



Guía del usuario

AWS Health



AWS Health: Guía del usuario

Copyright © 2024 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
¿Es la primera vez que usa AWS Health?	2
Conceptos para AWS Health	4
AWS Health evento	4
Evento específico de cuenta	5
Evento público	5
AWS Health Tablero	5
AWS Health Panel de control: estado del servicio	6
Código de tipo de evento	6
Categorías de tipos de eventos	6
Estado del evento	8
Entidades afectadas	8
AWS Health eventos en Amazon EventBridge	8
AWS Health API	9
Vista organizativa	9
AWS Health Panel de control: estado del servicio	10
Eventos del ciclo de vida planificados para AWS Health	13
¿Qué son los eventos del ciclo de vida planificado?	13
¿Qué debo esperar cuando recibo una notificación de un evento de ciclo de vida planificado?	14
Modelo de responsabilidad compartida para resiliencia	17
Acceder a los eventos planificados del ciclo de vida	17
Comience con su AWS Health panel de control: el estado de su cuenta	19
Consulta los eventos de la cuenta en el AWS Health panel de control	20
Problemas abiertos y recientes	20
Cambios programados	22
Otras notificaciones	23
Registro de eventos	23
Detalles del evento	24
Tipos de eventos	26
Vista del calendario	26
Vista de los recursos afectados	27
Configuración de la zona horaria	29
El estado de su organización	29

Configurar Amazon EventBridge	30
AWS Health Consciente	30
Alertas de eventos AWS Health	31
Configuración de notificaciones de usuario de AWS para AWS Health	32
Acceder al AWS Health API	33
puntos de conexión	33
Uso de la demostración de punto de conexión de alta disponibilidad	35
Uso de demostración para Java	35
Uso de la demostración de Python	38
Firmar solicitudes AWS Health API	41
Operaciones compatibles con AWS Health	41
Código Java de ejemplo	43
Paso 1: Inicializar las credenciales	44
Paso 2: Inicializar un cliente de API de AWS Health	44
Paso 3: Utilizar las operaciones de la API de AWS Health para obtener información sobre los eventos	44
Seguridad	48
Protección de datos	49
Cifrado de datos	50
Administración de identidades y accesos	50
Público	51
Autenticación con identidades	51
Administración de acceso mediante políticas	55
¿Cómo AWS Health funciona con IAM	57
Ejemplos de políticas basadas en identidades	63
Resolución de problemas	76
Uso de roles vinculados a servicios	79
AWS políticas gestionadas para AWS Health	81
Inicio de sesión y supervisión AWS Health	86
Validación de conformidad	87
Resiliencia	88
Seguridad de la infraestructura	89
Configuración y análisis de vulnerabilidades	89
Prácticas recomendadas de seguridad	89
Otorgue AWS Health a los usuarios los permisos mínimos posibles	90
Vea el AWS Health Dashboard	90

Intégrelo AWS Health con Amazon Chime o Slack	90
Supervise los AWS Health eventos	90
Agregar eventos de AWS Health	91
Requisitos previos	92
Vista organizativa (consola)	92
Habilitación de la vista organizativa (consola)	93
Visualización de eventos de vista organizativa (consola)	94
Visualización de las cuentas y los recursos afectados (consola)	98
Deshabilitación de la vista organizativa (consola)	100
Vista organizativa (CLI)	100
Habilitación de la vista organizativa (CLI)	101
Visualización de eventos de vista organizativa (CLI)	104
Deshabilitación de la vista organizativa (CLI)	105
Operaciones de la API de AWS Health de vista organizativa	105
Vista de administrador delegado de la organización	107
Registre un administrador delegado para su vista organizativa	107
Elimine un administrador delegado de la vista organizativa	108
Monitorización de eventos de Salud con EventBridge	109
Acerca de Regiones de AWS para AWS Health	110
Acerca de los eventos públicos para AWS Health	111
Procesador de eventos para AWS Health	113
Información relacionada	113
Crear una EventBridge regla para AWS Health	113
Cómo crear una regla para varios servicios y categorías	117
AWS HealthAmazon EventBridge Esquema de eventos	119
AWS Health Esquema de eventos	119
Public Health Event: problema EC2 operativo de Amazon	147
AWS Health Evento específico de la cuenta: problema con Elastic Load Balancing API	148
AWS Health Evento específico de la cuenta: disminución del rendimiento de Amazon EC2 Instance Store Drive	149
Paginación de eventos en AWS Health EventBridge	150
Agregar AWS Health eventos mediante la vista de la organización y el acceso de administrador delegado	150
Recibir eventos AWS Health con AWS Chatbot	151
Requisitos previos	151
Automatizar acciones para instancias de Amazon EC2	153

Requisitos previos	154
Cree una regla para EventBridge	158
Configure SMC los conectores para AWS Health	161
Supervisión AWS Health	162
Registrar AWS Health API las llamadas con AWS CloudTrail	162
AWS Health información en CloudTrail	163
Ejemplo: entradas de archivos de AWS Health registro	164
Historial de documentos	166
Actualizaciones anteriores	172
Glosario de AWS	173
.....	clxxiv

¿Qué es AWS Health?

AWS Health proporciona visibilidad continua del rendimiento de sus recursos y de la disponibilidad de su Servicios de AWS y sus cuentas. Puede utilizar los eventos de AWS Health 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 emite alertas y notificaciones que se activan cuando se producen cambios en el estado de los recursos de AWS, lo que le proporciona una visibilidad casi instantánea de los eventos, además de directrices para ayudarle a acelerar la resolución de problemas.

Todos los clientes pueden usar el [AWS Health Panel de control AWS](#), que funciona con la API AWS Health. El panel no requiere instalación y está listo para que lo utilicen los usuarios [autenticados AWS](#). Para conocer otros aspectos destacados del servicio, consulte la [AWS Health página de detalles del Panel de control](#).

Para comprender los conceptos básicos de AWS Health y cómo usar el servicio, consulte [¿Es la primera vez que usa AWS Health?](#).

Para ver una lista de los términos que verá cuando utilice AWS Health, consulte [Conceptos para AWS Health](#).

Notas

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

¿Es la primera vez que usa AWS Health?

Si es la primera vez que utiliza AWS Health, empiece leyendo las siguientes lecciones:

- [¿Qué es AWS Health?](#): en esta sección se describe el modelo de datos subyacente, las operaciones compatibles y los SDK de AWS que puede utilizar para interactuar con el servicio.
- [Conceptos para AWS Health](#): Conozca los conceptos básicos de AWS Health y los términos que encontrará al utilizar el servicio.
- [Cómo empezar a usar tu AWS Health panel de control: el estado de tu cuenta](#): Aprenda a ver los eventos y las entidades afectadas y a realizar un filtrado avanzado. Este panel incluye eventos específicos de su cuenta y organización.
- [AWS Health Panel de control: estado del servicio](#): Si no tiene un Cuenta de AWS, puede ver información sobre el estado y las situaciones de Servicios de AWS para cada Región de AWS.
- [Monitorización de AWS Health eventos con Amazon EventBridge](#): Puede usar Amazon EventBridge para recibir notificaciones push desde AWS Health.
- [Acceder al AWS Health API](#): En la sección de la API de AWS Health, se describen las operaciones que recuperan información sobre eventos y entidades.

AWS Health cuenta con una consola llamada Panel de control de AWS Health, que está disponible para todos los clientes. No es necesario escribir código ni realizar ninguna operación para instalar el panel.

Puede configurar una regla de EventBridge para recibir eventos de AWS Health en Amazon EventBridge. Esto proporciona una forma de utilizar las notificaciones push para automatizar la gestión de eventos de AWS Health mediante la creación de reglas de Amazon EventBridge para tomar medidas.

Si dispone de un plan de soporte Business, Enterprise On-Ramp o Enterprise, puede obtener acceso a la información que aparece en el panel mediante programación. Puede utilizar la AWS Command Line Interface (AWS CLI) o escribir código para realizar solicitudes, ya sea directamente a través de la API de REST o con los SDK de AWS.

Para obtener más información acerca del uso de eventos de AWS Health en Amazon EventBridge, consulte [Monitorización de AWS Health eventos con Amazon EventBridge](#) Para obtener más información sobre el uso de AWS Health con la AWS CLI, consulte la [Referencia de la AWS CLI de](#)

[AWS Health](#). Para obtener instrucciones sobre cómo instalar la AWS CLI, consulte [Instalación de la AWS Command Line Interface](#).

Conceptos para AWS Health

Obtenga información sobre 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 Tablero](#)
- [Código de tipo de evento](#)
- [Categorías de tipos de eventos](#)
- [Estado del evento](#)
- [Entidades afectadas](#)
- [AWS Health eventos en Amazon EventBridge](#)
- [AWS Health API](#)
- [Vista organizativa](#)

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 CloudWatch Events 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 EE.UU. Este (Ohio) AWS Health , proporciona información sobre el evento, incluso si no utilizas ese servicio o tienes buckets de 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 [Cómo empezar a usar tu AWS Health panel de control: el estado de tu cuenta](#).

Si no tiene una cuenta, consulte [AWS Health Panel de control: estado del servicio](#).

AWS Health Tablero

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 el AWS Health panel AWS Management Console de control en <https://health.aws.amazon.com/health/home>.

Para obtener más información, consulte [Cómo empezar a usar tu AWS Health panel de control: el estado de tu cuenta](#).

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.amazon.com/health/status> 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 Panel de control: estado del servicio](#).

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.

Le recomendamos que monitorice todas las categorías de tipo de eventos. Tenga en cuenta que cada categoría aparece para diferentes tipos de eventos. [También puedes usar la operación de la DescribeEvent API Types 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 instancia de Amazon EC2 requiere reinicializarse.
- `AWS_SAGEMAKER_SCHEDULED_MAINTENANCE`— SageMaker 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 el 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.

Entidades afectadas

Las entidades afectadas son AWS recursos que podrían verse afectados por el evento. Por ejemplo, si recibe un evento programado para el mantenimiento de Amazon EC2 para un tipo de instancia específico que está utilizando en su cuenta, puede usar el evento de estado 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 AWS Health eventos 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 [Agregar eventos de AWS Health en cuentas con vista organizativa](#).

AWS Health Panel de control: estado del servicio

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 pueden afectar a su cuenta y sus servicios. Para obtener más información, consulte [Cómo empezar a usar tu AWS Health panel de control: el estado de tu cuenta](#).

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

1. Diríjase a la página <https://health.aws.amazon.com/health/status>.

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, un Problema operativo: Amazon Elastic Compute Cloud (Norte de Virginia)
 - El nombre del servicio
 - La gravedad del evento, como informacional o Degradación
 - Cronología de las actualizaciones recientes del evento
 - Una lista de las 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](#).

- (Opcional) Junto al evento, seleccione RSS para suscribirse a una fuente RSS de este evento. Recibirá notificaciones sobre este servicio específico en el lugar especificado Región de AWS.
- Seleccione Historial de servicios para ver la tabla de Historial de servicios. En esta tabla se muestran todas Servicio de AWS las interrupciones de los últimos 12 meses.

Tip

Puede filtrar por Servicio, Región de AWS y fecha.

- Junto a un evento de servicio en curso, seleccione el icono de estado



para ver más información sobre el evento.

- (Opcional) Para ver esto como una lista de eventos históricos, pulse el botón de lista de eventos. Elija cualquier evento en la columna de eventos para ver más información sobre ese evento específico 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](#).

Note

Al seleccionar cualquier evento público después de septiembre de 2023, se completará la URL del navegador con un enlace a ese evento público AWS Health . Tras seleccionar

este enlace, accederás a la vista de lista de eventos con la ventana emergente de ese evento.

7. (Opcional) Elija RSS para suscribirse a una fuente RSS. Recibirá notificaciones sobre este servicio específico en el Región de AWS especificado.
8. (Opcional) Puede ver los eventos en su zona horaria local o en UTC. Para obtener más información, consulte [Configuración de la zona horaria](#).
9. (Opcional) Si tiene una cuenta, seleccione Abrir el estado de su cuenta para iniciar sesión. Después de iniciar sesión, podrá ver los eventos específicos de su cuenta. Para obtener más información, consulte [Cómo empezar a usar tu AWS Health panel de control: el estado de tu cuenta](#).

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.](#)
 - [Amazon WorkDocs Companion está llegando al final de su vida útil y ya no está disponible.](#)

Note

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

- 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

- 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 les asignará ningún estado.
- 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 ARN si la organización tiene un gran número de recursos Cuentas de AWS o afectados.

Visibilidad temprana de los eventos del ciclo de vida planificados: los eventos del ciclo de vida planificados están diseñados para tener un plazo mínimo de 180 días para las versiones o cambios principales y de 90 días para las versiones o cambios menores, siempre que sea posible.

