Guía del usuario de

AWS Centro de resiliencia

AWS Centro de resiliencia: Guía del usuario de

Table of Contents

AWS Centro de resiliencia

AWS Resilience Hub es una ubicación central en la que puede gestionar y mejorar la resiliencia de sus aplicaciones. AWS AWS Resilience Hub le permite definir sus objetivos de resiliencia, evaluar su postura de resiliencia en relación con dichos objetivos e implementar recomendaciones de mejora.

Temas

¿Qué es? AWS Resilience Hub?

AWS Resilience Hub es una ubicación central en la que puede gestionar y mejorar la resiliencia de sus aplicaciones. AWS AWS Resilience Hub le permite definir sus objetivos de resiliencia, evaluar su postura de resiliencia en relación con dichos objetivos e implementar recomendaciones de mejora basadas en el AWS Well-Architected Marco. También puede crear y ejecutar AWS Fault Injection Service experimentos, que imiten AWS Resilience Hub las interrupciones de la vida real en su aplicación para ayudarlo a comprender mejor las dependencias y descubrir posibles puntos débiles. AWS Resilience Hub proporciona un lugar central con todos los AWS servicios y herramientas que necesita para fortalecer continuamente su postura de resiliencia. AWS Resilience Hub trabaja con otros servicios para ofrecer recomendaciones y ayudarle a gestionar los recursos de sus aplicaciones. Para obtener más información, consulte Trabajar con otros servicios de.

La siguiente tabla proporciona los enlaces a la documentación de todos los servicios de resiliencia relacionados.

Relacionado AWS servicios y referencias de resiliencia

AWS servicio de resiliencia	Enlace a la documentación
AWS Elastic Disaster Recovery	Qué es Elastic Disaster Recovery
AWS Backup	¿Qué es AWS Backup
Amazon Application Recovery Controller (ARC) (ARC)	Qué es Amazon Application Recovery Controller (ARC)

Temas

AWS Resilience Hub — Gestión de la resiliencia

AWS Resilience Hub le proporciona un lugar central para definir, validar y realizar un seguimiento de la resiliencia de su AWS aplicación. AWS Resilience Hub le ayuda a proteger sus aplicaciones de las interrupciones y a reducir los costos de recuperación para optimizar la continuidad del negocio y ayudar a cumplir con los requisitos normativos y de conformidad. Puede utilizarlo AWS Resilience Hub para hacer lo siguiente:

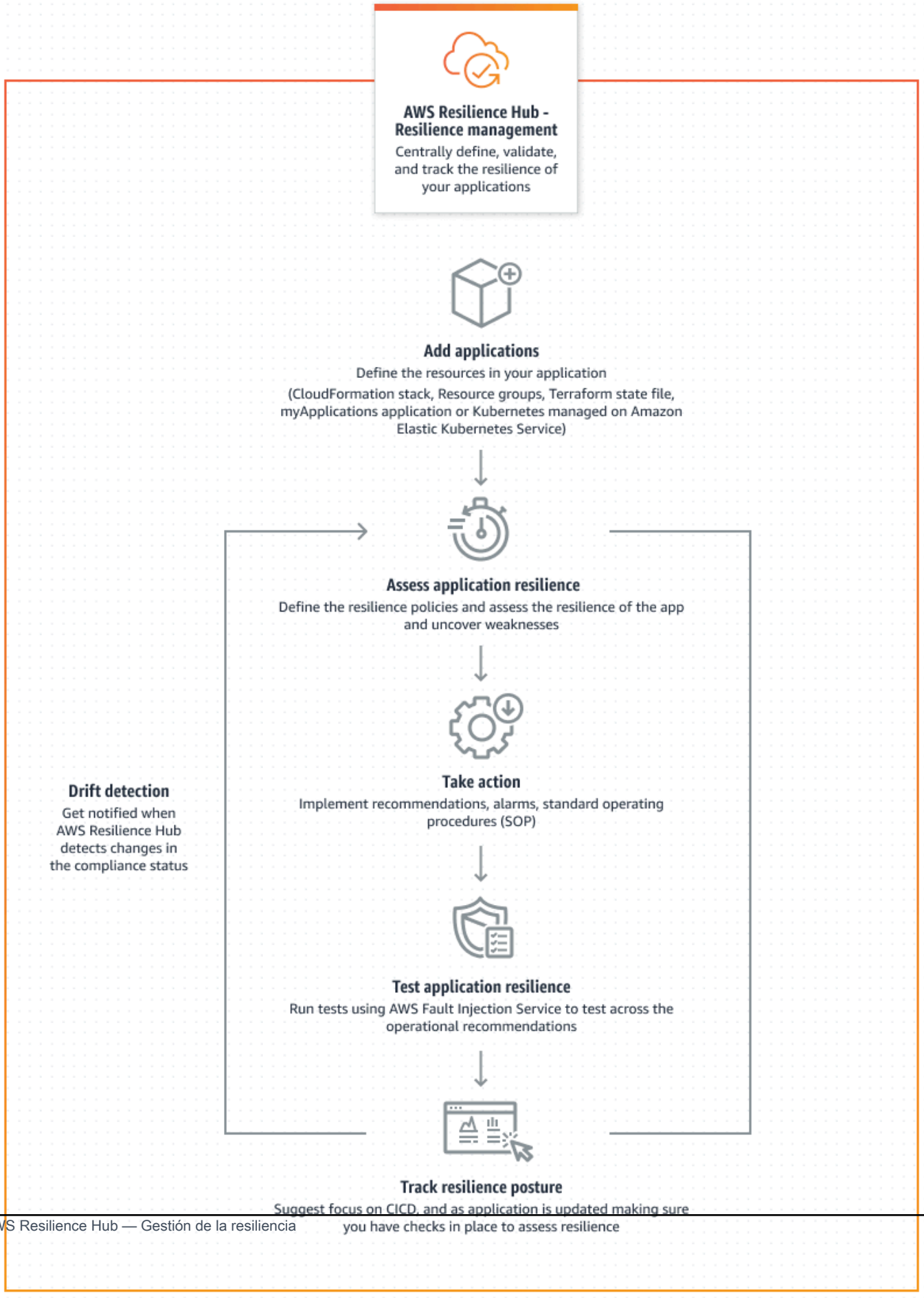
- Analice su infraestructura y obtenga recomendaciones para mejorar la resiliencia de sus aplicaciones. Además de una guía arquitectónica para mejorar la resiliencia de sus aplicaciones, las recomendaciones proporcionan un código para cumplir con su política de resiliencia e implementar pruebas, alarmas y procedimientos operativos estándar (SOP) que puede implementar y ejecutar con su aplicación en su proceso de integración y entrega (CI/CD).
- Evalúe los objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO) en diferentes condiciones.
- Optimice la continuidad empresarial y, al mismo tiempo, reduzca los costos de recuperación.

- Identifique y resuelva los problemas antes de que se produzcan en la producción.

Tras implementar una aplicación en producción, puede añadirla AWS Resilience Hub a su CI/CD proceso de creación para validar cada versión antes de ponerla en producción.

Cómo AWS Resilience Hub funciona

El siguiente diagrama proporciona un resumen detallado de su AWS Resilience Hub funcionamiento.


AWS Resilience Hub - Resilience management
Centrally define, validate, and track the resilience of your applications
Add applications
Define the resources in your application
(CloudFormation stack, Resource groups, Terraform state file, myApplications application or Kubernetes managed on Amazon Elastic Kubernetes Service)
Assess application resilience
Define the resilience policies and assess the resilience of the app and uncover weaknesses
Take action
Implement recommendations, alarms, standard operating procedures (SOP)
Test application resilience
Run tests using AWS Fault Injection Service to test across the operational recommendations
Track resilience posture
Suggest focus on CICD, and as application is updated making sure you have checks in place to assess resilience
Drift detection
Get notified when AWS Resilience Hub detects changes in the compliance status

Describir

Describa su aplicación importando recursos de AWS CloudFormation pilas, archivos de estado de Terraform o clústeres de Amazon Elastic Kubernetes Service Grupos de recursos de AWS, o puede elegir entre aplicaciones que ya están definidas en MyApplications.

Definir

Defina las políticas de resiliencia de sus aplicaciones. Estas políticas incluyen los objetivos de RTO y RPO para las interrupciones en las aplicaciones, la infraestructura, las zonas de disponibilidad y las regiones. Estos objetivos se usan para estimar si la aplicación cumple con la política de resiliencia.

Evaluar

Una vez que describa su aplicación y le adjunte una política de resiliencia, realice una evaluación de la resiliencia. La AWS Resilience Hub evaluación utiliza las mejores prácticas del AWS Well-Architected marco para analizar los componentes de una aplicación y descubrir posibles puntos débiles en materia de resiliencia. Estos pueden deberse a una configuración incompleta de la infraestructura, a una configuración incorrecta o a situaciones en las que se necesiten mejoras de configuración adicionales. Para mejorar la resiliencia, actualice su aplicación y su política de resiliencia de acuerdo con las recomendaciones del informe de evaluación. Las recomendaciones incluyen la configuración de los componentes, las alarmas, las pruebas y los SOP de recuperación. A continuación, puede realizar otra evaluación y comparar los resultados con el informe anterior para ver en qué medida mejora la resiliencia. Repita este proceso hasta que su RTO de carga de trabajo estimada y su RPO de carga de trabajo estimada cumplan sus objetivos de RTO y RPO.

Validar

Realice pruebas para medir la resiliencia de sus AWS recursos y el tiempo que tarda en recuperarse de la aplicación, la infraestructura, la zona de disponibilidad y Región de AWS los incidentes. Para medir la resiliencia, estas pruebas simulan las interrupciones de sus recursos. AWS Entre los ejemplos de interrupciones se incluyen los errores de red no disponibles, las conmutaciones por error, los procesos detenidos, la recuperación del arranque de Amazon RDS y los problemas con la zona de disponibilidad.

Visualización y seguimiento

Después de implementar una AWS aplicación en producción, puede utilizarla AWS Resilience Hub para seguir realizando un seguimiento del estado de resiliencia de la aplicación. Si se

produce una interrupción, el operador puede verla AWS Resilience Hub e iniciar el proceso de recuperación asociado.

AWS Resilience Hub — Pruebas de resiliencia

AWS Resilience Hub admite una integración mejorada con. AWS FIS Esta integración permite AWS Resilience Hub ofrecer recomendaciones personalizadas utilizando AWS FIS acciones y escenarios basados en el contexto específico de la aplicación que se está evaluando. Realizar los experimentos recomendados o realizar tus propias pruebas con el AWS FIS servicio contribuirá directamente a mejorar la puntuación de resiliencia de tu aplicación.

Estas AWS FIS acciones y escenarios ponen a prueba la capacidad de recuperación de una aplicación al crear eventos disruptivos para que pueda observar cómo responde su aplicación. AWS FIS proporciona varios escenarios prediseñados y una amplia selección de acciones que generan interrupciones. Además, también incluye los controles y las barreras de protección que se necesitan para ejecutar los experimentos en producción. Los controles y las barreras de protección incluyen opciones para revertir automáticamente el experimento o detener el experimento si se cumplen determinadas condiciones. Para empezar a utilizarla AWS FIS para ejecutar experimentos desde la AWS Resilience Hub consola, complete los requisitos previos que se definen en la sección. the section called “Requisitos previos”

En la siguiente tabla se enumeran todas las AWS FIS opciones disponibles en el panel de navegación y los enlaces a la AWS FIS documentación asociada, que contiene los procedimientos para empezar a utilizar AWS FIS las pruebas desde la AWS Resilience Hub consola.

AWS FIS opciones y referencias del menú de navegación

AWS FIS opción del menú de navegación	AWS FIS documentación
Pruebas de resiliencia	Crear una plantilla de experimento
Biblioteca de escenarios	AWS FIS biblioteca
Plantillas de experimentos	Plantillas de experimentos para AWS FIS

La siguiente tabla muestra todas las AWS FIS opciones disponibles en el menú desplegable de la sección de pruebas de resiliencia y los enlaces a la AWS FIS documentación asociada que contiene

los procedimientos para empezar a utilizar AWS FIS las pruebas desde la AWS Resilience Hub consola.

AWS FIS opciones y referencias del menú desplegable

AWS FIS opción de menú desplegable	AWS FIS documentación
Crear plantilla de experimento	Crear una plantilla de experimento
Crea un experimento a partir de un escenario	Uso de un escenario

AWS Resilience Hub conceptos

Estos conceptos pueden ayudarlo a comprender mejor el enfoque AWS Resilience Hub de la compañía para ayudar a mejorar la resiliencia de las aplicaciones y evitar las interrupciones de las aplicaciones.

Resiliencia

La capacidad de mantener la disponibilidad y recuperarse de las interrupciones operativas y del software en un plazo determinado.

Objetivo de punto de recuperación (RPO)

La cantidad de tiempo máximo aceptable desde el último punto de recuperación de datos. Esto determina qué se considera una pérdida de datos aceptable entre el último punto de recuperación y la interrupción del servicio.

Objetivo de tiempo de recuperación (RTO)

La demora máxima aceptable entre la interrupción del servicio y el restablecimiento del servicio. Esto determina qué período de tiempo se considera aceptable cuando el servicio no está disponible.

Objetivo de tiempo estimado de recuperación de la carga de trabajo

El objetivo de tiempo estimado de recuperación de la carga de trabajo (RTO estimado de la carga de trabajo) es el RTO que se estima que cumplirá su aplicación en función de la definición de aplicación importada y, a continuación, realizará una evaluación.

Objetivo de punto de recuperación de carga de trabajo estimado

El objetivo del punto de recuperación de la carga de trabajo estimado (RPO de carga de trabajo estimado) es el RPO que se estima que cumplirá su aplicación en función de la definición de aplicación importada y, a continuación, realizará una evaluación.

Aplicación

Una AWS Resilience Hub aplicación es un conjunto de recursos AWS compatibles que se supervisan y evalúan continuamente para gestionar su nivel de resiliencia.

Componente de aplicación

Grupo de AWS recursos relacionados que funcionan y fallan como una sola unidad. Por ejemplo, si tiene una base de datos principal y una réplica, ambas bases de datos pertenecen al mismo componente de aplicación (AppComponent).

AWS Resilience Hub determina qué AWS recursos pueden pertenecer a qué tipo de AppComponent. Por ejemplo, un `DBInstance` puede pertenecer a `AWS::ResilienceHub::DatabaseAppComponent` pero no a `AWS::ResilienceHub::ComputeAppComponent`.

Estado de conformidad de la aplicación

AWS Resilience Hub informa de los siguientes tipos de estado de conformidad para sus aplicaciones.

Se cumple la política

Se estima que la aplicación cumplirá los objetivos de RTO y RPO definidos en la política. Todos sus componentes cumplen con los objetivos políticos definidos. Por ejemplo, seleccionó un objetivo de 24 horas de RTO y RPO para las interrupciones en AWS todas las regiones. AWS Resilience Hub puede ver que sus copias de seguridad se copian en su región alternativa. Aún así, se espera que mantenga una recuperación a partir de un procedimiento operativo estándar (SOP) de respaldo y que la pruebe y cronometre. Esto se incluye en las recomendaciones operativas y forma parte de su puntuación general de resiliencia.

Política incumplida

No se pudo estimar que la aplicación cumpliera los objetivos de RTO y RPO definidos en la política. Uno o más de ellos AppComponents no satisfacen los objetivos de la política. Por ejemplo, ha seleccionado un objetivo de 24 horas de RTO y RPO para las interrupciones en todas las AWS

regiones, pero la configuración de su base de datos no incluye ningún método de recuperación entre regiones, como la replicación global y las copias de seguridad.

Sin evaluar

La aplicación requiere una evaluación. Actualmente no se evalúa ni se realiza un seguimiento.

Cambios detectados

Hay una nueva versión publicada de la aplicación que aún no se ha evaluado.

Detección de desviaciones

AWS Resilience Hub envía una notificación de errores mientras realiza una evaluación de su aplicación para comprobar si los cambios en las AppComponent configuraciones han afectado al estado de conformidad de la aplicación. Además, también comprueba y detecta cambios, como la adición o eliminación de recursos en las fuentes de entrada de la aplicación, y los notifica al respecto. A modo de comparación, AWS Resilience Hub utiliza la evaluación anterior en la que el componente de la aplicación cumplía con la política. AWS Resilience Hub detecta los siguientes tipos de desviaciones:

- Desviación en la política de aplicación: este tipo de desviación identifica a todas las personas AppComponents que cumplieron con la política en la evaluación anterior pero que no la cumplieron en la evaluación actual.
- Desviación de recursos de la aplicación: este tipo de desviación identifica todos los recursos desviados en la versión actual de la aplicación.

