a las [DescribeEventDetails](#) operaciones [DescribeAffectedEntities](#) and y no tienes permiso para acceder al AWS Health evento, aparece el `AccessDeniedException` error. Para obtener más información, consulte [Solución de problemas AWS Health de identidad y acceso](#).

Solución de problemas AWS Health de identidad y acceso

Utilice la siguiente información para diagnosticar y solucionar los problemas habituales que pueden surgir al trabajar con una AWS Health IAM.

Temas

- [No estoy autorizado a realizar ninguna acción en AWS Health](#)
- [No estoy autorizado a realizar iam: PassRole](#)
- [Quiero ver mis claves de acceso](#)
- [Soy administrador y quiero permitir que otras personas accedan AWS Health](#)
- [Quiero permitir que personas ajenas a mi AWS cuenta accedan a mis AWS Health recursos](#)

No estoy autorizado a realizar ninguna acción en AWS Health

Si Consola de administración de AWS le indica que no está autorizado a realizar una acción, debe ponerse en contacto con su administrador para obtener ayuda. El administrador es la persona que le facilitó el nombre de usuario y la contraseña.

El `AccessDeniedException` error aparece cuando un usuario no tiene permiso para usar AWS Health Dashboard las operaciones de la AWS Health API.

En este caso, el administrador del usuario debe actualizar la política para permitir su acceso.

La AWS Health API requiere un plan Business, Enterprise On-Ramp o Enterprise Support de [AWS Support](#). Si llama a la API de AWS Health desde una cuenta que no tenga un plan de soporte Business, Enterprise On-Ramp o Enterprise, se devuelve el código de error siguiente: `SubscriptionRequiredException`.

No estoy autorizado a realizar iam: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, las políticas deben actualizarse a fin de permitirle pasar un rol a AWS Health.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir la función al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en AWS Health. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:  
iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero ver mis claves de acceso

Después de crear sus claves de acceso de usuario de IAM, puede ver su ID de clave de acceso en cualquier momento. Sin embargo, no puede volver a ver su clave de acceso secreta. Si pierde la clave de acceso secreta, debe crear un nuevo par de claves de acceso.

Las claves de acceso se componen de dos partes: un ID de clave de acceso (por ejemplo, AKIAIOSFODNN7EXAMPLE) y una clave de acceso secreta (por ejemplo, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY). El ID de clave de acceso y la clave de acceso secreta se utilizan juntos, como un nombre de usuario y contraseña, para autenticar sus solicitudes. Administre sus claves de acceso con el mismo nivel de seguridad que para el nombre de usuario y la contraseña.

Important

No proporcione las claves de acceso a terceros, ni siquiera para que lo ayuden a [buscar el ID de usuario canónico](#). De este modo, podrías dar a alguien acceso permanente a tu Cuenta de AWS.

Cuando crea un par de claves de acceso, se le pide que guarde el ID de clave de acceso y la clave de acceso secreta en un lugar seguro. La clave de acceso secreta solo está disponible en el momento de su creación. Si pierde la clave de acceso secreta, debe agregar nuevas claves de acceso a su usuario de IAM. Puede tener un máximo de dos claves de acceso. Si ya cuenta con dos, debe eliminar un par de claves antes de crear una nueva. Para consultar las instrucciones, consulte [Administración de claves de acceso](#) en la Guía del usuario de IAM.

Soy administrador y quiero permitir que otras personas accedan AWS Health

Para permitir el acceso de otras personas AWS Health, debes conceder permiso a las personas o aplicaciones que necesitan acceso. Si usa AWS IAM Identity Center para administrar las personas y las aplicaciones, debe asignar conjuntos de permisos a los usuarios o grupos para definir su nivel de

acceso. Los conjuntos de permisos crean políticas de IAM y las asignan a los roles de IAM asociados a la persona o aplicación de forma automática. Para obtener más información, consulte la sección [Conjuntos de permisos](#) en la Guía del usuario de AWS IAM Identity Center .

Si no utiliza IAM Identity Center, debe crear entidades de IAM (usuarios o roles) para las personas o aplicaciones que necesitan acceso. A continuación, debe asociar una política a la entidad que le conceda los permisos correctos en AWS Health. Una vez concedidos los permisos, proporcione las credenciales al usuario o al desarrollador de la aplicación. Utilizarán esas credenciales para acceder a AWS. Para obtener más información sobre la creación de usuarios, grupos, políticas y permisos de IAM, consulte [Identidades de IAM](#) y [Políticas y permisos en IAM](#) en la Guía del usuario de IAM.

Quiero permitir que personas ajenas a mi AWS cuenta accedan a mis AWS Health recursos

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admiten políticas basadas en recursos o listas de control de acceso (ACLs), puedes usar esas políticas para permitir que las personas accedan a tus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si AWS Health es compatible con estas funciones, consulte [¿Cómo AWS Health funciona con IAM](#)
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte [Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en](#) la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo [proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros](#) en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte [Proporcionar acceso a usuarios autenticados externamente \(federación de identidades\)](#) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte [Acceso a recursos entre cuentas en IAM](#) en la Guía del usuario de IAM.

Cómo utilizar roles vinculados a servicios de AWS Health

AWS Health [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 Health Los roles vinculados a servicios están predefinidos por AWS Health e incluyen todos los permisos que el servicio requiere para llamar a otros Servicios de AWS en su nombre.

Puede utilizar un rol vinculado a un servicio para configurarlo y evitar tener que añadir manualmente AWS Health los permisos necesarios. AWS Health define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo AWS Health puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se puede asociar a ninguna otra entidad de IAM.

Permisos de roles vinculados a servicios de AWS Health

AWS Health tiene dos funciones vinculadas al servicio:

- [AWSServiceRoleForHealth_Organizations](#)— Este rol confía en que AWS Health (health.amazonaws.com) asumirá el rol al que accedes Servicios de AWS por ti. Esta función incluye la política Health_OrganizationsServiceRolePolicy AWS gestionada.
- [AWSServiceRoleForHealth_EventProcessor](#)— Este rol confía en que el director del AWS Health servicio (event-processor.health.amazonaws.com) asumirá el rol por usted. Esta función incluye la política AWSHealth_EventProcessorServiceRolePolicy AWS gestionada. El director del servicio utiliza la función para crear una regla EventBridge gestionada por Amazon para la detección y respuesta a AWS incidentes. Esta regla es la infraestructura que necesitas Cuenta de AWS para enviar la información sobre los cambios de estado de alarma desde tu cuenta a AWS Health.

Para obtener más información sobre las políticas AWS administradas, consulte[AWS políticas gestionadas para AWS Health](#).

Creación de un rol vinculado a un servicio de AWS Health

No necesita crear un rol vinculado a un servicio AWSServiceRoleForHealth_Organizations. Al llamar a la [EnableHealthServiceAccessForOrganization](#)operación, AWS Health crea este rol vinculado al servicio en la cuenta por usted.

Usted debe crear manualmente el rol vinculado al servicio `AWSServiceRoleForHealth_EventProcessor` en su cuenta. Para obtener más información, consulte [Creating a service-linked role](#) en la Guía del usuario de IAM.

Modificación de un rol vinculado a servicios de AWS Health

AWS Health no le permite editar el rol vinculado al servicio. Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. Sin embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte [Editar un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Eliminación de un rol vinculado a un servicio de AWS Health

Para eliminar el `AWSServiceRoleForHealth_Organizations` rol, primero debe llamar a la [DisableHealthServiceAccessForOrganization](#) operación. A continuación, puede eliminar el rol a través de la consola de IAM, la API de IAM o AWS Command Line Interface (AWS CLI).

Para eliminar el `AWSServiceRoleForHealth_EventProcessor` rol, ponte en contacto con ellos AWS Support y pídeles que excluyan tus cargas de trabajo del área de Detección y Respuesta a AWS Incidentes. Una vez finalizado este proceso, puede eliminar cualquiera de los roles a través de la consola de IAM, la API de IAM o AWS CLI.

Información relacionada

Para obtener más información, consulte [Uso de roles vinculados a servicios](#) en la Guía del usuario de IAM.

AWS políticas gestionadas para AWS Health

Una política AWS administrada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir [políticas administradas por el cliente](#) específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte [Políticas administradas por AWS](#) en la Guía del usuario de IAM.

AWS Health tiene las siguientes políticas gestionadas.

Contenido

- [Política administrada de AWS : AWSHealth_EventProcessorServiceRolePolicy](#)
- [Política administrada de AWS : Health_OrganizationsServiceRolePolicy](#)
- [AWS política gestionada: AWSHealthFullAccess](#)
- [AWS Health actualizaciones de las políticas AWS gestionadas](#)

Política administrada de AWS : AWSHealth_EventProcessorServiceRolePolicy

AWS Health utiliza la política [AWSHealth_EventProcessorServiceRolePolicy](#) AWS gestionada. Esta política administrada se adjunta al rol vinculado al servicio de `AWSServiceRoleForHealth_EventProcessor`. La política permite al rol vinculado al servicio completar acciones en su lugar. No puede adjuntar esta política a sus entidades de IAM. Para obtener más información, consulte [Cómo utilizar roles vinculados a servicios de AWS Health](#).

La política gestionada tiene los siguientes permisos para permitir el acceso AWS Health a la EventBridge regla de Amazon para la detección y respuesta a AWS incidentes.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `events`— Describe y elimina EventBridge las reglas, y describe y actualiza los objetivos de esas reglas.

JSON

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Condition": {  
                "StringEquals": {"events:ManagedBy": "event-  
processor.health.amazonaws.com"}  
            },  
            "Action": [  
                "events:DeleteRule",  
                "events:RemoveTargets",  
                "events:PutTargets",  
                "events:PutRule"  
            ],  
            "Resource": "*",  
            "Effect": "Allow"  
        },  
        {  
            "Action": [  
                "events>ListTargetsByRule",  
                "events:DescribeRule"  
            ],  
            "Resource": "*",  
            "Effect": "Allow"  
        }  
    ]  
}
```

Para obtener una lista de los cambios en la política, consulte [AWS Health actualizaciones de las políticas AWS gestionadas](#).

Política administrada de AWS : Health_OrganizationsServiceRolePolicy

AWS Health utiliza la política [Health_OrganizationsServiceRolePolicy](#) AWS gestionada. Esta política administrada se adjunta al rol vinculado al servicio de AWS `AWSServiceRoleForHealth_Organizations`. La política permite al rol vinculado al servicio completar acciones en su lugar. No puede adjuntar esta política a sus entidades de IAM. Para obtener más información, consulte [Cómo utilizar roles vinculados a servicios de AWS Health](#).

Esta política otorga permisos que permiten acceder AWS Health a los AWS Organizations detalles necesarios para la vista Organizacional de Salud.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- organizations— Describe las cuentas de AWS Organizations Organizations y las Servicios de AWS que se pueden usar con ellas.

JSON

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "organizations>ListAccounts",  
                "organizations>ListAWSAccessForOrganization",  
                "organizations>ListDelegatedAdministrators",  
                "organizations>DescribeOrganization",  
                "organizations>DescribeAccount"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

Para obtener una lista de los cambios en la política, consulte [AWS Health actualizaciones de las políticas AWS gestionadas](#).

AWS política gestionada: AWSHealthFullAccess

AWS Health utiliza la política [AWSHealthFullAccess](#) AWS gestionada. La política concede a las entidades (usuarios o roles de IAM) acceso a la AWS Health consola. Para obtener más información, consulte [Mediante la consola de AWS Health](#).

Detalles de los permisos

Esta política incluye los siguientes permisos.

- **organizations**— Activa o desactiva la función de visualización de la AWS Health organización para todas las cuentas de una AWS organización y consulta las unidades organizativas (OU) de la cuenta de administración
- **health**— Acceso a las operaciones y notificaciones de la AWS Health API
- **iam**: crea un rol de IAM que está vinculado a un servicio de AWS Health

JSON

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "OrganizationWriteAccess",  
            "Effect": "Allow",  
            "Action": [  
                "organizations:EnableAWSServiceAccess",  
                "organizations:DisableAWSServiceAccess"  
            ],  
            "Resource": "*",  
            "Condition": {  
                "StringEquals": {  
                    "organizations:ServicePrincipal": "health.amazonaws.com"  
                }  
            }  
        },  
        {  
            "Sid": "HealthFullAccess",  
            "Effect": "Allow",  
            "Action": [  
                "health:*",  
                "organizations:DescribeAccount",  
                "organizations>ListAccounts",  
                "organizations>ListDelegatedAdministrators",  
                "organizations>ListParents"  
            ],  
            "Resource": "*"  
        },  
        {  
            "Sid": "HealthReadOnlyAccess",  
            "Effect": "Allow",  
            "Action": [  
                "organizations:ListAccounts",  
                "organizations:ListDelegatedAdministrators",  
                "organizations:ListParents"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