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

- 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 Table Calendar

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

< 1 >

Event	Status	Region / Zone <small>Info</small>	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 ⚙️ ✕

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

Affected resources in account 745485236264 (5)

< 1 >

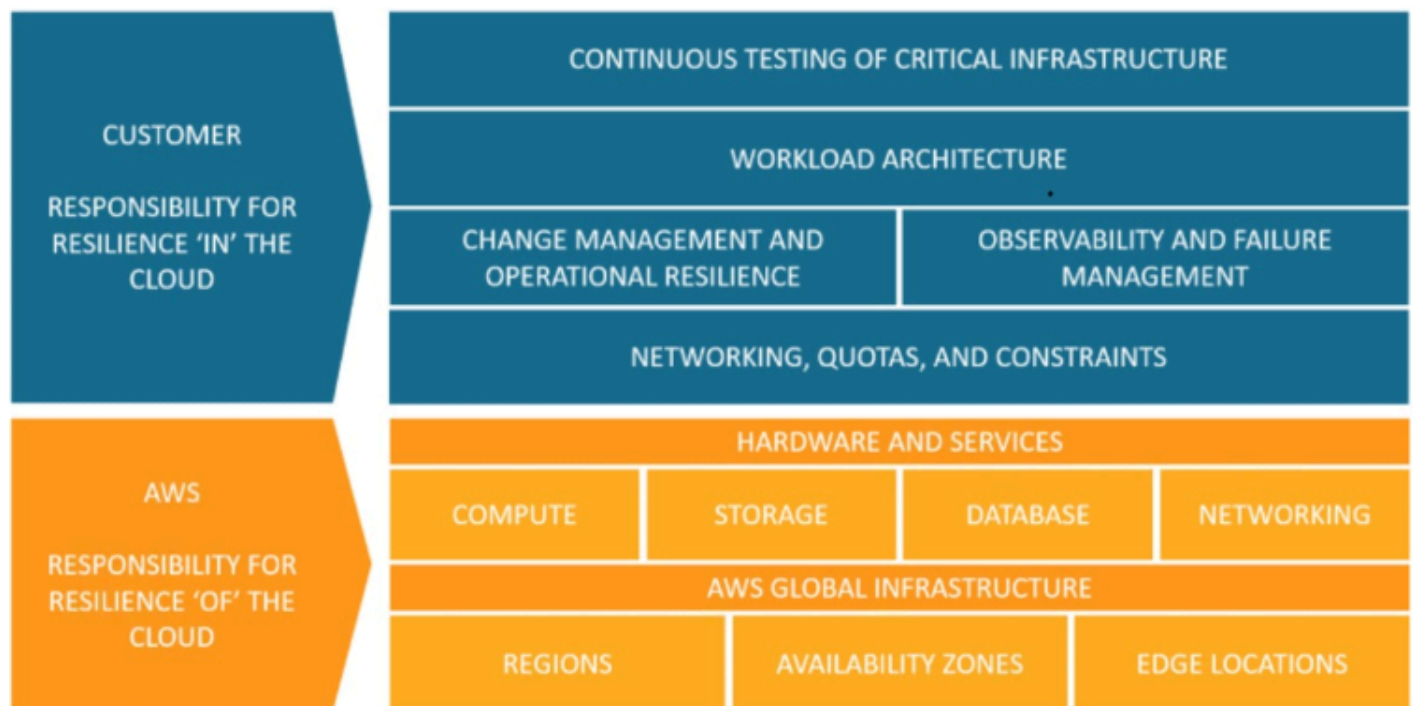
Resource ID / ARN	Resource status	Last update time
arn:aws:eks:us-west-2:745485236264:cluster/prod-ops-cluster	⏸ Pending	15 days ago
arn:aws:eks:us-west-2:745485236264:cluster/nonprod-dev5	⏸ Pending	15 days ago
arn:aws:eks:us-west-2:745485236264:cluster/n-preprd-eks	⏸ Pending	15 days ago
arn:aws:eks:us-west-2:745485236264:cluster/argoworkflows-refactor51	⏸ 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 evento de AWS Health cambiará al estado “Cerrado”.
3. Si tiene recursos pendientes después de la fecha que no se hayan resuelto, el evento de AWS Health permanecerá abierto durante 90 días después de la fecha de inicio o finalización. A continuación, se elimina el evento.

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 del resto del software de aplicación asociado, además de la configuración del firewall del grupo AWS de seguridad suministrado. 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](#)
 - [Vista del calendario](#)
 - [Vista de los recursos afectados](#)

- [Usa la AWS Health API](#)

Cómo empezar a usar tu AWS Health panel de control: el estado de tu cuenta

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 usarla [AWS Health Panel de control: estado del servicio](#) 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.

Contenido

- [Ver los eventos de su cuenta en el panel de control de AWS Health](#)
 - [Problemas abiertos y recientes](#)
 - [Cambios programados](#)
 - [Otras notificaciones](#)
 - [Registro de eventos](#)
- [Detalles del evento](#)
- [Tipos de eventos](#)

- [Vista del calendario](#)
- [Vista de los recursos afectados](#)
- [Configuración de la zona horaria](#)
- [El estado de su organización](#)
- [Configurar Amazon EventBridge](#)
- [AWS Health Consciente](#)
- [Alertas de eventos AWS Health](#)

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 de control

1. Abre tu AWS Health panel de control en <https://health.aws.amazon.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 (AmazonEC2)

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.

Service: Elastic Compute Cloud ✕

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	Start time
EC2	February 20, 2022 at 11:16:24 PM UTC-8
Status	End time
Open	-
Region / Availability Zone	Category
us-east-1	Issue
Account specific	Affected resources
No	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
- Evento
- Evento ARN
- Categoría de evento
- Hora de la última actualización
- Región
- 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).

Event log

Q Add filter

Region: US East N. Virginia (us-east-1), US East Ohio (us-east-2) X Clear filter

Event	Status	Event category	Region / Zone	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 ID del recurso (por ejemplo, un ID de EBS volumen de Amazon, como `vol-1a1b2c34f`) o el nombre del recurso de Amazon (ARN), si está disponible o es relevante.
- En el caso de los eventos de ciclo de vida planificados, esta lista de recursos afectados también contiene el estado más reciente de los recursos (pendiente, desconocido o resuelto). Esta lista se actualiza normalmente una vez cada 24 horas.

Puede filtrar los elementos que aparecen en los recursos. Puedes restringir tus resultados por ID de 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 displays the AWS Health console interface. On the left, the 'Event log' section includes a search filter for 'Region: US East N. Virginia (us-east-1), US East Ohio (us-east-2)' and a list of recent operational issues. The 'Event summary' section highlights the selected 'Lambda operational issue' with its last update time. On the right, the 'Lambda operational issue' details are shown, including the event name, status (Closed), region (us-east-1), and a detailed description of the issue and its resolution.

Event log

Q Add filter

Region: US East N. Virginia (us-east-1), US East Ohio (us-east-2) X

Clear filter

< 1 >

Event summary

- Lambda operational issue**
Last update: October 9, 2020 at 3:11:09 AM UTC-7 us-east-1
- EC2 operational issue**
Last update: October 9, 2020 at 11:54:16 AM UTC-7 us-east-1
- SNS operational issue**
Last update: September 30, 2020 at 11:42:54 AM UTC-7 us-east-1
- EC2 operational issue**
Last update: September 16, 2020 at 7:45:03 AM UTC-7 us-east-1
- Storagegateway operational issue**
Last update: September 13, 2020 at 6:32:24 PM UTC-7 us-east-1
- Deepracer operational issue**
Last update: August 31, 2020 at 9:10:12 PM UTC-7 us-east-1
- Sagemaker operational issue**
Last update: August 31, 2020 at 9:04:39 PM UTC-7 us-east-1
- Batch operational issue**

Lambda operational issue

Back to list view

Details | Affected resources

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 región que utilices, 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, consulte [Cómo empezar a usar tu AWS Health panel de control: el estado de tu cuenta](#).
- Utilice la AWS Health API para devolver el eventScopeCode parámetro. Los eventos pueden tener el valor PUBLIC, ACCOUNT_SPECIFIC o NONE. Para obtener más información, consulte la [DescribeEventDetails](#) operación en la AWS Health API Referencia.

Vista del calendario

La vista de calendario está disponible en la pestaña de cambios programados para proyectar AWS Health 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

Table Calendar

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

< **February 2024** >

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

30 January 2024
⋮
⚙️
✕

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 AWS Health evento. Para ver el estado, selecciona 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. Tras el resumen, aparece una lista de las cuentas afectadas y el número de recursos pendientes de 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 en la pestaña de recursos afectados en CSV nuestro JSON formato. En la vista de organización, el archivo descargado incluye todos los recursos de las cuentas de la lista. Navegue hasta el nivel de cuenta en la vista de organización para incluir solo los recursos de esa cuenta en el archivo descargado. Cada recurso afectado del archivo descargado incluye el Cuenta de AWS identificador, el eventoARN, el nombre de la entidad, la entidadARN, el estado y la hora de la última actualización del recurso. Si los filtros están activados, el archivo descargado solo incluye los resultados filtrados.

Solo 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 Región de AWS título del evento, la fecha de inicio del evento y la fecha de descarga.

Open and recent issues (0)
Scheduled changes (1)
Other notifications (0)
Event log

Scheduled changes (1) Table Calendar

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.](#)

< 1 >

Event	Status	Region / Zone Info	Start time	End time	Affected resources	
Lambda planned lifecycle event						
4	<div style="display: flex; flex-direction: column; gap: 5px;"> <div style="display: flex; align-items: center;"> <div> <p>4 Pending</p> <p>May require action</p> </div> <div style="margin-left: 20px;">100%</div> </div> <div style="display: flex; align-items: center;"> <div> <p>0 Unknown</p> <p>Not able to verify status</p> </div> <div style="margin-left: 20px;">0%</div> </div> <div style="display: flex; align-items: center;"> <div> <p>0 Resolved</p> <p>No actions required</p> </div> <div style="margin-left: 20px;">0%</div> </div> </div>	<p>Resource data is typically refreshed every 24 hours.</p>				
Affected resources (4) Download ▼						
<input type="text" value="Add filter"/> < 1 >						
Resource ID / ARN	▲ Resource status	Last update time				
arn:aws:lambda:us-east-1:959586608611:function:SpringClean-XUG3HH5R-AutoUpdateLambda-atNXDvDUU6P	⌚ 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

Puede ver los eventos en el AWS Health panel de control de su zona horaria local o enUTC. 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.amazon.com/health/](https://health.aws.amazon.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. Seleccione 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 eventos de AWS Health en cuentas con vista organizativa](#).


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

Configurar Amazon EventBridge

Úsalo 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.amazon.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 AWS Health eventos con Amazon EventBridge](#).

AWS Health Consciente

Puedes empezar a usarlo con [AWS Health Aware](#), una aplicación de bajo costo que puedes usar para enviar eventos de salud a Slack ServiceNow y más. AWS Health API JIRA

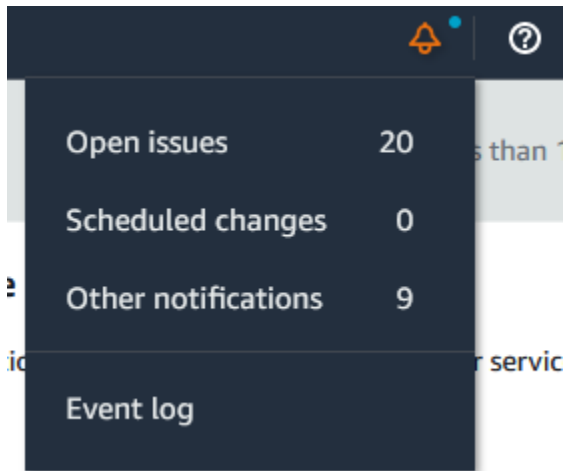
Alertas de eventos AWS Health

El AWS Health panel de control tiene un icono 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 icono de campana aparece en varias AWS consolas, como las de AmazonEC2, Amazon Relational Database Service (RDSAmazon) AWS Identity and Access Management , IAM () y AWS Trusted Advisor.

Elija el icono 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 notificaciones de usuario de AWS para AWS Health

AWS Health proporciona información sobre las operaciones del servicio, como los problemas operativos, el mantenimiento planificado y los eventos planificados del ciclo de vida del software. Para obtener una visibilidad completa de los detalles del evento de AWS Health, como los ID de los recursos afectados, el estado actual (abierto o cerrado) y el estado del recurso, se recomienda utilizar puntos de conexión AWS Health, como la API AWS Health, la fuente `aws.health` en Amazon EventBridge y el AWS Health Panel de control. Estos puntos de conexión proporcionan la información más detallada y en tiempo real sobre los eventos y cambios en curso que podrían afectar sus cargas de trabajo.

[AWS Las notificaciones de usuario](#) le informan a través de canales de experiencia de usuario adicionales (correo electrónico, chat o notificaciones push a la AWS Aplicación móvil de la consola). Las notificaciones de eventos de AWS Health no contienen tantos datos detallados como los puntos de conexión enumerados anteriormente; sin embargo, proporcionan una forma sencilla y eficaz de notificar a las partes interesadas los problemas y los cambios. En función de las reglas que cree, las notificaciones de usuario crean y envían una notificación cuando un evento coincide con los valores que especificó en una regla. Puede seleccionar a qué canales de entrega de experiencia de usuario se envía una notificación y configurar la agregación para reducir la cantidad de notificaciones generadas para eventos específicos. Las notificaciones también son visibles en el Centro de notificaciones de la consola. Por ejemplo, puede recibir notificaciones de chat si tiene recursos en su cuenta de AWS que estén programados para actualizaciones, como instancias de Amazon Elastic Compute Cloud (Amazon EC2).

Para obtener más información sobre cómo configurar las notificaciones de usuario de AWS, consulte [Introducción a las AWS notificaciones de usuario](#).

Acceder al AWS Health API

AWS Health es un servicio RESTful web que se utiliza HTTPS como formato de transporte y JSON serialización de mensajes. El código de su aplicación puede realizar solicitudes directamente al AWS Health API. Cuando lo utilice REST API directamente, deberá escribir el código necesario para firmar y autenticar sus solicitudes. Para obtener más información sobre las AWS Health operaciones y los parámetros, consulte la [AWS Health API Referencia](#).