Evaluación de resiliencia

AWS Resilience Hub utiliza una lista de deficiencias y posibles soluciones para medir la eficacia de una política seleccionada para recuperarse de un desastre y seguir adelante. Evalúa cada componente de la aplicación o el estado de conformidad de la aplicación con la política. Este informe incluye recomendaciones de optimización de costos y referencias a posibles problemas.

Puntuación de resiliencia

AWS Resilience Hub genera una puntuación que indica en qué medida su solicitud sigue nuestras recomendaciones para cumplir con la política de resiliencia, las alarmas, los procedimientos operativos estándar (SOP) y las pruebas de la aplicación.

Tipo de interrupción

AWS Resilience Hub le ayuda a evaluar la resiliencia frente a los siguientes tipos de interrupciones:

Aplicación

La infraestructura está en buen estado, pero la pila de aplicaciones o software no funciona según las necesidades. Esto puede suceder después de la implementación de un código nuevo, de cambios en la configuración, de la corrupción de los datos o del mal funcionamiento de las dependencias posteriores.

Infraestructura en la nube

La infraestructura de la nube no funciona como se esperaba debido a una interrupción. Se puede producir una interrupción debido a un error local en uno o más componentes. En la mayoría de los casos, este tipo de interrupción se resuelve reiniciando, reciclando o recargando los componentes defectuosos.

Interrupción de la infraestructura en la nube en zonas de disponibilidad

Una o varias zonas de disponibilidad no están disponibles. Este tipo de interrupción se puede resolver cambiando a una zona de disponibilidad diferente.

Incidente en la región de infraestructura de la nube

Una o más regiones no están disponibles. Este tipo de incidente se puede resolver cambiando a una Región de AWS diferente.

AWS FIS experimentos

AWS Resilience Hub recomienda realizar experimentos con AWS FIS acciones para verificar la resiliencia de las aplicaciones frente a distintos tipos de interrupciones. Estas interrupciones incluyen las aplicaciones, la infraestructura, las zonas de disponibilidad (AZ) o los Región de AWS incidentes relacionados con los componentes de la aplicación.

Estos experimentos le permiten hacer lo siguiente:

- Inyectar un error.
- Comprobar que las alarmas puedan detectar una interrupción.
- Compruebe que los procedimientos de recuperación, o los procedimientos operativos estándar (SOP), funcionan correctamente para recuperar la aplicación tras la interrupción.

Las pruebas de los SOP miden el RTO de la carga de trabajo estimada y el RPO de la carga de trabajo estimada. Puede probar diferentes configuraciones de aplicaciones y medir si el RTO y el RPO de salida cumplen los objetivos definidos en su política.

SOP

Un procedimiento operativo estándar (SOP) es un conjunto de pasos prescriptivos que están diseñados para recuperar la aplicación de manera eficiente en caso de que se produzca una interrupción o una alarma. Sobre la base de la evaluación de la aplicación, AWS Resilience Hub recomienda un conjunto de SOP y se recomienda preparar, probar y medir los SOP antes de que se produzca una interrupción para garantizar una recuperación oportuna.

AWS Resilience Hub personas

La creación de una aplicación empresarial requiere el esfuerzo de colaboración de diferentes equipos interdisciplinarios, como los de infraestructura, continuidad empresarial, propietario de la aplicación y otras partes interesadas responsables de la supervisión de las aplicaciones. Las distintas personas de los distintos equipos contribuyen a la creación y la gestión de las aplicaciones AWS Resilience Hub, y cada una de ellas desempeña funciones y responsabilidades diferentes. Para obtener más información sobre la concesión de permisos a diferentes personas, consultethe section called “AWS Resilience Hub referencia de personas y permisos de IAM”.

Para empezar a crear aplicaciones y ejecutar evaluaciones en AWS Resilience Hub ellas, le recomendamos que cree las siguientes personas:

- Administrador de aplicaciones de infraestructura: los usuarios con esta personalidad son responsables de instalar, configurar y mantener los recursos de infraestructura y aplicaciones, garantizando la confiabilidad y la seguridad de la aplicación. Sus responsabilidades incluyen las siguientes:
  - Garantizar que las aplicaciones se desplieguen y actualicen periódicamente
  - Supervisar el rendimiento del sistema
  - Solución de problemas de incidencias
  - Implementación de planes de respaldo y recuperación ante desastres
- Gerente de continuidad empresarial: los usuarios con esta personalidad son responsables de dictar las políticas de las aplicaciones y determinar la importancia empresarial de las aplicaciones. Sus responsabilidades incluyen las siguientes:
  - Tomar decisiones clave al establecer políticas

  - Evaluación de la criticidad empresarial
  - Asignación de recursos para aplicaciones críticas
  - Evaluación y gestión de los riesgos
- Propietario de la aplicación: los usuarios con esta personalidad son responsables de garantizar que las aplicaciones sean fiables y de alta disponibilidad. Sus responsabilidades incluyen las siguientes:
  - Definir los identificadores clave de rendimiento para medir y monitorear el rendimiento de las aplicaciones e identificar los cuellos de botella
  - Organizar capacitaciones para múltiples partes interesadas
  - Asegurarse de que la siguiente documentación esté actualizada:
    - Arquitectura de aplicaciones
    - Procesos de despliegue
    - Configuraciones de monitoreo
    - Técnicas de optimización del rendimiento
- Read-only acceso: los usuarios con esta personalidad están restringidos a permisos de solo lectura. Sus responsabilidades incluyen mantener la visibilidad y la supervisión del rendimiento y el estado de una aplicación mediante el monitoreo de la puntuación de resiliencia, las recomendaciones operativas y las recomendaciones de resiliencia. Además, también son responsables de identificar los problemas, las tendencias y las áreas de mejora para garantizar que la aplicación cumpla con los objetivos de la organización.

AWS Resilience Hub recursos compatibles

Los recursos que afectan al rendimiento de las aplicaciones en caso de una interrupción cuentan con el respaldo total de recursos AWS Resilience Hub de primer nivel, como `AWS::RDS::DBInstance` y`AWS::RDS::DBCluster`.

Para obtener más información sobre los permisos necesarios AWS Resilience Hub para incluir recursos de todos los servicios compatibles en su evaluación, consultethe section called “AWSResilienceHubAsssessmentExecutionPolicy”.

AWS Resilience Hub admite los recursos de los siguientes AWS servicios:

- Computación
  - Amazon Elastic Compute Cloud (Amazon EC2)

> **Note**
>
> AWS Resilience Hub no admite el antiguo formato de nombre de recurso de Amazon (ARN) para acceder a los recursos de Amazon EC2. El nuevo formato ARN utiliza su ID de AWS cuenta y permite una mayor capacidad de etiquetar los recursos del clúster, además de realizar un seguimiento del coste de los servicios y las tareas que se ejecutan en el clúster.
>
> - Formato antiguo (obsoleto): `arn:aws:ec2:<region>::instance/<instance-id>`
> - Formato nuevo — `arn:aws:ec2:<region>:<account-id>:instance/<instance-id>`
>
> Para obtener más información sobre el nuevo formato de ARN, consulte Migración de la implementación de Amazon ECS al nuevo formato de ARN e ID de recurso.

    - AWS Lambda
    - Amazon Elastic Kubernetes Service (Amazon EKS)
    - Amazon Elastic Container Service (Amazon ECS)
    - AWS Step Functions
- Base de datos
    - Amazon Relational Database Service (Amazon RDS)
    - Amazon DynamoDB
    - Amazon DocumentDB
    - Amazon ElastiCache
- Redes y entrega de contenido
    - Amazon Route 53
    - Elastic Load Balancing
    - Traducción de direcciones de red (NAT)
- Almacenamiento
    - Amazon Elastic Block Store (Amazon EBS)
    - Amazon Elastic File System (Amazon EFS)
    - Amazon Simple Storage Service (Amazon S3)
    - Amazon FSx para Windows File Server

- Otros
  - Amazon API Gateway
  - Controlador de recuperación de aplicaciones de Amazon (ARC) (Amazon ARC)
  - Amazon Simple Notification Service
  - Amazon Simple Queue Service
  - AWS Auto Scaling
  - AWS Backup
  - AWS Recuperación elástica ante desastres

> **Note**
>
> - AWS Resilience Hub proporciona una mayor transparencia a los recursos de su aplicación al permitirle ver las instancias compatibles de cada recurso. Además, AWS Resilience Hub proporciona recomendaciones de resiliencia más precisas al identificar una instancia única de cada recurso y, al mismo tiempo, descubrir las instancias del recurso durante el proceso de evaluación. Para obtener más información acerca de cómo agregar instancias de recursos a la aplicación, consulte Edición de los recursos AWS Resilience Hub de la aplicación.
> - AWS Resilience Hub es compatible con Amazon EKS y Amazon ECS en AWS Fargate.
> - AWS Resilience Hub admite la evaluación de AWS Backup los recursos como parte de los siguientes servicios:
>   - Amazon EBS
>   - Amazon EFS
>   - Amazon S3
>   - Base de datos global de Amazon Aurora
>   - Amazon DynamoDB
>   - Servicios de Amazon RDS
>   - Amazon FSx para Windows File Server
> - Amazon ARC in AWS Resilience Hub evalúa únicamente Amazon DynamoDB global, Elastic Load Balancing, Amazon RDS y grupos. AWS Auto Scaling
> - AWS Resilience Hub Para evaluar los recursos entre regiones, agrupe los recursos en un único componente de aplicación. Para obtener más información sobre los recursos

compatibles con cada uno de los componentes de la aplicación AWS Resilience Hub y los recursos de agrupación, consulte Agrupación de recursos en un componente de aplicación.

- Actualmente, AWS Resilience Hub no admite las evaluaciones entre regiones para los clústeres de Amazon EKS si el clúster de Amazon EKS está ubicado o si la aplicación se crea en una región con la opción de suscripción habilitada AWS .
- Actualmente, AWS Resilience Hub evalúa solo los siguientes tipos de recursos de Kubernetes:
  - Implementaciones
  - ReplicaSets
  - Pods
- Actualmente, solo AWS Resilience Hub admite los siguientes tipos de motores para los recursos: ElastiCache
  - Motores OSS de Redis

AWS Resilience Hub ignora los siguientes tipos de recursos:

- Recursos que no afectan al RTO de la carga de trabajo estimada o al RPO de la carga de trabajo estimada: los recursos como `AWS::RDS::DBParameterGroup`, que no afectan al RTO de la carga de trabajo estimada o al RPO de la carga de trabajo estimada no se tienen en cuenta por AWS Resilience Hub.
- Non-top recursos de nivel: AWS Resilience Hub solo importa los recursos de nivel superior, ya que pueden derivar otras propiedades consultando las propiedades de los recursos de nivel superior. Por ejemplo, `AWS::ApiGateway::RestApi` y `AWS::ApiGatewayV2::Api` son recursos compatibles con Amazon API Gateway. Sin embargo, `AWS::ApiGatewayV2::Stage` no es un recurso de nivel superior. Por lo tanto, no es importado por. AWS Resilience Hub

> **Note**
>
> Recursos no compatibles
>
> - No puede identificar varios recursos mediante los recursos Grupos de recursos de AWS (Amazon Route 53 RecordSets y API-GW HTTP) y Amazon Aurora Global. Si desea analizar estos recursos como parte de su evaluación, debe añadir el recurso manualmente

a la aplicación. Sin embargo, al añadir recursos globales de Amazon Aurora para su evaluación, deben agruparse con el componente de aplicación de la instancia de Amazon RDS. Para obtener más información acerca de recursos de edición, consulte the section called “Edición de recursos de aplicaciones”.

- Estos recursos pueden afectar a la recuperación de las aplicaciones, pero por AWS Resilience Hub el momento no son totalmente compatibles. AWS Resilience Hub se esfuerza por avisar a los usuarios sobre los recursos no compatibles si la aplicación está respaldada por una AWS CloudFormation pila, un archivo de estado de Terraform o una aplicación MyApplications. Grupos de recursos de AWS
- Durante el proceso de importación de los recursos de una aplicación AWS Resilience Hub, es posible que se ignoren algunos recursos. Cuando se ignoran los recursos, significa que no se pueden importar en absoluto. Sin embargo, los recursos marcados como no respaldados actualmente no son compatibles con, AWS Resilience Hub pero es posible que se apoyen en el futuro, lo que permite incluirlos en la solicitud de evaluación. Además, AWS Resilience Hub podría ignorar ciertos recursos si no están respaldados por Grupos de recursos de AWS. Para obtener más información sobre los recursos compatibles Grupos de recursos de AWS, consulte Tipos de recursos que puede utilizar con Grupos de recursos de AWS y el Editor de etiquetas.

AWS Resilience Hub y MyApplications

El widget de resiliencia del panel de control de MyApplications agiliza el proceso de evaluación y supervisión de la resiliencia de las aplicaciones. Le permite evaluar rápidamente la resiliencia de las aplicaciones definidas en MyApplications sin necesidad de volver a crearlas manualmente en la consola. AWS Resilience Hub Este enfoque integrado combina las capacidades de administración de aplicaciones de MyApplications con las funciones de evaluación de la resiliencia AWS Resilience Hub, lo que le permite aprovechar las ventajas de ambas plataformas. Al reunir las definiciones de las aplicaciones y las capacidades de evaluación de la resiliencia, el widget de resiliencia simplifica el flujo de trabajo y le permite acceder a la información relevante y tomar medidas para mejorar la resiliencia desde una ubicación centralizada. Cuando se evalúa una aplicación desde el widget de resiliencia, AWS Resilience Hub realiza lo siguiente:

- Crea la aplicación seleccionada en AWS Resilience Hub.
- Descubre y mapea automáticamente los recursos asociados al modelo.

- Crea y asigna una nueva política de resiliencia con valores predefinidos para el Objetivo de tiempo de recuperación (RTO) y el Objetivo de punto de recuperación (RPO). Esto equivale a cuatro horas para RTO y una hora para RPO. Tras generar una evaluación, puede modificar la política de resiliencia o asignar una política diferente desde la AWS Resilience Hub consola. Para obtener más información sobre cómo actualizar la política de resiliencia y adjuntar una política diferente, consulte. Administrar las políticas de resiliencia
- Evalúa la resiliencia de la aplicación frente a la RTO y la RPO definidas en la política de resiliencia para identificar las áreas que requieren mejoras en la arquitectura de la aplicación. Los escenarios de falla incluyen fallas en las zonas de disponibilidad, interrupciones regionales y otras posibles interrupciones.
- Supervisa continuamente los recursos y los cambios de configuración de la aplicación después de la evaluación inicial, y proporciona alertas o actualizaciones si algún cambio afecta a la resiliencia de la aplicación.

> **Note**
>
> Antes de iniciar las evaluaciones, le recomendamos que evalúe los posibles costos que implica la ejecución de las evaluaciones mediante AWS Resilience Hub. Para obtener información detallada sobre los precios, consulte los AWS Resilience Hub precios.

Tras evaluar la aplicación, podrá acceder a todas sus funciones AWS Resilience Hub desde el widget seleccionando Ir AWS Resilience Hub a para ver los detalles de la aplicación en la AWS Resilience Hub consola. El proceso para incluir las aplicaciones de MyApplications en AWS Resilience Hub se rige por las siguientes reglas y restricciones:

- Solo puede asociar una aplicación de MyApplications a una aplicación en. AWS Resilience Hub Es decir, puede asociar una aplicación de MyApplications a una AWS Resilience Hub aplicación ejecutando una evaluación desde el widget de resiliencia del panel de control de MyApplications o completando el Uso de las aplicaciones MyApplications procedimiento mientras se describe la aplicación en la consola. AWS Resilience Hub
- Solo puede incluir, evaluar y ver las aplicaciones de MyApplications que residan en la misma AWS región y límites de AWS cuenta que su entorno de MyApplications. Las aplicaciones creadas en diferentes AWS regiones o con AWS cuentas distintas no estarán visibles ni se podrá acceder a ellas a través de este widget.

- Solo puede añadir, eliminar y actualizar recursos desde el panel de control de MyApplications. Al modificar los recursos de la aplicación desde el panel de control de MyApplications, debe volver a importarlos AWS Resilience Hub para ver los cambios en los recursos. AWS Resilience Hub

Más información

Para obtener más información sobre la administración de aplicaciones y recursos en el panel de control de MyApplications, consulte los siguientes temas de la documentación: AWS Console Home

- ¿En qué está MyApplications? AWS
- Crear su primera aplicación en MyApplications
- Administrar recursos
- Widget de resiliencia

Para obtener más información sobre la descripción de las aplicaciones y la ejecución de las evaluaciones en AWS Resilience Hub ellas, consulte los siguientes temas:

- Para realizar una evaluación de resiliencia de una aplicación MyApplications existente desde el widget Resiliency por primera vez
- Para volver a ejecutar una evaluación de resiliencia de una aplicación MyApplications existente desde el widget Resiliency
- Revisar el resumen de la evaluación en el widget de resiliencia

Introducción

En esta sección se describe cómo empezar a utilizar AWS Resilience Hub. Esto incluye la creación de permisos de AWS Identity and Access Management (IAM) para una cuenta.