```
    {
        "Sid": "ServiceLinkAccess",
        "Effect": "Allow",
        "Action": "iam:CreateServiceLinkedRole",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "iam:AWSServiceName": "health.amazonaws.com"
            }
        }
    }
]
```

Para obtener una lista de los cambios en la política, consulte [AWS Health actualizaciones de las políticas AWS gestionadas](#).

AWS Health actualizaciones de las políticas AWS gestionadas

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas AWS Health desde que este servicio comenzó a rastrear estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de [Historial de documentos para AWS Health](#).

En la siguiente tabla se describen las actualizaciones importantes de las políticas AWS Health administradas desde el 13 de enero de 2022.

AWS Health

Cambio	Descripción	Fecha
AWS política gestionada: AWSHealthFullAccess	AWS Health ha ampliado la AWSHealth FullAccess política a todas AWS GovCloud (US) Regions las regiones de China.	16 de octubre de 2023

Cambio	Descripción	Fecha
<u>Política administrada de AWS : Health_OrganizationsServiceRolePolicy</u> : actualización de una política existente	AWS Health agregó nuevas AWS Organizations acciones para permitir que la función vinculada al servicio describa las cuentas y los AWS servicios con los que se puede utilizar. AWS Organizations	19 de julio de 2023
Registro de cambios publicado	Registro de cambios de las políticas AWS Health gestionadas.	13 de enero de 2023

Inicio de sesión y supervisión AWS Health

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de AWS Health y las demás soluciones. AWS proporciona las siguientes herramientas de supervisión para observar AWS Health, informar cuando algo va mal y tomar las medidas necesarias:

- Amazon CloudWatch monitorea tus AWS recursos y las aplicaciones en las que AWS ejecuta en tiempo real. Puede recopilar métricas y realizar un seguimiento de las métricas, crear paneles personalizados y definir alarmas que le advierten o que toman medidas cuando una métrica determinada alcanza el umbral que se especifique. Por ejemplo, puede CloudWatch hacer un seguimiento del uso de la CPU u otras métricas de sus instancias de Amazon Elastic Compute Cloud (Amazon EC2) y lanzar nuevas instancias automáticamente cuando sea necesario. Para obtener más información, consulta la [Guía del CloudWatch usuario de Amazon](#).
- Amazon EventBridge ofrece un near-real-time flujo de eventos del sistema que describen los cambios en AWS los recursos. EventBridge permite la computación automatizada basada en eventos. Puede escribir reglas que vigilan determinados eventos y activen acciones automatizadas en otros servicios de AWS cuando se produzcan estos eventos. Para obtener más información, consulte [Monitorización de eventos AWS Health con Amazon EventBridge](#).
- AWS CloudTrail captura las llamadas a la API y los eventos relacionados realizados por su AWS cuenta o en su nombre y envía los archivos de registro a un depósito de Amazon Simple Storage Service (Amazon S3) que especifique. Puede identificar qué usuarios y cuentas llamaron AWS,

la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. Para obtener más información, consulte la [Guía del usuario de AWS CloudTrail](#).

Para obtener más información, consulte [Supervisión AWS Health](#).

Validación de conformidad para AWS Health

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](#).

Resiliencia en AWS Health

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. AWS Las regiones proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

AWS Health los eventos se almacenan y replican en varias zonas de disponibilidad. Este enfoque garantiza que pueda acceder a ellos desde las operaciones de la AWS Health API AWS Health Dashboard o desde ellas. Puede ver AWS Health los eventos hasta 90 días después de que se produzcan.

Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte [Infraestructura AWS global](#).

Seguridad de la infraestructura en AWS Health

Como servicio gestionado, AWS Health está protegido por los procedimientos de seguridad de red AWS global que se describen en el documento técnico [Amazon Web Services: Overview of Security Processes](#).

Utiliza las llamadas a la API AWS publicadas para acceder a AWS Health través de la red. Los clientes deben ser compatibles con la seguridad de la capa de transporte (TLS) 1.0 o una versión posterior. Recomendamos TLS 1.2 o una versión posterior. Los clientes también deben ser compatibles con conjuntos de cifrado con confidencialidad directa total (PFS) tales como Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (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.

Análisis de configuración y vulnerabilidad en AWS Health

La configuración y los controles de TI son una responsabilidad compartida entre usted AWS y usted, nuestro cliente. Para obtener más información, consulte el [modelo de responsabilidad AWS compartida](#).

Prácticas recomendadas de seguridad para AWS Health

Consulte las siguientes prácticas recomendadas para trabajar con él AWS Health.

Otorgue AWS Health a los usuarios los permisos mínimos posibles

Para seguir el principio de privilegios mínimos, utilice el conjunto mínimo de permisos de la política de acceso para los usuarios y los grupos de . Por ejemplo, puede permitir que un usuario AWS Identity and Access Management (de IAM) acceda al AWS Health Dashboard. Sin embargo, puede no permitir que ese mismo usuario habilite o des habilite el acceso a AWS Organizations.

Para obtener más información, consulte [AWS Health ejemplos de políticas basadas en la identidad](#).

Vea el AWS Health Dashboard

AWS Health Dashboard Compruébelo con frecuencia para identificar los eventos que puedan afectar a su cuenta o a sus aplicaciones. Por ejemplo, puede recibir una notificación de evento sobre sus recursos, como una instancia de Amazon Elastic Compute Cloud (Amazon EC2) que deba actualizarse.

Para obtener más información, consulte [Introducción al Panel de AWS Health](#).

Intégralo AWS Health con Amazon Chime o Slack

Puede integrarlo AWS Health con sus herramientas de chat. Esta integración te permite a ti y a tu equipo recibir notificaciones sobre AWS Health los eventos en tiempo real. Para obtener más información, consulta las [AWS Health herramientas](#) en GitHub.

Supervise los AWS Health eventos

Puede integrarse AWS Health con Amazon CloudWatch Events para crear reglas para eventos específicos. Cuando CloudWatch Events detecta un evento que coincide con su regla, se le notifica y, a continuación, puede tomar medidas. CloudWatch Los eventos y eventos son específicos de una región, por lo que debe configurar este servicio en la región en la que reside su aplicación o infraestructura.

En algunos casos, no se puede determinar la región del AWS Health evento. Si esto ocurre, el evento aparece en la región Este de EE. UU. (Norte de Virginia) de forma predeterminada. Puedes configurar CloudWatch eventos en esta región para asegurarte de supervisarlos.

Para obtener más información, consulte [Monitorización de eventos AWS Health con Amazon EventBridge](#).

Agregar AWS Health eventos en todas las cuentas

De forma predeterminada, se puede utilizar AWS Health para ver los AWS Health eventos de una sola AWS cuenta. Si la utilizas AWS Organizations, también puedes ver AWS Health los eventos de forma centralizada en toda la organización. Esta característica proporciona acceso a la misma información que las operaciones de una sola cuenta. Puede usar filtros para ver los eventos en AWS regiones, cuentas y servicios específicos.

Puede agregar eventos para identificar cuentas de su organización afectadas por un evento operativo o recibir notificaciones de vulnerabilidades de seguridad. Puede luego utilizar esta información para administrar y automatizar de forma proactiva eventos de mantenimiento de recursos en su organización. Utilice esta función para mantenerse informado de los próximos cambios en los AWS servicios que puedan requerir actualizaciones o cambios de código.

Se recomienda utilizar la función de [administrador delegado](#) para delegar el acceso a la vista AWS Health organizacional a la cuenta de un miembro. Esto facilita a los equipos operativos el acceso a los AWS Health eventos de su organización. La característica de administrador delegado le permite mantener restringida su cuenta de administración y, al mismo tiempo, proporciona a los equipos la visibilidad que necesitan para actuar a partir de eventos de AWS Health .

Important

- AWS Health los eventos que se enviaron para las cuentas de su organización aparecerán en la vista de la organización mientras el evento esté disponible (hasta 90 días), incluso si una o más de esas cuentas abandonan la organización.
- Los eventos organizativos están disponibles durante 90 días antes de que se eliminen. Esta cuota no se puede aumentar.

Requisitos previos

Antes de utilizar la vista organizativa, debe:

- Formar parte de una organización con [todas las características](#) habilitadas.
- Inicie sesión en la cuenta de administración como usuario AWS Identity and Access Management (IAM) o asuma una función de IAM.

También puede iniciar sesión como usuario raíz (no es recomendable hacerlo) en la cuenta de administración de su organización. Para obtener más información, consulte [Bloquear las claves de acceso del usuario raíz de la AWS cuenta](#) en la Guía del usuario de IAM.

- Si inicia sesión como usuario de IAM, utilice una política de IAM que conceda acceso a AWS Health y a acciones de las organizaciones, como la política de [AWSHealthFullAccess](#). Para obtener más información, consulte [AWS Health ejemplos de políticas basadas en la identidad](#).

Temas

- [Habilitación de la vista organizativa](#)
- [Visualización de una vista organizativa](#)
- [Deshabilitación de la vista organizativa](#)
- [Administración de vistas de administrador delegado para una organización](#)

Habilitación de la vista organizativa

Puede usar la AWS Health consola para obtener una vista centralizada de los eventos de salud en su AWS organización.

La vista organizativa está disponible en la AWS Health consola para todos los AWS Support planes sin costo adicional.

 Note

Si desea permitir que los usuarios accedan a esta característica en la cuenta de administración, deben tener permisos como los de la política de [AWSHealthFullAccess](#). Para obtener más información, consulte [AWS Health ejemplos de políticas basadas en la identidad](#).

Enabling organizational view (Console)

Puede activar la vista organizativa desde la AWS Health consola. Debe iniciar sesión en la cuenta de administración de su AWS organización.

Para ver el AWS Health panel de control de su organización

1. Abre tu AWS Health panel de control en <https://health.aws.com/health/casa>.
2. En el panel de navegación, en Your organization health, elija Configurations.
3. En la página de Enable organizational view, elija Enable organizational view.
4. (Opcional) Si quieras realizar cambios en tus AWS organizaciones, como crear unidades organizativas (OUs), selecciona Administrar AWS Organizations.

Para obtener más información, consulte el [Cómo empezar a usar AWS Organizations](#) en la Guía del usuario de AWS Organizations .

Notas

- Cuando habilitas la vista AWS Health organizativa, el proceso inicial de carga de la cuenta se ejecuta en segundo plano y puede tardar varios minutos en completarse. Puedes cerrar la AWS Health consola y volver más tarde, ya que no necesitas esperar a que finalice el proceso. Los eventos de salud históricos (aquellos que se crearon antes de activar la función) pueden tardar hasta 24 horas en aparecer en la vista de la organización.
- Si tienes un plan Business, Enterprise On-Ramp o Enterprise Support, puedes llamar a la operación de la [DescribeHealthServiceStatusForOrganization](#) API para comprobar el estado del proceso.
- Al habilitar esta función, el rol `AWSServiceRoleForHealth_Organizations` vinculado al servicio con la política `Health_OrganizationsServiceRolePolicy` AWS administrada se aplica a la cuenta de administración de la organización. Para obtener más información, consulte [Cómo utilizar roles vinculados a servicios de AWS Health](#).

Enabling organizational view (CLI)

Puede habilitar la vista de la organización mediante la operación de [EnableHealthServiceAccessForOrganization](#) API.

Puedes usar el AWS Command Line Interface (AWS CLI) o tu propio código para llamar a esta operación.

Note

- Debe tener un plan [Business](#), [Enterprise On-Ramp](#) o [Enterprise](#) Support para llamar a la AWS Health API.
- Debe usar el punto de conexión de la región Este de EE. UU. (Norte de Virginia).

Example

El siguiente AWS CLI comando habilita esta función desde su AWS cuenta. Puede utilizar este comando desde la cuenta de administración o desde una cuenta que pueda asumir el rol con los permisos necesarios.

```
aws health enable-health-service-access-for-organization --region us-east-1
```

Los siguientes ejemplos de código llaman a la operación [EnableHealthServiceAccessForOrganizationAPI](#).

Python

```
import boto3

client = boto3.client('health', region_name='us-east-1')

response = client.enable_health_service_access_for_organization()

print(response)
```

Java

Puede usar el AWS SDK de la versión Java 2.0 en el siguiente ejemplo.

```
import software.amazon.awssdk.services.health.HealthClient;
import software.amazon.awssdk.services.health.HealthClientBuilder;

import software.amazon.awssdk.services.health.model.ConcurrentModificationException;
import
software.amazon.awssdk.services.health.model.EnableHealthServiceAccessForOrganizationRequest
import
software.amazon.awssdk.services.health.model.EnableHealthServiceAccessForOrganizationResponse
```

```
import software.amazon.awssdk.services.health.model.DescribeHealthServiceStatusForOrganizationRequest;
import software.amazon.awssdk.services.health.model.DescribeHealthServiceStatusForOrganizationResponse;

import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;

import software.amazon.awssdk.regions.Region;

public class EnableHealthServiceAccessDemo {
    public static void main(String[] args) {
        HealthClient client = HealthClient.builder()
            .region(Region.US_EAST_1)
            .credentialsProvider(
                DefaultCredentialsProvider.builder().build()
            )
            .build();

        try {
            DescribeHealthServiceStatusForOrganizationResponse statusResponse =
client.describeHealthServiceStatusForOrganization(
                DescribeHealthServiceStatusForOrganizationRequest.builder().build()
            );

            String status =
statusResponse.healthServiceAccessStatusForOrganization();
            if ("ENABLED".equals(status)) {
                System.out.println("EnableHealthServiceAccessForOrganization already
enabled!");
                return;
            }

            client.enableHealthServiceAccessForOrganization(
                EnableHealthServiceAccessForOrganizationRequest.builder().build()
            );

            System.out.println("EnableHealthServiceAccessForOrganization is in
progress");
        } catch (ConcurrentModificationException cme) {
            System.out.println("EnableHealthServiceAccessForOrganization is already
in progress. Wait for the action to complete before trying again.");
        } catch (Exception e) {
            System.out.println("EnableHealthServiceAccessForOrganization FAILED: " +
e);
        }
    }
}
```