Note

Debe tener un plan Business, Enterprise On-Ramp o Enterprise Support desde [AWS Support](#) para poder utilizar el AWS Health API. Si llamas AWS Health API desde una AWS cuenta que no tiene un plan Business, Enterprise On-Ramp o Enterprise Support, recibirás un `SubscriptionRequiredException` mensaje de error.

Puede usarlo AWS SDKs para cerrar las AWS Health REST API llamadas, lo que puede simplificar el desarrollo de su 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 AWS Management Console que puede utilizar para ver y buscar eventos y entidades afectadas. Consulte [Cómo empezar a usar tu AWS Health panel de control: el estado de tu cuenta](#).


puntos de conexión

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 DNS conmutación por error activo-pasiva, proporciona un único punto final global. AWS Health Puede realizar una DNS búsqueda 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 de conexión debe utilizar en su código, de modo que pueda obtener la información más reciente de AWS Health.

Al realizar una solicitud al punto de enlace global, debe especificar sus credenciales de AWS acceso al punto de enlace 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 API](#).

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.amazonaws.com	HTTPS
Pasivo	us-east-2	health.us-east-2.amazonaws.com	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 DNS búsqueda en el punto final global y CNAME, a continuación, extraiga la AWS región del nombre resuelto.

Example : DNS buscar en el punto final global

A continuación, el devuelve el punto de conexión de la región us-east-1. Este resultado te indica para qué punto final debes usar. 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.

Uso de la demostración de punto de conexión de alta disponibilidad

En los siguientes ejemplos de código, AWS Health utiliza una DNS búsqueda en el punto final global para determinar el punto final regional activo y la región de firma. A continuación, el código reinicia el flujo de trabajo si cambia el punto de conexión activo.

Temas

- [Uso de demostración para Java](#)
- [Uso de la demostración de Python](#)

Uso de demostración para Java

Requisito previo

Debe instalar [Gradle](#).

Para usar el ejemplo de Java

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

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

Firmar solicitudes AWS Health API

Al utilizar AWS SDKs o AWS Command Line Interface (AWS CLI) para realizar solicitudes AWS, estas herramientas firman automáticamente las solicitudes por usted con la clave de acceso que especifique al configurar las herramientas. Por ejemplo, si las utiliza AWS SDK for 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 utilizarlos AWS Health API con AWS SDK for 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 ellas AWS Health. Puedes usar las credenciales de un IAM usuario. Para obtener más información, consulte [Bloquear las claves de acceso de los usuarios raíz de su AWS cuenta](#) en la Guía del IAM usuario.

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 AWS API solicitudes](#) en Referencia general de AWS.

Operaciones compatibles con AWS Health

AWS Health admite las siguientes operaciones para obtener información sobre los eventos que afectan a una cuenta de AWS:

- Tipos de eventos compatibles con AWS Health.
- Información sobre uno o varios eventos que coinciden con los criterios de filtro especificados.

- Información sobre las entidades afectadas por uno o varios eventos.
- Recuentos clasificados de eventos o entidades que coinciden con los criterios de filtro especificados.

Ninguna de las operaciones realiza cambios. Es decir, estas operaciones recuperan datos, pero no los modifican. En las secciones siguientes se resumen las operaciones de AWS Health:

Tipos de eventos

La operación [DescribeEventTypes](#) recupera tipos de eventos que coinciden con un filtro especificado opcional. Un tipo de evento es una definición de plantilla de un servicio de AWS, un código de tipo de evento y una categoría de un evento. Los tipos de eventos y los eventos son equivalentes a las clases y los objetos que se usan en la programación orientada a objetos. El número de tipos de eventos admitidos por AWS Health aumentará con el tiempo.

Eventos

La operación [DescribeEvents](#) recupera información resumida sobre los eventos relacionados con una cuenta de AWS. Los eventos pueden estar relacionados con los problemas operativos de AWS, los cambios programados en la infraestructura de AWS o las notificaciones de seguridad y facturación. La operación [DescribeEventDetails](#) recupera información detallada sobre uno o varios eventos, como el servicio de AWS, la región, la zona de disponibilidad, las fechas de inicio y finalización del evento, y un texto descriptivo.

Entidades afectadas

La operación [DescribeAffectedEntities](#) recupera información sobre las entidades afectadas por uno o varios eventos. Los resultados pueden filtrarse usando criterios adicionales, como el estado, que podrían estar asignados a los recursos de AWS.

Agregación

La operación [DescribeEventAggregates](#) recupera el número de eventos de cada categoría de tipos de eventos, que pueden filtrarse utilizando otros criterios. La operación [DescribeEntityAggregates](#) recupera el número de entidades (recursos) afectadas por uno o varios eventos especificados.

AWS Organizations y la Vista de organización

DescribeEventsForOrganization

[DescribeEventsForOrganization](#) devuelve información resumida sobre los eventos de AWS Organizations que satisfacen los criterios de filtro especificados.

DescribeAffectedAccountsForOrganization

[DescribeAffectedAccountsForOrganization](#) devuelve una lista de las cuentas de AWS de la AWS Organizations que se ven afectadas por el evento proporcionado.

DescribeEventDetailsForOrganization

[DescribeEventDetailsForOrganization](#) devuelve información detallada sobre uno o más eventos especificados para una o más cuentas de AWS Organizations.

DescribeAffectedEntitiesForOrganization

[DescribeAffectedEntitiesForOrganization](#) devuelve una lista de entidades que se han visto afectadas por uno o varios eventos de una o varias cuentas de su organización, según los criterios de filtro.

EnableHealthServiceAccessForOrganization

La operación [EnableHealthServiceAccessForOrganization](#) concede al servicio AWS Health permiso para interactuar con AWS Organizations en nombre del cliente y aplica un rol vinculado al servicio a la cuenta de administración de su organización.

DisableHealthServiceAccessForOrganization

La operación [DisableHealthServiceAccessForOrganization](#) revoca el permiso para que el servicio AWS Health interactúe con AWS Organizations en nombre del cliente.

DescribeHealthServiceStatusForOrganization

La operación [DescribeHealthServiceStatusForOrganization](#) proporciona información de estado sobre cómo habilitar o deshabilitar el funcionamiento de AWS Health en su organización

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

Ejemplo de código Java para la API de AWS Health

En los siguientes ejemplos de código Java se muestra cómo se inicializa un cliente de AWS Health y se recupera información sobre eventos y entidades.

Paso 1: Inicializar las credenciales

Es necesario contar con credenciales válidas para poder comunicarse con la API de AWS Health. Puede utilizar el par de claves de cualquier usuario de IAM asociado a la cuenta de AWS.

Cree e inicialice una instancia de [AWSCredentials](#):

```
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 cliente de API de AWS Health

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: Utilizar las operaciones de la API de AWS Health 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](#) la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. 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. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es 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 la sección [Privacidad de datos FAQ](#). Para obtener información sobre la protección de datos en Europa, consulte el [modelo de responsabilidad AWS compartida y](#) la entrada del GDPR blog sobre AWS seguridad.

Para proteger los 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:

- Utilice la autenticación multifactorial (MFA) con cada cuenta.
- UseSSL/TLSpara comunicarse con AWS los recursos. Necesitamos TLS 1.2 y recomendamos TLS 1.3.
- Configure API y registre la actividad del usuario con AWS CloudTrail.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita entre FIPS 140 y 3 módulos criptográficos validados para acceder a AWS través de una interfaz de línea de comandos o unaAPI, utilice un FIPS terminal. Para obtener más información sobre los FIPS puntos finales disponibles, consulte la [Norma federal de procesamiento de información \(\) 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, API AWS CLI, o. AWS SDKs Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, le recomendamos encarecidamente que no incluya información sobre las credenciales URL para validar la solicitud a 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 Transport Layer Security (TLS) o en reposo mediante el cifrado del lado del cliente.

AWS Health no registra información de identificación personal (PII), como direcciones de correo electrónico o nombres de clientes, en 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 AWS los recursos. IAM los administradores controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar AWS Health los recursos. IAM es una Servicio de AWS que puede utilizar sin coste adicional.

Temas

- [Público](#)
- [Autenticación con identidades](#)
- [Administración de acceso mediante 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](#)

- [Uso de 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 el trabajo en el que se realice AWS Health.

Usuario del servicio: si utiliza el AWS Health servicio para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más AWS Health funciones para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en AWS Health, consulte [Solución de problemas AWS Health de identidad y acceso](#).

Administrador de servicios: si estás a cargo de AWS Health los recursos de tu empresa, probablemente tengas acceso total a ellos AWS Health. Su trabajo consiste en determinar a qué AWS Health funciones y recursos deben acceder los usuarios del servicio. A continuación, debe enviar solicitudes a su IAM administrador para cambiar los permisos de los usuarios del servicio. Revise la información de esta página para comprender los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con AWS Health, consulte [¿Cómo AWS Health funciona con IAM](#).

IAM administrador: si es IAM administrador, puede que desee obtener más información sobre cómo puede redactar políticas para administrar el acceso a ellas AWS Health. Para ver ejemplos de políticas AWS Health basadas en la identidad que puede utilizar IAM, consulte [AWS Health ejemplos de políticas basadas en la identidad](#)

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como IAM usuario o asumiendo un IAM rol.

Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (IAM Identity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, el administrador

configuró previamente la federación de identidades mediante roles. IAM Cuando accede AWS mediante la federación, asume indirectamente un rol.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte [Cómo iniciar sesión Cuenta de AWS en su](#) Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS incluye un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte [Firmar AWS API las solicitudes](#) en la Guía del IAM usuario.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactorial (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte [Autenticación multifactorial](#) en la Guía del AWS IAM Identity Center usuario y [Uso de la autenticación multifactorial \(MFA\) AWS en](#) la Guía del IAM usuario.

AWS usuario raíz de la cuenta

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de tareas que requieren que inicie sesión como usuario root, consulte [Tareas que requieren credenciales de usuario root](#) en la Guía del IAM usuario.

Usuarios y grupos de IAM

Un [IAMusuario](#) es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos utilizar credenciales temporales en lugar de crear IAM usuarios con credenciales de larga duración, como contraseñas y claves de acceso. Sin embargo, si tiene casos de uso específicos que requieren credenciales a largo plazo con IAM los usuarios, le recomendamos que rote las claves de acceso. Para obtener más información, consulte [Rotar las claves de acceso con regularidad para los casos de uso que requieran credenciales de larga duración](#) en la Guía del IAM usuario.

Un [IAMgrupo](#) es una identidad que especifica un conjunto de IAM usuarios. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos para administrar IAM los recursos.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte [Cuándo crear un IAM usuario \(en lugar de un rol\)](#) en la Guía del IAM usuario.

IAMroles

Un [IAMrol](#) es una identidad dentro de tu Cuenta de AWS que tiene permisos específicos. Es similar a un IAM usuario, pero no está asociado a una persona específica. Puede asumir temporalmente un IAM rol en el AWS Management Console [cambiando de rol](#). Puede asumir un rol llamando a una AWS API operación AWS CLI o utilizando una operación personalizadaURL. Para obtener más información sobre los métodos de uso de roles, consulte [Uso de IAM roles](#) en la Guía del IAM usuario.

IAMlos roles con credenciales temporales son útiles en las siguientes situaciones:

- **Acceso de usuario federado:** para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información sobre los roles para la federación, consulte [Creación de un rol para un proveedor de identidad externo](#) en la Guía del IAM usuario. Si usa IAM Identity Center, configura un conjunto de permisos. Para controlar a qué pueden acceder sus identidades después de autenticarse, IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM. Para obtener información acerca de los conjuntos de permisos, consulte [Conjuntos de permisos](#) en la Guía del usuario de AWS IAM Identity Center .
- **Permisos IAM de usuario temporales:** un IAM usuario o rol puede asumir un IAM rol para asumir temporalmente diferentes permisos para una tarea específica.
- **Acceso multicuenta:** puedes usar un IAM rol para permitir que alguien (un responsable de confianza) de una cuenta diferente acceda a los recursos de tu cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunos Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para conocer

la diferencia entre las funciones y las políticas basadas en recursos para el acceso multicuenta, consulta el tema sobre el acceso a los [recursos entre cuentas IAM en](#) la Guía del IAM usuario.

- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros. Servicios de AWS Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
- Sesiones de acceso directo (FAS): cuando utilizas un IAM usuario o un rol para realizar acciones en AWS ellas, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama a un Servicio de AWS, junto con los que solicitan, Servicio de AWS para realizar solicitudes a los servicios descendentes. FAS las solicitudes solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener detalles sobre la política a la hora de realizar FAS solicitudes, consulte [Reenviar sesiones de acceso](#).
- Función de servicio: una función de servicio es una [IAM función](#) que un servicio asume para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentro IAM. Para obtener más información, consulte [Crear un rol para delegar permisos Servicio de AWS en un rol](#) en el IAM Manual del usuario.
- Función vinculada a un servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un IAM administrador puede ver los permisos de los roles vinculados al servicio, pero no editarlos.
- Aplicaciones que se ejecutan en Amazon EC2: puedes usar un IAM rol para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y que realizan AWS CLI o AWS API solicitan. Esto es preferible a almacenar las claves de acceso en la EC2 instancia. Para asignar un AWS rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte [Uso de un IAM rol para conceder permisos a aplicaciones que se ejecutan en EC2 instancias de Amazon](#) en la Guía del IAM usuario.

Para saber si se deben usar IAM roles o IAM usuarios, consulte [Cuándo crear un IAM rol \(en lugar de un usuario\)](#) en la Guía del IAM usuario.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como JSON documentos. Para obtener más información sobre la estructura y el contenido de los documentos de JSON políticas, consulte [Descripción general de JSON las políticas](#) en la Guía del IAM usuario.

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

De forma predeterminada, los usuarios y los roles no tienen permisos. Para conceder a los usuarios permiso para realizar acciones en los recursos que necesitan, un IAM administrador puede crear IAM políticas. A continuación, el administrador puede añadir las IAM políticas a las funciones y los usuarios pueden asumir las funciones.

IAM las políticas definen los permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de AWS Management Console AWS CLI, el o el AWS API.

Políticas basadas en identidad

Las políticas basadas en la identidad son documentos de política de JSON permisos que se pueden adjuntar a una identidad, como un IAM usuario, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener información sobre cómo crear una política basada en la identidad, consulte [Creación de IAM políticas](#) en la Guía del usuario. IAM

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y funciones de su empresa. Cuenta de AWS Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para saber cómo elegir entre una política

gestionada o una política integrada, consulte [Elegir entre políticas gestionadas y políticas integradas en la Guía del IAM](#) usuario.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de JSON política que se adjuntan a un recurso. Algunos ejemplos de políticas basadas en recursos son las políticas de confianza de IAM roles 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. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe [especificar una entidad principal](#) en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puede usar políticas AWS administradas desde una política IAM 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 IAM usuario 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 JSON políticas.

Amazon S3 AWS WAF y Amazon VPC son ejemplos de servicios compatibles 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 y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- **Límites de permisos:** un límite de permisos es una función avanzada en la que se establecen los permisos máximos que una política basada en la identidad puede conceder a una IAM entidad (IAMusuario o rol). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte los [límites de los permisos para IAM las entidades](#) en la Guía del IAMusuario.
- **Políticas de control de servicios (SCPs):** SCPs son JSON políticas que especifican los permisos máximos para una organización o unidad organizativa (OU) AWS Organizations. AWS Organizations es un servicio para agrupar y administrar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus cuentas. SCPLimita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una Usuario raíz de la cuenta de AWS. Para obtener más información sobre OrganizationsSCPs, consulte las [políticas de control de servicios](#) en la Guía del AWS Organizations usuario.
- **Políticas de sesión:** las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información, consulte [las políticas de sesión](#) en la Guía del IAM usuario.

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 IAM usuario.

¿Cómo AWS Health funciona con IAM

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

Temas

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

Políticas de AWS Health basadas en identidades

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

Acciones

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

El `Action` elemento de una JSON política describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones de política suelen tener el mismo nombre que la AWS API operación asociada. Hay algunas excepciones, como las acciones que solo permiten permisos y que no tienen una operación coincidente. API También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

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 permiso a alguien para ver información detallada sobre eventos específicos de la [DescribeEventDetails](#) API operación, 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 IAM usuario.

Recursos

Los administradores pueden usar AWS JSON políticas 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 JSON de política especifica el objeto o los objetos a los que se aplica la acción. Las instrucciones deben contener un elemento Resource o NotResource. Como práctica recomendada, especifique un recurso mediante su [nombre de recurso de Amazon \(ARN\)](#). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, 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 EC2_INSTANCE_RETIREMENT_SCHEDULED_ABC123-DEF456 evento en su declaración, utilice lo siguienteARN.