Temas

- Requisitos previos
- Añadir una aplicación a AWS Resilience Hub

Requisitos previos

Antes de poder utilizar el AWS Resilience Hub, debe cumplir los siguientes requisitos previos:

- AWS cuentas: cree una o más AWS cuentas para cada tipo de cuenta (primary/secondary/cuentas de recursos) que desee utilizar. AWS Resilience Hub Para obtener más información sobre la creación y administración de AWS cuentas, consulte lo siguiente:
  - AWS Usuario primerizo: Primeros pasos: ¿Es usted un AWS usuario primerizo?
  - Administrar la AWS cuenta — https://docs.aws.amazon.com/accounts/latest/reference/managing-accounts.html
- AWS Identity and Access Management Permisos (IAM): después de crear las AWS cuentas, debe configurar las funciones y los permisos de IAM necesarios para cada una de las cuentas que haya creado. Por ejemplo, si ha creado una AWS cuenta para acceder a los recursos de la aplicación, debe configurar un nuevo rol y configurar los permisos de IAM necesarios para acceder AWS Resilience Hub a los recursos de la aplicación desde su cuenta. Para obtener más información sobre los permisos de IAM, consulte the section called “Cómo AWS Resilience Hub funciona con IAM” y para obtener más información sobre cómo añadir una política al rol, consulte the section called “Definir la política de confianza mediante un archivo JSON”.

  Para empezar rápidamente a añadir permisos de IAM a usuarios, grupos y roles, puede utilizar nuestras políticas AWS gestionadas ()the section called “AWS políticas gestionadas”. Es más fácil utilizar las políticas AWS gestionadas para cubrir los casos de uso más comunes que están disponibles en las tuyas Cuenta de AWS que redactar las políticas tú mismo. AWS Resilience Hub añade permisos adicionales a una política AWS gestionada para ampliar el soporte a otros AWS servicios e incluir nuevas funciones. Por lo tanto:

  - Si ya es cliente y desea que su aplicación utilice las últimas mejoras en su evaluación, debe publicar una nueva versión de la aplicación y, a continuación, ejecutar una nueva evaluación. Para obtener más información, consulte los temas siguientes:
    - the section called “Publicar una nueva versión de la aplicación”
    - the section called “Realizar evaluaciones de resiliencia en AWS Resilience Hub”
  - Si no utiliza políticas AWS administradas para asignar los permisos de IAM adecuados a los usuarios, grupos y roles, debe configurar estos permisos manualmente. Para obtener más información sobre las políticas AWS administradas, consultethe section called “AWSResilienceHubAsssessmentExecutionPolicy”.

Añadir una aplicación a AWS Resilience Hub

AWS Resilience Hub ofrece una evaluación y validación de la resiliencia que se integran en el ciclo de vida del desarrollo de software. AWS Resilience Hub le ayuda a preparar y proteger sus AWS aplicaciones de forma proactiva contra las interrupciones mediante:

- La detección de los puntos débiles de la resiliencia.
- La estimación de si se puede cumplir con el objetivo de tiempo de recuperación (RTO) y el objetivo de punto de recuperación (RPO).
- La resolución de los problemas antes de que se pongan en producción.

Esta sección le guía a través de cómo agregar una aplicación. Reúne recursos de una aplicación MyApplications existente, de AWS CloudFormation pilas o crea una política Grupos de recursos de AWS de resiliencia adecuada. Tras describir una aplicación, puede publicarla y generar un informe de evaluación sobre la resiliencia de la aplicación. AWS Resilience Hub A continuación, puede usar las recomendaciones de la evaluación para mejorar la resiliencia. Puede realizar otra evaluación, comparar los resultados y, a continuación, realizar iteraciones hasta que el RTO de carga de trabajo estimado y el RPO de carga de trabajo estimado alcancen sus objetivos de RTO y RPO.

Temas

Comience por añadir una aplicación

Comience AWS Resilience Hub describiendo los detalles de su AWS aplicación y elaborando un informe para evaluar la resiliencia.

Para empezar, en la página de AWS Resilience Hub inicio, en Comenzar, selecciona Añadir aplicación.

Para obtener más información sobre los costos y la facturación asociados AWS Resilience Hub, consulta AWS Resilience Hub los precios.

Describa los detalles de su solicitud en AWS Resilience Hub

En esta sección se muestra cómo describir los detalles de su AWS solicitud actual en AWS Resilience Hub.

Para describir los detalles de su aplicación

1. Escriba un nombre para la aplicación.
2. (Opcional) Escriba una descripción para la aplicación.

Next

Selección de cómo se administra esta aplicación

Selección de cómo se administra esta aplicación

Además de las AWS CloudFormation pilas Grupos de recursos de AWS, las aplicaciones de MyApplications y los archivos de estado de Terraform, puede añadir recursos que se encuentren en los clústeres de Amazon Elastic Kubernetes Service (Amazon EKS). Es decir, AWS Resilience Hub le permite añadir recursos que se encuentran en sus clústeres de Amazon EKS como recursos opcionales. En esta sección se proporcionan las siguientes opciones, que le ayudan a determinar la ubicación de los recursos de su aplicación.

- Colecciones de recursos: seleccione esta opción si desea detectar los recursos de una de las colecciones de recursos. Las colecciones de recursos incluyen AWS CloudFormation pilas, aplicaciones de MyApplications y archivos de estado de Grupos de recursos de AWS Terraform.

  Si selecciona esta opción, debe completar uno de los procedimientos de the section called “Agregar colecciones de recursos”.
- Solo EKS: seleccione esta opción si desea detectar recursos de los espacios de nombres de los clústeres de Amazon EKS.

  Si selecciona esta opción, debe completar uno de los procedimientos de the section called “Añadir clústeres de EKS”

- Colecciones de recursos y EKS: seleccione esta opción si desea descubrir recursos de AWS CloudFormation pilas Grupos de recursos de AWS, archivos de estado de Terraform y clústeres de Amazon EKS.

  Si selecciona esta opción, complete uno de los procedimientos de the section called “Agregar colecciones de recursos” y, a continuación, complete el procedimiento de the section called “Añadir clústeres de EKS”.

> **Note**
>
> Para obtener información sobre la cantidad de recursos admitidos por aplicación, consulte Service Quotas.

Next

Agregar colecciones de recursos

Agregar colecciones de recursos

En esta sección se describen las siguientes opciones que puede usar para formar la base de la estructura de su aplicación:

- Agregar colecciones de recursos
- Añadir clústeres de EKS

Agregar colecciones de recursos

En esta sección se describen los siguientes métodos que se usan para formar la base de la estructura de la aplicación:

- Uso de AWS CloudFormation pilas
- Usando Grupos de recursos de AWS
- Uso de las aplicaciones MyApplications
- Uso de archivos de estado de Terraform

Uso de AWS CloudFormation pilas

Elige las AWS CloudFormation pilas que contienen los recursos que quieres usar en la aplicación que estás describiendo. Las pilas pueden ser de las Cuenta de AWS que estás usando para describir la aplicación o pueden provenir de cuentas o regiones diferentes.

Para detectar los recursos que forman la base de la estructura de su aplicación

1. Selecciona CloudFormation una pila para descubrir tus recursos basados en pilas.
2. Elige las pilas de la lista desplegable Elige las pilas que estén asociadas a tu región y a tu región. Cuenta de AWS

   Para usar pilas que estén en una región diferente Cuenta de AWS, diferente o en ambas, selecciona la flecha derecha situada junto a Añadir pila fuera de la AWS región e introduce el nombre de recurso de Amazon (ARN) de la pila en el cuadro Introducir un ARN de pila y, a continuación, selecciona Añadir ARN de pila. Para obtener más información ARNs, consulte Amazon Resource Names (ARNs) en la Referencia AWS general.

Usando Grupos de recursos de AWS

Elija los Grupos de recursos de AWS que contengan los recursos que desea utilizar en la aplicación que está describiendo.

Para detectar los recursos que forman la base de la estructura de su aplicación

1. Seleccione los grupos de recursos para descubrir los Grupos de recursos de AWS que contienen los recursos.
2. Elija los recursos de la lista desplegable Elija un grupo de recursos.

   Para usarlos Grupos de recursos de AWS en una región diferente Cuenta de AWS, diferente o en ambas, elija la flecha derecha junto al ARN del grupo de recursos: e introduzca el nombre de recurso de Amazon (ARN) del Grupos de recursos de AWS en el cuadro Introduzca un ARN de grupo de recursos y, a continuación, elija Agregar ARN de grupo de recursos. Para obtener más información ARNs, consulte Amazon Resource Names (ARNs) en la Referencia AWS general.

Uso de las aplicaciones MyApplications

Elija la aplicación MyApplications que desee incluir en AWS Resilience Hub

Para incluir la aplicación MyApplications en AWS Resilience Hub

1. Seleccione Mis aplicaciones.
2. Elija una aplicación de la lista desplegable Seleccionar aplicación.

Uso de archivos de estado de Terraform

Elija el archivo de estado de Terraform que contiene los recursos de su bucket de Amazon S3 que desee usar en la aplicación que describe. Puede ir a la ubicación de su archivo de estado de Terraform o proporcionar un enlace a un archivo de estado de Terraform al que tenga acceso y que esté ubicado en una región diferente.

> **Note**
>
> AWS Resilience Hub es compatible con la versión del archivo de estado de Terraform `0.12` y versiones posteriores.

Para detectar los recursos que forman la base de la estructura de su aplicación

1. Seleccione Archivos de estado de Terraform para descubrir los recursos de su bucket de S3.
2. En la sección Seleccionar archivos de estado::, selecciona Browse S3 para ir a la ubicación de tu archivo de estado de Terraform.

   Para usar los archivos de estado de Terraform ubicados en una región diferente, proporciona el enlace a la ubicación del archivo de estado de Terraform en el campo URI de S3 y selecciona Agregar URL de S3.

   El límite de los archivos de estado de Terraform es de 4 megabytes (MB).
3. En el cuadro de diálogo Elegir un archivo en S3, seleccione su depósito de Amazon Simple Storage Service en la sección Depósitos.
4. En la sección Objetos, seleccione una clave y seleccione Seleccionar.

Añadir clústeres de EKS

En esta sección se describe el uso de los clústeres de Amazon EKS como base de la estructura de su aplicación.

> **Note**
>
> Debe tener permisos de Amazon EKS y roles de IAM adicionales para conectarse al clúster de Amazon EKS. Para obtener más información sobre cómo añadir permisos de Amazon EKS para una o varias cuentas y roles de IAM adicionales para conectarse al clúster, consulte los siguientes temas:
>
> - AWS Resilience Hub referencia de permisos de acceso
> - the section called “Habilitar el AWS Resilience Hub acceso a su clúster de Amazon EKS”

Seleccione los clústeres y espacios de nombres de Amazon EKS que contengan los recursos que desee usar en la aplicación que está describiendo. Los clústeres de Amazon EKS pueden provenir de la Cuenta de AWS que está utilizando para describir la aplicación o pueden provenir de cuentas o regiones diferentes.

> **Note**
>
> AWS Resilience Hub Para evaluar sus clústeres de Amazon EKS, debe añadir manualmente los espacios de nombres correspondientes a cada uno de los clústeres de Amazon EKS en la sección de clústeres y espacios de nombres de EKS. El nombre del espacio de nombres debe coincidir exactamente con el nombre del espacio de nombres de sus clústeres de Amazon EKS.

Para agregar clústeres de Amazon EKS

1. En 1. Seleccione la sección Clústeres de EKS y elija los clústeres de Amazon EKS de la lista desplegable Elegir clústeres de EKS que estén asociados a su región Cuenta de AWS y a su región.
2. Para utilizar clústeres de Amazon EKS que se encuentren en una región diferente Cuenta de AWS, diferente o en ambas, elija la flecha derecha situada junto a Añadir un clúster de EKS dentro de una cuenta o región diferente e introduzca el nombre de recurso de Amazon (ARN) del clúster de Amazon EKS en el cuadro Introduzca un ARN de EKS y, a continuación, seleccione Añadir ARN de EKS. Para obtener más información ARNs, consulte Amazon Resource Names (ARNs) en la Referencia AWS general.

Para obtener más información sobre cómo añadir permisos para acceder a los clústeres de Amazon Elastic Kubernetes Service entre regiones, consulte the section called “Habilitar el AWS Resilience Hub acceso a su clúster de Amazon EKS”.

Para añadir espacios de nombres de los clústeres de Amazon EKS seleccionados

1. En la sección Añadir espacios de nombres, en la tabla Clústeres y espacios de nombres de EKS, seleccione el botón de radio situado a la izquierda del nombre del clúster de Amazon EKS y, a continuación, seleccione Actualizar espacios de nombres.

   Puede identificar los clústeres de Amazon EKS de la siguiente manera:

   - Nombre del clúster de EKS: indica el nombre de los clústeres de Amazon EKS seleccionados.
   - Número de espacios de nombres: indica el número de espacios de nombres seleccionados en los clústeres de Amazon EKS.
   - Estado: indica si AWS Resilience Hub ha incluido los espacios de nombres de los clústeres de Amazon EKS seleccionados en su aplicación. Puede identificar el estado mediante las siguientes opciones:
     - Espacio de nombres obligatorio: indica que no ha incluido ningún espacio de nombres del clúster de Amazon EKS.
     - Espacios de nombres agregados: indica que ha incluido uno o más espacios de nombres del clúster de Amazon EKS.
2. Para añadir un espacio de nombres, en el cuadro de diálogo Actualizar espacios de nombres, seleccione Añadir un nuevo espacio de nombres.

   El cuadro de diálogo Actualizar espacios de nombres muestra todos los espacios de nombres que ha seleccionado de su clúster de Amazon EKS, como una opción editable.
3. En el cuadro de diálogo Actualizar espacios de nombres, tiene las siguientes opciones de edición:

   - Para añadir un nuevo espacio de nombres, seleccione Añadir un nuevo espacio de nombres y, a continuación, introduzca el nombre del espacio de nombres en el cuadro espacio de nombres.

     El nombre del espacio de nombres debe coincidir exactamente con el nombre del espacio de nombres del clúster de Amazon EKS.

- Para eliminar un espacio de nombres, seleccione Eliminar, situado junto al espacio de nombres.
- Para aplicar los espacios de nombres seleccionados a todos los clústeres de Amazon EKS, seleccione Aplicar espacios de nombres a todos los clústeres de EKS.

  Si elige esta opción, la selección de espacio de nombres anterior en los demás clústeres de Amazon EKS se sustituirá por la selección de espacio de nombres actual.

4. Para incluir los espacios de nombres actualizados en su aplicación, seleccione Actualizar.

Next

Configuración de RTO y RPO

Configuración de RTO y RPO

Puede definir una nueva política de resiliencia con sus propios RTO/RPO objetivos o puede elegir una política de resiliencia existente con objetivos predefinidos. RTO/RPO Si desea usar una de las políticas de resiliencia existentes, seleccione Elegir una opción de política existente y seleccione una aplicación de destino existente en la lista desplegable Elemento de opción.

Para definir sus propios objetivos RTO/RPO

1. Seleccione Crear una nueva opción de política de resiliencia.
2. Introduzca un nombre para la política de resiliencia en el cuadro Introducir el nombre de la política (en Nombre).

   Hemos rellenado previamente este campo con un nombre generado automáticamente. Puede elegir usar el mismo nombre o proporcionar un nombre diferente.
3. (Opcional) Introduzca una descripción de la política de resiliencia en el cuadro Descripción.
4. Defina sus objetivos RTO/RPO en la sección de objetivos de RTO/RPO.

> **Note**
>
> - Hemos rellenado previamente un RTO y un RPO predeterminados para su aplicación. Puede cambiar el RTO y el RPO ahora o después de evaluar la aplicación.
> - AWS Resilience Hub le permite introducir un valor cero en los campos RTO y RPO de su política de resiliencia. Sin embargo, al evaluar su aplicación, el resultado de

evaluación más bajo posible es cercano a cero. Por lo tanto, si introduce un valor cero en los campos RTO y RPO, los resultados estimados de RTO y RPO de carga de trabajo serán próximos a cero y el Estado de conformidad de su aplicación pasará a ser Política infringida.

5. Para definirlo RTO/RPO para su infraestructura y su zona de disponibilidad, elija la flecha derecha para ampliar la sección RTO y RPO de infraestructura.
6. En Objetivos de RTO/RPO, introduzca un valor numérico en el cuadro y, a continuación, seleccione la unidad de tiempo que representa el valor tanto para RTO como para RPO.