```
    }  
}  
}
```

Para obtener más información, consulte la [Guía para desarrolladores de AWS SDK para Java 2.0](#).

Al habilitar esta función, el [rol AWSServiceRoleForHealth_Organizations vinculado al servicio](#) con la política `Health_OrganizationsServiceRolePolicy` AWS administrada se aplica a la cuenta de administración de la organización.

 Note

La habilitación de esta característica es un proceso asíncrono y tardará un tiempo en completarse. Puede llamar a la [DescribeHealthServiceStatusForOrganization](#) operación para comprobar el estado del proceso.

Visualización de una vista organizativa

Puede usar la AWS Health consola para obtener una vista centralizada de los eventos de salud en su AWS organización.

La vista organizativa está disponible en la AWS Health consola para todos los AWS Support planes sin costo adicional.

 Note

Si desea permitir que los usuarios accedan a esta característica en la cuenta de administración, deben tener permisos como los de la política de [AWSHealthFullAccess](#).

Para obtener más información, consulte [AWS Health ejemplos de políticas basadas en la identidad](#).

Viewing organizational view events (Console)

Una vez habilitada la vista organizativa, AWS Health muestra los eventos de salud de todas las cuentas de la organización.

Cuando una cuenta se une a su organización, la agrega AWS Health automáticamente a la vista de la organización. Cuando una cuenta abandona la organización, los nuevos eventos

de esa cuenta ya no se registran en la vista organizativa. Sin embargo, los eventos existentes permanecen y todavía puede consultarlos con un límite de 90 días.

AWS conserva los datos de la política de la cuenta durante 90 días a partir de la fecha de entrada en vigor del cierre de la cuenta del administrador. Al final del período de 90 días, elimina AWS permanentemente todos los datos de la política de la cuenta.

- Si desea conservar los resultados por más de 90 días, puede archivar las políticas. También puedes usar una acción personalizada con una EventBridge regla para almacenar los resultados en un bucket de S3.
- Mientras se AWS conserven los datos de la política, al volver a abrir la cuenta cerrada, se la AWS reasignará como administradora del servicio y se recuperarán los datos de la política de servicio de la cuenta.
- Para obtener más información, consulte [Closing an account](#).

 **Important**

Para los clientes de las regiones: AWS GovCloud (US)

- Antes de cerrar la cuenta, realice una copia de seguridad y, luego, elimine los recursos de la cuenta. Ya no tendrá acceso a ellos después de cerrar la cuenta.

 **Note**

Al activar esta función, la AWS Health consola puede mostrar los eventos públicos desde el [AWS Health panel de control: estado del servicio](#) durante los últimos 7 días. Estos eventos públicos no son específicos de las cuentas de su organización. Eventos del AWS Health panel de control: el estado del servicio proporciona información pública sobre la disponibilidad regional de AWS los servicios.

Puede consultar los eventos organizativos en las siguientes páginas.

Problemas abiertos y recientes

Puede usar la pestaña Problemas abiertos y recientes para ver los eventos que podrían afectar a su AWS infraestructura, como los cambios Servicios de AWS y los recursos que afectan a su organización.

Visualizar eventos de vista organizativa

1. Abre el AWS Health panel de control en <https://health.aws.com/health/casa>.
2. En el panel de navegación, en Your organization health, seleccione Problemas abiertos y recientes para ver los eventos notificados recientemente.
3. Elija un evento. En la pestaña Details, puede revisar la siguiente información sobre el evento:
 - Nombre de evento
 - Status
 - Región / Zona de disponibilidad
 - Cuentas afectadas
 - Hora de inicio
 - Hora de finalización
 - Categoría
 - Description (Descripción)

Cambios programados

Utilice la pestaña Scheduled changes para ver los próximos eventos que podrían afectar a su organización. Estos eventos pueden incluir actividades de mantenimiento programadas para los servicios.

Otras notificaciones

Utilice la pestaña Notifications para ver todas las demás notificaciones y eventos en curso de los últimos siete días que puedan afectar su organización. Esto puede incluir eventos, como la rotación de certificados, las notificaciones de facturación y las vulnerabilidades de seguridad.

Event Log (Registro de eventos)

También puede usar la pestaña Registro de eventos para ver los eventos de AWS Health y tener una vista organizativa. El diseño y el comportamiento de las columnas son similares a los de las pestañas Problemas abiertos y recientes, excepto que la pestaña Registro de eventos incluye

columnas y opciones de filtro adicionales, como la categoría del evento, el estado y la hora de inicio.

Para ver los eventos organizacionales y ver eventos en la pestaña Registro de eventos.

1. Abre tu AWS Health panel de control en <https://health.aws.com/health/casa>.
2. En el panel de navegación, en Estado de su organización, elija Registro de eventos.
3. En Registro de eventos, elija el nombre del evento. Puede revisar la siguiente información sobre el evento:
 - Nombre de evento
 - Status
 - Región / Zona de disponibilidad
 - Cuentas afectadas
 - Hora de inicio
 - Hora de finalización
 - Categoría
 - Description (Descripción)

Viewing affected accounts and resources (Console)

En Estado de su organización, puede ver las cuentas de su organización afectadas por el evento y cualquier recurso relacionado. Por ejemplo, si hay un evento próximo para el mantenimiento de instancias de Amazon Elastic Compute Cloud (Amazon EC2), las cuentas de tu organización que tengan EC2 instancias de Amazon pueden aparecer en la pestaña Detalles. Puede identificar los recursos específicos y, a continuación, ponerse en contacto con el propietario de la cuenta.

Cómo visualizar de las cuentas y los recursos afectados

1. Abre tu AWS Health panel de control en <https://health.aws.com/health/casa>.
2. En el panel de navegación, en Estado de su organización, elija una de las pestañas.
3. Elija un evento que tenga un valor para las Cuentas afectadas.
4. Seleccione la pestaña Cuentas afectadas.
5. Seleccione Show account details para ver la siguiente información de las cuentas:
 - ID de cuenta

- Nombre de cuenta
 - Correo electrónico principal
 - Unidad organizativa (OU)
6. Expanda la cuenta para consultar los recursos afectados.
7. Si hay más de 10 recursos, seleccione Ver todos los recursos para verlos.
8. Para filtrar por ID de cuenta para este evento específico, haga lo siguiente:
- a. En la pestaña Affected accounts, seleccione Add filter, seleccione el ID de la cuenta y, a continuación, intodúzcalo. Solo puede ingresar un ID de cuenta a la vez.
 - b. Seleccione Apply. La cuenta que ha introducido aparece en la lista.

Viewing organizational view events (CLI)

Después de activar esta función, AWS Health comienza a registrar los eventos que afectan a las cuentas de la organización. Cuando una cuenta se une a la organización, AWS Health agrega automáticamente la cuenta a la vista organizativa.

 Note

AWS Health no registra los eventos que ocurrieron en su organización antes de activar la vista organizacional.

Cuando una cuenta abandona la organización, los nuevos eventos de esa cuenta ya no se registran en la vista organizativa. Sin embargo, los eventos existentes permanecen y todavía puede consultarlos con un límite de 90 días.

AWS conserva los datos de la política de la cuenta durante 90 días a partir de la fecha de entrada en vigor del cierre de la cuenta de administrador. Al final del período de 90 días, elimina AWS permanentemente todos los datos de la política de la cuenta.

- Si desea conservar los resultados por más de 90 días, puede archivar las políticas. También puedes usar una acción personalizada con una EventBridge regla para almacenar los resultados en un bucket de S3.
- Mientras se AWS conserven los datos de la política, al volver a abrir la cuenta cerrada, se la AWS reasignará como administradora del servicio y se recuperarán los datos de la política de servicio de la cuenta.

- Para obtener más información, consulte [Closing an account](#).

⚠ Important

Para los clientes de las regiones: AWS GovCloud (US)

- Antes de cerrar la cuenta, realice una copia de seguridad y, luego, elimine los recursos de la cuenta. Ya no tendrá acceso a ellos después de cerrar la cuenta.

Puedes usar las operaciones de la AWS Health API para mostrar eventos desde la vista de la organización.

Example : Describir eventos de vista organizativa

El siguiente AWS CLI comando devuelve los eventos de estado de AWS las cuentas de tu organización.

```
aws health describe-events-for-organization --region us-east-1
```

Deshabilitación de la vista organizativa

Si no quieres agregar eventos para tu organización, puedes desactivar esta función desde la cuenta de administración o puedes deshabilitar la vista de la organización mediante la operación de [DisableHealthServiceAccessForOrganizationAPI](#).

Disabling organizational view events (Console)

AWS Health deja de agregar eventos para todas las demás cuentas de la organización. Puede seguir viendo los eventos anteriores de su organización hasta que se eliminan.

Para desactivar la vista organizativa

1. Abre tu AWS Health panel de control en <https://health.aws.com/health/casa>.
2. En el panel de navegación, en Your organization health, elija Configurations.
3. En la página Enable organizational view, seleccione Disable organizational view.

Después de desactivar esta función, ya AWS Health no agrega eventos de tu organización. Sin embargo, la función vinculada al servicio permanece en la cuenta de administración hasta que la elimines mediante la consola AWS Identity and Access Management (IAM), la API de IAM o AWS CLI. Para obtener más información, consulte [Eliminación de un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Disabling organizational view events (CLI)

Example

El siguiente AWS CLI comando deshabilita esta función de tu cuenta.

```
aws health disable-health-service-access-for-organization --region us-east-1
```

Note

También puede deshabilitar la función organizativa mediante la operación API Organizations [Disable AWS Service Access](#). Tras ejecutar esta operación, AWS Health deja de agregar eventos para todas las demás cuentas de la organización. Si llamas a la AWS Health API de operaciones para ver la organización, AWS Health devuelve un error. AWS Health sigue acumulando los eventos de salud de tu AWS cuenta.

Después de deshabilitar esta función, ya AWS Health no agrega los eventos de su organización. Sin embargo, el rol vinculado al servicio permanece en la cuenta de administración hasta que lo elimines a través de la consola AWS Identity and Access Management (IAM), la API de IAM o AWS CLI. Para obtener más información, consulte [Eliminar un rol vinculado a un servicio](#) en la Guía del usuario de IAM.

Administración de vistas de administrador delegado para una organización

Con AWS Health, puede aprovechar la función de administrador delegado AWS Organizations que permite que una cuenta distinta de la cuenta de administración vea los AWS Health eventos agregados en el AWS Health panel de control o mediante programación a través de la API AWS Health. La característica de administrador delegado proporciona a los diferentes equipos la flexibilidad para ver y administrar los eventos de estado en toda la organización. Una buena práctica de AWS

seguridad consiste en delegar responsabilidades fuera de la cuenta de administración siempre que sea posible.

Contenido

- [Registro de un administrador delegado para la vista organizativa](#)
- [Eliminación de un administrador delegado de la vista organizativa](#)

Registro de un administrador delegado para la vista organizativa

Una vez que habilite la vista organizativa para su organización, podrá registrar hasta cinco cuentas de miembros en su organización como administrador delegado. Para ello, llama a la operación de la [RegisterDelegatedAdministrator](#) API. Después de registrar las cuentas de los miembros, se les delega la administración de las cuentas y pueden acceder a la vista de la AWS Health organización desde el AWS Health panel de control. Si la cuenta tiene un plan [Business](#), [Enterprise On-Ramp](#) o [Enterprise](#) Support, los administradores delegados pueden usar la AWS Health API para acceder a la vista de la AWS Health organización.

Para establecer un administrador delegado, desde la cuenta de administración de su organización, ejecute el siguiente comando AWS Command Line Interface (AWS CLI). Puede usar este comando desde la cuenta de administración o desde una cuenta que pueda asumir el rol con los AWS Identity and Access Management permisos necesarios. En el siguiente comando de ejemplo, sustituye ACCOUNT_ID por el ID de cuenta de miembro que deseas registrar junto con el director de AWS Health servicio «health.amazonaws.com».

```
aws organizations register-delegated-administrator --account-id ACCOUNT_ID --service-principal health.amazonaws.com
```

Una vez registrado un administrador delegado, podrá ver todos los eventos de AWS Health que afectan las cuentas de su organización. Puede ver el historial de eventos de los últimos 90 días o desde que se activó por primera vez la característica de vista organizativa, lo que sea más reciente. Tenga en cuenta que habilitar la característica de administrador delegado es un proceso asíncrono y tarda hasta un minuto en completarse.

Eliminación de un administrador delegado de la vista organizativa

Para eliminar el acceso de un administrador delegado, llama a la operación de la API.

[DeregisterDelegatedAdministrator](#)

Desde la cuenta de administración de tu organización, ejecuta el siguiente AWS CLI comando para eliminar la cuenta de un miembro como administrador delegado. En el siguiente comando de ejemplo, sustituya ACCOUNT_ID por el ID de la cuenta del miembro que deseé eliminar.