```
"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 API las operaciones pueden implicar varios recursos. Por ejemplo, la [DescribeEvents](#) operación devuelve información sobre los eventos que cumplen un criterio de filtro especificado. Esto significa que un IAM usuario 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 salud y solo para las [DescribeAffectedEntities](#) operaciones y [DescribeEventDetails](#) 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 respectivos tipos ARNs, consulte [los recursos definidos por AWS Health](#) en la Guía del IAM usuario. Para saber con qué acciones puede especificar cada recurso, consulte [Acciones definidas por AWS Health](#). ARN

Claves de condición

Los administradores pueden usar AWS JSON políticas 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` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen [operadores de condición](#), tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación AND lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una OR operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder a un IAM usuario permiso para acceder a un recurso solo si está etiquetado con su nombre de IAM usuario. Para obtener más información, consulte [los elementos IAM de la política: variables y etiquetas](#) en la Guía del IAM usuario.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de [contexto de condición AWS globales](#) en la Guía del IAM usuario.

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 IAM usuario.

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

Para ver una lista de claves de AWS Health condición, consulte [Claves de condición AWS Health](#) en la Guía del IAM usuario. Para saber con qué acciones y recursos puede utilizar una clave condicionada, 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 JSON de políticas 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, puedes especificar una cuenta completa o IAM entidades de otra cuenta como [principal en 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 en [qué se diferencian IAM los roles de las políticas basadas en recursos](#) en la Guía del IAMusuario.

AWS Health solo admite políticas basadas en recursos para las operaciones y.

[DescribeAffectedEntitiesDescribeEventDetails](#)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 IAMroles

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

Usar credenciales temporales con AWS Health

Puede usar credenciales temporales para iniciar sesión con la federación, asumir un IAM rol o asumir un rol multicuenta. Para obtener credenciales de seguridad temporales, puede llamar a AWS STS API operaciones como [AssumeRole](#)o [GetFederationToken](#).

AWS Health admite el uso de credenciales temporales.

Roles vinculados al servicio

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 al servicio aparecen en tu

IAM cuenta y son propiedad del servicio. Un IAM administrador puede ver los permisos de los roles vinculados al servicio, pero no editarlos.

AWS Health admite la integración de roles vinculados a servicios. 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 IAM consola IAMAPI, o AWS Command Line Interface (AWS CLI). Para obtener más información, consulte [Uso de funciones vinculadas a servicios](#) en la Guía del IAMusuario.

Para obtener más información, consulte [Agregar eventos de AWS Health en cuentas con vista organizativa](#).

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 IAM cuenta y son propiedad de la cuenta. Esto significa que un IAM administrador 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, IAM los usuarios y los roles no tienen permiso para crear o modificar AWS Health recursos. Tampoco pueden realizar tareas con AWS Management Console AWS CLI, o AWS API. IAMEl administrador debe crear IAM políticas que concedan a los usuarios y roles permisos para realizar API operaciones específicas en los recursos específicos que necesitan. A continuación, el administrador debe adjuntar esas políticas a los IAM usuarios o grupos que requieran esos permisos.

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

Temas

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

Prácticas recomendadas sobre las 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. Para obtener más información, consulte [las políticas AWS gestionadas](#) o [las políticas AWS gestionadas para las funciones laborales](#) en la Guía del IAM usuario.
- Aplique permisos con privilegios mínimos: cuando establezca permisos con IAM políticas, 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. Para obtener más información sobre cómo IAM aplicar permisos, consulte [Políticas y permisos IAM en](#) la IAM Guía del usuario.
- Utilice las condiciones en IAM las políticas para restringir aún más el acceso: puede añadir una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de política para especificar que todas las solicitudes deben enviarse medianteSSL. 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 AWS CloudFormation. Para obtener más información, consulte [los elementos IAM JSON de la política: Condición](#) en la Guía del IAM usuario.
- Utilice IAM Access Analyzer para validar sus IAM políticas y garantizar permisos seguros y funcionales: IAM Access Analyzer valida las políticas nuevas y existentes para que se ajusten

al lenguaje de las políticas (JSON) y IAM a las IAM mejores prácticas. IAMAccess Analyzer proporciona más de 100 comprobaciones de políticas y recomendaciones prácticas para ayudarle a crear políticas seguras y funcionales. Para obtener más información, consulte la [validación de políticas de IAM Access Analyzer](#) en la Guía del IAM usuario.

- Requerir autenticación multifactorial (MFA): si se encuentra en una situación en la que se requieren IAM usuarios o un usuario raíz Cuenta de AWS, actívela MFA para aumentar la seguridad. Para solicitarlo MFA cuando se convoque a API las operaciones, añada MFA condiciones a sus políticas. Para obtener más información, consulte [Configuración del API acceso MFA protegido](#) en la Guía del IAM usuario.

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

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 creas una política basada en la identidad que sea más restrictiva que los permisos mínimos requeridos, la consola no funcionará según lo previsto para las entidades (IAM usuarios o roles) que cuenten con 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 API operaciones y notificaciones
- Vea información sobre las cuentas que forman parte de su AWS organización
- Consulte las unidades organizativas (OU) de la cuenta de administración

Example : `AWSHealthFullAccess`

```
{  
  "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 [Uso de roles vinculados a servicios de AWS Health](#).

No es necesario que concedas permisos mínimos de consola a los usuarios que solo llamen al AWS CLI o al AWS API. En su lugar, permita el acceso únicamente a las acciones que coincidan con la API operación que está intentando realizar.

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

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo se muestra cómo se puede crear una política que permita a IAM los usuarios ver las políticas integradas y administradas asociadas a su identidad de usuario. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la tecla o. AWS CLI AWS API

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "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 al y al AWS Health DashboardAWS Health API

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

Puede utilizarlo IAM para crear entidades (usuarios, grupos o roles) y, a continuación, conceder a esas entidades permisos para acceder a AWS Health Dashboard y al AWS Health API.

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

Después de crear IAM los usuarios, puede proporcionarles contraseñas individuales. 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 IAM usuario 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 IAM política concede acceso únicamente a AWS Health API, AWS Health Dashboard y el usuario o rol al que se aplica la política, podrá acceder a toda la información

publicada sobre los AWS servicios y los recursos relacionados, incluso si otras IAM políticas no permiten ese acceso.

Puedes usar dos grupos de APIs para 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 API operaciones disponibles, consulte la [AWS Health APIReferencia](#).

Acciones individuales

Puede establecer el Action elemento de una IAM política en `health:Describe*`. Esto permite el acceso a la 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 AWS Health Dashboard y a cualquiera de `Describe*` AWS Health API ellas. Por ejemplo, un IAM usuario con esta política puede acceder a AWS Health Dashboard la AWS Health `DescribeEvents` API operación AWS Management Console y llamarla.

Example : describir el acceso

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

```
}
```

Denegar el acceso

Esta declaración de política deniega el acceso a AWS Health Dashboard y al AWS Health API. Un IAM usuario con esta política no puede ver ni llamar a ninguna de las AWS Health API operaciones. AWS Health Dashboard AWS Management Console

Example : denegar el acceso

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

Vista organizativa

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

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

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

Para conocer los permisos exactos que se necesitan para cada uno de ellos APIs, consulte [las acciones definidas por AWS Health APIs y las notificaciones](#) en la Guía del IAM usuario.

Note

Debe utilizar las credenciales de la cuenta de administración para que una organización pueda acceder al AWS Health APIs formulario AWS Organizations. Para obtener más información, consulte [Agregar eventos de AWS Health en cuentas con vista organizativa](#).

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

```
{
  "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": "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

```

{
  "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 quieres conceder permisos ya tiene una IAM política, puedes añadir la declaración AWS Health de política específica a esa política.

Condiciones basadas en recursos y en acciones

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

Para ello, actualice el `Condition` bloque de la IAM política o defina el `Resource` elemento. Puede utilizar [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 [DescribeEventDetails](#) API operaciones [DescribeAffectedEntities](#) admiten permisos a nivel de recurso. Por ejemplo, puede crear una política para permitir o rechazar eventos específicos de AWS Health .

- Las [DescribeEventDetailsForOrganization](#) API operaciones [DescribeAffectedEntitiesForOrganization](#) no admiten permisos a nivel de recursos.
- Para obtener más información, consulte [Acciones, recursos y claves de condición AWS Health APIs y notificaciones](#) en la Referencia de autorización de servicios.

Example : condición basada en acciones

Esta declaración de política otorga acceso a Amazon AWS Health Dashboard y a AWS Health Describe* API sus operaciones, pero deniega el acceso a cualquier AWS Health evento relacionado con AmazonEC2.

```
{
  "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.

```
{
```



```

"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 Describe* API las operaciones AWS Health Dashboard y las mismas, pero deniega el acceso a cualquier AWS Health evento eventTypeCode que coincida con las mismasAWS_EC2_*

```

{
  "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](#) y no tienes permiso para acceder al AWS Health evento, aparecerá 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 puedan surgir al trabajar con AWS Health y 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 el acceso de otras personas 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 AWS Management Console le indica que no está autorizado a realizar una acción, debe ponerse en contacto con su administrador para obtener ayuda. Su administrador es la persona que le facilitó su nombre de usuario y contraseña.

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

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

AWS Health API requiere un plan Business, Enterprise On-Ramp o Enterprise Support de [AWS Support](#). Si llamas AWS Health API desde una cuenta que no tiene un plan Business, Enterprise On-Ramp o Enterprise Support, se devuelve el siguiente código de error: `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.

Algunos 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 el rol al servicio.

El siguiente ejemplo de error se produce cuando un IAM usuario denominado `marymajor` intenta utilizar la consola para realizar una acción en ella. 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 AWS el administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero ver mis claves de acceso

Después de crear las claves IAM de acceso de usuario, podrá 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 pierdes tu clave de acceso secreta, debes añadir nuevas claves de acceso a tu IAM usuario. 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 ver las instrucciones, consulte [Administrar las claves de acceso](#) en la Guía del IAM usuario.

Soy administrador y quiero permitir el acceso de otras personas AWS Health

Para permitir el acceso de otras personas AWS Health, debes conceder permiso a las personas o aplicaciones que necesitan acceso. Si lo utiliza AWS IAM Identity Center para administrar personas y aplicaciones, debe asignar conjuntos de permisos a los usuarios o grupos para definir su nivel de acceso. Los conjuntos de permisos crean y asignan automáticamente IAM políticas a las IAM funciones asociadas a la persona o la aplicación. Para obtener más información, consulte los [conjuntos de permisos](#) en la Guía del AWS IAM Identity Center usuario.