   Repita estas entradas para Infraestructura y Zona de disponibilidad en la sección RTO y RPO de infraestructura.
7. (Opcional) Si tienes una aplicación multirregional y quieres definir un RTO y un RPO regionales, activa Región: opcional.

   En RTO y RPO, introduzca un valor numérico en el cuadro y, a continuación, seleccione la unidad de tiempo que representa el valor tanto para RTO como para RPO.

Next

the section called “Configure la evaluación programada y la notificación de desviaciones”

Configuración de las evaluaciones programadas y la notificación de desviaciones

AWS Resilience Hub le permite configurar evaluaciones programadas y notificaciones de desviación para evaluar su aplicación a diario y recibir notificaciones cuando se detecte una desviación.

Para configurar la notificación de desviación

1. Para evaluar tu solicitud a diario, activa la opción Evaluar automáticamente todos los días.

   Si esta opción está activada, el programa de evaluación diaria comenzará si se dan las siguientes condiciones:

   - La aplicación se evalúa manualmente con éxito por primera vez.
   - La aplicación está configurada con un rol de IAM adecuado.
   - Si su aplicación está configurada con los permisos de usuario de IAM actuales, debe crear el rol `AWSResilienceHubAsssessmentExecutionPolicy`

mediante el procedimiento adecuado en the section called “Cómo AWS Resilience Hub funciona con IAM”.

2. Para recibir una notificación cuando AWS Resilience Hub detecte cualquier desviación en las políticas de resiliencia o cuando sus recursos se hayan desviado, activa Recibir notificaciones cuando la aplicación se desvíe.

   Si esta opción está activada, para recibir notificaciones de desviaciones, debe especificar un tema de Amazon Simple Notification Service (Amazon SNS). Para proporcionar un tema de Amazon SNS, en la sección Proporcionar un tema de SNS, seleccione la opción Elegir un tema de SNS y seleccione un tema de Amazon SNS de la lista desplegable Elegir un tema de SNS.

   > **Note**
   >
   > - AWS Resilience Hub Para permitir la publicación de notificaciones en sus temas de Amazon SNS, su tema de Amazon SNS debe estar configurado con los permisos adecuados. Para obtener más información acerca de la configuración de permisos, consulte the section called “ AWS Resilience Hub Habilitar la publicación en sus temas de Amazon SNS”.
   > - Las evaluaciones diarias pueden afectar a su cuota de ejecuciones. Para obtener más información sobre cuotas, consulte Puntos de conexión y cuotas de AWS Resilience Hub en la Referencia general de AWS .

   Para usar temas de Amazon SNS que estén en una región diferente Cuenta de AWS o diferente, o en ambas, seleccione Introducir el ARN del tema de SNS e introduzca el nombre de recurso de Amazon (ARN) del tema de Amazon SNS en el cuadro Proporcione un tema de SNS. Para obtener más información ARNs, consulte Amazon Resource Names (ARNs) en la Referencia AWS general.

Next

Configuración de permisos

Configuración de permisos

AWS Resilience Hub permite configurar los permisos necesarios para que la cuenta principal y la cuenta secundaria descubran y evalúen los recursos. Sin embargo, debe ejecutar el procedimiento por separado para configurar los permisos de cada cuenta.

Para configurar las los permisos y roles de IAM

1. Para seleccionar una función de IAM existente que se utilizará para acceder a los recursos de la cuenta actual, seleccione una función de IAM en la lista desplegable Seleccione una función de IAM.

   > **Note**
   >
   > Para una configuración multicuenta, si no especifica los nombres de los recursos de Amazon (ARNs) de la función de IAM en el cuadro ARN Introducir una función de IAM, AWS Resilience Hub utilizará la función de IAM que haya seleccionado en la lista desplegable Seleccionar una función de IAM para todas las cuentas.

   Si no hay ningún rol de IAM asociado a su cuenta, puede crear un rol de IAM mediante una de las siguientes opciones:

   - AWS Consola de IAM: si elige esta opción, debe completar el procedimiento descrito en Para crear su función en la consola de IAM. AWS Resilience Hub
   - AWS CLI: si elige esta opción, debe completar todos los pasos de la AWS CLI.
   - CloudFormation plantilla: si elige esta opción, según el tipo de cuenta (cuenta principal o cuenta secundaria), debe crear los roles utilizando la AWS CloudFormation plantilla adecuada.
2. Seleccione la flecha derecha para ampliar la sección Añadir roles de IAM desde una cuenta cruzada (opcional).
3. Para seleccionar las funciones de IAM de una cuenta cruzada, introduzca la función ARNs de IAM en el cuadro ARN Introduzca una función de IAM. Asegúrese de que las funciones ARNs de IAM que va a introducir no pertenezcan a la cuenta actual.
4. Si desea usar el usuario de IAM actual para descubrir los recursos de su aplicación, seleccione la flecha derecha para ampliar la sección Usar los permisos del usuario de IAM actual y seleccione Entiendo que debo configurar manualmente los permisos para habilitar la funcionalidad requerida en AWS Resilience Hub.

Si selecciona esta opción, es posible que algunas de las AWS Resilience Hub funciones (como la notificación de desviaciones) no funcionen según lo esperado y se ignorarán las entradas que haya proporcionado para crear una nueva aplicación.

Next

Configure los parámetros de configuración de la aplicación

Configure los parámetros de configuración de la aplicación

Esta sección le permite proporcionar los detalles de su soporte de conmutación por error entre regiones mediante. AWS Elastic Disaster Recovery AWS Resilience Hub utilizará esta información para proporcionar recomendaciones de resiliencia.

Para obtener más información acerca de los parámetros de configuración de la aplicación, consulte Parámetros de configuración de la aplicación.

Para añadir parámetros de configuración de la aplicación (opcional)

1. Para expandir la sección Parámetros de configuración de la aplicación, seleccione la flecha derecha.
2. Introduzca el ID de la cuenta de conmutación por error en el cuadro ID de cuenta. De forma predeterminada, hemos rellenado previamente este campo con el identificador de cuenta utilizado AWS Resilience Hub, que se puede cambiar.
3. Seleccione una región de conmutación por error en la lista desplegable Región.

> **Note**
>
> Si desea deshabilitar esta característica, seleccione "—" en la lista desplegable.

Next

Agregar etiquetas.

Agregar etiquetas.

Asigna una etiqueta o rótulo a un AWS recurso para buscar y filtrar tus recursos, o haz un seguimiento de tus AWS costos.

(Opcional) Para añadir etiquetas a la aplicación, seleccione Añadir nueva etiqueta si desea asociar una o más etiquetas a la aplicación. Para más información sobre las etiquetas, consulte Etiquetado de recursos en la Guía de referencia general de AWS .

Seleccione Añadir aplicación para crear su aplicación.

Next

Revisa y publica tu AWS Resilience Hub solicitud

Revisa y publica tu AWS Resilience Hub solicitud

Tras crear la aplicación, podrá revisarla y editar sus recursos. Cuando termine, seleccione Publicar para publicar la aplicación.

> **Note**
>
> AWS Resilience Hub escanea los recursos de la aplicación en segundo plano y comprueba si se pueden agrupar de una manera más eficiente que mejore la precisión de las evaluaciones. Si AWS Resilience Hub identifica los recursos que se pueden agrupar según corresponda AppComponents, mostrará una alerta informativa sobre las recomendaciones de agrupación de recursos en la pestaña Estructura de la aplicación de la página de la aplicación y podrá revisarlas seleccionando Revisar recomendaciones. Para obtener más información, consulte the section called “AWS Resilience Hub recomendaciones de agrupamiento de recursos”.

Para obtener más información acerca de la revisión de la aplicación y la edición de sus recursos, consulte lo siguiente:

- the section called “Visualización del resumen de aplicación”
- the section called “Edición de recursos de aplicaciones”

Next

Realice una evaluación de su aplicación AWS Resilience Hub

Realice una evaluación de su aplicación AWS Resilience Hub

La aplicación que ha publicado aparece en la página de Resumen.

Tras publicar la AWS Resilience Hub solicitud, se le redirigirá a la página de resumen de la aplicación, donde podrá realizar una evaluación de resiliencia. La evaluación evalúa la configuración de la aplicación en función de la política de resiliencia adjunta a la aplicación. Se genera un informe de evaluación que muestra cómo se compara su aplicación con los objetivos de su política de resiliencia.

Para realizar una evaluación de resiliencia

1. En la página Resumen de aplicaciones, seleccione Evaluar resiliencia.
2. En el cuadro de diálogo Ejecutar una evaluación de resiliencia, introduzca un nombre único para el informe o utilice el nombre generado en el cuadro Nombre del informe.
3. Elija Ejecutar.
4. Cuando se le notifique que se ha generado el informe de evaluación, seleccione la pestaña Evaluaciones y su evaluación para ver el informe.
5. Seleccione la pestaña Revisar para ver el informe de evaluación de su aplicación.

Utilización AWS Resilience Hub

AWS Resilience Hub le ayuda a mejorar la resiliencia de sus aplicaciones AWS y a reducir el tiempo de recuperación en caso de interrupciones de las aplicaciones.

Temas:

AWS Resilience Hub resumen

AWS Resilience Hub proporciona un resumen visual con tablas y gráficos que le ofrece una at-a-glance visión del grado de resiliencia de su aplicación en varios AWS servicios y recursos. Este resumen visual completo y conciso le permite identificar rápidamente las posibles brechas de resiliencia, priorizar las acciones y realizar un seguimiento del progreso en la mejora de la capacidad de su aplicación para recuperarse de las interrupciones. Cuando eliges Exportar, y si exporta las métricas por primera vez, AWS Resilience Hub crea un nuevo bucket de Amazon S3 en la región desde la que accedes AWS Resilience Hub. Este bucket de Amazon S3 se crea solo por primera vez y se utilizará para guardar las métricas exportadas una vez que se complete correctamente. Se aplican cargos adicionales por almacenar los datos exportados en Amazon S3. Para obtener más información sobre estos cargos, consulte los precios de Amazon S3.

Los cuadros y gráficos de los widgets le ayudan a comprender lo siguiente:

- Descripción general de la puntuación de resiliencia general de la aplicación y del estado operativo actual.
- Las posibles infracciones de las políticas o las desviaciones de las mejores prácticas, destacando las aplicaciones que no cumplen con las políticas establecidas o que se han desviado de las configuraciones recomendadas. Además, también destaca áreas específicas que le permiten priorizarlas y abordarlas.
- Recursos o aplicaciones fundamentales que requieren atención inmediata.
- Recomendaciones para mejorar las prácticas de resiliencia, como implementar alarmas, realizar AWS Fault Injection Service (AWS FIS) experimentos y establecer procedimientos operativos estándar. Estas recomendaciones se rastrean a lo largo del tiempo, lo que le permite supervisar el progreso de la implementación y medir el impacto en la postura general de resiliencia de la aplicación.

Widgets

- Estado de la solicitud
- Principales recomendaciones de infraestructura por tipo de recurso
- Recomendaciones de infraestructura
- Recomendaciones operativas no implementadas
- Recomendaciones de alarmas
- Recomendaciones de SOP

- AWS FIS recomendaciones de experimentos
- Aplicaciones con derivas
- Puntuación de resiliencia
- Las 10 solicitudes más bajas en cuanto a la puntuación de resiliencia
- Estado de la solicitud por política

Estado de la solicitud

Este widget indica si sus aplicaciones cumplen o no con la política de resiliencia. Elija el número adyacente al número de aplicaciones en la ventana emergente para ver todas las aplicaciones asociadas en el panel Aplicaciones. Para ver todas las aplicaciones que ha creado, seleccione Ver aplicaciones. Para obtener más información sobre la administración de aplicaciones en AWS Resilience Hub, consulteVisualización del resumen AWS Resilience Hub de una solicitud.

Principales recomendaciones de infraestructura por tipo de recurso

Este widget muestra el número de recomendaciones de infraestructura para cada tipo de recurso de tus AWS recursos que proporcionaste en la última evaluación exitosa para mejorar su postura de resiliencia. Para identificar los detalles, coloca el cursor sobre ellos o navega hasta ellos. Para ver todas las aplicaciones que ha creado, seleccione Ver aplicaciones. Para obtener más información sobre las recomendaciones de infraestructura, consulteRevisar las recomendaciones de resiliencia.

Recomendaciones de infraestructura

Este widget muestra un máximo de 10 aplicaciones que cuentan con el número máximo de recomendaciones de infraestructura proporcionadas en la última evaluación exitosa para mejorar su capacidad de recuperación. Para ver todas las aplicaciones que ha creado, seleccione Ver aplicaciones. Para obtener más información sobre las recomendaciones de infraestructura, consulteRevisar las recomendaciones de resiliencia.

Puede identificar los detalles mediante lo siguiente:

- Nombre de la aplicación: nombre de la aplicación que proporcionó al definirla AWS Resilience Hub.
- Recuento: indica el número de recomendaciones de infraestructura proporcionadas AWS Resilience Hub en la última evaluación satisfactoria. Elija el número para ver todas las recomendaciones de infraestructura incluidas en el informe de evaluación.

- Última evaluación: indica la fecha y la hora en que su solicitud se evaluó correctamente por última vez.

Recomendaciones operativas no implementadas

Este widget muestra un máximo de 10 aplicaciones que tienen el número máximo de recomendaciones operativas no implementadas que se proporcionaron en la última evaluación exitosa para mejorar su postura de resiliencia. Para ver todas las aplicaciones que ha creado, seleccione Ver aplicaciones. Para obtener más información sobre las recomendaciones operativas, consulteRevisar las recomendaciones operativas.

Puede identificar los detalles mediante lo siguiente:

- Nombre de la aplicación: nombre de la aplicación que proporcionó al definirla AWS Resilience Hub.
- Recuento: indica el número de recomendaciones operativas proporcionadas AWS Resilience Hub en la última evaluación satisfactoria. Elija el número para ver todas las recomendaciones operativas no implementadas en el informe de evaluación.
- Hora de la última evaluación: indica la fecha y la hora en que su solicitud se evaluó correctamente por última vez.

Recomendaciones de alarmas

Este widget enumera todas las recomendaciones de CloudWatch alarmas de Amazon proporcionadas para mejorar la postura de resiliencia durante un período de tiempo seleccionado. Las diferentes categorías (implementadas, no implementadas y excluidas) indican su estado de implementación en la aplicación. Para ver el número de recomendaciones de CloudWatch alarmas de Amazon para cada categoría, coloca el cursor sobre ellas o navega hasta ellas. Para ver todas las aplicaciones que ha creado, seleccione Ver aplicaciones. Para obtener más información sobre las recomendaciones de alarmas, consulteRevisar las recomendaciones operativas.

Recomendaciones de SOP

Este widget enumera todas las recomendaciones de procedimientos operativos estándar (SOP) que se proporcionan para mejorar la postura de resiliencia durante un período de tiempo seleccionado. Las diferentes categorías (implementadas, no implementadas y excluidas) indican su estado de implementación en la aplicación. Puede ver el número de recomendaciones de SOP de cada categoría pasando el ratón sobre ellas o navegando hasta ellas. Para ver todas las aplicaciones que

ha creado, seleccione Ver aplicaciones. Para obtener más información sobre las recomendaciones operativas, consulteRevisar las recomendaciones operativas.

AWS FIS recomendaciones de experimentos

Este widget enumera todas las recomendaciones de AWS FIS experimentos proporcionadas para mejorar la postura de resiliencia durante un período de tiempo seleccionado. Las diferentes categorías (implementadas, no implementadas, implementadas parcialmente y excluidas) indican su estado de implementación en la aplicación. Para ver el número de recomendaciones de AWS FIS experimentos de cada categoría, coloca el cursor sobre ellas o navega hasta ellas. Para ver todas las aplicaciones que ha creado, seleccione Ver aplicaciones. Para obtener más información sobre las recomendaciones de AWS FIS experimentos, consulteGestión de los procedimientos operativos estándar.

Aplicaciones con derivas

En este widget se enumeran todas las aplicaciones que, en la última evaluación satisfactoria, se han desviado del estado de conformidad anterior. Para ver todas las aplicaciones que ha creado, seleccione Ver aplicaciones. Para obtener más información sobre la administración de aplicaciones en AWS Resilience Hub, consulteVisualización del resumen AWS Resilience Hub de una solicitud.

Puede identificar los detalles mediante lo siguiente:

- Nombre de la aplicación: nombre de la aplicación que proporcionó al definirla AWS Resilience Hub.
- Variante de política: elija el número adyacente al nombre de la aplicación para ver todos los componentes de la aplicación que cumplieron con la política en la evaluación anterior pero que no la cumplieron en la evaluación actual.
- Desviaciones de recursos: elija el número siguiente para ver todos los recursos cuya configuración se modificó en la última importación.