```
aws organizations deregister-delegated-administrator --account-id ACCOUNT_ID --service-principal health.amazonaws.com
```

Monitorización de eventos AWS Health con Amazon EventBridge

Puedes usar Amazon EventBridge para detectar AWS Health eventos y reaccionar ante ellos. A continuación, en función de las reglas que usted cree, EventBridge invoca una o más acciones objetivo cuando un evento coincide con los valores que especifique en una regla. Dependiendo del tipo de evento, puede capturar información sobre el evento, iniciar eventos adicionales, enviar notificaciones, tomar medidas correctivas o realizar otras acciones. Por ejemplo, puede utilizarlos AWS Health para recibir notificaciones por correo electrónico si tiene AWS recursos programados para actualizaciones, como las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Cuenta de AWS

Notas

- AWS Health entrega eventos de forma duradera e intenta entregarlos satisfactoriamente al EventBridge menos una vez.
- EventBridge Las reglas que crees solo pueden recibir notificaciones para tu Cuenta de AWS. Para recibir eventos organizativos para otras cuentas de tu cuenta AWS Organizations, consulta Cómo [agregar AWS Health eventos mediante la vista de organización y el acceso de administrador delegado](#).
- Los eventos de salud pública pueden tardar hasta una hora en empezar a enviarse después de crear una EventBridge regla.

Puedes elegir entre varios tipos de objetivos EventBridge como parte de tu AWS Health flujo de trabajo, entre los que se incluyen:

- AWS Lambda funciones
- Amazon Kinesis Data Streams
- Colas de Amazon Simple Queue Service (Amazon SQS)
- Objetivos integrados (como acciones CloudWatch de alarma)
- Temas de Amazon Simple Notification Service (Amazon SNS)

Por ejemplo, puede utilizar una función de Lambda para pasar una notificación a un canal de Slack cuando se produce un evento de AWS Health. O bien, puede usar Lambda y EventBridge enviar notificaciones personalizadas de texto o SMS con Amazon SNS cuando se AWS Health produzca un evento.

Para ver ejemplos de alertas personalizadas y de automatización que puede crear en respuesta a AWS Health eventos, consulte las [AWS Health herramientas](#) en GitHub

Temas

- [Crear EventBridge reglas de Región de AWS cobertura](#)
- [Monitoreo de eventos públicos y específicos de cuenta para AWS Health](#)
- [Visualización de listas paginadas de eventos en AWS Health EventBridge](#)
- [Aregar AWS Health eventos mediante la vista organizativa y el acceso de administrador delegado](#)
- [Integrar la supervisión y las notificaciones de AWS Health eventos con JIRA y ServiceNow](#)
- [Configurar una EventBridge regla para enviar notificaciones sobre eventos en AWS Health](#)
- [Configuración de Amazon Q Developer en aplicaciones de chat para enviar notificaciones sobre eventos en AWS Health](#)
- [Ejecutar operaciones en las EC2 instancias de forma automática en respuesta a los eventos de AWS Health](#)
- [Referencia: Amazon EventBridge esquema de AWS Health eventos](#)

Crear EventBridge reglas de Región de AWS cobertura

Puedes crear una EventBridge regla para cada región para la que quieras recibir AWS Health eventos. Por ejemplo, para recibir eventos de la región de Europa (Fráncfort), puedes crear una regla para esta región.

Para mejorar la fiabilidad de AWS Health las notificaciones, puedes configurar reglas en las regiones de respaldo específicas. En la AWS partición estándar, la región EE.UU. Oeste (Oregón) actúa como región de respaldo para todas las demás regiones, mientras que la región EE.UU. Este (Norte de Virginia) actúa como región de respaldo para la región EE.UU. Oeste (Oregón). Cuando se producen eventos de salud, se envían automáticamente tanto a la región principal como a la región de respaldo designada. Por ejemplo, si monitorizas los eventos en la región de Europa (Fráncfort), los eventos de salud se envían tanto a la región de Europa (Fráncfort) como a la región de EE. UU. oeste (Oregón). Este sistema garantiza que sigas recibiendo notificaciones de salud incluso si tu región principal tiene

problemas. Para crear una regla de respaldo, siga el procedimiento de [Configurar una EventBridge regla para enviar notificaciones sobre eventos en AWS Health](#).

Si prefiere no utilizar la funcionalidad de copia de seguridad, debe añadir un filtro a la regla de región de copia de seguridad. Por ejemplo, implemente un filtro para `detail.backupEvent = False`. Esto evita que reciba eventos de respaldo de otras regiones.

Configuración de alta disponibilidad (opcional)

Si desea crear una EventBridge integración con alta disponibilidad, asegúrese de haber implementado las reglas tanto en las regiones pertinentes como en las de respaldo y, a continuación, implemente la deduplicación mediante `detail.communicationId`. Esto garantiza que reciba todos los eventos y, al mismo tiempo, evite los duplicados. Para obtener más información, consulte [Referencia: Amazon EventBridge esquema de AWS Health eventos](#).

Integración simplificada

Si desea capturar eventos de varios Regiones de AWS, pero prefiere configurar solo una regla, la integración simplificada es la opción adecuada. Para recibir AWS Health eventos de todas las regiones de la AWS partición estándar, puede configurar una regla central en la región EE.UU. Oeste (Oregón). Esta regla única agrega automáticamente los eventos de todas las regiones de partición estándar en las que recibe eventos de Health. Sin embargo, no tendrá una configuración de alta disponibilidad.

Eventos globales

Algunos AWS Health eventos no son específicos de una región. Los eventos que no son específicos de una región se llaman eventos globales. Estos incluyen eventos enviados para AWS Identity and Access Management (IAM). Para recibir eventos globales, debes crear una regla para la región EE.UU. Este (Virginia del Norte).

Monitoreo de eventos públicos y específicos de cuenta para AWS Health

Al crear una EventBridge regla para supervisar los eventos AWS Health, la regla incluye tanto eventos específicos de la cuenta como eventos públicos:

- Los eventos específicos de la cuenta afectan a su cuenta y a sus recursos, como un evento que le informa sobre una actualización obligatoria de una EC2 instancia de Amazon u otros eventos de cambio programados.
- Los eventos públicos aparecen en el [panel de control de AWS Health : estado del servicio](#). Los eventos públicos no son específicos de Cuentas de AWS ni proporcionan información pública sobre la disponibilidad regional de un servicio.

Important

Para recibir ambos tipos de eventos, la regla debe usar el valor de "source":

["aws.health"]. Los caracteres comodín, como "source": ["aws.health*"], no coincidirán con el patrón para permitir monitorizar ningún evento.

Puedes identificar si un evento es público o específico de una cuenta en EventBridge, mediante el parámetro. eventScopeCode Los eventos pueden tener PUBLIC o ACCOUNT_SPECIFIC. También puede filtrar la regla según este parámetro.

Ejemplo: eventos públicos para Amazon Elastic Compute Cloud

El siguiente evento muestra un problema operativo de Amazon EC2 en la región EE.UU. Este (Norte de Virginia).

```
{  
  "version": "0",  
  "id": "fd9d4512-1eb0-50f6-0491-d016ae56aef0",  
  "detail-type": "AWS Health Event",  
  "source": "aws.health",  
  "account": "123456789012",  
  "time": "2023-02-15T10:07:10Z",  
  "region": "us-east-1",  
  "resources": [],  
  "detail": {  
    "eventArn": "arn:aws:health:us-east-1::event/EC2/AWS_EC2_OPERATIONAL_ISSUE",  
    "service": "EC2",  
    "eventTypeCode": "AWS_EC2_OPERATIONAL_ISSUE",  
    "eventTypeCategory": "issue",  
    "eventScopeCode": "PUBLIC",  
    "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",  
  }  
}
```

```
  "startTime": "Wed, 15 Feb 2023 22:07:07 GMT",
  "lastUpdatedTime": "Wed, 15 Feb 2023 22:07:07 GMT",
  "statusCode": "open",
  "eventRegion": "us-east-1",
  "eventDescription": [
    {
      "latestDescription": "We are investigating increased API Error rates and
Latencies for Amazon Elastic Compute Cloud in the US-EAST-1 Region.",
      "language": "en_US"
    },
    {
      "page": "1",
      "totalPages": "1",
      "affectedAccount": "123456789012"
    }
  ]
}
```

Reglas de Backup para AWS Health eventos

Si monitorizas eventos públicos desde una Región de AWS, te recomendamos que crees una regla de respaldo. Los eventos públicos para AWS Health se envían simultáneamente a la región afectada y a la región de respaldo cuando se establece una regla válida en la región afectada.

AWS Health envía eventos específicos de la cuenta tanto a la región afectada como a la región de respaldo, independientemente de las reglas configuradas en la región afectada.

Le recomendamos que deduplique AWS Health los eventos utilizando eventARN y communicationId porque estos valores siguen siendo los mismos para los AWS Health mensajes que se envían a la región de respaldo.

Visualización de listas paginadas de eventos en AWS Health EventBridge

AWS Health admite la paginación de AWS Health eventos cuando la lista resources o affectedEntities hace que el tamaño del mensaje supere el límite EventBridge de 256 KB.

AWS Health incluye todos los detail.affectedEntities campos resources y del mensaje. Si esta lista de detail.affectedEntities valores resources y supera los 256 KB, AWS Health divide el evento de salud en varias páginas y publica estas páginas como mensajes individuales. EventBridge Cada página retiene los mismos valores de eventARN y communicationId para

ayudar recombinar la lista de `resources` o `detail.affectedEntities` una vez recibidas todas las páginas.

Estos mensajes adicionales pueden provocar mensajes innecesarios, por ejemplo, cuando la EventBridge regla se dirige a una interfaz legible para las personas, como el correo electrónico o el chat. Los clientes con notificaciones legibles por humanos pueden agregar un filtro para el campo `detail.page` para procesar solo la primera página, lo que elimina los mensajes innecesarios creados a partir de páginas subsiguientes.

En el esquema, cada `communicationId` incluye el número de página dividido con un guion después del `communicationId`, aunque solo haya una página. Los campos `detail.page` y `detail.totalPages` describen el número de página actual y el número total de páginas del evento. AWS Health La información contenida en cada mensaje paginado es la misma, salvo por la lista de `detail.affectedEntities` o `resources`. Estas listas se pueden reconstruir después de recibir todas las páginas. Las páginas de recursos y entidades afectados son independientes de criterios de orden.

Agregar AWS Health eventos mediante la vista organizativa y el acceso de administrador delegado

AWS Health admite la vista organizativa y el acceso de administrador delegado para AWS Health los eventos publicados en Amazon EventBridge. Cuando la vista de la organización está activada AWS Health, la cuenta de administración o la cuenta de administrador delegado recibe un único resumen de los AWS Health eventos de todas las cuentas de tu organización. AWS Organizations

Esta función está diseñada para proporcionar una vista centralizada que ayude a gestionar AWS Health los eventos en toda la organización. Al configurar una vista organizativa y una EventBridge regla en la cuenta de administración no se desactivan EventBridge las reglas de otras cuentas de la organización.

Para obtener más información sobre cómo activar la vista de la organización y el acceso de administrador delegado AWS Health, consulta Cómo [agregar AWS Health](#) eventos.

Integrar la supervisión y las notificaciones de AWS Health eventos con JIRA y ServiceNow

Puede integrar AWS Health los eventos con JIRA y ServiceNow recibir información operativa y de cuentas, prepararse para los cambios programados y gestionar los eventos de Health mediante el

Service Management Connector (SMC). La integración de SMC con AWS Health puede utilizar los eventos de Health enviados EventBridge para crear, mapear y actualizar automáticamente los tickets e ServiceNow incidentes de JIRA.

Puedes usar la vista organizativa y el acceso de administrador delegado para gestionar fácilmente los eventos de Salud en toda la organización dentro de JIRA e ServiceNow incorporar la AWS Health información directamente en el flujo de trabajo de tu equipo.

[Para obtener más información sobre la ServiceNow integración mediante el SMC, consulta Integrar en AWS Health ServiceNow](#)

Para obtener más información sobre la integración de JIRA Management Cloud mediante SMC, consulte [AWS Health en JIRA](#).

Configurar una EventBridge regla para enviar notificaciones sobre eventos en AWS Health

Puedes crear una EventBridge regla para recibir notificaciones de AWS Health los eventos de tu cuenta. Antes de crear las reglas de un evento AWS Health, haga lo siguiente:

- Familiarícese con los eventos, las reglas y los objetivos en EventBridge. Para obtener más información, consulta [¿Qué es Amazon EventBridge?](#) en la Guía del EventBridge usuario de Amazon y en lo [nuevo EventBridge : rastrea y responde a los cambios en tus AWS recursos](#).
- Crear el destino o destinos que se van a usar en las reglas de eventos.

Para crear una EventBridge regla para AWS Health

1. Abre la EventBridge consola de Amazon en <https://console.aws.amazon.com/events/>.
2. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página. Elija la región en la que desee realizar un seguimiento de los eventos de AWS Health .
3. En el panel de navegación, seleccione Reglas.
4. Elija Create rule (Crear regla).
5. En la página Crear detalles de la regla, ingrese un nombre y una descripción para su regla.
6. Mantenga los valores predeterminados para Event bus (Bus de eventos) y Rules type (Tipo de regla) y luego seleccione Next (Siguiente).

7. En la página Crear un patrón de eventos, en Origen del evento, selecciona AWS eventos y eventos EventBridge asociados.
8. En Patrón de eventos, para Origen del evento, elija Servicios de AWS.
9. En Patrón de eventos, para Servicio de AWS, elija Estado.
10. En Tipo de evento, elija una de las siguientes opciones:
 - Eventos de abuso de la salud específico: cree una regla para eventos de AWS Health que tengan la palabra Abuse en el nombre del tipo de evento.
 - Eventos de salud específicos: crea una regla para los eventos de un evento específico Servicio de AWS, como Amazon EC2.
11. Puede elegir cualquier servicio o uno o varios servicios específicos. Si opta por un servicio específico, elija una de las siguientes opciones:
 - Elija Any event type category para crear una regla que se aplique a todas las categorías de tipos de eventos.
 - Elija Specific event type category(s) y, a continuación, elija un valor de la lista, como issue, accountNotification o scheduledChange.

 Tip

- Para supervisar todos los AWS Health eventos de un servicio específico, le recomendamos que elija Cualquier tipo de evento, categoría y Cualquier recurso. Esto garantiza que la regla supervise cualquier AWS Health evento, incluidos los códigos de tipo de evento nuevos, del servicio especificado. Para ver un ejemplo de regla, consulta [todos los EC2 eventos de Amazon](#).
- Puede crear una regla para monitorizar más de una categoría de servicio o tipo de evento. Para ello, debe actualizar manualmente el patrón del evento para la regla. Para obtener más información, consulte [Cómo crear una regla para varios servicios y categorías](#).

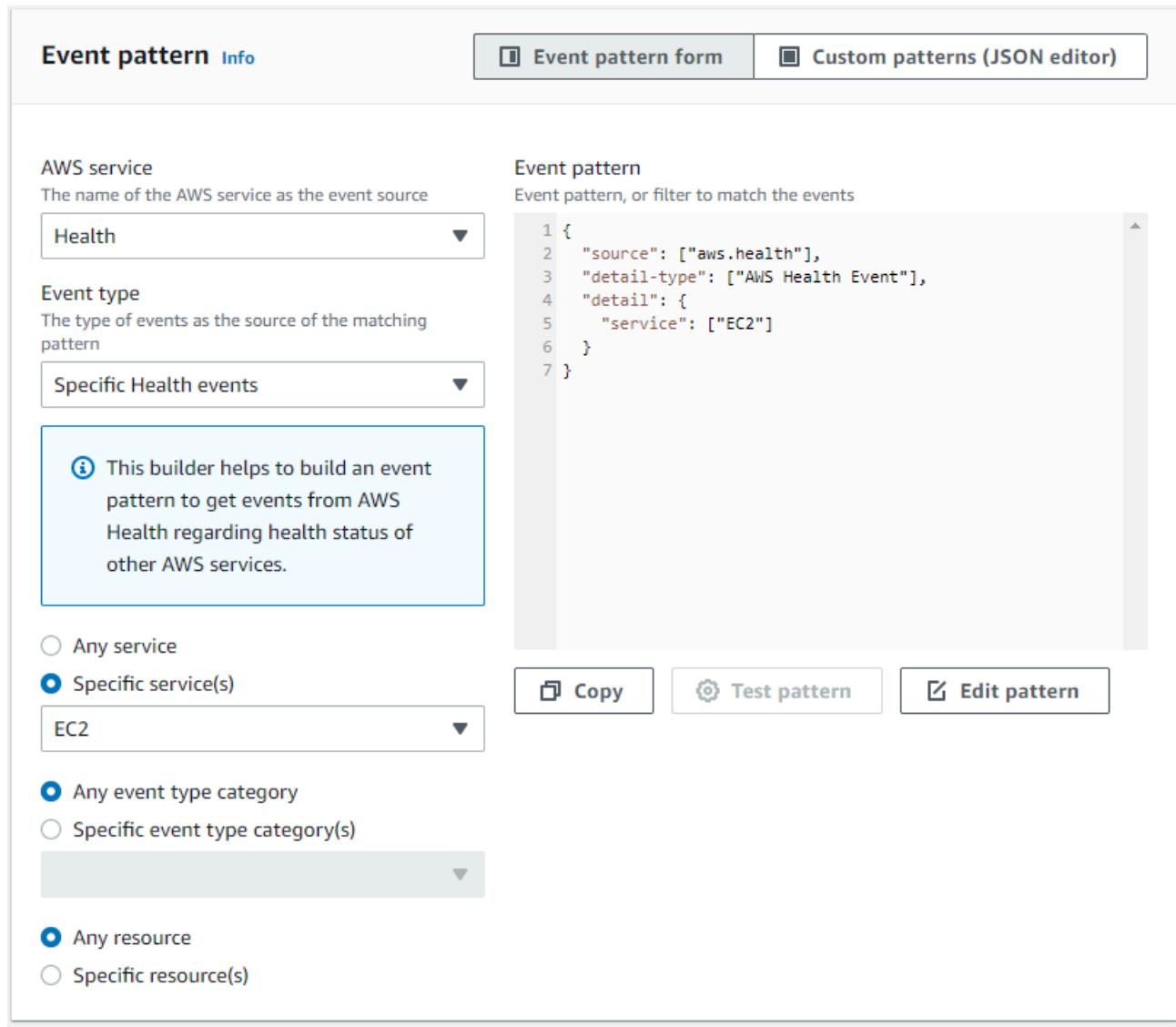
12. Si ha elegido un servicio específico y una categoría de tipo de evento, elija una de las siguientes opciones para los códigos de tipo de evento.
 - Elija Cualquier código de tipo de evento para crear una regla que se aplique a todos los códigos de tipos de eventos.
 - Elija Código o códigos de tipo de evento específico y, a continuación, elija uno o más valores de la lista. Esto crea una regla que se aplica solo a códigos de tipos de

eventos específicos. Por ejemplo, si elige **AWS_EC2_INSTANCE_STOP_SCHEDULED** y **AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED**, su regla solo se aplicará a estos eventos cuando ocurran en su cuenta.

13. Elija una de las siguientes opciones para los recursos afectados.
 - Elija Cualquier recurso para crear una regla que se aplique a todos los recursos.
 - Elija un recurso o recursos específicos e introduzca IDs uno o más recursos. Por ejemplo, puedes especificar un ID de EC2 instancia de Amazon, por ejemplo *i-EXAMPLEa1b2c3de4*, para supervisar los eventos que afectan únicamente a este recurso.
14. Revise la configuración de sus reglas para asegurarse de que se ajusta a los requisitos de supervisión de sus eventos.
15. Elija Siguiente.
16. En la página Seleccionar objetivos, elija el tipo de destino que haya creado para esta regla y, a continuación, configure las opciones adicionales necesarias para dicho tipo. Por ejemplo: puede enviar el evento a una cola de Amazon SQS o a un tema de Amazon SNS.
17. Elija Siguiente.
18. (Opcional) En la página Add tags (Aregar etiquetas) agregue etiquetas a su clave y, a continuación, elija Next (Siguiente).
 - Nota: Actualmente, la fuente aws.health no envía las etiquetas. EventBridge
19. En la página Revisar y crear, revise la configuración de sus reglas y asegúrese de que cumpla con sus requisitos de monitoreo de eventos.
20. Seleccione Creación de regla.

Example : Regla para todos los EC2 eventos de Amazon

El siguiente ejemplo crea una regla para EventBridge supervisar todos los EC2 eventos de Amazon, incluidas las categorías de tipos de eventos, los códigos de eventos y los recursos.



AWS service

The name of the AWS service as the event source

Health

Event type

The type of events as the source of the matching pattern

Specific Health events

ⓘ This builder helps to build an event pattern to get events from AWS Health regarding health status of other AWS services.

Any service

Specific service(s)

EC2

Any event type category

Specific event type category(s)

Any resource

Specific resource(s)

Event pattern

Event pattern, or filter to match the events