Si no utiliza IAM Identity Center, debe crear IAM entidades (usuarios o roles) para las personas o aplicaciones a las 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 AWS. Para obtener más información sobre la creación de IAM usuarios, grupos, políticas y permisos, consulte [IAMIdentidades](#) y [políticas y permisos IAM en](#) la Guía del IAM usuario.

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

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. 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 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 propiedad, consulte [Proporcionar acceso a un IAM usuario en otro Cuenta de AWS de su propiedad](#) en la Guía del IAM usuario. Cuentas de AWS
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo permitir el [acceso a recursos que Cuentas de AWS son propiedad de terceros](#) en la Guía del IAM usuario.
- Para obtener información sobre cómo proporcionar acceso mediante la federación de identidades, consulte [Proporcionar acceso a usuarios autenticados externamente \(federación de identidades\)](#) en la Guía del IAM usuario.
- Para saber la diferencia entre el uso de roles y políticas basadas en recursos para el acceso entre cuentas, consulte el acceso a [recursos entre cuentas IAM en la Guía](#) del usuario. IAM

Uso de roles vinculados a servicios de AWS Health

AWS Health usa AWS Identity and Access Management (IAM) roles vinculados al [servicio](#). Un rol vinculado a un servicio es un tipo único de IAM rol 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 AWS Health que añadir manualmente 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 la política de confianza y la política de permisos, y esa política de permisos no se puede adjuntar a ninguna otra IAM entidad.

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 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 [Creación de un rol vinculado a un servicio](#) en la Guía del usuario. IAM

Modificación de un rol vinculado a servicios de AWS Health

AWS Health no 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 utilizando. IAM Para obtener más información, consulte [Edición de un rol vinculado a un servicio](#) en la Guía del IAM usuario.

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 IAM consola IAMAPI, 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 de la Detección y Respuesta a AWS Incidentes. Una vez finalizado este proceso, puedes eliminar cualquiera de los roles a través de la IAM consola IAMAPI, o. AWS CLI

Información relacionada

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

AWS políticas gestionadas para AWS Health

Una política AWS administrada es una política independiente creada y administrada por 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 haya nuevas API operaciones disponibles para los servicios existentes.

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

AWS Health tiene las siguientes políticas administradas.

Contenido

- [Política administrada de AWS : AWSHealth_EventProcessorServiceRolePolicy](#)
- [Política administrada de AWS : Health_OrganizationsServiceRolePolicy](#)
- [Política administrada de AWS : 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 puedes adjuntar esta política a tus IAM entidades. Para obtener más información, consulte [Uso de 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.

```
{
  "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 `AWSServiceRoleForHealth_Organizations`. La política permite al rol vinculado al servicio completar acciones en su lugar. No puedes adjuntar esta política a tus IAM entidades. Para obtener más información, consulte [Uso de 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 los Servicios de AWS que se pueden usar con ellas.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "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](#).

Política administrada de AWS : AWSHealthFullAccess

AWS Health utiliza la política [AWSHealthFullAccess](#) AWS gestionada. La política concede a las entidades (IAM usuarios o roles) 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 AWS Health API operaciones y notificaciones
- `iam`— Crea un IAM rol que está vinculado al AWS Health servicio

```
{
  "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": "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 realizar el seguimiento de estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbese al RSS feed de la [Historial de documentos para AWS Health](#) página.

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

AWS Health

Cambio	Descripción	Fecha
Política administrada de AWS : AWSHealthFullAccess : actualización de una política existente	AWS Health ha ampliado la AWSHealthFullAccess política a todas AWS GovCloud (US) Regions las regiones de China.	16 de octubre de 2023
Política administrada de AWS : Health_OrganizationsServiceRolePolicy : 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 AWS 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 ejecutas 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 CPU uso u otras métricas de sus instancias de Amazon Elastic Compute Cloud (AmazonEC2) 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 vigilen determinados eventos y activen acciones automatizadas en otros AWS servicios cuando se produzcan estos eventos. Para obtener más información, consulte [Monitorización de AWS Health eventos con Amazon EventBridge](#).
- AWS CloudTrail captura API las llamadas 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 [AWS CloudTrail Guía del usuario de](#) .

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. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- [Guías de inicio rápido sobre seguridad y cumplimiento](#): estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- [Diseñando una arquitectura basada en la HIPAA seguridad y el cumplimiento en Amazon Web Services](#): en este documento técnico se describe cómo pueden utilizar las empresas AWS para crear HIPAA aplicaciones aptas.

Note

No todos son aptos. Servicios de AWS HIPAA Para obtener más información, consulta la [Referencia de servicios HIPAA aptos](#).

- [AWS Recursos](#) de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- [AWS Guías de cumplimiento para clientes](#): comprenda el modelo de responsabilidad compartida desde la perspectiva del cumplimiento. En las guías se resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y se orientan a los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- [Evaluación de los recursos con reglas](#) en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- [AWS Security Hub](#)— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la [Referencia de controles de Security Hub](#).
- [Amazon GuardDuty](#): Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, por ejemplo PCIDSS, cumpliendo con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- [AWS Audit Manager](#)— Esto le Servicio de AWS ayuda a auditar continuamente su AWS consumo para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

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 AWS Health API operaciones 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 API llamadas AWS publicadas para acceder a AWS Health través de la red. Los clientes deben ser compatibles con Transport Layer Security (TLS) 1.0 o una versión posterior. Recomendamos la versión TLS 1.2 o una versión posterior. Los clientes también deben admitir conjuntos de cifrado con total confidencialidad (PFS), como Ephemeral Diffie-Hellman () o Elliptic Curve Ephemeral Diffie-Hellman (DHE). ECDHE La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben firmarse con un identificador de clave de acceso y una clave de acceso secreta asociada a un director. IAM También puede 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, puedes permitir que un usuario AWS Identity and Access Management (IAM) acceda a AWS Health Dashboard. Sin embargo, puede no permitir que ese mismo usuario habilite o deshabilite 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 (AmazonEC2) que deba actualizarse.

Para obtener más información, consulte [Cómo empezar a usar tu AWS Health panel de control: el estado de tu cuenta](#).

Intégrelo 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 AWS Health eventos con Amazon EventBridge](#).

Agregar eventos de AWS Health en cuentas con vista organizativa

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

Puede agregar eventos de 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 característica para mantenerse informado de los próximos cambios en los servicios de AWS que es posible que requieran actualizaciones o cambios en el código.

Se recomienda utilizar la característica de [Administrador delegado](#) para delegar el acceso a la AWS Health Vista organizativa para una cuenta de miembro. Esto facilita a los equipos operativos el acceso a los eventos de AWS Health 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 no registra los eventos que sucedieron en la organización antes de que habilitase la vista organizativa. Por ejemplo, si una cuenta de miembro (111122223333) de su organización recibió un evento para Amazon Elastic Compute Cloud (Amazon EC2) antes de activar esta característica, este evento no aparecerá en su vista organizativa.
- Los eventos de AWS Health que se enviaron para las cuentas de su organización aparecerán en la vista organizativa mientras el evento esté disponible (hasta 90 días), incluso si una o más de esas cuentas abandonan su 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.
- Iniciar sesión en la cuenta de administración como usuario de AWS Identity and Access Management (IAM) o asumir un rol 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 [Proteger las claves de acceso AWS de usuario raíz](#) de su 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

- [Vista organizativa \(consola\)](#)
- [Vista organizativa \(CLI\)](#)
- [Vista de administrador delegado de la organización](#)

Vista organizativa (consola)

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

La vista organizativa está disponible en la consola de AWS Health para todos los planes de AWS Support 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](#).

Contenido

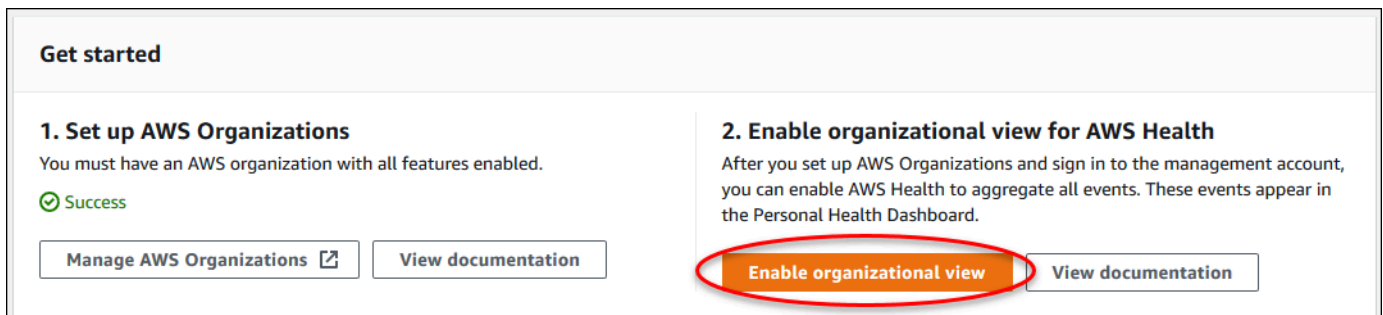
- [Habilitación de la vista organizativa \(consola\)](#)
- [Visualización de eventos de vista organizativa \(consola\)](#)
 - [Problemas abiertos y recientes](#)
 - [Cambios programados](#)
 - [Otras notificaciones](#)
 - [Registro de eventos](#)
- [Visualización de las cuentas y los recursos afectados \(consola\)](#)
- [Deshabilitación de la vista organizativa \(consola\)](#)

Habilitación de la vista organizativa (consola)

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

Para ver el Panel de control de AWS Health de su organización

1. Abra su AWS Health Panel de control en <https://health.aws.amazon.com/health/home>.
2. En el panel de navegación, en Estado de su organización, elija Configuraciones.
3. En la página de Activar la vista organizativa, elija Activar la vista organizativa.



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](#)

4. (Opcional) Si desea realizar cambios en sus organizaciones de AWS, como crear unidades organizativas (OUs), elija Administrar AWS Organizations.

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

Notas

- La habilitación de esta característica es un proceso asíncrono y tardará un tiempo en completarse. En función del número de cuentas de la organización, puede que se necesiten varios minutos para que se puedan cargar las cuentas. Puede salir de la consola de AWS Health y echarle un vistazo más tarde.
- Si dispone de un plan de soporte Business, Enterprise On-Ramp o Enterprise, puede realizar la operación de API [DescribeHealthServiceStatusForOrganization](#) para comprobar el estado del proceso.
- Cuando habilita esta característica, se aplica el `AWSServiceRoleForHealth_Organizations` rol vinculado al servicio con la política administrada de `Health_OrganizationsServiceRolePolicy` AWS a la cuenta de administración de la organización. Para obtener más información, consulte [Uso de roles vinculados a servicios de AWS Health](#).

Visualización de eventos de vista organizativa (consola)

Después de habilitar la vista organizativa, AWS Health muestra eventos para todas las cuentas de la organización.

Cuando una cuenta se une a la organización, AWS Health agrega automáticamente la cuenta a la vista organizativa. 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 periodo de 90 días, AWS eliminará de forma permanente todos los datos de la política de la cuenta.

- Si desea conservar los resultados por más de 90 días, puede archivar las políticas. También puede utilizar una acción personalizada con una regla de EventBridge para almacenar los resultados en un bucket de S3.
- Mientras AWS conserva los datos de la política, cuando vuelva a abrir la cuenta cerrada, AWS reasignará la cuenta como administrador del servicio y recuperará los datos de la política de servicio de la cuenta.
- Para obtener más información, consulte [Cierre de una cuenta](#).

⚠ 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.

ℹ Note

Al activar esta característica, la consola de AWS Health 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. Los eventos del AWS Health Panel de control: estado del servicio proporcionan información pública sobre la disponibilidad regional de servicios de AWS.

Puede consultar los eventos organizativos en las siguientes páginas.

Temas

- [Problemas abiertos y recientes](#)
- [Cambios programados](#)
- [Otras notificaciones](#)
- [Registro de eventos](#)

Problemas abiertos y recientes

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

Visualizar eventos de vista organizativa

1. Abra su AWS Health Panel de control en <https://health.aws.amazon.com/health/home>.
2. En el panel de navegación, en Estado de su organización, seleccione Problemas abiertos y recientes para ver los eventos notificados recientemente.

3. Elija un evento. En la pestaña Detalles, puede revisar la siguiente información sobre el evento:

- Nombre de evento
- Estado
- Región / Zona de disponibilidad
- Cuentas afectadas
- Hora de inicio
- Hora de finalización
- Categoría
- Descripción

Example : Problemas abiertos para la vista organizativa

El siguiente evento de Amazon Relational Database Service (Amazon RDS) aparece en la pestaña Problemas abiertos y recientes de la vista organizativa y afecta a una cuenta de la organización.

The screenshot displays the AWS Health console interface. On the left, the 'Open issues' section shows a list of events. The 'RDS storage issue' is highlighted. On the right, the 'Details' tab for this issue is active, showing event data and a description.

Event data	
Event	RDS storage issue
Start time	November 18, 2020 at 7:50:10 AM UTC-8
Status	Open
End time	-
Region / Availability Zone	us-east-1a
Category	Issue
Affected accounts	1
Description	
Unfortunately, there was an unrecoverable storage failure on your Amazon RDS instance associated with this event. As a result, your instance has been put in a storage failed state.	
You can recover your database instance at your earliest convenience by using one of the following methods:	
1) Using your latest snapshot - you can view the available backups on the AWS Management Console under the "Snapshots" tab. More information on restoring from a DB snapshot can be found here:	
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ShareSnapshot.html	

Cambios programados

Utilice la pestaña Cambios programados 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 Notificaciones 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.