Puntuación de resiliencia

Este widget muestra la tendencia de la puntuación de resiliencia de la aplicación durante un período de tiempo seleccionado para un máximo de cinco aplicaciones. Para ver la puntuación de resiliencia de una aplicación, sitúe el cursor sobre la línea asociada al nombre de la aplicación o navegue hasta ella y, a continuación, elija el nombre de la aplicación para ver el resumen de la aplicación. Para ver todas las aplicaciones que ha creado, seleccione Ver aplicaciones. Para obtener más información sobre la puntuación de resiliencia, consulteComprender las puntuaciones de resiliencia.

Las 10 solicitudes más bajas en cuanto a la puntuación de resiliencia

Este widget enumera hasta 10 aplicaciones con las puntuaciones de resiliencia más bajas de sus evaluaciones más recientes, y destaca las aplicaciones que requieren atención inmediata para mejorar su resiliencia. Para ver todas las aplicaciones que ha creado, seleccione Ver aplicaciones. Para obtener más información sobre la puntuación de resiliencia, consulteComprender las puntuaciones de resiliencia.

Puede identificar los detalles mediante lo siguiente:

- Nombre de la aplicación: nombre de la aplicación que proporcionó al definirla AWS Resilience Hub.
- Puntuación de resiliencia: la puntuación de resiliencia general determinada AWS Resilience Hub por su aplicación después de ejecutar la evaluación.
- Hora de la última evaluación: indica la fecha y la hora en que la solicitud se evaluó correctamente por última vez.

Estado de la solicitud por política

Este widget muestra todas tus políticas y el número de solicitudes que las han infringido, que las han cumplido o que aún no se han evaluado en relación con ellas. Para ver todas las políticas que ha creado, elija Ver políticas. Para obtener más información sobre la puntuación de resiliencia, consulteAdministrar las políticas de resiliencia.

Puede identificar los detalles mediante lo siguiente:

- Nombre de la política: indica el nombre de la política que proporcionó al definirla AWS Resilience Hub.
- Tipo: indica el tipo de política (política de resiliencia) adjunto a la solicitud.
- Nombre de la política: indica el número de aplicaciones que han incumplido los objetivos de RTO y RPO definidos en la política de resiliencia.
- Aplicaciones cumplidas: indica la cantidad de aplicaciones que cumplen con la política de resiliencia.
- Aplicaciones no evaluadas: indica la cantidad de aplicaciones que aún no se han evaluado en relación con la política de resiliencia.
- Puntuación de resiliencia: la puntuación de resiliencia general determinada AWS Resilience Hub por la aplicación después de ejecutar la evaluación.

- Hora de la última evaluación: indica la fecha y la hora en que la solicitud se evaluó correctamente por última vez.

AWS Resilience Hub salpicadero

El panel de control proporciona una visión completa del estado de resiliencia de su cartera de aplicaciones. El panel agrega y organiza los eventos de resiliencia (por ejemplo, una base de datos no disponible o una validación de resiliencia fallida), las alertas y la información de servicios como CloudWatch y AWS Fault Injection Service (AWS FIS).

El panel también genera una puntuación de resiliencia para cada aplicación que se evalúa. Esta puntuación indica el rendimiento de la aplicación si se compara con las políticas de resiliencia, las alarmas, los procedimientos operativos estándar de recuperación (SOPs) y las pruebas recomendadas. Puede utilizar esta puntuación para medir las mejoras en la resiliencia a lo largo del tiempo.

Para ver el AWS Resilience Hub panel de control, seleccione Panel de control en el menú de navegación. La página del panel de control muestra las siguientes secciones:

Estado de la solicitud

El estado de las solicitudes indica si las solicitudes han sido evaluadas para determinar si cumplen con la política de resiliencia adjunta o no. Además, una vez finalizada la evaluación, el estado también indica si las fuentes de entrada de sus solicitudes se han modificado o no. Elija un número debajo de cada uno de los siguientes estados para ver todas las solicitudes que comparten el mismo estado en la página de solicitudes:

- Las solicitudes en la política: indica todas las aplicaciones que cumplen con la política de resiliencia adjunta.
- Solicitudes que infringen la política de resiliencia: indica todas las solicitudes que no cumplen con la política de resiliencia adjunta.
- Solicitudes no evaluadas: indica todas las solicitudes cuyo cumplimiento aún no se ha evaluado o rastreado.
- Solicitudes desviadas: indica todas las aplicaciones que se han desviado de su política de resiliencia o si sus recursos se han desviado.

Puntuación de resiliencia de las aplicaciones a lo largo del tiempo

Con la puntuación de resiliencia de las aplicaciones a lo largo del tiempo, puede ver un gráfico de la resiliencia de la aplicación en los últimos 30 días. Si bien el menú desplegable puede enumerar 10 de sus aplicaciones, AWS Resilience Hub solo muestra un gráfico de hasta cuatro aplicaciones a la vez. Para obtener más información sobre la puntuación de resiliencia, consulte. Comprender las puntuaciones de resiliencia

> **Note**
>
> AWS Resilience Hub no ejecuta evaluaciones programadas al mismo tiempo. En consecuencia, es posible que tenga que volver al gráfico de la puntuación de resiliencia a lo largo del tiempo más adelante para ver la evaluación diaria de sus aplicaciones.

AWS Resilience Hub también usa Amazon CloudWatch para generar estos gráficos. Seleccione Ver métricas CloudWatch para crear y ver información más detallada sobre la resiliencia de su aplicación en su CloudWatch panel de control. Para obtener más información al respecto CloudWatch, consulte Uso de paneles en la Guía del CloudWatch usuario de Amazon.

Alarmas implementadas

En esta sección se enumeran todas las alarmas que has configurado en Amazon CloudWatch para supervisar todas las aplicaciones. Para obtener más información, consulte Visualizar alarmas.

Experimentos implementados

En esta sección se enumeran todos los experimentos de inyección de errores que ha implementado en todas las aplicaciones. Para obtener más información, consulte Visualización AWS FIS experimentos.

Descripción y administración de AWS Resilience Hub aplicaciones

Una AWS Resilience Hub aplicación es un conjunto de AWS recursos que están estructurados para prevenir y recuperar las interrupciones de las AWS aplicaciones.

Para describir una AWS Resilience Hub aplicación, debe proporcionar el nombre de la aplicación, los recursos de uno o más CloudFormation conjuntos y una política de resiliencia adecuada. También puede usar cualquier aplicación de AWS Resilience Hub existente como plantilla para describir su aplicación.

Después de describir una AWS Resilience Hub aplicación, debe publicarla para poder realizar una evaluación de resiliencia en ella. A continuación, puede utilizar las recomendaciones de la evaluación para mejorar la capacidad de recuperación mediante la ejecución de otra evaluación, la comparación de los resultados y la repetición del proceso hasta que su RPO de carga de trabajo estimada y su RPO de carga de trabajo estimada cumplan sus objetivos de RPO y RPO.

Para ver la página Aplicaciones, seleccione Aplicaciones en el panel de navegación. Puede identificar sus aplicaciones en la página de aplicaciones de la siguiente manera:

- Nombre: el nombre de la aplicación que proporcionó al definirla en AWS Resilience Hub.
- Descripción: la descripción de la aplicación que proporcionó al definirla en AWS Resilience Hub.
- Estado de conformidad: AWS Resilience Hub establece el estado de la solicitud como Evaluada, No evaluada, Incumplida la política o Se han detectado cambios.
  - Evaluada: AWS Resilience Hub ha evaluado su solicitud.
  - No evaluada: no AWS Resilience Hub ha evaluado su solicitud.
  - Política infringida: AWS Resilience Hub ha determinado que su solicitud no cumplía los objetivos de su política de resiliencia en relación con el objetivo de tiempo de recuperación (RTO) y el objetivo de punto de recuperación (RPO). Revise y utilice las recomendaciones que se proporcionan AWS Resilience Hub antes de volver a evaluar la resiliencia de su solicitud. Para obtener más información sobre recomendaciones, consulte Añadir una aplicación a AWS Resilience Hub.
  - Cambios detectados: AWS Resilience Hub ha detectado cambios en la política de resiliencia asociada a su solicitud. Debe volver a evaluar su solicitud AWS Resilience Hub para determinar si cumple con los objetivos de su política de resiliencia.
- Evaluaciones programadas: el tipo de recurso identifica el recurso componente de su aplicación. Para obtener más información sobre las evaluaciones programadas, consulte Resiliencia de la aplicación.
  - Activa: esto indica que su aplicación se evalúa automáticamente todos los días mediante AWS Resilience Hub.
  - Inhabilitada: esto indica que su solicitud no se evalúa automáticamente a diario AWS Resilience Hub y que debe evaluarla manualmente.
- Estado de desviación: indica si la aplicación se ha desviado o no de la evaluación correcta anterior y define uno de los siguientes estados:
  - Desviada: indica que la aplicación, que cumplía con su política de resiliencia en la anterior evaluación satisfactoria, ahora la ha infringido y la aplicación está en peligro. Además, también

indica si los recursos de los orígenes de entrada, que están incluidos en la versión actual de la aplicación, se agregaron o eliminaron.

  - Sin desviar: indica que se estima que la aplicación sigue cumpliendo los objetivos de RTO y RPO definidos en la política. Además, también indica que los recursos de los orígenes de entrada, que se incluyen en la versión actual de la aplicación, no se agregaron ni eliminaron.
- RTO de carga de trabajo estimada: indica el RTO máximo de carga de trabajo estimado posible de la aplicación. Este valor es el RTO máximo estimado de la carga de trabajo de todos los tipos de interrupciones de la última evaluación exitosa.
- RPO de carga de trabajo estimado: indica el RPO de carga de trabajo estimado máximo posible de su aplicación. Este valor es el RTO máximo estimado de la carga de trabajo de todos los tipos de interrupciones de la última evaluación exitosa.
- Hora de la última evaluación: indica la fecha y la hora en que su aplicación se evaluó correctamente por última vez.
- Hora de creación: fecha y hora en que se creó la aplicación.
- ARN: el nombre de recurso de Amazon (ARN) de su aplicación. Para obtener más información ARNs, consulte Amazon Resource Names (ARNs) en la Referencia AWS general.

> **Note**
>
> AWS Resilience Hub puede evaluar completamente la resiliencia de los recursos de Amazon ECS entre regiones solo si utiliza Amazon ECR para el repositorio de imágenes.

Además, también puede filtrar la lista de aplicaciones mediante una de las siguientes opciones de la página Aplicaciones:

- Buscar aplicaciones: introduzca el nombre de la aplicación para filtrar los resultados por el nombre de la aplicación.
- Filtrar la hora de la última evaluación por un intervalo de fechas y horas: para aplicar este filtro, seleccione el icono del calendario y seleccione una de las siguientes opciones para filtrar por los resultados que coincidan con el intervalo de tiempo:
  - Rango relativo: seleccione una de las opciones disponibles y seleccione Aplicar.

Si elige la opción Rango personalizado, introduzca una duración en el cuadro Introducir duración y seleccione la unidad de tiempo correspondiente en la lista desplegable Unidades de tiempo y, a continuación, seleccione Aplicar.

- Rango absoluto: para especificar el rango de fecha y hora, proporcione la hora de inicio y la hora de finalización y, a continuación, seleccione Aplicar.

Los siguientes temas muestran los diferentes enfoques para describir una AWS Resilience Hub aplicación y cómo administrarla.

Temas

Visualización del resumen AWS Resilience Hub de una solicitud

La página de resumen de la aplicación de la AWS Resilience Hub consola proporciona una descripción general de la información de la aplicación y del estado de resiliencia.

Para ver un resumen de la aplicación

1. Seleccione Aplicaciones en el panel de navegación.
2. En la página Aplicaciones, elija el nombre de la aplicación que desee ver.

La página de resumen de aplicaciones contiene las siguientes secciones.

Temas

- Resiliencia de la aplicación
- Alarmas implementadas
- Experimentos implementados

Resumen de la evaluación

En esta sección se proporciona un resumen de la última evaluación satisfactoria y se destacan las recomendaciones críticas como información práctica. AWS Resilience Hub utiliza las capacidades de IA generativa de Amazon Bedrock para ayudar a centrar a los usuarios en las recomendaciones de resiliencia más importantes que ofrece. AWS Resilience Hub AI centrarse en los elementos críticos, puede centrarse en las recomendaciones más importantes que mejoran la resiliencia de su aplicación. Elija una recomendación para ver su resumen y elija Ver detalles para ver más detalles sobre las recomendaciones en la sección correspondiente del informe de evaluación. Para obtener más información sobre la revisión del informe de evaluación, consultethe section called “Revisar los informes de evaluación”.

> **Note**
>
> - Este resumen de la evaluación solo está disponible en la región EE.UU. Este (Virginia del Norte).
> - El resumen de la evaluación generado por los modelos lingüísticos de gran tamaño (LLMs) en Amazon Bedrock son solo sugerencias. El nivel actual de la tecnología de IA generativa no es perfecto ni LLMs infalible. Es de esperar respuestas sesgadas e incorrectas, aunque raras. Revise cada recomendación del resumen de la evaluación antes de utilizar los resultados de un LLM.

Resumen

Esta sección proporciona un resumen de la solicitud seleccionada en las siguientes secciones:

- Información de la aplicación: en esta sección se proporciona la siguiente información sobre la aplicación seleccionada:
  - Estado de la solicitud: indica el estado de la solicitud.
  - Descripción: descripción de la aplicación.
  - Versión: indica la versión actualmente evaluada de la aplicación.

  - Política de resiliencia: indica la política de resiliencia que se adjunta a la solicitud. Para obtener más información sobre las políticas de resiliencia, consulte Administrar las políticas de resiliencia.
- Desviaciones en la aplicación: en esta sección se destacan las desviaciones detectadas al realizar una evaluación de la aplicación seleccionada para comprobar si cumple con su política de resiliencia. Además, también comprueba si alguno de los recursos se ha añadido o eliminado desde la última vez que se publicó la versión de la aplicación. En esta sección se muestra la siguiente información:
  - Cambios en las políticas: elija el número que aparece a continuación para ver todos los componentes de la aplicación que cumplieron con la política en la evaluación anterior pero que no la cumplieron en la evaluación actual.
  - Desviaciones de recursos: elija el número que aparece a continuación para ver todos los recursos desviados de la última evaluación.

Resiliencia de la aplicación

Las métricas que se muestran en la sección de puntuación de resiliencia provienen de la evaluación de resiliencia más reciente de la aplicación.

Puntuación de resiliencia

La puntuación de resiliencia le ayuda a cuantificar su preparación para hacer frente a una posible interrupción. Esta puntuación refleja en qué medida su aplicación ha seguido las AWS Resilience Hub recomendaciones para cumplir con la política de resiliencia, las alarmas, los procedimientos operativos estándar (SOPs) y las pruebas de la aplicación.

La puntuación máxima de resiliencia que puede alcanzar su aplicación es del 100 %. La puntuación representa todas las pruebas recomendadas que se ejecutan en un período de tiempo predefinido. Indica que las pruebas están iniciando la alarma correcta y que la alarma inicia el SOP correcto.

Por ejemplo, supongamos que se AWS Resilience Hub recomienda una prueba con una alarma y un SOP. Cuando se ejecuta la prueba, la alarma inicia el SOP asociado y, a continuación, se ejecuta correctamente. Para obtener más información sobre la puntuación de resiliencia, consulte Comprender las puntuaciones de resiliencia.

Alarmas implementadas

En la sección Alarmas implementadas del resumen de la aplicación se enumeran las alarmas que configuraste en Amazon CloudWatch para monitorear la aplicación. Para obtener más información sobre las alarmas, consulte Administración de alarmas.

Experimentos implementados

El resumen de la aplicación en la sección Experimentos de inyección de errores muestra una lista de los experimentos de inyección de errores. Para obtener más información acerca de los experimentos de inserción de errores, vea Administración AWS Fault Injection Service experimentos.

Edición de los recursos AWS Resilience Hub de la aplicación

Para recibir evaluaciones de resiliencia precisas y útiles, asegúrese de que la descripción de su solicitud esté actualizada y coincida con su AWS aplicación y sus recursos reales. Los informes de evaluación, la validación y las recomendaciones se basan en los recursos enumerados. Si añades o eliminas recursos de una AWS aplicación, debes reflejar esos cambios en AWS Resilience Hub ella.

AWS Resilience Hub proporciona transparencia sobre las fuentes de las aplicaciones. Puede identificar y editar los recursos y los orígenes de la aplicación en su aplicación.

> **Note**
>
> Al editar los recursos, solo se modifica la AWS Resilience Hub referencia de la aplicación. No se realizan cambios en los recursos reales.