```
1 {  
2 "source": ["aws.health"],  
3 "detail-type": ["AWS Health Event"],  
4 "detail": {  
5 "service": ["EC2"]  
6 }  
7 }
```

Copy

Test pattern

Edit pattern

Example : Regla para EC2 eventos específicos de Amazon

En el siguiente ejemplo, se crea una regla para EventBridge supervisar lo siguiente:

- El EC2 servicio Amazon
- La categoría de tipo de evento scheduledChange
- Los códigos de tipo de evento para AWS_EC2_INSTANCE_TERMINATION_SCHEDULED y AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED
- La instancia con el ID i-EXAMPLEa1b2c3de4

AWS service
The name of the AWS service as the event source

Health ▾

Event type
The type of events as the source of the matching pattern

Specific Health events ▾

i This builder helps to build an event pattern to get events from AWS Health regarding health status of other AWS services.

Any service

Specific service(s)

EC2 ▾

Any event type category

Specific event type category(s)

scheduledChange ▾

Any event type code

Specific event type code(s)

Any resource

Specific resource(s)

i-EXAMPLEa1b2c3de4

Cómo crear una regla para varios servicios y categorías

Los ejemplos en el procedimiento anterior muestran cómo crear una regla para una sola categoría de servicio y tipo de evento. También puede crear una regla para varios servicios y categorías de tipos de eventos. De esta forma, no tiene que crear una regla por separado para cada servicio y categoría

que desee supervisar. Para ello, debe modificar el patrón del evento y luego introducir los cambios manualmente.

Puede utilizar una de las siguientes opciones.

Inclusión de servicios y categorías en una regla existente

1. En la EventBridge consola, en la página de reglas, elige el nombre de la regla.
2. En la esquina superior derecha, elija Edit (Editar).
3. Elija Siguiente.
4. En Patrón del evento, elija Editar patrón y, a continuación, introduzca los cambios en el campo de texto.
5. Elija Siguiente hasta llegar a la página Revisar y actualizar.
6. Elija Actualizar regla para guardar los cambios.

Inclusión de servicios y categorías en una nueva regla

1. Siga el procedimiento en [Configurar una EventBridge regla para enviar notificaciones sobre eventos en AWS Health](#) para el [paso 9](#).
2. En lugar de elegir un solo servicio o categoría de las listas, en Patrón del evento, elija Editar patrón.
3. Introduzca los cambios en el campo de texto. Consulte el siguiente [patrón de ejemplo](#) como modelo para crear su propio patrón de evento.
4. Revise el patrón de evento y, a continuación, siga el resto del procedimiento en [Configurar una EventBridge regla para enviar notificaciones sobre eventos en AWS Health](#) para crear la regla.

Usa la API o AWS Command Line Interface (AWS CLI)

Para una regla nueva o existente, usa la operación de la [PutRule](#) API o el `aws events put-rule` comando para actualizar el patrón de eventos. Para ver un AWS CLI comando de ejemplo, consulta [put-rule](#) en la Referencia de AWS CLI comandos.

Example Ejemplo: varias categorías de servicios y de tipos de eventos

El siguiente patrón de eventos crea una regla para monitorear los eventos de las `issue` categorías y tipos de `scheduledChange` eventos de tres AWS servicios: Amazon EC2, Amazon EC2 Auto Scaling y Amazon VPC. `accountNotification`

```
{  
  "detail": {  
    "eventTypeCategory": [  
      "issue",  
      "accountNotification",  
      "scheduledChange"  
    ],  
    "service": [  
      "AUTOSCALING",  
      "VPC",  
      "EC2"  
    ]  
  },  
  "detail-type": [  
    "AWS Health Event"  
  ],  
  "source": [  
    "aws.health"  
  ]  
}
```

Configuración de Amazon Q Developer en aplicaciones de chat para enviar notificaciones sobre eventos en AWS Health

Puedes recibir AWS Health eventos directamente en tus clientes de chat, como Slack y Amazon Chime. Puedes usar este evento para identificar problemas de AWS servicio recientes que puedan afectar a tus AWS aplicaciones e infraestructura. A continuación, puedes iniciar sesión en su [panel de AWS Health](#) para obtener más información sobre la actualización. Por ejemplo, si monitorizas el tipo de AWS_EC2_INSTANCE_STOP_SCHEDULED evento en tu AWS cuenta, el AWS Health evento puede aparecer directamente en tu canal de Slack.

Requisitos previos

Antes de comenzar, debe tener lo siguiente:

- Un cliente de chat configurado con Amazon Q Developer en aplicaciones de chat. Puedes configurar Amazon Chime y Slack. Para obtener más información, consulte [Introducción a Amazon Q Developer en aplicaciones de chat](#) en la Guía del administrador de aplicaciones de chat Amazon Q Developer in chat.

- Un tema de Amazon SNS que haya creado y al que esté suscrito. Si ya tiene un tema SNS, puede utilizarlo. Para obtener más información, consulte [Introducción a Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Notification Service.

Para recibir AWS Health eventos con Amazon Q Developer en aplicaciones de chat

1. Siga el procedimiento de [Configurar una EventBridge regla para enviar notificaciones sobre eventos en AWS Health](#) hasta el paso 13.
 - a. Cuando termine de configurar el patrón de eventos en el paso 13, añada una coma a la última línea del patrón y añada la siguiente línea para eliminar los mensajes de chat innecesarios de los eventos paginados AWS Health . Consulte [Visualización de listas paginadas de eventos en AWS Health EventBridge](#).
"detail.page": ["1"]
 - b. Cuando elija el objetivo en el [paso 14](#), elija un tema de SNS. Utilizará este mismo tema de SNS en la consola de aplicaciones de chat de Amazon Q Developer.
 - c. Complete el resto del procedimiento para crear la regla.
2. Navegue hasta [Amazon Q Developer en la consola de aplicaciones de chat](#).
3. Elija su cliente de chat, como el nombre de su canal de Slack, y luego elija Editar.
4. En la sección Notifications - optional, en Topics, elija el mismo tema SNS que especificó en el paso 1.
5. Seleccione Save.

Cuando AWS Health envíe un evento EventBridge que coincida con tu regla, el AWS Health evento aparecerá en tu cliente de chat.

6. Elige el nombre del evento para ver más información en tu AWS Health panel de control.

Example : AWS Health eventos enviados a Slack

El siguiente es un ejemplo de dos AWS Health eventos para Amazon EC2 y Amazon Simple Storage Service (Amazon S3) en la región EE.UU. Este (Virginia del Norte) que aparecen en el canal de Slack.

AWS APP 11:46 AM

AWS Health Event | us-east-1 | Account: 123456789012 | open

Event type code: AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED

EC2 has detected degradation of the underlying hardware hosting your Amazon EC2 instance associated with this event in the us-east-1 region. Due to this degradation your instance could already be unreachable. We will stop your instance after 2021-03-19 18:36:40 PST. Please take appropriate action before this time.\n\nYou can find more information about retirement events scheduled for your EC2 instances in the AWS Management Console <https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#Events>\n* What will happen to my instance?\nYour instance will be stopped after the specified retirement date. You can start it again...\n

[Show more](#)

Start time: Sat, 20 Mar 2021 01:35:40 GMT

End time: Sat, 20 Mar 2021 01:36:40 GMT

AWS APP 12:08 PM

AWS Health Event | us-east-1 | Account: 123456789012 | open

Event type code: AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION

We are writing to notify you that you may have exposed your S3 bucket/s to a larger audience than you intended. AWS recommends that you review your bucket permissions and ACLs to determine whether the access is appropriate. S3 bucket permissions should never contain \"Principal\":\"*\" unless you intend to grant public access to your data. Additionally, S3 bucket ACLs should be appropriately scoped to prevent unintended access to \"Authenticated Users\" or \"Everyone\" unless your use case requires it.\n\nThe list of buckets with this configuration is associated with this event.\n\nThe following links provide an overview of S3 bucket permissions and ACLs:

[Show more](#)

Start time: Sat, 20 Mar 2021 01:35:40 GMT

End time: Sat, 20 Mar 2021 01:36:40 GMT

Ejecutar operaciones en las EC2 instancias de forma automática en respuesta a los eventos de AWS Health

Puedes automatizar las acciones que respondan a los eventos programados para tus EC2 instancias de Amazon. Cuando AWS Health envía un evento a tu AWS cuenta, tu EventBridge regla puede invocar objetivos, como documentos de AWS Systems Manager automatización, para automatizar las acciones en tu nombre.

Por ejemplo, cuando se programe un evento de retirada de una EC2 instancia de Amazon para una instancia EC2 respaldada por Amazon Elastic Block Store (Amazon EBS) AWS Health , enviará AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED el tipo de evento a tu panel de control. AWS Health Cuando la regla detecte este tipo de evento, podrá automatizar la detención y el inicio de la instancia. De esta forma, no tiene que realizar estas acciones manualmente.

Note

Para automatizar las acciones de sus EC2 instancias de Amazon, las instancias deben ser administradas por Systems Manager.

Para obtener más información, consulta [Automatizar Amazon EC2 con EventBridge](#) en la Guía del EC2 usuario de Amazon.

Requisitos previos

Debe crear una política AWS Identity and Access Management (de IAM), crear un rol de IAM y actualizar la política de confianza del rol antes de poder crear una regla.

Creación de una política de IAM

Siga este procedimiento para crear una política administrada por el cliente para su rol. Esta política da al rol permiso para llevar a cabo acciones en su nombre. Este procedimiento usa el editor de políticas JSON en la consola de IAM.

Para crear una política de IAM

1. Inicie sesión en la consola de IAM Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/iam/>
2. En el panel de navegación, seleccione Políticas.
3. Elija Crear política.
4. Seleccione la pestaña JSON.
5. Copie la siguiente JSON y luego sustituya la JSON por defecto en el editor.

JSON

{