Registro de eventos

También puede usar la pestaña Registro de eventos para ver los AWS Health eventos 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. Abra su AWS Health Panel de control en <https://health.aws.amazon.com/health/home>.
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
 - Estado
 - Región / Zona de disponibilidad
 - Cuentas afectadas
 - Hora de inicio
 - Hora de finalización
 - Categoría
 - Descripción

Example : Pestaña de registro de eventos para vista organizativa

El siguiente ejemplo de evento de Amazon DynamoDB (DynamoDB) aparece en la pestaña Registro de eventos y afecta a dos cuentas de la organización.

The screenshot displays the AWS Health console interface. On the left, the 'Event log' section shows a list of events, with 'EC2 instance network maintenance scheduled' highlighted. The main area shows the details for this event, including the event name, status (Upcoming), region (us-east-1a), and affected accounts (2). The description explains that maintenance is scheduled for EC2 instances, leading to a loss of network connectivity, and provides instructions on how to migrate to replacement instances. It also includes a link to the AWS Management Console for more information and a link to the AWS Support Team.

Visualización de las cuentas y los recursos afectados (consola)

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 próximo evento de mantenimiento de instancias de Amazon Elastic Compute Cloud (Amazon EC2), las cuentas de su organización que tengan instancias de Amazon EC2 pueden aparecer en la pestaña Detalles. Puede identificar los recursos específicos y, a continuación, ponerse en contacto con el propietario de la cuenta.

Visualización de las cuentas y los recursos afectados

1. Abra su AWS Health Panel de control en <https://health.aws.amazon.com/health/home>.
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 Mostrar detalles de la cuenta para ver la siguiente información de las cuentas:

- ID de cuenta
- Nombre de cuenta
- Correo electrónico principal
- Unidad organizativa (OU)

The screenshot shows the 'Affected accounts' tab for an event titled 'EC2 instance network maintenance scheduled'. It features a search bar with the placeholder 'Add filter', a 'Show account details' toggle, and a table with the following data:

Account ID	Account name	Primary email	Organizational unit
▼ 123456789012	Jane Doe AWS account	janedoe@example.com	r-abcd

6. Expanda la cuenta para consultar los recursos afectados.

This screenshot shows the same 'Affected accounts' tab, but with the account '123456789012' expanded. Below the table, two resource ARNs are listed:

```
arn:aws:ec2:us-east-1:123456789012:instance/i-01cdfc3fc1example
arn:aws:ec2:us-east-1:123456789012:instance/example-entity-name-2
```

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:

- En la pestaña Cuentas afectadas, seleccione Añadir filtro, seleccione el ID de cuenta y, a continuación, introduzca el ID de la cuenta. Solo puede ingresar un ID de cuenta a la vez.

- b. Seleccione Aplicar. La cuenta que ha introducido aparece en la lista.

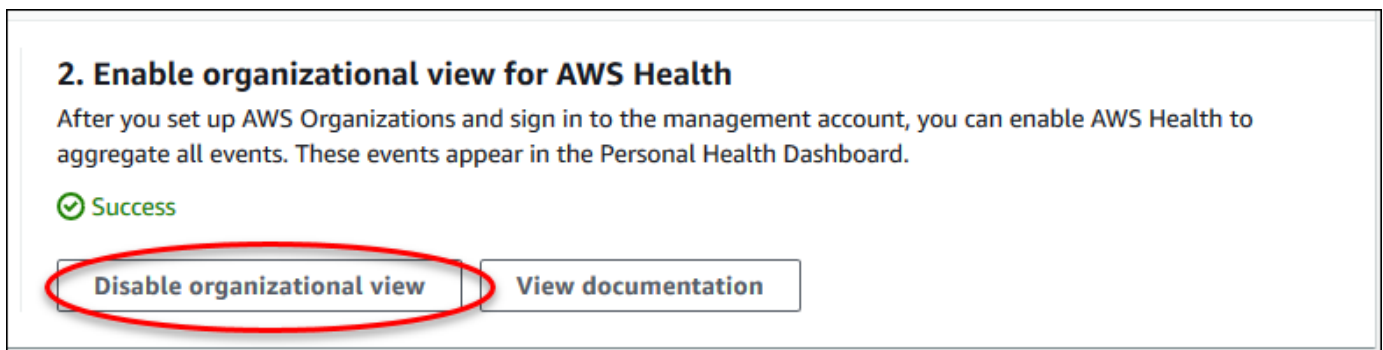
Deshabilitación de la vista organizativa (consola)

Si no desea agregar eventos para su organización, puede desactivar esta característica desde la cuenta de administración.

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

Para desactivar la vista organizativa

1. Abra su AWS Health Panel de control en <https://health.aws.amazon.com/health/home>.
2. En el panel de navegación, en Estado de su organización, elija Configuraciones.
3. En la página Activar la vista organizativa, seleccione Desactivar la vista organizativa.



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

Vista organizativa (CLI)

También puede activar la característica de vista organizativa desde el AWS Command Line Interface (AWS CLI) en lugar de la consola de AWS Health. Para utilizar la consola, consulte [Habilitación de la vista organizativa \(consola\)](#).

Note

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

Contenido

- [Habilitación de la vista organizativa \(CLI\)](#)
- [Visualización de eventos de vista organizativa \(CLI\)](#)
- [Deshabilitación de la vista organizativa \(CLI\)](#)
- [Operaciones de la API de AWS Health de vista organizativa](#)

Habilitación de la vista organizativa (CLI)

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

Puede usar AWS Command Line Interface (AWS CLI) o su propio código para llamar a esta operación.

Note

- Para poder llamar a la API de AWS Health, debe contar con un plan de soporte [Business](#), [Enterprise On-Ramp](#) o [Enterprise](#).
- Debe usar el punto de conexión de la región Este de EE. UU. (Norte de Virginia).

Example

El siguiente comando de la AWS CLI habilita esta característica desde su cuenta de AWS. 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 ejemplos de código siguientes llaman a la operación de la API [EnableHealthServiceAccessForOrganization](#).

Python

```
import boto3

client = boto3.client('health')

response = client.enable_health_service_access_for_organization()

print(response)
```

Java

Puede usar el AWS SDK para Java versión 2.0 para 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](#).

Cuando habilita esta característica, se aplica el `AWSServiceRoleForHealth_Organizations` rol [vinculado al servicio](#) con la `Health_OrganizationsServiceRolePolicy` AWS política administrada 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 operación [DescribeHealthServiceStatusForOrganization](#) para comprobar el estado del proceso.

Visualización de eventos de vista organizativa (CLI)

Después de habilitar esta característica, 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 sucedieron en la organización antes de que se habilite la vista organizativa.

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 periodo de 90 días, AWS eliminará de forma permanente todos los datos de la política de la cuenta.

- Si desea conservar los resultados por más de 90 días, puede archivar las políticas. También puede utilizar una acción personalizada con una regla de EventBridge para almacenar los resultados en un bucket de S3.
- Mientras AWS conserva los datos de la política, cuando vuelva a abrir la cuenta cerrada, AWS reasignará la cuenta como administrador del servicio y recuperará los datos de la política de servicio de la cuenta.
- Para obtener más información, consulte [Cierre de una cuenta](#).

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.

Puede utilizar las operaciones de la API de AWS Health para devolver eventos desde la vista organizativa.

Example : Describir eventos de vista organizativa

El siguiente comando de la AWS CLI devuelve eventos de estado para cuentas de AWS de la organización.

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

Consulte la siguiente sección para otras operaciones de la API de AWS Health.

Deshabilitación de la vista organizativa (CLI)

Puede deshabilitar la vista organizativa mediante la operación de la API [DisableHealthServiceAccessForOrganization](#).

Example

El siguiente comando de la AWS CLI deshabilita esta característica desde su cuenta.

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

Note

También puede deshabilitar la característica organizativa mediante la operación de la API de [DisableAWSServiceAccess](#) de Organizaciones. Después de llamar a esta operación, AWS Health deja de agregar eventos para todas las demás cuentas de la organización. Si llama a las operaciones de la API de AWS Health para la vista organizativa, AWS Health devuelve un error. AWS Health continúa agregando eventos de estado para su cuenta de AWS.

Después de deshabilitar esta característica, AWS Health ya no agrega eventos de su organización. Sin embargo, el rol vinculado al servicio permanece en la cuenta de administración de la organización hasta que lo elimine a través de la AWS Identity and Access Management consola de (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.

Operaciones de la API de AWS Health de vista organizativa

Puede utilizar las siguientes operaciones de la API de AWS Health para la vista organizativa:

- [DescribeEventsForOrganization](#): devuelve información resumida sobre los eventos de la organización.
- [DescribeAffectedAccountsForOrganization](#): devuelve una lista de las cuentas de AWS de la organización que se ven afectadas por el evento especificado.
- [DescribeEventDetailsForOrganization](#): devuelve información detallada sobre los eventos especificados para una o más cuentas de la organización.
- [DescribeAffectedEntitiesForOrganization](#): devuelve una lista de entidades que se han visto afectadas por uno o varios eventos de una o varias cuentas de una organización.

Puede utilizar la siguientes operaciones para habilitar o deshabilitar el funcionamiento de AWS Health con las Organizaciones:

- [EnableHealthServiceAccessForOrganization](#): AWS Health otorga permiso para interactuar con las Organizaciones y aplica la SLR a la cuenta de administración de la organización.
- [DisableHealthServiceAccessForOrganization](#): revoca el permiso para que AWS Health interactúe con las Organizaciones.
- [DescribeHealthServiceStatusForOrganization](#): devuelve información de estado sobre si AWS Health está habilitado para su organización.

Para poder llamar a estas operaciones de la API, debe contar con un plan de soporte Business, Enterprise On-Ramp o Enterprise. Si llama a las operaciones `DescribeEventForOrganization` y `DescribeAffectedAccountsForOrganization` desde una cuenta que tiene al menos un plan de soporte Business, puede devolver información sobre cualquier cuenta de la organización, independientemente del nivel de soporte de las cuentas individuales. Vea los siguientes ejemplos.

Example Ejemplo: una organización con cuentas que tienen planes de soporte Business y Developer

- Tiene tres cuentas en su organización. La cuenta de administración tiene un plan de soporte Business y las otras dos cuentas tienen un plan de soporte Developer.
- Se llama a la operación de la API `DescribeEventForOrganization` desde la cuenta de administración o desde una cuenta que puede asumir el rol con los permisos necesarios.
- AWS Health devuelve información para las tres cuentas.

Si llama a las operaciones de la API `DescribeEventDetailsForOrganization` y `DescribeAffectedEntitiesForOrganization` desde una cuenta que tiene al menos un plan

de soporte Business, solo puede devolver información sobre las cuentas de la organización que tienen un plan de soporte Business, Enterprise On-Ramp o Enterprise.

Example Ejemplo: una organización con cuentas que tienen planes de soporte Enterprise, Business y Developer

- Tiene cinco cuentas en su organización. La cuenta de administración tiene un plan de soporte Enterprise, dos cuentas tienen un plan de soporte Business y dos cuentas tienen un plan de soporte Developer.
- Se llama a la operación de la API `DescribeEventDetailsForOrganization` desde la cuenta de administración.
- AWS Health devuelve información solo para las cuentas que tienen un plan de soporte Enterprise o Business. Las cuentas que tienen un plan de soporte Developer aparecen en `failedSet` de la respuesta.

Vista de administrador delegado de la organización

Con AWS Health, puede aprovechar la característica de administrador delegado de AWS Organizations que le permite a una cuenta distinta de la cuenta de administración ver los eventos agregados de AWS Health en el [AWS HealthPanel de control](#) o mediante programación a través de la [AWS Health API](#). 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 seguridad de AWS consiste en delegar responsabilidades fuera de la cuenta de administración siempre que sea posible.

Contenido

- [Registre un administrador delegado para su vista organizativa](#)
- [Elimine un administrador delegado de la vista organizativa](#)

Registre un administrador delegado para su 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, llame a la operación de API [RegisterDelegatedAdministrator](#). Después de registrar las cuentas de los miembros, se les delega la administración de las cuentas y pueden acceder a la vista organizativa de AWS Health desde el Panel de control de AWS Health. Si la cuenta tiene un plan de soporte [Business](#),

[Enterprise On-Ramp](#) o [Enterprise](#), los administradores delegados pueden usar la API de AWS Health para acceder a la vista organizativa de AWS Health.

Para establecer un administrador delegado, desde la cuenta de administración de su organización, ejecute el siguiente comando AWS Command Line Interface (AWS CLI). Puede utilizar este comando desde la cuenta de administración de AWS Identity and Access Management o desde una cuenta que pueda asumir el rol con los permisos necesarios. En el siguiente comando de ejemplo, sustituya ACCOUNT_ID por el ID de cuenta de miembro que desee registrar junto con la entidad principal de servicio AWS Health “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.

Elimine un administrador delegado de la vista organizativa

Para eliminar el acceso de un administrador delegado, llame a la operación de API [DeregisterDelegatedAdministrator](#).

Desde la cuenta de administración de su organización, ejecute el siguiente comando AWS CLI 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 desee eliminar.

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

Monitorización de AWS Health eventos 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 (AmazonEC2). Cuenta de AWS

Notas

- AWS Health organiza los eventos en función del mejor esfuerzo. No siempre se garantiza la entrega de los eventos a EventBridge.
- EventBridge Las reglas que crees solo pueden recibir notificaciones para ti 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](#).