Puede agregar los recursos que faltan, modificar los recursos existentes o eliminar los recursos que no necesite. Los recursos se agrupan en componentes de aplicación lógicos (AppComponents). Puede editarlo AppComponents para que refleje mejor la estructura de la aplicación.

Añada o actualice los recursos de la aplicación editando una versión preliminar de la aplicación y publicando los cambios en una nueva versión (publicada). AWS Resilience Hub utiliza la versión de lanzamiento (que incluye los recursos actualizados) de la aplicación para ejecutar las evaluaciones de resiliencia.

Para evaluar la resiliencia de su aplicación

1. En el panel de navegación, elija Aplicaciones.

2. En la página Aplicaciones, seleccione el nombre de la aplicación que desea editar.
3. En el menú Acciones, seleccione Evaluar la resiliencia.
4. En el cuadro de diálogo Ejecutar una evaluación de resiliencia, introduzca un nombre único para el informe o utilice el nombre generado en el cuadro Nombre del informe.
5. Elija Ejecutar.
6. Cuando se le notifique que se ha generado el informe de evaluación, seleccione la pestaña Evaluaciones y su evaluación para ver el informe.
7. Seleccione la pestaña Revisar para ver el informe de evaluación de su aplicación.

Para habilitar la evaluación programada

1. En el panel de navegación, elija Aplicaciones.
2. En la página de solicitudes, seleccione la aplicación para la que desee activar la evaluación programada.
3. Active la opción Evaluar automáticamente todos los días.

Para deshabilitar la evaluación programada

1. En el panel de navegación, elija Aplicaciones.
2. En la página de aplicaciones, seleccione la aplicación para la que desee activar la evaluación programada.
3. Desactive Evaluar automáticamente todos los días.

> **Note**
>
> Si se desactiva la evaluación programada, se desactivará la notificación de desviación.

4. Seleccione Desactivar.

Para habilitar la notificación de deriva en su aplicación

1. En el panel de navegación, elija Aplicaciones.
2. En la página de aplicaciones, seleccione la aplicación para la que desee activar la notificación de deriva o edite la configuración de la notificación de deriva.
3. Puede editar la notificación de deriva seleccionando una de las siguientes opciones:

- En Acciones, selecciona Activar la notificación de derrapes.
- Selecciona Activar la notificación en la sección de desviaciones de aplicaciones.

4. Complete los pasos indicados yConfiguración de las evaluaciones programadas y la notificación de desviaciones, a continuación, vuelva a este procedimiento.
5. Seleccione Habilitar.

   Al habilitar la notificación de desviaciones, también se habilitará la evaluación programada.

Para editar la notificación de deriva para su aplicación

> **Note**
>
> Este procedimiento es aplicable si ha activado la evaluación programada (la opción Evaluar automáticamente todos los días está activada) y la notificación de desviaciones.

1. En el panel de navegación, elija Aplicaciones.
2. En la página de aplicaciones, selecciona la aplicación para la que quieres activar la notificación de deriva o edita la configuración de la notificación de deriva.
3. Puede editar la notificación de deriva seleccionando una de las siguientes opciones:

   - En Acciones, selecciona Editar notificación de deriva.
   - Selecciona Editar notificación en la sección de desviaciones de la aplicación.

4. Complete los pasos descritos yConfiguración de las evaluaciones programadas y la notificación de desviaciones, a continuación, vuelva a este procedimiento.
5. Seleccione Guardar.

Para actualizar los permisos de seguridad de su aplicación

1. En el panel de navegación, elija Aplicaciones.
2. En la página Aplicaciones, seleccione la aplicación para la que desee actualizar los permisos de seguridad.
3. En Acciones, seleccione Actualizar permisos.
4. Para actualizar los permisos de seguridad, complete los pasos que se indican en Configuración de permisos y, a continuación, vuelva a este procedimiento.

5. Elija Guardar y actualizar.

Para adjuntar una política de resiliencia a su aplicación

1. En el panel de navegación, elija Aplicaciones.
2. En la página Aplicaciones, seleccione el nombre de la aplicación que desea editar.
3. En el menú Acciones, seleccione Adjuntar política de resiliencia.
4. En el cuadro de diálogo Adjuntar política, seleccione una política de resiliencia en la lista desplegable Seleccionar política de resiliencia.
5. Elija Adjuntar.

Para editar las fuentes de entrada, los recursos y AppComponents la aplicación

1. En el panel de navegación, elija Aplicaciones.
2. En la página Aplicaciones, seleccione el nombre de la aplicación que desea editar.
3. Seleccione la pestaña Estructura de la aplicación.
4. Seleccione el signo más + antes de Versión y, a continuación, seleccione la versión de la aplicación con el estado Borrador.
5. Para editar las fuentes de entrada, los recursos y AppComponents los elementos de la aplicación, complete los pasos de los siguientes procedimientos.

Para editar los orígenes de entrada de su aplicación

1. Para editar los orígenes de entrada de su aplicación, seleccione la pestaña Orígenes de entrada.

   En la sección Orígenes de entrada se enumeran todos los orígenes de entrada de los recursos de su aplicación. Puede identificar los orígenes de entrada de la siguiente manera:

   - Nombre de origen: el nombre de la fuente de entrada. Seleccione un nombre de origen para ver sus detalles en la aplicación correspondiente. En el caso de los orígenes de entrada añadidos manualmente, el enlace no estará disponible. Por ejemplo, si elige el nombre de la fuente que se importa de una AWS CloudFormation pila, se le redirigirá a la página de detalles de la pila en la AWS CloudFormation consola.
   - ARN de origen: el nombre de recurso de Amazon (ARN) del origen de entrada. seleccione un ARN para ver sus detalles en la aplicación correspondiente. En el caso de los orígenes de

entrada añadidos manualmente, el enlace no estará disponible. Por ejemplo, si elige un ARN importado de una pila de AWS CloudFormation , se le redirigirá a la página de detalles de la pila en la consola AWS CloudFormation .

- Tipo de origen: el tipo de origen de entrada. Las fuentes de entrada incluyen clústeres de Amazon EKS, AWS CloudFormation pilas, aplicaciones de MyApplications Grupos de recursos de AWS, archivos de estado de Terraform y recursos añadidos manualmente.
- Recursos asociados: el número de recursos que están asociados al origen de entrada. Seleccione un número para ver todos los recursos asociados a un origen de entrada en la pestaña Recursos.

2. Para añadir orígenes de entrada a la aplicación, en la sección Orígenes de entrada, seleccione Añadir orígenes de entrada. Para obtener más información sobre cómo agregar fuentes de entrada, consulte the section called “Añada recursos a su aplicación AWS Resilience Hub ”.
3. Para editar los orígenes de entrada, seleccione los orígenes de entrada y seleccione una de las siguientes opciones en Acciones:

   - Reimportar orígenes de entrada (hasta 5): reimporta hasta cinco orígenes de entrada seleccionados.
   - Eliminar orígenes de entrada: elimina los orígenes de entrada seleccionados.

     Para publicar una aplicación, debe contener como mínimo un origen de entrada. Si elimina todos los orígenes de entrada, se deshabilitará Publicar una nueva versión.

Para editar los recursos de su aplicación

1. Para editar los recursos de su aplicación, seleccione la pestaña Recursos.

   > **Note**
   >
   > Para ver la lista de recursos no evaluados, seleccione Ver recursos no evaluados.

   La sección Recursos muestra los recursos de la aplicación que eligió usar como plantilla para la descripción de la aplicación. Para mejorar su experiencia de búsqueda, AWS Resilience Hub ha agrupado los recursos en función de varios criterios de búsqueda. Estos criterios de búsqueda incluyen los AppComponent tipos, los recursos no admitidos y los recursos excluidos. Para filtrar

los recursos en función de un criterio de búsqueda de la tabla Recursos, elija el número que aparece debajo de cada uno de los criterios de búsqueda.

Puede identificar los recursos de la siguiente manera:

- ID lógico: un ID lógico es un nombre que se utiliza para identificar los recursos de su AWS CloudFormation pila, el archivo de estado de Terraform, la aplicación agregada manualmente, la aplicación MyApplications o. Grupos de recursos de AWS

  > **Note**
  >
  > - Terraform le permite usar el mismo nombre para diferentes tipos de recursos. Por lo tanto, verá "- tipo de recurso" al final del ID lógico para los recursos que comparten el mismo nombre.
  > - Para ver las instancias de todos los recursos de la aplicación, seleccione el signo más (+) situado antes del ID lógico. Para ver todas las instancias de un recurso de aplicación, seleccione el signo más (+) antes del ID lógico de cada recurso.
  >
  >   Para obtener más información sobre los recursos admitidos, consulte the section called “ AWS Resilience Hub Recursos compatibles”.

- Tipo de recurso: el tipo de recurso identifica el recurso componente de la aplicación. Por ejemplo, `AWS::EC2::Instance` declara una EC2 instancia de Amazon. Para obtener más información sobre la agrupación de AppComponent recursos, consulteAgrupación de recursos en un componente de aplicación.
- Nombre de origen: el nombre de la fuente de entrada. Seleccione un nombre de origen para ver sus detalles en la aplicación correspondiente. En el caso de los orígenes de entrada añadidos manualmente, el enlace no estará disponible. Por ejemplo, si elige el nombre de origen que se importa de una AWS CloudFormation pila, se le redirigirá a la página de detalles de la pila en. AWS CloudFormation
- Tipo de origen: el tipo de origen de entrada. Las fuentes de entrada incluyen AWS CloudFormation pilas, aplicaciones de MyApplications Grupos de recursos de AWS, archivos de estado de Terraform y recursos añadidos manualmente.

> **Note**
>
> Para editar sus clústeres de Amazon EKS, complete los pasos del procedimiento Editar los orígenes de entrada de su aplicación AWS Resilience Hub .

- Pila de origen: la AWS CloudFormation pila que contiene el recurso. Esta columna depende del tipo de estructura de aplicación que haya seleccionado.
- ID físico: el identificador asignado real a ese recurso, como un ID de EC2 instancia de Amazon o un nombre de bucket de S3.
- Incluido: indica si AWS Resilience Hub incluye estos recursos en la aplicación.
- Evaluable: esto indica si AWS Resilience Hub evaluará la resiliencia de su recurso.
- AppComponents— El AWS Resilience Hub componente que se asignó a este recurso cuando se descubrió la estructura de su aplicación.
- Nombre: el nombre del recurso de la aplicación.
- Cuenta: la AWS cuenta propietaria del recurso físico.

2. Para buscar un recurso que no esté en la lista, introduzca el ID lógico del recurso en el cuadro de búsqueda.
3. Para eliminar un recurso de la aplicación, selecciónelo y, a continuación, seleccione Excluir el recurso de las acciones.
4. Para resolver los recursos de la aplicación, seleccione Actualizar recursos.
5. Para modificar los recursos de la aplicación existentes, complete los pasos siguientes:

   a. Seleccione un recurso y, a continuación, seleccione Actualizar pilas desde Acciones.

   b. En la página Actualizar pilas, para actualizar los recursos, complete los procedimientos correspondientes en Agregar colecciones de recursos y, a continuación, vuelva a este procedimiento.

   c. Seleccione Guardar.

6. Para agregar un recurso a la aplicación, en Acciones, seleccione Agregar recurso y complete los pasos siguientes:

   a. Seleccione un tipo de recurso de la lista desplegable Tipo de recurso.

   b. Seleccione una AppComponent de la lista AppComponentdesplegable.

   c. Introduzca el ID lógico del recurso en el cuadro Nombre del recurso.

d. Introduzca el ID del recurso físico, el nombre del recurso o el ARN del recurso en el cuadro Identificador del recurso.

e. Elija Agregar.

7. Para editar el nombre del recurso, seleccione un recurso, seleccione Editar el nombre del recurso en Acciones y, a continuación, complete los siguientes pasos:

   a. Introduzca el ID lógico del recurso en el cuadro Nombre del recurso.

   b. Seleccione Guardar.

8. Para editar el identificador del recurso, seleccione un recurso, seleccione Editar el identificador del recurso en Acciones y, a continuación, complete los siguientes pasos:

   a. Introduzca el ID del recurso físico, el nombre del recurso o el ARN del recurso en el cuadro Identificador del recurso.

   b. Seleccione Guardar.

9. Para cambiarlo AppComponent, selecciona un recurso, elige Cambiar AppComponent de acciones y sigue estos pasos:

   a. Seleccione una AppComponent de la lista AppComponentdesplegable.

   b. Elija Agregar.

10. Para eliminar un recurso, selecciónelo y, a continuación, seleccione Eliminar recurso de las acciones.

11. Para incluir un recurso, selecciónelo y, a continuación, seleccione Incluir un recurso de las acciones.

Para editar la AppComponents de su solicitud

1. Para editar la AppComponents de su solicitud, seleccione la AppComponentspestaña.

> **Note**
>
> Para obtener más información sobre la agrupación de AppComponent recursos, consulteAgrupación de recursos en un componente de aplicación.

AppComponentsEn la sección se enumeran todos los componentes lógicos en los que se agrupan los recursos. Puede identificarlos de AppComponents la siguiente manera:

- AppComponent nombre: el nombre del AWS Resilience Hub componente que se asignó a este recurso cuando se descubrió la estructura de su aplicación.
- AppComponent tipo: tipo de AWS Resilience Hub componente.
- Nombre de origen: el nombre de la fuente de entrada. Seleccione un nombre de origen para ver sus detalles en la aplicación correspondiente. Por ejemplo, si elige el nombre del origen que se importa de una pila de AWS CloudFormation , se le redirigirá a la página de detalles de la pila en AWS CloudFormation.
- Recuento de recursos: el número de recursos que están asociados al origen de entrada. Seleccione un número para ver todos los recursos asociados a un origen de entrada en la pestaña Recursos.

2. Para crear un AppComponent, en el menú Acciones, seleccione Crear nuevo AppComponent y complete los pasos siguientes:

   a. Introduzca un nombre para el elemento AppComponent en el cuadro de AppComponentnombres. Como referencia, hemos rellenado previamente este campo con un nombre de ejemplo.

   b. Seleccione el tipo AppComponent de en la lista desplegable AppComponentde tipos.

   c. Seleccione Guardar.

3. Para editar una AppComponent, selecciónela y AppComponent, a continuación, elija Editar AppComponent de las acciones.
4. Para eliminar una AppComponent, selecciónela y AppComponent, a continuación, elija AppComponentEliminar de las acciones.

Tras realizar cambios en la lista de recursos, recibirá una alerta que le indicará que se han realizado cambios en la versión preliminar de la aplicación. Para realizar una evaluación de resiliencia precisa, debe publicar una nueva versión de la aplicación. Para obtener más información acerca de cómo publicar una nueva versión, consulte Publicar una nueva versión AWS Resilience Hub de la aplicación.

Gestión de los componentes de la aplicación

Un componente de aplicación (AppComponent) es un grupo de AWS recursos relacionados que funcionan y fallan como una sola unidad. Por ejemplo, si tiene una base de datos principal y una réplica, ambas bases de datos pertenecen a la misma base de datos AppComponent. AWS Resilience Hub tiene reglas que rigen qué AWS

recursos pueden pertenecer a qué AppComponent tipo. Por ejemplo, a `DBInstance` puede pertenecer `AWS::ResilienceHub::DatabaseAppComponent` y no a`AWS::ResilienceHub::ComputeAppComponent`.

AWS Resilience Hub AppComponents Admiten los siguientes recursos:

- `AWS::ResilienceHub::ComputeAppComponent`
  - `AWS::ApiGateway::RestApi`
  - `AWS::ApiGatewayV2::Api`
  - `AWS::AutoScaling::AutoScalingGroup`
  - `AWS::EC2::Instance`
  - `AWS::ECS::Service`
  - `AWS::EKS::Deployment`
  - `AWS::EKS::ReplicaSet`
  - `AWS::EKS::Pod`
  - `AWS::Lambda::Function`
  - `AWS::StepFunctions::StateMachine`
- `AWS::ResilienceHub::DatabaseAppComponent`
  - `AWS::DocDB::DBCluster`
  - `AWS::DynamoDB::Table`
  - `AWS::ElastiCache::CacheCluster`
  - `AWS::ElastiCache::GlobalReplicationGroup`
  - `AWS::ElastiCache::ReplicationGroup`
  - `AWS::ElastiCache::ServerlessCache`
  - `AWS::RDS::DBCluster`
  - `AWS::RDS::DBInstance`
- `AWS::ResilienceHub::NetworkingAppComponent`
  - `AWS::EC2::NatGateway`
  - `AWS::ElasticLoadBalancing::LoadBalancer`
  - `AWS::ElasticLoadBalancingV2::LoadBalancer`
  - `AWS::Route53::RecordSet`
- `AWS:ResilienceHub::NotificationAppComponent`

  - `AWS::SNS::Topic`
- `AWS::ResilienceHub::QueueAppComponent`
  - `AWS::SQS::Queue`
- `AWS::ResilienceHub::StorageAppComponent`
  - `AWS::Backup::BackupPlan`
  - `AWS::EC2::Volume`
  - `AWS::EFS::FileSystem`
  - `AWS::FSx::FileSystem`

    > **Note**
    >
    > Actualmente, solo AWS Resilience Hub es compatible con Amazon FSx para Windows File Server.