```
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "ec2:StartInstances",
      "ec2:StopInstances",
      "ec2:DescribeInstanceStatus"
    ],
    "Resource": [
      "*"
    ],
  },
  {
    "Effect": "Allow",
    "Action": [
      "ssm:)"
    ],
    "Resource": [
      "*"
    ],
  },
  {
    "Effect": "Allow",
    "Action": [
      "sns:Publish"
    ],
    "Resource": [
      "arn:aws:sns:*::*:Automation*"
    ],
  },
  {
    "Effect": "Allow",
    "Action": [
      "iam:PassRole"
    ],
    "Resource": "arn:aws:iam::123456789012:role/AutomationEVRole"
  }
]
```

- a. En el Resource parámetro, para el Amazon Resource Name (ARN), introduce tu ID de AWS cuenta.
 - b. También puede sustituir el nombre del rol o usar el predeterminado. En este ejemplo se utiliza *AutomationEVRole*.
6. Elija Siguiente: etiquetas.
 7. (Opcional) Puede usar etiquetas como pares clave-valor para agregar metadatos a la política.
 8. Elija Siguiente: Revisar.
 9. En la página de revisión de la política, introduzca un nombre, por ejemplo, *AutomationEVRolePolicy* y una descripción opcional.
 10. Revise la página Resumen para ver los permisos que permite la política. Si está satisfecho con su política, seleccione Crear política.

Esta política define las acciones que puede llevar a cabo el rol. Para obtener más información, consulte [Creación de políticas de IAM \(Consola\)](#) en la Guía del usuario de IAM.

Creación de un rol de IAM

Después de crear esta política, debe crear el rol de IAM y, a continuación, asociar la política a ese rol.

Para crear un rol para un AWS servicio

1. Inicie sesión en la consola de IAM Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/iam/>.
2. En el panel de navegación, seleccione Roles y luego seleccione Crear rol.
3. En Seleccionar el tipo de entidad de confianza, elija Servicio de AWS .
4. Elija EC2el servicio al que quiere permitir que asuma esta función.
5. Elija Siguiente: permisos.
6. Introduzca el nombre de la política que creó, por ejemplo, y*AutomationEVRolePolicy*, a continuación, active la casilla de verificación situada junto a la política.
7. Elija Siguiente: etiquetas.
8. (Opcional) Puede usar etiquetas como valores clave-valor para agregar metadatos al rol.
9. Elija Next: Review (Siguiente: revisar).

10. En Role name (Nombre del rol), introduzca **AutomationEVRole**. Este nombre debe ser el mismo que aparece en el ARN de la política de IAM que ha creado.
11. (Opcional) En Role description (Descripción del rol), ingrese una descripción para el rol.
12. Revise el rol y, a continuación, seleccione Crear rol.

Para obtener más información, consulte [Creación de un rol para un AWS servicio](#) en la Guía del usuario de IAM.

Actualice la política de confianza

Por último, puede actualizar la política de confianza para el rol que ha creado. Debe completar este procedimiento para poder elegir este rol en la EventBridge consola.

Para actualizar la política de confianza de el rol

1. Inicie sesión en la consola de IAM Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/iam/>.
2. Seleccione Roles en el panel de navegación.
3. En la lista de funciones de su AWS cuenta, elija el nombre de la función que creó, por ejemplo. **AutomationEVRole**
4. Elija la pestaña Relaciones de confianza y, a continuación, Editar relación de confianza.
5. En el documento de política, copie la siguiente JSON, elimine la política predeterminada y pegue la JSON copiada en su lugar.

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "Service": [  
          "ssm.amazonaws.com",  
          "events.amazonaws.com"  
        ]  
      },  
      "Action": "sts:AssumeRole"  
    }  
  ]}
```

```
    }  
]  
}
```

6. Elija Actualizar política de confianza.

Para obtener más información, consulte [Modificación de una política de confianza de rol \(consola\)](#) en la Guía del usuario de IAM.

Crea una regla para EventBridge

Siga este procedimiento para crear una regla en la EventBridge consola de modo que pueda automatizar la detención y el inicio de EC2 las instancias cuya retirada está programada.

Para crear una regla EventBridge para las acciones automatizadas de Systems Manager

1. Abre la EventBridge consola de Amazon en <https://console.aws.amazon.com/events/>.
2. En el panel de navegación, en Events (Eventos), seleccione Rules (Reglas).
3. En la página Crear regla, escriba un nombre y una descripción para su regla.
4. En Define pattern (Definir patrón) elija Event pattern (Patrón de eventos), a continuación, elija Pre-defined pattern by service (Patrón predeterminado por servicio).
5. En Proveedor de servicios, elija AWS.
6. En Nombre de servicio, elija Estado.
7. En Tipo de evento, elija Eventos de estado específicos.
8. Selecciona Servicio (s) específico (s) y, a continuación, elige EC2.
9. Elija Categorías de tipo de evento específicas y, a continuación, elija scheduledChange.
10. Elija Código o códigos de tipos de evento específicos y, a continuación, elija el código del tipo de evento.

Por ejemplo, para las instancias EC2 respaldadas por Amazon EBS, elija.

AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED Para EC2 instancias de Amazon respaldadas en tiendas, elige. **AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED**

11. Elija Add resource (Agregar recurso).

Su Patrón del evento será similar al ejemplo siguiente.

Example

```
{  
  "source": [  
    "aws.health"  
,  
  "detail-type": [  
    "AWS Health Event"  
,  
  "detail": {  
    "service": [  
      "EC2"  
,  
    "eventTypeCategory": [  
      "scheduledChange"  
,  
    "eventTypeCode": [  
      "AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED"  
,  
    ]  
  }  
}
```

12. Agregue el destino del documento de Systems Manager Automation. En Seleccionar destinos, para Destino, elija SSM Automation.
13. En Document (Documento), elija AWS-RestartEC2Instance.
14. Expanda Configurar parámetros de automatización y, a continuación, seleccione Transformador de entrada.
15. Para el campo Ruta de entrada, introduzca **{"Instances": "\$.resources"}**.
16. Para el segundo campo, introduzca **{"InstanceId": <Instances>}**.
17. Elija Usar el rol existente y, a continuación, elija el rol de IAM que creó, por ejemplo, *AutomationEVRole*

El destino debería ser similar al siguiente ejemplo:

Target Remove

Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule).

SSM Automation

Document

AWS-RestartEC2Instance

▶ **Configure document version**

▼ **Configure automation parameter(s)**

No Parameter(s)

Constant

Input Transformer

`{"Instances": "$.resources"}`

`{"InstanceId": <Instances>}`

EventBridge needs permission to call SSM Start Automation Execution with your supplied Automation document and parameters. By continuing, you are allowing us to do so.

Create a new role for this specific resource

Use existing role

AutomationEVRole

Note

Si no tiene un rol de IAM existente con los permisos necesarios EC2 y de Systems Manager y una relación de confianza, su rol no aparecerá en la lista. Para obtener más información, consulte [Requisitos previos](#).

18. Elija Crear.

Si se produce un evento en su cuenta que coincide con su regla, EventBridge enviará el evento a su destino especificado.

Referencia: Amazon EventBridge esquema de AWS Health eventos

El siguiente es el esquema de los AWS Health eventos. El contenido del parámetro de detalles se muestra en una segunda tabla. Se proporcionan ejemplos de cargas útiles después de las tablas del esquema.

AWS Health esquema de eventos

AWS Health esquema de eventos

Parámetro	Description (Descripción)	Obligatorio
versión	EventBridge versión, actualmente «0».	Sí
id	El identificador único del EventBridge evento.	Sí
detail-type	Tipo de detalle. Para AWS Health los eventos, los valores admitidos son &AWS Health Event y AWS Health	Sí

Parámetro	Description (Descripción)	Obligatorio
	Abuse Event	
origen	La fuente del bus de eventos. Para AWS Health los eventos, el valor admitido es aws.health	Sí

Parámetro	Description (Descripción)	Obligatorio
account	El ID de cuenta a la que se envió el AWS Health evento.	Sí

 Note

Para la vistas organizativas, se tratará de una cuenta distinta de la cuenta afectada si se recibe en la cuenta de administración o de administrador

Parámetro	Description (Descripción)	Obligatorio
	delegado.	
time	La hora a la que se envió la notificación EventBridge. Formato: yyyy-mm-ddThh:mm:ssZ .	Sí

Parámetro	Description (Descripción)	Obligatorio
region	A la Región de AWS que se envió la notificación.	Sí

 Note

Este campo no indica la región afectada por este AWS Health evento. Esa información se ofrece en detail.eventRegion.

Parámetro	Description (Descripción)	Obligatorio
resources	<p>Describe la lista de recursos afectados, en su caso, de una cuenta.</p> <p>Este campo está vacío si no se hace referencia a ningún recurso.</p>	No
detail	<p>La sección que contiene los detalles del AWS Health evento, tal como se describe en la tabla que sigue a este.</p>	Sí

Contenido del esquema del parámetro “detail”

La siguiente tabla documenta el contenido del parámetro de detalle del esquema del AWS Health evento.

AWS Health esquema de eventos: contenido detallado del parámetro

contenido del parámetro "detail"	Description (Descripción)	Obligatorio
eventArn	<p>El identificador único del AWS Health evento para la región específica, incluidos la región y el identificador del evento.</p> <div style="border: 1px solid #ccc; padding: 10px; border-radius: 10px; margin-top: 10px;"> <p>i Note</p> <p>El ARN de un evento no es exclusivo de una región Cuenta de AWS o región específica.</p> </div>	Sí
service	<p>El Servicio de AWS afectado por el AWS Health evento. Por ejemplo, Amazon EC2, Amazon Simple Storage Service, Amazon Redshift o Amazon Relational Database Service.</p>	Sí
eventTypeCode	<p>El identificador único para el tipo de evento. Por ejemplo: AWS_EC2_INSTANCE_NETWORK_MAINTENANCE_SCHEDULED y AWS_EC2_INSTANCE_REBOOT_MAINTENANCE_SCHEDULED. Los eventos que incluyen MAINTENANCE_SCHEDULED suelen producirse aproximadamente dos</p>	Sí

contenido del parámetro "detail"	Description (Descripción)	Obligatorio
	<p>semanas antes de la hora de inicio.</p> <div style="border: 1px solid #ccc; padding: 10px; border-radius: 10px; margin-top: 10px;"> <p> Note</p> <p>Todos los nuevos eventos del ciclo de vida planificados tienen el tipo de evento AWS_{SERVICE}_PLAN_NED_LIFECYCLE_EVENT .</p> </div>	
eventTypeCategory	El código de categoría del evento. Los valores admitidos son issue, accountNotification, investigation y scheduledChange .	Sí
eventScopeCode	Indica si el AWS Health evento es público o específico de la cuenta. Los valores admitidos son ACCOUNT_SPECIFIC o PUBLIC.	Sí

contenido del parámetro "detail"	Description (Descripción)	Obligatorio
communicationId	<p>Un identificador único para esta comunicación del AWS Health evento.</p> <p>Los mensajes con el mismo identificador de comunicación pueden ser mensajes de respaldo o páginas de un solo AWS Health evento. Este identificador se puede utilizar con el ID de la cuenta para ayudar a desduplicar mensajes.</p> <p>Gracias a la AWS Health función de paginación de eventos, el identificador de comunicación incluye el número de página para que el identificador de comunicación sea único en todas las páginas, por ejemplo, 12345678910-1. Para obtener más información, consulte Visualización de listas paginadas de eventos en AWS Health EventBridge.</p>	Sí

contenido del parámetro "detail"	Description (Descripción)	Obligatorio
startTime	<p>La hora de inicio del AWS Health evento, en el formato. DoW, DD, MMM, YYYY, HH:MM:SS TZ</p> <p>La hora de inicio puede ser en el futuro para eventos programados.</p>	Sí
endTime	<p>La hora de finalización del AWS Health evento, en el formato:DoW, DD MMM YYYY HH:MM:SS TZ.</p> <p>No se puede proporcionar la hora de finalización de eventos programados en una hora futura.</p>	No
lastUpdatedTime	<p>La hora de la última actualización del AWS Health evento, en el formatoDoW, DD MMM YYYY HH:MM:SS TZ.</p>	Sí
statusCode	<p>El estado del AWS Health evento.</p> <p>Los valores admitidos son open, closed y upcoming.</p>	Sí
eventRegion	<p>La región afectada descrita por este AWS Health evento.</p>	Sí

contenido del parámetro "detail"	Description (Descripción)	Obligatorio
eventDescription	<p>Una sección que describe el AWS Health evento. Incluye campos de idioma y texto para describir el evento.</p> <ul style="list-style-type: none">• idioma: el código del idioma utilizado en el AWS Health evento. Por lo general, esto lo determina la región en la que se publica el evento. Por ejemplo, en la región <code>us-east-1</code> suele ser <code>en_US</code>.• Última descripción: describe el AWS Health evento tal como se representa desde la AWS Health API y, por lo general, aparece en el AWS Health panel de control.	Sí

 Note

En el caso de eventos públicos, solo contiene la última actualización y no el historial completo del evento.