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 (AmazonSQS)
- Objetivos integrados (como las acciones de CloudWatch alarma)
- Temas de Amazon Simple Notification Service (AmazonSNS)

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

mensajes de texto o SMS notificaciones personalizados 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

- [Acerca de Regiones de AWS para AWS Health](#)
- [Acerca de los eventos públicos para AWS Health](#)
- [Procesador de eventos para AWS Health](#)
- [Crear una EventBridge regla para AWS Health](#)
- [AWS HealthAmazon EventBridge Esquema de eventos](#)
- [Paginación de eventos en AWS Health EventBridge](#)
- [Agregar AWS Health eventos mediante la vista de la organización y el acceso de administrador delegado](#)
- [Recibir eventos AWS Health con AWS Chatbot](#)
- [Automatizar acciones para instancias de Amazon EC2](#)
- [Configure SMC los conectores para AWS Health](#)

Acerca de Regiones de AWS para AWS Health

Debes crear una EventBridge regla para cada región para la que quieras recibir AWS Health eventos. Si no crea una regla, no recibirá eventos. Por ejemplo, para recibir eventos de la región Oeste de EE. UU. (Oregón), debe crear una regla para esa región.

La configuración de una regla adicional en una región de respaldo añade un nivel adicional de resiliencia a sus flujos de trabajo, en caso de que su regla principal se vea afectada por un evento en curso. Los eventos públicos AWS Health se envían simultáneamente a la región afectada y a una región alternativa. Consulte [Acerca de los eventos públicos de AWS Salud](#) para obtener más información. Para todas las regiones de la AWS partición estándar, puedes configurar una regla en el oeste de EE. UU. (Oregón) como alternativa para seguir recibiendo eventos incluso si tu región principal se ve afectada por un problema continuo. La región de respaldo para el Oeste de EE. UU. (Oregón) es la región de Este de EE. UU. (Norte de Virginia).

Por ejemplo, si monitorizas eventos en la región de Europa (Fráncfort) y esa región no está disponible temporalmente, también AWS Health enviarás ese evento a la región de EE. UU.

Oeste (Oregón). A continuación, la EventBridge regla de respaldo envía el evento a los destinos que especificó. Para crear una regla de respaldo, siga el siguiente procedimiento para [Crear una EventBridge regla para AWS Health](#) y utilice la región Oeste de EE. UU. (Oregón).

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 los eventos enviados para AWS Identity and Access Management (IAM). Para recibir eventos globales, debe crear una regla para el Este de EE. UU. (Norte de Virginia) respecto a la región principal y la región Oeste de EE. UU. (Oregón) como región de respaldo.

Para recibir eventos globales en AWS GovCloud (US), debes crear una regla en la región AWS GovCloud (EE. UU. Oeste).

Acerca de los eventos públicos 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.

Si monitorizas los 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 una región alternativa. Se recomienda deduplicar AWS Health los eventos mediante EventARN, communicationId ya que estos siguen siendo consistentes en AWS Health los mensajes que se envían a la región de respaldo.

Puede identificar si un evento es público o específico de una cuenta en EventBridge, mediante el parámetro. `eventScopeCode` Los eventos pueden tener la `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"
  }
}
```

Procesador de eventos para AWS Health

Si utilizas la detección y respuesta a AWS incidentes para tu cuenta, debes [instalar el rol `AWSServiceRoleForHealth_EventProcessor` vinculado al servicio](#) en tu cuenta.

Este rol confía en el servicio principal de `event-processor.health.amazonaws.com` para asumir el rol. Esta función incluye la política `AWSHealth_EventProcessorServiceRolePolicy` AWS gestionada. Esta política enumera los permisos que puede cumplir el rol, Servicios de AWS por ejemplo, llamar a otro en tu nombre.

A continuación, este rol crea una regla EventBridge gestionada por Amazon en tu cuenta. La regla se denomina “`AWSHealthEventProcessor-DO-NOT-DELETE`”. Esta regla es la infraestructura necesaria para que tu cuenta EventBridge pueda enviar información sobre los cambios de estado de alarma desde tu cuenta a AWS Health.

Información relacionada

Para obtener más información, consulte los temas siguientes:

- [Uso de roles vinculados a servicios de AWS Health](#)
- [Política administrada de AWS : `AWSHealth_EventProcessorServiceRolePolicy`](#)

Crear una EventBridge regla para 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 (Siguiendo).
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 AmazonEC2.
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.
 - Elige categorías de tipos de eventos específicos y, a continuación, elige un valor de la lista, como un problema o scheduledChange. accountNotification

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 monitoree cualquier evento de AWS Health, 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, como *i-EXAMPLEa1b2c3de4*, para monitorear 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 Next (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, puedes enviar el evento a una SQS cola de Amazon o a un SNS tema de Amazon.
17. Elija Next (Siguiente).
18. (Opcional) En la página Add tags (Agregar 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 Review and create (Revisar y crear), revise la configuración de las reglas para asegurarse de que se ajustan a los requisitos de supervisión de eventos.
20. Elija Crear 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.

Event pattern [Info](#)

Event pattern form

Custom patterns (JSON editor)

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)

▼

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 `scheduledChange` del tipo de evento
- 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)

▼

AWS_EC2_INSTANCE_TERMINATION_SCHEDULED ✕

AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED ✕

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 Next (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 [Crear una EventBridge regla para 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 [Crear una EventBridge regla para AWS Health](#) para crear la regla.

Utilice API o AWS Command Line Interface (AWS CLI)

Para una regla nueva o existente, utilice la [PutRule](#) API operación o el `aws events put-rule` comando para actualizar el patrón de eventos. Para ver un AWS CLI comando de ejemplo, consulte [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: AmazonEC2, Amazon EC2 Auto Scaling y AmazonVPC. `accountNotification`

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

AWS HealthAmazon EventBridge Esquema de eventos


El siguiente es el esquema de los AWS Health eventos. Los cambios o adiciones a la versión anterior del esquema aparecen resaltados como “Nuevos”. Se proporciona un ejemplo de carga útil después del esquema.

AWS Health Esquema de eventos


AWS Health Esquema de eventos


Parámetro	Descripción	Obligatorio
versión	EventBridge Versión, actualmente «0»	Sí
id	El uniqueEventBridge	Sí

Parámetro	Descripción	Obligatorio
	identificador del evento	
tipo de detalle	Describe el tipo de detalle. Para AWS Health eventos, será o &AWS Health Event AWS Health Abuse Event	Sí
origen	La fuente del bus de eventos. Para AWS Health eventos, será aws.health	Sí


Parámetro	Descripción	Obligatorio
account	<p>La accountId dirección a la que se envió el AWS Health evento.</p> <div data-bbox="1068 541 1269 1671"><p> Note</p><p>En el caso de la organización, será diferente de affectedAccount si se recibe en la cuenta de administración o de administrador delegado.</p></div>	Sí

Parámetro	Descripción	Obligatorio
time	Hora a la que se envió la notificación. EventBridge Formato: yyyy-mm-ddThh:mm:ssZ .	Sí


Parámetro	Descripción	Obligatorio
region	<p>Identifica a Región de AWS el destinatario de la notificación.</p> <div data-bbox="1068 541 1273 1619"><p> Note Este campo no indica la región afectada por este AWS Health evento. Esto lo proporciona «detalle» . eventRegion».</p></div>	Sí

Parámetro	Descripción	Obligatorio
resources	<p data-bbox="1068 226 1256 594">Describe la lista de recursos afectados de una cuenta, si hay recursos afectados.</p> <div data-bbox="1068 636 1271 1476" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p data-bbox="1101 678 1271 1434"> Note Este campo puede estar vacío si no hay ningún recurso al que se haga referencia.</p></div>	No

Parámetro	Descripción	Obligatorio
detalle	Esta sección contiene todos los detalles del AWS Health evento, tal y como se detalla a continuación.	Sí


Parámetro	Descripción	Obligatorio	
	<p data-bbox="354 226 483 258">eventArn</p>	<p data-bbox="1068 226 1253 688">Identificador único del AWS Health evento para la región específica, que incluye la región y el identificador del evento.</p> <div data-bbox="1068 730 1269 1528"><p data-bbox="1101 772 1221 804"> Note</p><p data-bbox="1149 835 1279 1486">Un eventArn no es exclusivo de una cuenta de cliente específica o de una región.</p></div>	<p data-bbox="1308 226 1341 258">Sí</p>

Parámetro	Descripción	Obligatorio	
	servicio	El Servicio de AWS afectado por el AWS Health evento. Por ejemplo, AmazonEC2 , Amazon Simple Storage Service, Amazon Redshift o Amazon Relational Database Service.	Sí


Parámetro		Descripción	Obligatorio
	eventTypeCode	<p>El identificador único para el tipo de evento.</p> <p>Por ejemplo:</p> <p>AWS_EC2_INSTANCE_NETWORK_MAINTENANCE_SCHEDULED y AWS_EC2_INSTANCE_REBOOT_MAINTENANCE_SCHEDULED</p> <p>. Los eventos que incluyen generalmente MAINTENANCE_SCHEDULED se publican aproximadamente dos semanas antes del startTime</p> <div data-bbox="1068 1646 1269 1873" style="border: 1px solid #add8e6; border-radius: 10px; padding: 5px; margin-top: 10px;"> <p> Note</p> <p>Todos los nuevos</p> </div>	Sí


Parámetro		Descripción	Obligatorio
		<p>eventos del ciclo de vida planificados tienen el tipo de evento <code>AWS_{SERVICE}_PLANNED_LIFECYCLE_EVENT</code>.</p>	
	<p><code>eventTypeCategory</code></p>	<p>El código de categoría del evento. Los valores posibles son <code>issue</code>, <code>accountNotification</code>, <code>investigation</code> y <code>scheduledChange</code>.</p>	<p>Sí</p>

Parámetro	Descripción	Obligatorio	
	eventScopeCode	Indica si el AWS Health evento es público o específico de la cuenta. Los valores posibles son ACCOUNT_SPECIFIC o PUBLIC.	Sí

Parámetro	Descripción	Obligatorio
	<p>communicationId (Nuevo)</p> <p>Un identificador único para esta comunicación del AWS Health evento.</p> <p>Los mensajes con el mismo communicationId nombre son posibles mensajes de respaldo o páginas de un solo AWS Health evento. Este identificador se puede usar con el accountId para ayudar a deduplicar los mensajes.</p> <div data-bbox="1068 1478 1269 1852" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>Con el lanzamiento de la función</p> </div>	Sí


Parámetro	Descripción	Obligatorio
	<p>de paginación, communicationId incluye el número de página para mantener la exclusividad en todas las communicationId páginas, por ejemplo, 12345678 10-1. Para obtener más información, consulte Paginación de eventos en</p>	

Parámetro	Descripción	Obligatorio
	AWS Health EventBridge .	
startTime	La hora de inicio del AWS Health evento en el formato: DoW, DD, MMM, YYYY, HH:MM:SS TZ  Note La hora de inicio puede ser en el futuro para eventos programados.	Sí


Parámetro	Descripción	Obligatorio
	<p>endTime</p>	<p>La hora de finalización del AWS Health evento en el formato:DoW, DD MMM YYYY HH:MM:SS TZ.</p> <div data-bbox="1068 735 1273 1528"><p> Note endTime es posible que no se proporcione para eventos que se programen en el futuro.</p></div>

Parámetro	Descripción	Obligatorio	
	<code>lastUpdatedTime</code>	La hora de la última actualización del AWS Health evento en el formato:DoW, DD MMM YYYY HH:MM:SS TZ.	Sí
	<code>statusCode</code>	Estado del AWS Health evento. Los valores posibles son open, closed, o upcoming.	Sí
	<code>eventRegion</code>	La región afectada descrita por este AWS Health evento.	Sí

Parámetro	Descripción	Obligatorio		
	eventDescription	Una sección que describe el AWS Health evento. Incluye campos de idioma y texto para describir el evento.	Sí	
		language	Idioma utilizado en el AWS Health evento. Por lo general, esto lo determina la región en la que se publica el evento. Para la región us-east-1, normalmente es "en_US".	Sí

Parámetro	Descripción	Obligatorio
	<p>latestDescription</p> <p>Describe el AWS Health evento tal como se representa desde el AWS Health panel de control AWS Health API y, por lo general, aparece en él.</p> <div data-bbox="1068 924 1273 1810" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>En el caso de eventos públicos, solo contiene la última actualización y no el historial completo del evento.</p></div>	Sí

Parámetro	Descripción	Obligatorio	
	eventMetadata	Metadatos del evento adicional es que se pueden proporcionar para el evento de AWS Health .	No


Parámetro	Descripción	Obligatorio
	<p data-bbox="591 226 932 260"><clave de metadatos 1></p> <p data-bbox="1068 226 1247 499">clave de metadatos , cadenas de valores "keysting1": "keyvalue1"</p> <div data-bbox="1068 541 1269 1528" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p data-bbox="1101 583 1221 617"> Note</p><p data-bbox="1149 638 1295 1486">Los pares clave-valor de los metadatos del evento los determina el servicio que envió el AWS Health evento.</p></div>	No

Parámetro	Descripción	Obligatorio
affectedEntities	Matriz que describe el valor de los recursos y el estado de los recursos afectados en este AWS Health evento.	No
entityValue	El ID del recurso o de la entidad	No
lastUpdatedtime (Nuevo)	La hora en que se actualizó por última vez el estado de este recurso o entidad en el formato: DoW, DD MMM YYYY HH:MM:SS TZ	No

Parámetro	Descripción	Obligatorio	
	estado (nuevo)	El estado del recurso o de la entidad afectados. Los valores posibles incluyen IMPAIREDUNIT, PENDING, RE	No

VN.


Parámetro	Descripción	Obligatorio
	<p>página (Nueva)</p>	<p>Sí</p>

 **Note**

La paginación solo se produce en los recursos. Otras causas del incumplimiento del límite de tamaño de 256 KB podrían

Parámetro	Descripción	Obligatorio
	provocar un error en la comunicación.	

Parámetro	Descripción	Obligatorio
	<p>totalPages (Nuevo)</p>	<p>Sí</p>

 **Note**

Puede usarlo para determinar si recibió todas las páginas de una comunicación de varias páginas para

Parámetro	Descripción	Obligatorio
	una cuenta.	

Parámetro	Descripción	Obligatorio
	<p>affectedAccount (Nuevo)</p>	<p>Esta es la accountId de la cuenta afectada.</p> <p>Note Puede ser diferente del campo «cuenta» si este problema de salud se envía a una cuenta que forma parte de una AWS Organizations y se recibe en la cuenta de</p>

Parámetro	Descripción	Obligatorio
	administración o de administrador delegado.	

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": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-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",
    "affectedAccount": "123456789012"
  }
}
```

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

```
{
  "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": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-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",
    "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": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-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",
    "affectedAccount": "123456789012"
  }
}
```

Paginación de eventos en AWS Health EventBridge

AWS Health admite la paginación de AWS Health eventos cuando la lista de «recursos» o «affectedEntities» hace que el tamaño del mensaje supere el EventBridge límite de 256 KB. Anteriormente, AWS Health no comunicaba la lista completa de recursos con los eventos cuando superaba este límite.