  - `AWS::S3::Bucket`

Temas

- Agrupación de recursos en un componente de aplicación

Agrupación de recursos en un componente de aplicación

Al importar la aplicación AWS Resilience Hub junto con sus recursos, AWS Resilience Hub hace todo lo posible por agrupar los recursos relacionados en una misma unidad AppComponent al importar la aplicación, pero es posible que la agrupación no siempre sea exacta al 100 por cien. Algunos recursos están bloqueados debido a la agrupación manual y se agruparán automáticamente cuando proceda, ya que estos servicios tienen dependencias estrictas que requieren configuraciones de agrupamiento específicas. Para obtener una lista completa de los servicios cuya agrupación manual está bloqueada, consulte. the section called “Servicios bloqueados para la agrupación manual”

AWS Resilience Hub realiza las siguientes actividades una vez que la aplicación y sus recursos se hayan importado correctamente:

- Analiza los recursos para comprobar si se pueden reagrupar en nuevos AppComponents para mejorar la precisión de la evaluación.

- Si AWS Resilience Hub identifica los recursos que se pueden reagrupar en nuevos AppComponents, muestra lo mismo que las recomendaciones y le permite aceptarlas o rechazarlas. En AWS Resilience Hub, el nivel de confianza asignado a una recomendación de agrupación indica el grado de certeza con el que se deben agrupar los recursos en función de sus atributos y metadatos. Un nivel de confianza alto indica que AWS Resilience Hub tiene un nivel de confianza del 90% o superior en cuanto a que los recursos de ese grupo están relacionados y deben agruparse. Un nivel de confianza medio indica que AWS Resilience Hub tiene un nivel de confianza entre el 70 y el 90% de que los recursos de ese grupo están relacionados y deben agruparse.

> **Note**
>
> AWS Resilience Hub requiere la agrupación correcta para poder calcular el RTO de la carga de trabajo estimada y el RPO de la carga de trabajo estimada para generar recomendaciones.

Los siguientes son ejemplos de agrupaciones correctas:

- Agrupe las bases de datos y réplicas principales en una sola. AppComponent
- Agrupe las instancias de Amazon EC2 que ejecutan la misma aplicación en una sola instancia. AppComponent
- Agrupe los servicios de Amazon ECS en una región y realice la conmutación por error de los servicios de Amazon ECS en otra región en una sola AppComponent.

Para obtener más información sobre cómo revisar e incluir las recomendaciones de agrupamiento de recursos AWS Resilience Hub, consulte los siguientes temas:

- AWS Resilience Hub recomendaciones de agrupamiento de recursos
- Agrupar los recursos manualmente en un AppComponent

Servicios bloqueados para la agrupación manual

AWS Resilience Hub le impide agrupar manualmente los recursos de determinados AWS servicios para evitar errores de configuración que podrían afectar a la evaluación de la resiliencia y a las recomendaciones de su aplicación. Estos servicios se agrupan automáticamente en función de sus

dependencias y configuraciones. Al definir una aplicación que incluya estos recursos AWS Resilience Hub, se analizarán sus relaciones, dependencias y requisitos de resiliencia para crear agrupaciones óptimas que garanticen unos resultados de evaluación precisos.

Lista de AWS servicios bloqueados por la agrupación manual:

- Amazon API Gateway
- Amazon DocumentDB
- Amazon DynamoDB
- Amazon Elastic Block Store
- Amazon Elastic File System
- Amazon Relational Database Service
- Amazon S3
- Amazon Simple Queue Service
- FSx para Windows File Server
- Gateway NAT

AWS Resilience Hub recomendaciones de agrupamiento de recursos

En esta sección se explica cómo generar y revisar las recomendaciones de agrupamiento de recursos en. AWS Resilience Hub

> **Note**
>
> Puede conceder los permisos de IAM necesarios para trabajar con ellos AWS Resilience Hub mediante una política `AWSResilienceHubAsssessmentExecutionPolicy` AWS gestionada. Para obtener más información sobre la política AWS gestionada, consulte[AWSResilienceHubAsssessmentExecutionPolicy](#).

Para ver las recomendaciones de agrupamiento de recursos

1. En el panel de navegación, elija Aplicaciones.
2. Seleccione la página Añadir aplicación y elija el nombre de la aplicación para la que desee revisar las recomendaciones de agrupación de recursos.
3. Seleccione la pestaña Estructura de la aplicación.

4. Si AWS Resilience Hub muestra una alerta de información, seleccione Revisar recomendaciones para ver todas las recomendaciones de agrupamiento de recursos. De lo contrario, complete los siguientes pasos para generar manualmente las recomendaciones de agrupación de recursos:

   a. Seleccione Recursos.

   b. Seleccione Obtener recomendaciones de agrupamiento en el menú Acciones.

      AWS Resilience Hub analiza sus recursos para comprobar cómo agruparlos de la mejor manera posible en relevantes AppComponents para mejorar la precisión de las evaluaciones. Si AWS Resilience Hub descubre que sus recursos se pueden agrupar, mostrará una alerta informativa sobre los mismos recursos.

   c. Si aparece la alerta de información, seleccione Revisar recomendaciones para ver todas las recomendaciones de agrupamiento de recursos.

   Puede identificarlas AppComponents en la sección Revisar las recomendaciones de agrupamiento de recursos mediante lo siguiente:

   - AppComponent nombre: nombre del grupo AppComponent en el que se agruparán los recursos.
   - Nivel de confianza: indica el nivel de confianza de AWS Resilience Hub en la recomendación de agrupación.
   - Recuento de recursos: indica la cantidad de recursos que se agruparán en. AppComponent
   - AppComponent tipo: indica el tipo de AppComponent.

Para ver los recursos que se agruparán en AppComponents

1. Complete los pasos del Para ver las recomendaciones de agrupamiento de recursosprocedimiento y, a continuación, vuelva a este procedimiento.
2. En la sección Revisar las recomendaciones de agrupamiento de recursos, active la casilla de verificación (junto al AppComponent nombre) para ver todos los recursos que se agruparán dentro de los recursos seleccionados AppComponent. Si selecciona varias casillas de verificación, se AWS Resilience Hub muestra una sección de recomendaciones seleccionadas generada dinámicamente que agrupa las seleccionadas AppComponents según su AppComponent tipo respectivo. Elija el número que aparece debajo AppComponent de cada tipo para ver todos los recursos que se agruparán dentro de los recursos seleccionados AppComponent.

Puede identificar los recursos que se agruparán en los seleccionados AppComponent de la sección Recursos de la siguiente manera:

- ID lógico: indica el ID lógico del recurso. Un ID lógico es un nombre que se utiliza para identificar los recursos de su AWS CloudFormation pila, el archivo de estado de Terraform, la aplicación MyApplications o. Grupos de recursos de AWS
- ID físico: el identificador asignado real al recurso, como un ID de instancia de Amazon EC2 o un nombre de bucket de Amazon S3.
- Tipo: indica el tipo de recurso.
- Región: AWS región en la que se encuentra el recurso.

Para aceptar las recomendaciones de agrupamiento de recursos

1. Complete los pasos del Para ver las recomendaciones de agrupamiento de recursosprocedimiento y, a continuación, vuelva a este procedimiento.
2. En la sección Revisar las recomendaciones de agrupamiento de recursos, active todas las casillas de verificación adyacentes al AppComponentnombre. Para buscar un nombre específico AppComponent, introduzca el AppComponent nombre en el AppComponents cuadro Buscar.

   > **Note**
   >
   > De forma predeterminada, AWS Resilience Hub muestra todas las recomendaciones de agrupamiento de recursos. Para filtrar la tabla con las recomendaciones de agrupamiento de recursos rechazadas anteriormente, seleccione Rechazadas anteriormente en el menú desplegable junto al cuadro Buscar. AppComponents

3. Elija Aceptar.
4. Seleccione Aceptar en el cuadro de diálogo Aceptar la recomendación de agrupamiento de recursos.

   AWS Resilience Hub muestra una alerta informativa si la agrupación de recursos se ha realizado correctamente. Si ha aceptado solo un subconjunto de recomendaciones de agrupamiento de recursos, la sección Revisar las recomendaciones de agrupamiento de recursos muestra todas las recomendaciones de agrupamiento de recursos que no ha aceptado.

Para rechazar las recomendaciones de agrupamiento de recursos

1. Complete los pasos del Para ver las recomendaciones de agrupamiento de recursosprocedimiento y, a continuación, vuelva a este procedimiento.
2. En la sección Revisar las recomendaciones de agrupamiento de recursos, active todas las casillas de verificación adyacentes al AppComponentnombre. Para buscar un nombre específico AppComponent, introduzca el AppComponent nombre en el AppComponents cuadro Buscar.

   > **Note**
   >
   > De forma predeterminada, AWS Resilience Hub muestra todas las recomendaciones de agrupamiento de recursos. Para filtrar la tabla con las recomendaciones de agrupamiento de recursos rechazadas anteriormente, seleccione Rechazadas anteriormente en el menú desplegable adyacente al cuadro Buscar. AppComponents

3. Seleccione Rechazar.
4. Seleccione uno de los motivos para rechazar la recomendación de agrupación de recursos y, a continuación, elija Rechazar en el cuadro de diálogo Rechazar la recomendación de agrupación de recursos.

   AWS Resilience Hub muestra una alerta informativa que confirma lo mismo. Si ha rechazado solo un subconjunto de recomendaciones de agrupamiento de recursos, la sección Revisar las recomendaciones de agrupamiento de recursos muestra todas las recomendaciones de agrupamiento de recursos que no ha aceptado.

Agrupar los recursos manualmente en un AppComponent

En esta sección se explica cómo agrupar manualmente los recursos en un AppComponent y cómo asignarlos diferentes AppComponent a un recurso en. AWS Resilience Hub

Para recursos de grupo

1. En el panel de navegación, elija Aplicaciones.
2. En la página Aplicaciones, seleccione el nombre de la aplicación que contenga los recursos que desee agrupar.
3. Seleccione la pestaña Estructura de la aplicación.
4. En la pestaña Versión, seleccione la versión de la aplicación con el estado Borrador.

5. Elija la pestaña Recursos.
6. Seleccione las casillas de verificación que se encuentran junto al identificador lógico para seleccionar todos los recursos que desee agrupar.

   > **Note**
   >
   > No puede elegir recursos añadidos manualmente.

7. Elija Acciones y luego elija Recursos de grupo.
8. Seleccione una AppComponent de las opciones de la lista AppComponent desplegable Elegir en la que desee agrupar el recurso.
9. Seleccione Save.
10. Elija Publicar nueva versión.
11. Seleccione la pestaña Estructura de la aplicación.
12. Para ver la versión publicada de la aplicación, complete los pasos siguientes:

    a. En la pestaña Versión, seleccione la versión de la aplicación con el estado Publicación actual.

    b. Elija la pestaña Recursos.

Para asignar recursos a un AppComponent

1. En el panel de navegación, elija Aplicaciones.
2. En la página Aplicaciones, seleccione el nombre de la aplicación que contiene el recurso que desea reagrupar.
3. Seleccione la pestaña Estructura de la aplicación.
4. En Versión, seleccione la versión de la aplicación con el estado Borrador.
5. Elija la pestaña Recursos.
6. Seleccione la casilla de verificación adyacente al identificador lógico para seleccionar el recurso.
7. Seleccione Cambiar en el AppComponent menú Acciones.
8. Para eliminar lo actual AppComponent de la AppComponentsección, selecciona una X en la esquina superior derecha de la etiqueta que muestra tu nombre actual AppComponent .
9. Para agrupar el recurso en una forma diferente AppComponent, elija otra AppComponent en la AppComponent lista desplegable Elegir.

10. Elija Añadir.
11. Elimine cualquier elemento vacío AppComponents de la AppComponentspestaña.
12. Elija Publicar nueva versión.
13. Seleccione la pestaña Estructura de la aplicación.
14. Para ver la versión publicada de la aplicación, complete los pasos siguientes:

    a. En la pestaña Versión, seleccione la versión de la aplicación con el estado Publicación actual.

    b. Elija la pestaña Recursos.

Publicar una nueva versión AWS Resilience Hub de la aplicación

Tras realizar los cambios en los recursos de AWS Resilience Hub la aplicación tal y como se describe enEdición de los recursos AWS Resilience Hub de la aplicación, debe publicar una nueva versión de la aplicación para realizar una evaluación de la resiliencia precisa. Además, es posible que deba publicar una nueva versión de la aplicación si ha agregado nuevas alarmas y pruebas recomendadas a la aplicación. SOPs

Para publicar una nueva versión de su aplicación

1. En el panel de navegación, elija Aplicaciones.
2. En la página Aplicaciones, elija el nombre de la aplicación.
3. Seleccione la pestaña Estructura de la aplicación.
4. Elija Publicar nueva versión.
5. En el cuadro de diálogo Publicar versión, en el cuadro Nombre, introduzca un nombre para la versión de la aplicación o puede utilizar el nombre predeterminado sugerido por AWS Resilience Hub.
6. Elija Publicar.

   Al publicar una nueva versión de la aplicación, se convierte en la versión que se evalúa al ejecutar las evaluaciones de resiliencia. Además, la versión preliminar será idéntica a la versión publicada hasta que realice algún cambio.

Tras publicar una nueva versión de la aplicación, le recomendamos que elabore un nuevo informe de evaluación de la resiliencia para confirmar que la aplicación sigue cumpliendo su política de

resiliencia. Para obtener más información acerca de la ejecución de una evaluación, consulte Ejecutar y gestionar las evaluaciones de resiliencia en AWS Resilience Hub.

Ver todas las versiones de AWS Resilience Hub la aplicación

Para facilitar el seguimiento de los cambios en la aplicación, AWS Resilience Hub muestra las versiones anteriores de la aplicación desde el momento en que se creó AWS Resilience Hub.

Para ver todas las versiones de la aplicación

1. En el panel de navegación, elija Aplicaciones.
2. En la página Aplicaciones, elija el nombre de la aplicación.
3. Seleccione la pestaña Estructura de la aplicación.
4. Para ver todas las versiones anteriores de la aplicación, selecciona el signo más (+) antes de Ver todas las versiones. AWS Resilience Hub indica la versión preliminar y la versión publicada recientemente de la aplicación con los estados Borrador y Versión actual, respectivamente. Puede elegir cualquier versión de la aplicación para ver sus recursos AppComponent, fuentes de entrada y otra información asociada.

   Además, también puede filtrar la lista si opta por una de las opciones siguientes:

   - Filtrar por nombre de versión: introduzca un nombre para filtrar los resultados por el nombre de la versión de la aplicación.
   - Filtrar por intervalo de fechas y horas: para aplicar este filtro, seleccione el icono del calendario y seleccione una de las siguientes opciones para filtrar por los resultados que coincidan con el intervalo de tiempo:
     - Rango relativo: seleccione una de las opciones disponibles y seleccione Aplicar.

       Si elige la opción Rango personalizado, introduzca una duración en el cuadro Introducir duración y seleccione la unidad de tiempo correspondiente en la lista desplegable Unidad de tiempo y, a continuación, seleccione Aplicar.
     - Intervalo relativo: para especificar el intervalo de fechas y horas, indique la hora de inicio y la hora de finalización y, a continuación, seleccione Aplicar.

Visualización de los recursos de la AWS Resilience Hub aplicación

Para ver los recursos de su aplicación

1. En el panel de navegación, elija Aplicaciones.
2. En la página Aplicaciones, seleccione la aplicación para la que desee actualizar los permisos de seguridad.
3. En Acciones, seleccione Ver recursos.

   En la pestaña Recursos, puede identificar los recursos de la tabla Recursos de la siguiente manera:

   - ID lógico: un ID lógico es un nombre que se utiliza para identificar los recursos de su AWS CloudFormation pila, el archivo de estado de Terraform, la aplicación MyApplications o. Grupos de recursos de AWS

     > **Note**
     >
     > - Terraform le permite usar el mismo nombre para diferentes tipos de recursos. Por lo tanto, verá "- tipo de recurso" al final del ID lógico para los recursos que comparten el mismo nombre.
     > - Para ver las instancias de todos los recursos de la aplicación, seleccione el signo más (+) situado antes del ID lógico. Para ver todas las instancias de un recurso de aplicación, seleccione el signo más (+) antes del ID lógico de cada recurso.
     >
     >   Para obtener más información sobre los recursos admitidos, consulte the section called “ AWS Resilience Hub Recursos compatibles”.