contenido del parámetro “detail”	Description (Descripción)	Obligatorio
eventMetadata	<p>Metadatos del evento adicionales que se pueden proporcionar para el evento de AWS Health .</p> <ul style="list-style-type: none">• <clave de metadatos 1>: cadenas de pares clave-valor de metadatos: “cadenclave1”: “valorclave1” <p>Los pares clave-valor de los metadatos del evento los determina el servicio que envió el evento. AWS Health</p>	No

contenido del parámetro "detail"	Description (Descripción)	Obligatorio
affectedEntities	<p>Matriz que describe el valor de los recursos y el estado de los recursos afectados dentro del AWS Health evento.</p> <ul style="list-style-type: none"> • EntityValue: el resource/entity ID. • lastUpdatedTime: hora a la que se actualizó este resource/entity estado por última vez, en el formato. DoW, DD MMM YYYY HH:MM:SS TZ • status: estado del recurso o la entidad afectados. Los valores admitidos son IMPAIRED, UNIMPAIRE D, PENDING, RESOLVED y UNKNOWN. 	No

contenido del parámetro "detail"	Description (Descripción)	Obligatorio
page	<p>La página que representa este mensaje. Para obtener más información, consulte Visualización de listas paginadas de eventos en AWS Health EventBridge.</p> <div style="border: 1px solid #ccc; padding: 10px; border-radius: 10px; margin-top: 10px;"> <p>i Note</p> <p>La paginación solo se produce en los recursos. Si se supera el límite de tamaño de 256 KB por otro motivo, se producirá un error en la comunicación.</p> </div>	Sí
totalPages	<p>La cantidad total de páginas para este evento de estado. Para obtener más información, consulte Visualización de listas paginadas de eventos en AWS Health EventBridge.</p> <p>Puede utilizar este valor para averiguar si ha recibido todas las páginas de una comunicación de varias páginas para una cuenta.</p>	Sí

contenido del parámetro "detail"	Description (Descripción)	Obligatorio
Evento de copia de seguridad	Este indicador filtra los eventos de respaldo en la región de respaldo designada dentro de una partición si los clientes no desean aprovechar la redundancia. Este valor puede ser verdadero o falso.	Sí
affectedAccount	<p>ID de cuenta de la cuenta afectada.</p> <p>Puede ser diferente del valor del account campo si este evento de salud se envía a una cuenta que forma parte de una AWS Organizations y se recibe en la cuenta de administración o de administrador delegado.</p>	Sí
capacidad de acción	<p>Metadatos para activar la determinación programática de qué eventos requieren una acción sin necesidad de una inspección manual.</p> <p>El valor posible (único) puede ser ACTION_REQUIRED , ACTION_MAILED , ACTION_BE_REQUIRED , o INFORMATIONAL .</p>	No

contenido del parámetro "detail"	Description (Descripción)	Obligatorio
personas	Esta lista de metadatos activa la determinación programática de a qué parte interesada dirigir el evento. Los valores posibles (múltiples) son OPERATIONAL SECURITY, y BILLING.	No

Public Health Event: problema EC2 operativo de Amazon

```
{
  "version": "0",
  "id": "7bf73129-1428-4cd3-a780-95db273d1602",
  "detail-type": "AWS Health Event",
  "source": "aws.health",
  "account": "123456789012",
  "time": "2023-01-27T09:01:22Z",
  "region": "af-south-1",
  "resources": [],
  "detail": {
    "eventArn": "arn:aws:health:af-south-1::event/EC2/AWS_EC2_OPERATIONAL_ISSUE/AWS_EC2_OPERATIONAL_ISSUE_7f35c8ae-af1f-54e6-a526-d0179ed6d68f",
    "service": "EC2",
    "eventTypeCode": "AWS_EC2_OPERATIONAL_ISSUE",
    "eventTypeCategory": "issue",
    "eventScopeCode": "PUBLIC",
    "communicationId": "01b0993207d81a09dc552ebd1e633e36cf1f09a-1",
    "startTime": "Fri, 27 Jan 2023 06:02:51 GMT",
    "endTime": "Fri, 27 Jan 2023 09:01:22 GMT",
    "lastUpdatedTime": "Fri, 27 Jan 2023 09:01:22 GMT",
    "statusCode": "open",
    "eventRegion": "af-south-1",
    "eventDescription": [
      {
        "language": "en_US",
        "latestDescription": "Current severity level: Operating normally\n\n[RESOLVED] \n\n [03:15 PM PST] We continue see recovery\n\nThe following AWS"
    }
  ]
}
```

```
services were previously impacted but are now operating normally: APPSYNC, BACKUP,  
EVENTS."  
        ],  
        "affectedEntities": [],  
        "page": "1",  
        "totalPages": "1",  
        "backupEvent": "true",  
        "affectedAccount": "123456789012"  
    }  
}
```

AWS Health Evento específico de la cuenta: problema con la API de Elastic Load Balancing

```
{  
    "version": "0",  
    "id": "121345678-1234-1234-1234-123456789012",  
    "detail-type": "AWS Health Event",  
    "source": "aws.health",  
    "account": "123456789012",  
    "time": "2022-06-10T06:27:57Z",  
    "region": "ap-southeast-2",  
    "resources": [],  
    "detail": {  
        "eventArn": "arn:aws:health:ap-southeast-2::event/  
AWS_ELASTICLOADBALANCING_API_ISSUE_90353408594353980",  
        "service": "ELASTICLOADBALANCING",  
        "eventTypeCode": "AWS_ELASTICLOADBALANCING_API_ISSUE",  
        "eventTypeCategory": "issue",  
        "eventScopeCode": "ACCOUNT_SPECIFIC",  
        "communicationId": "01b0993207d81a09dc552ebd1e633e36cf1f09a-1",  
        "startTime": "Fri, 10 Jun 2022 05:01:10 GMT",  
        "endTime": "Fri, 10 Jun 2022 05:30:57 GMT",  
        "statusCode": "open",  
        "eventRegion": "ap-southeast-2",  
        "eventDescription": [{  
            "language": "en_US",  
            "latestDescription": "A description of the event will be provided here"  
        }],  
        "page": "1",  
        "totalPages": "1",  
        "backupEvent": "true",  
    }  
}
```

```
        "affectedAccount": "123456789012"
    }
}
```

AWS Health Evento específico de la cuenta: disminución del rendimiento de Amazon EC2 Instance Store Drive

```
{
    "version": "0",
    "id": "121345678-1234-1234-1234-123456789012",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2022-06-03T06:27:57Z",
    "region": "us-west-2",
    "resources": [
        "i-abcd1111"
    ],
    "detail": {
        "eventArn": "arn:aws:health:us-west-2::event/
AWS_EC2_INSTANCE_STORE_DRIVE_PERFORMANCE_DEGRADED_90353408594353980",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_INSTANCE_STORE_DRIVE_PERFORMANCE_DEGRADED",
        "eventTypeCategory": "issue",
        "eventScopeCode": "ACCOUNT_SPECIFIC",
        "communicationId": "01b0993207d81a09dc552ebd1e633e36cf1f09a-1",
        "startTime": "Fri, 3 Jun 2022 05:01:10 GMT",
        "endTime": "Fri, 3 Jun 2022 05:30:57 GMT",
        "statusCode": "open",
        "eventRegion": "us-west-2",
        "eventDescription": [
            {
                "language": "en_US",
                "latestDescription": "A description of the event will be provided here"
            }
        ],
        "affectedEntities": [
            {
                "entityValue": "i-abcd1111"
            }
        ],
        "page": "1",
        "totalPages": "1",
        "backupEvent": "true",
        "affectedAccount": "123456789012"
    }
}
```

}

Supervisión AWS Health

El monitoreo es una parte importante del mantenimiento de la confiabilidad, la disponibilidad y el rendimiento de AWS Health sus demás AWS soluciones. AWS proporciona las siguientes herramientas de supervisión para observar AWS Health, informar cuando algo va mal y tomar las medidas necesarias:

- Amazon CloudWatch monitorea tus AWS recursos y las aplicaciones en las que AWS ejecuta en tiempo real. Puede recopilar métricas y realizar un seguimiento de las métricas, crear paneles personalizados y definir alarmas que le advierten o que toman medidas cuando una métrica determinada alcanza el umbral que se especifique. Para obtener más información, consulta la [Guía del CloudWatch usuario de Amazon](#).

Puedes usar Amazon EventBridge para recibir notificaciones sobre AWS Health eventos que puedan afectar a tus servicios y recursos. Por ejemplo, si AWS Health publica un evento sobre tus EC2 instancias de Amazon, puedes usar estas notificaciones para tomar medidas y actualizar o reemplazar tus recursos según sea necesario. Para obtener más información, consulte [Monitorización de eventos AWS Health con Amazon EventBridge](#).

- AWS CloudTrail captura las llamadas a la API y los eventos relacionados realizados por su AWS cuenta o en su nombre y entrega los archivos de registro a un bucket de Amazon S3 que especifique. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. Para obtener más información, consulte la [Guía del usuario de AWS CloudTrail](#).

Temas

- [Registrar las llamadas a la AWS Health API con AWS CloudTrail](#)

Registrar las llamadas a la AWS Health API con AWS CloudTrail

AWS Health está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en AWS Health. CloudTrail captura las llamadas a la API AWS Health como eventos. Las llamadas capturadas incluyen llamadas desde la AWS Health consola y llamadas en código a las operaciones de la AWS Health API. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos para AWS Health. Si no configura una ruta, podrá ver los eventos más recientes en la

CloudTrail consola, en el historial de eventos. Con la información recopilada por usted CloudTrail, puede determinar el destinatario de la solicitud AWS Health, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, incluido cómo configurarla y habilitarla, consulta la [Guía del AWS CloudTrail usuario](#).

AWS Health información en CloudTrail

CloudTrail está habilitada en su AWS cuenta al crear la cuenta. Cuando se produce una actividad de eventos admitida AWS Health, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puedes ver, buscar y descargar los eventos recientes en tu AWS cuenta. Para obtener más información, consulte [Visualización de eventos con el historial de CloudTrail eventos](#).

Para tener un registro continuo de los eventos de tu AWS cuenta, incluidos los eventos de tu cuenta AWS Health, crea una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando crea una ruta en la consola, la ruta se aplica a todas AWS las regiones. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- [Introducción a la creación de registros de seguimiento](#)
- [CloudTrail Integraciones y servicios compatibles](#)
- [Configuración de las notificaciones de Amazon SNS para CloudTrail](#)
- [Recibir archivos de CloudTrail registro de varias regiones](#) y [recibir archivos de CloudTrail registro de varias cuentas](#)

Todas las operaciones de la AWS Health API se registran CloudTrail y se documentan en la [Referencia de la AWS Health API](#). Por ejemplo, las llamadas a las `DescribeEvents` `DescribeAffectedEntities` operaciones y las operaciones generan entradas en los archivos de CloudTrail registro. `DescribeEventDetails`

AWS Health admite el registro de las siguientes acciones como eventos en los archivos de CloudTrail registro:

- Si la solicitud se realizó con las credenciales raíz o las credenciales de IAM
- si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado
- Si la solicitud la realizó otro AWS servicio

Para obtener más información, consulte el [Elemento userIdentity de CloudTrail](#).

Puede almacenar sus archivos de registro en el bucket de Amazon S3 durante el tiempo que quiera. También puede definir reglas de ciclo de vida de Amazon S3 para archivar o eliminar archivos de registros de forma automática. De forma predeterminada, los archivos de registro se cifran con cifrado del servidor (SSE) de Amazon S3.

Para recibir una notificación cuando se entreguen los archivos de registro, puede CloudTrail configurar la publicación de notificaciones de Amazon SNS cuando se entreguen nuevos archivos de registro. Para obtener más información, consulte [Configuring Amazon SNS Notifications for CloudTrail](#).

También puede AWS Health agrupar archivos de registro de varias AWS regiones y AWS cuentas en un único bucket de Amazon S3.

Para obtener más información, consulte [Recibir archivos de registro de CloudTrail de varias regiones](#) y [Recibir archivos de registro de CloudTrail de varias cuentas](#).

Ejemplo: entradas de archivos de AWS Health 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 demuestra la [DescribeEntityAggregates](#) operación.

```
{  
  "Records": [  
    {  
      "eventVersion": "1.05",  
      "awsRegion": "us-east-1",  
      "sourceService": "Amazon CloudWatch Metrics",  
      "sourceType": "CloudWatch Metrics",  
      "awsRequestID": "12345678901234567890123456789012",  
      "eventTime": "2018-01-01T00:00:00Z",  
      "eventName": "DescribeEntityAggregates",  
      "userIdentity": {  
        "type": "AWS",  
        "principal": "arn:aws:iam::123456789012:root",  
        "arn": "arn:aws:iam::123456789012:root",  
        "accountId": "123456789012",  
        "accessKeyId": "ASIAQWERTYUICL",  
        "sessionContext": {  
          "sessionIssuer": {  
            "type": "AWS",  
            "principal": "arn:aws:iam::123456789012:root",  
            "arn": "arn:aws:iam::123456789012:root",  
            "accountId": "123456789012",  
            "accessKeyId": "ASIAQWERTYUICL",  
            "sessionName": "CloudTrail-Session-12345678901234567890123456789012",  
            "sessionDuration": 3600  
          },  
          "stsAssumeRoleContext": {  
            "roleArn": "arn:aws:iam::123456789012:role/CloudTrail-Role-12345678901234567890123456789012",  
            "roleSessionName": "CloudTrail-Session-12345678901234567890123456789012",  
            "awsSdkVersion": "aws-sdk-nodejs",  
            "stsSessionToken": "WJLk...PQ",  
            "stsSessionId": "12345678901234567890123456789012",  
            "stsExternalId": null  
          }  
        }  
      }  
    }  
  ]  
}
```

```
"userIdentity": {  
    "type": "IAMUser",  
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",  
    "arn": "arn:aws:iam::123456789012:user/JaneDoe",  
    "accountId": "123456789012",  
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",  
    "userName": "JaneDoe",  
    "sessionContext": {"attributes": {  
        "mfaAuthenticated": "false",  
        "creationDate": "2016-11-21T07:06:15Z"  
    }},  
    "invokedBy": "AWS Internal"  
},  
"eventTime": "2016-11-21T07:06:28Z",  
"eventSource": "health.amazonaws.com",  
"eventName": "DescribeEntityAggregates",  
"awsRegion": "us-east-1",  
"sourceIPAddress": "203.0.113.0",  
"userAgent": "AWS Internal",  
"requestParameters": {"eventArns": ["arn:aws:health:us-east-1::event/EBS/  
EBS_LOST_VOLUME/EBS_LOST_VOLUME_123"]},  
"responseElements": null,  
"requestID": "05b299bc-afb9-11e6-8ef4-c34387f40bd4",  
"eventID": "e4deb9dc-dbc2-4bdb-8515-73e8abcbc29b",  
"eventType": "AwsApiCall",  
"recipientAccountId": "123456789012"  
}  
],  
...  
}
```

Historial de documentos para AWS Health

En la siguiente tabla se describe la documentación de esta versión de AWS Health.