AWS Health ahora incluye todos los «recursos» y «detalles». affectedEntities» en el mensaje. Si esta lista de «recursos» y «detalles». affectedEntities» supera los 256 KB y, a continuación, AWS Health divide el evento de salud en varias páginas y las publica como mensajes individuales. EventBridge Cada página conserva el mismo evento ARN communicationId para ayudar a volver a combinar la lista de «recursos» o «detalles». 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 añadir un filtro al campo “detail.page” para procesar solo la primera página, lo que elimina los mensajes innecesarios que se crean en las páginas siguientes.

Se incluyen varios cambios en el esquema para facilitar el inicio de la paginación. communicationIdAhora, cada uno incluye el número de página dividido con guiones después delcommunicationId, incluso si solo hay una página. También hay dos campos nuevos, detail.page y detail. totalPages, que 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 excepto en la lista de «detalles». affectedEntities» o «recursos». 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 de la organización 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.

Recibir eventos AWS Health con AWS Chatbot

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, puede 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 AWS Chatbot. Puede configurar Amazon Chime y Slack. Para obtener más información, consulte [Getting started with AWS Chatbot](#) en la AWS Chatbot Guía de administración.
- Un SNS tema de Amazon que has creado y al que estás suscrito. Si ya tienes un SNS tema, puedes usar uno existente. 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 AWS Chatbot

1. Siga el procedimiento de [Crear una EventBridge regla para AWS Health](#) hasta el paso 13.
 - a. Cuando termines de configurar el patrón de eventos en el paso 13, añade una coma a la última línea del patrón y añade la siguiente línea para eliminar los mensajes de chat innecesarios de los eventos paginados AWS Health . Consulte [Paginación de eventos en AWS Health EventBridge](#).

```
"detail.page": ["1"]
```
 - b. Cuando elijas el objetivo en el [paso 14](#), elige un SNS tema. Utilizará este mismo SNS tema en la AWS Chatbot consola.

- c. Complete el resto del procedimiento para crear la regla.
2. Vaya a la [consola de AWS Chatbot](#).
3. Elija su cliente de chat, como el nombre de su canal de Slack, y luego elija Editar.
4. En la sección Notificaciones (opcional), en Temas, elija el mismo SNS tema que especificó en el paso 1.
5. Seleccione Guardar.

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\\n* What will happen to my instance?\\nYour instance will be stopped after the specified retirement date. You can start it agai...

[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 overv...

[Show more](#)

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

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

Automatizar acciones para instancias de Amazon EC2

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 programa un evento de retirada de una EC2 instancia de Amazon para una EC2 instancia respaldada por Amazon Elastic Block Store (AmazonEBS), AWS Health enviará el tipo de `AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED` evento a tu AWS Health panel de control. 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

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

Creación de una IAM política

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 utiliza el editor JSON de políticas de la IAM consola.

Creación de una política de IAM

1. Inicie sesión en AWS Management Console y abra la IAM consola en <https://console.aws.amazon.com/iam/>.
2. En el panel de navegación, seleccione Políticas.
3. Elija Create Policy (Crear política).
4. Seleccione la pestaña JSON.
5. Copie lo siguiente JSON y, a continuación, sustituya la predeterminada JSON en el editor.

```
{
  "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"
  }
]
}

```

- En el Resource parámetro, para el nombre del recurso de Amazon (ARN), introduce tu ID de AWS cuenta.
- 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, como *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 IAM políticas \(consola\)](#) en la Guía del IAM usuario.

Cree un IAM rol

Después de crear la política, debe crear un IAM rol y, a continuación, adjuntar la política a ese rol.

Para crear un rol para un AWS servicio

1. Inicie sesión en AWS Management Console y abra la IAM consola 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, como *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 Siguiente: Revisar.
10. En Nombre del rol, escriba *AutomationEVRole*. Este nombre debe ser el mismo que aparece en ARN la IAM política que creó.
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 [Crear un rol para un AWS servicio](#) en la Guía del IAM usuario.

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 AWS Management Console y abra la IAM consola 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, como *AutomationEVRole*.
4. Elija la pestaña Relaciones de confianza y, a continuación, Editar relación de confianza.
5. En el documento de política, copie lo siguienteJSON, elimine la política predeterminada y pegue la copia JSON en su lugar.

```
{
  "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 roles \(consola\)](#) en la Guía del IAM usuario.

Cree una regla para EventBridge

Siga este procedimiento para crear una regla en la EventBridge consola que le permita 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. Abra 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. Seleccione Servicios específicos 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 EBS respaldadas por Amazon, elija **AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED**. Para EC2 instancias de Amazon respaldadas en tiendas, elija **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 objetivos, en Target, selecciona SSM Automatización.
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 IAM rol que creó, como *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 IAM rol existente con los permisos de Systems Manager necesarios EC2 y una relación de confianza, su rol no aparecerá en la lista. Para obtener más información, consulte [Requisitos previos](#).

18. Seleccione Crear.

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

Configure SMC los conectores para AWS Health

Puede integrar AWS Health 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 SMC integración con AWS Health puede utilizar los eventos de Salud enviados EventBridge para crear, mapear y actualizar automáticamente los JIRA tickets e ServiceNow incidentes.

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

Para obtener más información sobre la ServiceNow integración mediante elSMC, consulte [Integrar AWS Health en ServiceNow](#).

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

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 ejecutas 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 AWS Health eventos con Amazon EventBridge](#).

- AWS CloudTrail captura API las llamadas y los eventos relacionados realizados por su AWS cuenta o en su nombre y envía 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 [AWS CloudTrail Guía del usuario de](#).

Temas

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

Registrar AWS Health API las llamadas con AWS CloudTrail

AWS Health está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, rol o AWS servicio en AWS Health. CloudTrail captura API las llamadas AWS Health como eventos. Las llamadas capturadas incluyen las llamadas desde la AWS Health consola y las llamadas en código a las AWS Health API operaciones. 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 Amazon SNS Notifications para CloudTrail](#)
- [Recibir archivos de CloudTrail registro de varias regiones](#) y [recibir archivos de CloudTrail registro de varias cuentas](#)

Todas AWS Health API las operaciones se registran CloudTrail y se documentan en la [AWS Health APIReferencia](#). Por ejemplo, las llamadas a las DescribeEvents DescribeAffectedEntities operaciones y las llamadas 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 root o con IAM credenciales
- 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 [CloudTrail userIdentityElemento](#).

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 el cifrado del lado del servidor de Amazon S3 (SSE).

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

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

Para obtener más información, consulte [Recepción de archivos de CloudTrail registro de varias regiones](#) y [Recepción de archivos de CloudTrail registro 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 API llamadas públicas, por lo que no aparecen en ningún orden específico.

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la [DescribeEntityAggregates](#) operación.

```
{
  "Records": [
    {
      "eventVersion": "1.05",
```

```
"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-8515-73e8abcabc29b",
"eventType": "AwsApiCall",
"recipientAccountId": "123456789012"
}
],
...
}
```

Historial de documentos para AWS Health

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

- API versión: 4 de agosto de 2016

En la siguiente tabla se describen las actualizaciones importantes de la AWS Health documentación, que comenzaron el 28 de agosto de 2020. Puedes suscribirte al RSS feed para recibir notificaciones sobre las actualizaciones.

Cambio	Descripción	Fecha
Corregido JSON en Monitorin g AWS Health events with Amazon EventBridge	Para obtener más informaci ón, consulta Supervisar AWS Health eventos con Amazon EventBridge .	3 de septiembre de 2024
Información actualizada sobre la descarga de los recursos afectados	Para obtener más información, consulte la vista de recursos afectados .	27 de julio de 2024
Se ha eliminado la privacidad del tráfico entre redes de la documentación de la sección AWS Health de seguridad	Para obtener más información, consulte Seguridad en AWS Health .	27 de marzo de 2024
Se actualizó el AWS Health panel de control: el estado del servicio y los eventos del ciclo de vida planificado para obtener AWS Health do cumentación.	Para obtener más informaci ón, consulte AWS Health Pa nel: Eventos del estado del servicio y del ciclo de vida planificado para AWS Health .	15 de febrero de 2024
Se ha eliminado una viñeta duplicada al crear una EventBridge regla para AWS Health	Se ha eliminado una viñeta duplicada en Crear una EventBridge regla para AWS Health .	4 de diciembre de 2023

Documentación añadida para Eventos del ciclo de vida planificado	Para obtener más información, consulte Eventos del ciclo de vida planificado para AWS Health .	31 de octubre de 2023
Documentación actualizada para AWSHealthFullAccess	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
Se agregó documentación para configurar las notificaciones AWS de usuario en AWS Health.	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
Se agregó documentación sobre la función de administrador delegado a la sección de agregación de AWS Health eventos.	Para obtener más información, consulte Vista de administrador delegado de la organización .	27 de julio de 2023
SLRactualización de la política	Actualización de la política AWS gestionada: Health_OrganizationsServiceRolePolicy. Para más información, consulte Políticas administradas de AWS para AWS Health .	19 de julio de 2023

[AWS Health El esquema ahora admite metadatos de eventos](#)

Ahora puede recibir metadatos de AWS Health eventos de los eventos. Para obtener más información, consulta [Supervisar AWS Health eventos con Amazon EventBridge](#).

[Documentación actualizada para Amazon EventBridge](#)

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 [Supervisar AWS Health eventos con Amazon EventBridge](#).

[Se ha añadido documentación para las políticas AWS gestionadas](#)

Documentación añadida para las políticas administradas por [AWS para AWS Health](#) y el [uso de roles vinculados a servicios para AWS Health](#).

[Documentación añadida sobre la configuración de la zona horaria](#)

Utilice la nueva función de zona horaria para ver el AWS Health panel de control en su zona horaria local o enUTC. Para obtener más información, consulta [Cómo empezar con el AWS Health panel de control: El estado de tu cuenta](#) y el [AWS Health panel de control: estado del servicio](#).

Documentación actualizada	Se agregó documentación para AWS Health Aware. Para obtener más información, consulte AWS Health Aware .	25 de mayo de 2022
Documentación actualizada	Los Service Health Dashboard y los AWS Personal Health Dashboard han cambiado de nombre a AWS Health Dashboard. Para obtener más información, consulte Cómo empezar con el AWS Health panel de control: estado de su cuenta y AWS Health Panel de control: estado del servicio .	28 de febrero de 2022
Documentación actualizada para Amazon EventBridge	Nuevo tema sobre AWS Health el uso de Amazon EventBridge para monitorear eventos de Salud. Para obtener más información, consulta Supervisar AWS Health eventos con Amazon EventBridge .	3 de febrero de 2022
Documentación actualizada	Si tiene un plan Enterprise On-Ramp Support, puede utilizar el AWS Health API.	24 de noviembre de 2021
Documentación agregada	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 AWS Chatbot](#).

16 de marzo de 2021

Documentación actualizada	<p>Se han actualizado los temas siguientes:</p> <ul style="list-style-type: none">• Se ha actualizado el tema Cómo agregar AWS Health eventos• Se reorganizó y actualizó el tema Monitor de AWS Health eventos con Amazon CloudWatch Events• Se actualizó la sección Condiciones basadas en recursos y acciones	29 de enero de 2021
Se agregó el AWS Health panel de control para una vista organizativa en la AWS Health consola	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
Demostración del punto de conexión de alta disponibilidad	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
Actualizaciones de la Guía del usuario de AWS Health	La organización actualiza y añade un RSS feed 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 Agregar eventos de AWS Health en cuentas con vista organizativa .	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 Agregar eventos de AWS Health en cuentas con vista organizativa .	18 de diciembre de 2019
Se agregó una nueva sección «Condiciones basadas en recursos y acciones» para explicar las restricciones de eventos vendidas por el. AWS Health API	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

Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el [Glosario de AWS](#) en la Referencia de Glosario de AWS.

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.