- Versión de API: 2016-08-04

En la siguiente tabla se describen las actualizaciones importantes de la AWS Health documentación, que comenzarán el 28 de agosto de 2020. Puede suscribirse a una fuente RSS para recibir notificaciones sobre actualizaciones.

Cambio	Descripción	Fecha
<u>Se actualizó la opción Administrar AWS Health notificaciones en AWS User Notifications</u>	información actualizada en esta sección para reflejar la migración de AWS Health eventos a AWS User Notifications. Para obtener más información, consulte <u>Administrar AWS Health notificaciones en AWS User Notifications</u> .	22 de diciembre de 2025
<u>Se actualizó el monitoreo de eventos públicos y específicos de la cuenta para AWS Health</u>	Se agregó información a esta sección que detalla el comportamiento de las reglas de respaldo para eventos públicos y eventos específicos de la cuenta. Para obtener más información, consulte <u>Reglas de Backup para AWS Health eventos</u> .	11 de diciembre de 2025
<u>Se agregó información sobre los campos Actionability y Personas para los eventos de Health</u>	Se agregó información sobre los campos Actionability y Personas en la sección Conceptos de la AWS Health sección Conceptos y sobre	20 de noviembre de 2025

el contenido del esquema del parámetro «detalles» en la sección Referencia: Amazon EventBridge esquema de AWS Health eventos. Para obtener más información, consulte [Conceptos AWS Health](#) y [referencia: Amazon EventBridge esquema de AWS Health eventos](#).

[Sección actualizada: Creación de EventBridge reglas de Región de AWS cobertura](#)

Información actualizada para crear EventBridge reglas. Para obtener más información, consulte [Crear EventBridge reglas de Región de AWS cobertura](#).

[Sección actualizada: Administrar AWS Health las notificaciones en AWS User Notifications](#)

Información actualizada sobre los pasos para configurar tu suscripción a notificaciones AWS gestionadas para AWS Health eventos. Para obtener más información, consulte [Administrar AWS Health las notificaciones en AWS User Notifications](#).

[Sección actualizada: Monitorización de eventos en AWS Health Amazon EventBridge](#)

Información actualizada en la nota para AWS Health enviar eventos a EventBridge. Para obtener más información, consulta [Supervisar eventos en AWS Health Amazon EventBridge](#).

3 de noviembre de 2025

16 de septiembre de 2025

15 de septiembre de 2025

<u>Sección actualizada: AWS Health Panel de control</u>	Se eliminaron los pasos opcionales para suscribirse a la fuente RSS para eventos de salud. Se ha añadido una nota que para recibir notificaciones de eventos de salud, los clientes pueden utilizar EventBridge. Para obtener más información, consulte el AWS Health Panel de control .	15 de agosto de 2025
<u>Sección actualizada: Monitorización de eventos en AWS Health Amazon EventBridge</u>	Se ha eliminado el tema Instalación de un rol vinculado a un servicio para usar la detección y respuesta a AWS incidentes al monitorear eventos en Amazon AWS Health EventBridge	8 de agosto de 2025
<u>Sección actualizada: Monitorización de eventos en AWS Health Amazon EventBridge</u>	Se agregó información a la sección Notas que indica que puede haber un retraso de hasta una hora antes de que comience a recibir notificaciones de eventos de salud pública. Para obtener más información, consulta Monitorización de eventos en AWS Health Amazon EventBridge	22 de julio de 2025

<u>Sección actualizada: Habilitar la visión organizacional</u>	<p>Se agregó información a la sección de notas que indica que, al activar la vista organizacional, se agregan AWS Health automáticamente todos los eventos de salud históricos de la organización. Los eventos históricos pueden tardar hasta 24 horas en aparecer en la vista de la organización. Para obtener más información, consulta Cómo habilitar la vista organizacional</p>	27 de junio de 2025
<u>Sección actualizada: Agregación de AWS Health eventos entre cuentas</u>	<p>Se ha eliminado una nota que AWS Health no muestra los eventos que ocurrieron antes de activar la vista de organización. Para obtener más información, consulta Cómo agregar AWS Health eventos entre cuentas</p>	27 de junio de 2025
<u>WorkDocs en desuso</u>	<p>Se eliminaron las referencias a lo obsoleto WorkDocs en los eventos del ciclo de vida planificado para AWS Health</p>	19 de junio de 2025

<u>Se agregó una nota sobre el cronograma de migración de las notificaciones AWS administradas</u>	Se ha añadido una nota sobre las fechas clave de la migración del correo electrónico a las notificaciones AWS gestionadas en AWS User Notifications. Para obtener más información, consulte <u>Administrador AWS Health notificaciones en AWS User Notifications</u> .	28 de abril de 2025
<u>Eventos del ciclo de vida planificados actualizados</u>	Se actualizaron los eventos del ciclo de vida planificado para indicar que AWS Health los eventos permanecen abiertos durante 4 años en lugar de 90 días en el caso de los recursos no resueltos. Para obtener más información, consulta la sección ¿Qué debo esperar cuando reciba una notificación sobre un evento del ciclo de vida planificado? en la sección <u>Eventos del ciclo de vida planificado para AWS Health</u> .	18 de abril de 2025

<u>Se actualizó la descripción de la lista de recursos afectados para los eventos del ciclo de vida planificados</u>	<p>La lista de recursos afectados para los eventos del ciclo de vida planificado normalmente se actualiza una vez cada 24 horas, pero puede tardar hasta 72 horas en reflejar el estado actual de los recursos. Para obtener más información, consulte la sección Detalles del evento en Cómo ver los eventos de su cuenta en el AWS Health panel de control.</p>	7 de abril de 2025
<u>Se ha añadido una sección de preguntas frecuentes para gestionar AWS Health las notificaciones en AWS User Notifications</u>	<p>Para obtener más información, consulta Administrar las notificaciones en las AWS User Notifications Preguntas frecuentes.</p>	18 de febrero de 2025
<u>Se agregó información sobre las solicitudes IPv6 exclusivas a puntos finales.</u>	<p>Para obtener más información, consulta Elegir puntos de enlace para AWS Health las solicitudes de API.</p>	28 de enero de 2025
<u>Gestione las AWS Health notificaciones en AWS User Notifications</u>	<p>Para obtener más información, consulte Administrar notificaciones en AWS User Notifications.</p>	16 de enero de 2025
<u>Se corrigió el JSON en la monitorización de AWS Health eventos con Amazon EventBridge</u>	<p>Para obtener más información, consulta Supervisar AWS Health eventos con Amazon EventBridge.</p>	3 de septiembre de 2024
<u>Se actualizó la información sobre la descarga de recursos afectados</u>	<p>Para obtener más información, consulte Vista de recursos afectados.</p>	27 de julio de 2024

<u>Se eliminó la privacidad del tráfico entre redes de la sección Seguridad de la documentación de AWS Health</u>	Para obtener más información, consulte Seguridad en AWS Health .	27 de marzo de 2024
<u>Se actualizó la documentación de AWS Health Dashboard: estado del servicio y Eventos del ciclo de vida planificado para AWS Health .</u>	Para obtener más información, consulte AWS Health Dashboard: estado del servicio y Eventos del ciclo de vida planificado para AWS Health.	15 de febrero de 2024
<u>Se ha eliminado una viñeta duplicada al crear una EventBridge regla para AWS Health</u>	Se ha eliminado una viñeta duplicada en Crear una EventBridge regla para AWS Health .	4 de diciembre de 2023
<u>Documentación añadida para Eventos del ciclo de vida planificado</u>	Para obtener más información, consulte Eventos del ciclo de vida planificado para AWS Health .	31 de octubre de 2023
<u>Documentación actualizada para AWSHealthFullAccess</u>	Ahora puede utilizar la política administrada por AWSHealthFullAccess en las AWS GovCloud (US) Regions. Consulte las políticas AWS gestionadas para AWS Health .	16 de octubre de 2023
<u>Se agregó documentación para configurar las notificaciones AWS de usuario en AWS Health.</u>	Ahora puede configurar las notificaciones AWS de usuario en AWS Health. Para obtener más información, consulte Configurar las notificaciones AWS de usuario para AWS Health .	30 de agosto de 2023

<u>Se agregó documentación sobre la función de administrador delegado a la sección de agregación de AWS Health eventos.</u>	Para obtener más información, consulte <u>Vista de administrador delegado de la organización.</u>	27 de julio de 2023
<u>Actualización de la política de SLR</u>	Actualización de la política AWS gestionada: Health_. OrganizationsServiceRolePolicy Para más información, consulte <u>Políticas administradas de AWS para AWS Health.</u>	19 de julio de 2023
<u>AWS Health El esquema ahora admite metadatos de eventos</u>	Ahora puede recibir metadatos de AWS Health eventos de los eventos. Para obtener más información, consulta <u>Supervisar AWS Health eventos con Amazon EventBridge.</u>	20 de junio de 2023
<u>Documentación actualizada para Amazon EventBridge</u>	Ahora puedes usar una EventBridge regla de Amazon para monitorear tanto los eventos públicos como los específicos de la cuenta. Para obtener más información, consulta <u>Supervisar AWS Health eventos con Amazon EventBridge.</u>	2 de mayo de 2023
<u>Se ha añadido documentación para las políticas AWS gestionadas</u>	Documentación añadida para las políticas administradas por <u>AWS para AWS Health</u> y el <u>uso de roles vinculados a servicios para AWS Health.</u>	18 de enero de 2023

<u>Documentación añadida sobre la configuración de la zona horaria</u>	Usa la nueva función de zona horaria para ver el AWS Health panel en tu zona horaria local o en UTC. Para obtener más información, consulta <u>Cómo empezar con el AWS Health panel de control: El estado de tu cuenta</u> y el <u>AWS Health panel de control: estado del servicio</u> .	21 de septiembre de 2022
<u>Documentación actualizada</u>	Se agregó documentación para AWS Health Aware. Para obtener más información, consulte <u>AWS Health Aware</u> .	25 de mayo de 2022
<u>Documentación actualizada</u>	Los Service Health Dashboard y los AWS Personal Health Dashboard han cambiado de nombre a AWS Health Dashboard. Para obtener más información, consulte <u>Cómo empezar con el AWS Health panel de control: estado de su cuenta</u> y <u>AWS Health Panel de control: estado del servicio</u> .	28 de febrero de 2022
<u>Documentación actualizada para Amazon EventBridge</u>	Nuevo tema sobre AWS Health el uso de Amazon EventBridge para monitorear eventos de Salud. Para obtener más información, consulta <u>Supervisar AWS Health eventos con Amazon EventBridge</u> .	3 de febrero de 2022

Documentación actualizada	Si tienes un plan Enterprise On-Ramp Support, puedes usar la AWS Health API.	24 de noviembre de 2021
Se agregó documentación	Nuevo tema de AWS Health conceptos. Para obtener más información, consulte Conceptos de AWS Health .	29 de julio de 2021
Documentación actualizada para CloudWatch eventos	Se agregó una sección sobre cómo crear una regla para varios servicios y categorías de tipos de eventos. Para obtener más información, consulte Cómo crear una regla para varios servicios y categorías .	7 de mayo de 2021
Documentación actualizada para CloudWatch eventos	Se ha actualizado la sección para automatizar AWS Systems Manager las acciones de las reglas de Amazon CloudWatch Events. Para obtener más información, consulta Automatizar acciones para EC2 instancias de Amazon .	28 de abril de 2021
Documentación actualizada para eventos CloudWatch	Se ha añadido una sección para recibir AWS Health eventos en tu cliente de chat. Para obtener más información, consulte Recibir AWS Health eventos con Amazon Q Developer en aplicaciones de chat .	16 de marzo de 2021

<u>Documentación actualizada</u>	Se han actualizado los temas siguientes: <ul style="list-style-type: none">• Se ha actualizado el tema <u>Cómo agregar AWS Health eventos</u>• Se reorganizó y actualizó el <u>tema Monitor de AWS Health eventos con Amazon CloudWatch Events</u>• Se actualizó la sección <u>Condiciones basadas en recursos y acciones</u>	29 de enero de 2021
<u>Se agregó el AWS Health panel de control para ver la organización en la AWS Health consola</u>	Puede utilizar la AWS Health consola para activar la función de visualización de la organización. A continuación, podrá ver los eventos de estado de las cuentas de los miembros de su organización de AWS .	14 de diciembre de 2020
<u>Demostración del punto de conexión de alta disponibilidad</u>	Puede usar el código de ejemplo para determinar el punto final regional activo y la AWS región de firma para la que se está firmando AWS Health.	22 de octubre de 2020
<u>Actualizaciones de la Guía del usuario de AWS Health</u>	La organización actualiza y añade una fuente RSS para que puedas suscribirte a las últimas actualizaciones de la AWS Health documentación.	28 de agosto de 2020

Actualizaciones anteriores

Cambio	Descripción	Fecha
Se ha actualizado el tema de la vista organizativa para incluir ejemplos.	Consulte Aregar AWS Health eventos en todas las cuentas.	3 de junio de 2020
Seguridad y AWS Health	Se ha agregado información sobre las consideraciones de seguridad cuando se utiliza AWS Health. Consulte Seguridad en AWS Health.	5 de mayo de 2020
Se ha agregado una nueva sección para explicar cómo utilizar la vista organizativa para los eventos agregados en todas las cuentas de AWS Organizations.	Consulte Aregar AWS Health eventos en todas las cuentas.	18 de diciembre de 2019
Se agregó una nueva sección «Condiciones basadas en recursos y acciones» para explicar las restricciones de eventos que ofrece la API. AWS Health	Consulte Administración de identidades y accesos para AWS Health.	2 de agosto de 2018
Se agregó una nota sobre la visibilidad de la información. AWS Health	Consulte Administración de identidades y accesos para AWS Health.	16 de agosto de 2017
Lanzamiento del servicio.	AWS Health publicado.	1 de diciembre de 2016

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la versión original de inglés, prevalecerá la versión en inglés.