   - Estado: indica si AWS Resilience Hub evaluará la resiliencia del recurso.
   - Tipo de recurso: el tipo de recurso identifica el recurso componente de la aplicación. Por ejemplo, `AWS::EC2::Instance` declara una instancia de Amazon EC2. Para obtener más información sobre la agrupación de AppComponent recursos, consulte. Agrupación de recursos en un componente de aplicación
   - Nombre de origen: el nombre de la fuente de entrada. Seleccione un nombre de origen para ver sus detalles en la aplicación correspondiente. En el caso de los orígenes de entrada añadidos manualmente, el enlace no estará disponible. Por ejemplo, si elige el nombre de

origen que se importa de una AWS CloudFormation pila, se le redirigirá a la página de detalles de la pila en. AWS CloudFormation

- Tipo de origen: el tipo de origen de entrada.
- AppComponent tipo: el tipo de fuente de entrada. Las fuentes de entrada incluyen AWS CloudFormation pilas, aplicaciones de MyApplications Grupos de recursos de AWS, archivos de estado de Terraform y recursos añadidos manualmente.

> **Note**
>
> Para editar sus clústeres de Amazon EKS, complete los pasos del procedimiento Editar los orígenes de entrada de su aplicación AWS Resilience Hub .

- ID físicos: el identificador asignado real de dicho recurso, como un ID de instancia de Amazon EC2 o un nombre de bucket de S3.
- Incluido: indica si AWS Resilience Hub incluye estos recursos en la aplicación.
- AppComponents— El AWS Resilience Hub componente que se asignó a este recurso cuando se descubrió la estructura de su aplicación.
- Nombre: el nombre del recurso de la aplicación.
- Cuenta: la AWS cuenta propietaria del recurso físico.

4. Elija Guardar y actualizar.

Eliminar una AWS Resilience Hub aplicación

Cuando haya alcanzado el límite máximo de 50 aplicaciones, debe eliminar una o más aplicaciones antes de poder añadir más.

Para eliminar una aplicación de

1. En el panel de navegación, elija Aplicaciones.
2. En la página Aplicaciones, seleccione todas la aplicación que desee eliminar.
3. Elija Acciones y, a continuación, elija Eliminar aplicación.
4. Para confirmar la eliminación, introduzca Eliminar en el cuadro Eliminar y elija Eliminar.

Parámetros de configuración de la aplicación

AWS Resilience Hub proporciona un mecanismo de entrada para recopilar información adicional sobre los recursos asociados a sus aplicaciones. Con esta información, AWS Resilience Hub obtendrá una comprensión más profunda de sus recursos y proporcionará mejores recomendaciones de resiliencia.

En la sección Parámetros de configuración de la aplicación se enumeran todos los parámetros de configuración de su soporte de conmutación por error entre regiones de AWS Elastic Disaster Recovery. Puede identificar los parámetros de configuración de la siguiente manera:

- Tema: indica el área de la aplicación que está configurada. Por ejemplo, la configuración de conmutación por error.
- Propósito: indica el motivo por el AWS Resilience Hub que solicitó la información.
- Parámetro: indica los detalles específicos del área de aplicación, que se AWS Resilience Hub utilizarán para proporcionar recomendaciones para su aplicación. Actualmente, este parámetro utiliza un valor clave de solo una región de conmutación por error y una cuenta asociada.

Actualizar los parámetros de configuración de la aplicación

Esta sección le permite actualizar los parámetros de configuración de su aplicación AWS Elastic Disaster Recovery y publicar la aplicación para incluir los parámetros actualizados para las evaluaciones de resiliencia.

Para actualizar los parámetros de configuración de la aplicación

1. En el panel de navegación, elija Aplicaciones.
2. En la página Aplicaciones, seleccione el nombre de la aplicación que desea editar.
3. Seleccione la pestaña Parámetros de configuración de la aplicación.
4. Elija Actualizar.
5. Introduzca el ID de la cuenta de conmutación por error en el cuadro ID de cuenta.
6. Seleccione una región de conmutación por error en la lista desplegable Región.

> **Note**
>
> Si desea deshabilitar esta característica, seleccione "—" en la lista desplegable.

7. Seleccione Actualizar y publicar.

Administrar las políticas de resiliencia

En esta sección, se describe cómo crear políticas de resiliencia para sus aplicaciones. Configurar correctamente las políticas de resiliencia le permite comprender la postura de resiliencia de su aplicación. Una política de resiliencia contiene información y objetivos que se utilizan para evaluar si se estima que su aplicación se recuperará de un tipo de interrupción, como el software, el hardware, la zona de disponibilidad o AWS la región. Estas políticas no cambian ni afectan a una aplicación real. Varias aplicaciones pueden tener la misma política de resiliencia.

Cuando crea una política de resiliencia, define los objetivos objetivo: objetivo de tiempo de recuperación (RTO) y objetivo de punto de recuperación (RPO). Los objetivos determinan si la aplicación cumple con la política de resiliencia. Asocie la política a su aplicación y realice una evaluación de resiliencia. Puede crear diferentes políticas para los distintos tipos de aplicaciones de su cartera. Por ejemplo, una aplicación de negociación en tiempo real tendría una política de resiliencia diferente a la de una aplicación de informes mensuales.

> **Note**
>
> AWS Resilience Hub le permite introducir un valor cero en los campos RTO y RPO de su política de resiliencia. Sin embargo, al evaluar su aplicación, el resultado de evaluación más bajo posible es cercano a cero. Por lo tanto, si introduce un valor cero en los campos RTO y RPO, el resultado estimado del RTO de la carga de trabajo y del RPO de la carga de trabajo estimado será próximo a cero y el estado de conformidad de su aplicación pasará a ser Política infringida.

La evaluación evalúa la configuración de la aplicación en función de la política de resiliencia adjunta. Al final del proceso, AWS Resilience Hub proporciona una evaluación del modo en que su solicitud se compara con los objetivos de recuperación de su política de resiliencia.

Puede crear políticas de resiliencia en Aplicaciones y también en Políticas de resiliencia. Puede acceder a los datos pertinentes sobre sus políticas y también modificarlos y eliminarlos.

AWS Resilience Hub utiliza sus objetivos de RTO y RPO para medir la resiliencia ante estos posibles tipos de interrupciones:

- Aplicación: pérdida de un servicio o proceso de software necesario.

- Infraestructura de nube: pérdida de hardware, como instancias EC2.
- Zona de disponibilidad (AZ) de la infraestructura de nube: una o más zonas de disponibilidad no están disponibles.
- Región de infraestructura de nube: una o más regiones no están disponibles.

AWS Resilience Hub le permite crear políticas de resiliencia personalizadas o utilizar nuestras políticas de resiliencia de estándar abierto recomendadas. Al crear políticas personalizadas, asigne un nombre y una descripción a la política y seleccione el nivel o nivel adecuado que la defina. Estos niveles incluyen: Servicios básicos de TI, Misión crítica, Críticos, Importantes y No críticos.

Seleccione el nivel adecuado para su clase de aplicación. Por ejemplo, puede clasificar un sistema de negociación en tiempo real como crítico, mientras que puede clasificar una aplicación de informes mensuales como no crítica. Al utilizar nuestras políticas estándar, puede elegir una política de resiliencia con un nivel y valores preconfigurados para los objetivos de RTO y RPO por tipo de interrupción. Si fuera necesario, puede cambiar el nivel y los objetivos de RTO y RPO.

Puede crear políticas de resiliencia en Políticas de resiliencia o al describir una nueva aplicación.

Crear políticas de resiliencia

En AWS Resilience Hub, puede crear una política de resiliencia. Una política de resiliencia contiene información y objetivos que se utilizan para evaluar si la aplicación puede recuperarse de un tipo de interrupción, como el software, el hardware, la zona de disponibilidad o AWS la región. Estas políticas no cambian ni afectan a una aplicación real. Varias aplicaciones pueden tener la misma política de resiliencia.

Cuando crea una política de resiliencia, define los objetivos de tiempo de recuperación (RTO) y los objetivos de punto de recuperación (RPO). Al realizar una evaluación, AWS Resilience Hub determine si se estima que la aplicación cumple los objetivos definidos en la política de resiliencia.

La evaluación evalúa la configuración de la aplicación en función de la política de resiliencia adjunta. Al final del proceso, AWS Resilience Hub proporciona una evaluación de la forma en que su solicitud se compara con los objetivos de su política de resiliencia.

> **Note**
>
> AWS Resilience Hub le permite introducir un valor cero en los campos RTO y RPO de su política de resiliencia. Sin embargo, al evaluar su aplicación, el resultado de evaluación más

bajo posible es cercano a cero. Por lo tanto, si introduce un valor cero en los campos RTO y RPO, el resultado estimado del RTO de la carga de trabajo y del RPO de la carga de trabajo estimado será próximo a cero y el estado de conformidad de su aplicación pasará a ser Política infringida.

Puede crear políticas de resiliencia en Aplicaciones y también en Políticas de resiliencia. Puede acceder a los datos pertinentes sobre sus políticas y también modificarlos y eliminarlos.

Para crear políticas de resiliencia en Aplicaciones

1. En el menú de navegación a la izquierda, elija Aplicaciones.
2. Complete los procedimientos de the section called “Comience por añadir una aplicación” a the section called “Añade etiquetas a tu aplicación ”.
3. En la sección Políticas de resiliencia, seleccione Crear política de resiliencia.

   Aparece la página Crear una política de resiliencia.
4. En la sección Elegir un método de creación, seleccione Crear una política.
5. Introduzca un nombre para la política.
6. (Opcional) Escriba una descripción de la política.
7. Elija una de las siguientes opciones en la lista desplegable Nivel:

   - Servicios básicos fundamentales de TI
   - Misión crítica
   - Critical
   - Importante
   - No crítico
8. Para los objetivos de RTO y RPO, en RTO y RPO de las aplicaciones del cliente, introduzca un valor numérico en el cuadro y, a continuación, seleccione la unidad de tiempo que representa el valor.

   Repita estas entradas en Infraestructura RTO y RPO para Infraestructura y Zona de disponibilidad.
9. (Opcional) Si tiene una aplicación multirregional, puede que desee definir los objetivos de RTO y RPO de una región.

Active Región. Para los objetivos de RTO y RPO de la región, en RTO y RPO de la aplicación del cliente, introduzca un valor numérico en el cuadro y, a continuación, seleccione la unidad de tiempo que representa el valor.

10. (Opcional) Si desea añadir etiquetas, puede hacerlo más adelante a medida que vaya creando la política. Para más información sobre las etiquetas, consulte Etiquetado de recursos en la Guía de referencia general de AWS .
11. Elija Crear para crear la política.

Para crear políticas de resiliencia en Políticas de resiliencia

1. En el menú de navegación izquierdo, elija Políticas.
2. En la sección Políticas de resiliencia, seleccione Crear política de resiliencia.

   Aparece la página Crear una política de resiliencia.
3. Introduzca un nombre para la política.
4. (Opcional) Escriba una descripción de la política.
5. Elija uno de los siguientes del Nivel:

   - Servicios básicos fundamentales de TI
   - Misión crítica
   - Critical
   - Importante
   - No crítico
6. Para los objetivos de RTO y RPO, en RTO y RPO de las aplicaciones del cliente, introduzca un valor numérico en el cuadro y, a continuación, seleccione la unidad de tiempo que representa el valor.

   Repita estas entradas en Infraestructura RTO y RPO para Infraestructura y Zona de disponibilidad.
7. (Opcional) Si tiene una aplicación multirregional, puede que desee definir los objetivos de RTO y RPO de una región.

   Active Región. Para los objetivos de RTO y RPO, en RTO y RPO de las aplicaciones del cliente, introduzca un valor numérico en el cuadro y, a continuación, seleccione la unidad de tiempo que representa el valor.

8. (Opcional) Si desea añadir etiquetas, puede hacerlo más adelante a medida que vaya creando la política. Para más información sobre las etiquetas, consulte Etiquetado de recursos en la Guía de referencia general de AWS .
9. Elija Crear para crear la política.

Para crear políticas de resiliencia basadas en una política sugerida

1. En el menú de navegación izquierdo, elija Políticas.
2. En la sección Elegir un método de creación, seleccione Seleccionar una política en función de una política sugerida.
3. En la sección Políticas de resiliencia, seleccione Crear política de resiliencia.

   Aparece la página Crear una política de resiliencia.
4. Introduzca un nombre para la política de resiliencia.
5. (Opcional) Escriba una descripción de la política.
6. En la sección Políticas de resiliencia sugeridas, consulte y seleccione uno de los siguientes niveles de política de resiliencia predeterminados:

   - Aplicación no crítica
   - Aplicación importante
   - Aplicación crítica
   - Aplicación crítica global
   - Aplicación de misión crítica
   - Aplicación de misión crítica global
   - Servicio básico fundamental
7. Para crear la política de resiliencia, seleccione Crear política.

Acceder a la información relativa a la política de resiliencia

Al abrir una política de resiliencia, verá información importante sobre esta. También puede editar o eliminar la resiliencia.

La información relativa a de la política de resiliencia consta de dos puntos de vista principales: Resumen y Etiquetas.

Resumen

Información básica

Proporciona la siguiente información sobre la política de resiliencia: nombre, descripción, nivel, nivel de costo y fecha de creación.

RTO estimado de la carga de trabajo y RPO estimado de la carga de trabajo

Muestra el RTO estimado de la carga de trabajo y el tipo de interrupción del RPO estimado de la carga de trabajo asociados a esta política de resiliencia.

Etiquetas

Utilice esta vista para administrar, añadir y eliminar etiquetas internas de esta aplicación.

Para editar las políticas de resiliencia en Detalles de la política de resiliencia

1. En el menú de navegación izquierdo, elija Políticas.
2. En Políticas de resiliencia, abra una política de resiliencia.
3. Elija Editar. Introduzca los cambios correspondientes en los campos Información básica, RTO y RPO. A continuación, elija Guardar cambios.

Para editar las políticas de resiliencia en Política de resiliencia

1. En el menú de navegación izquierdo, elija Políticas.
2. En Políticas de resiliencia, seleccione una política de resiliencia.
3. Seleccione Acciones y luego seleccione Editar.
4. Introduzca los cambios correspondientes en los campos Información básica, RTO y RPO. A continuación, elija Guardar cambios.

Para eliminar las políticas de resiliencia en Detalles de la política de resiliencia

1. En el menú de navegación izquierdo, elija Políticas.
2. En Políticas de resiliencia, abra una política de resiliencia.
3. Elija Eliminar. Confirme su eliminación y luego elija Eliminar.

Para eliminar las políticas de resiliencia en Política de resiliencia

1. En el menú de navegación izquierdo, elija Políticas.
2. En Políticas de resiliencia, seleccione una política de resiliencia.
3. Seleccione Acciones y, a continuación, elija Eliminar.
4. Confirme su eliminación y luego elija Eliminar.

Ejecutar y gestionar las evaluaciones de resiliencia en AWS Resilience Hub

Cuando su aplicación cambie, debe realizar una evaluación de resiliencia. La evaluación compara la configuración de cada componente de la aplicación con la política y formula recomendaciones de alarma, SOP y pruebas. Estas recomendaciones de configuración pueden mejorar la velocidad de los procedimientos de recuperación.

Las recomendaciones de alarmas le ayudan a configurar alarmas que detecten las interrupciones. Las recomendaciones de SOP proporcionan scripts que administran los procesos de recuperación habituales, como la recuperación a partir de una copia de seguridad. Las recomendaciones de prueba ofrecen sugerencias para comprobar que las configuraciones funcionan correctamente. Por ejemplo, puede comprobar si una aplicación se recupera durante los procesos de recuperación automática, como el escalado automático o el equilibrio de carga, debido a problemas de red. Puede comprobar si las alarmas de la aplicación se activan cuando los recursos alcanzan sus límites. También puede comprobar si SOPs funcionan bien en las condiciones que usted indique.

Temas:

Realizar evaluaciones de resiliencia en AWS Resilience Hub

Puede realizar evaluaciones de resiliencia desde varios lugares en. AWS Resilience Hub Para obtener más información acerca de su aplicación, consulte the section called “Administración de las aplicaciones de ”.

Para realizar una evaluación de resiliencia desde el menú Acciones

1. En el menú de navegación a la izquierda, elija Aplicaciones.

2. Seleccione una aplicación de la tabla Aplicaciones.
3. Seleccione Evaluar la resiliencia en el menú Acciones.
4. En el cuadro de diálogo Ejecutar una evaluación de la resiliencia, puede introducir un nombre único o utilizar el nombre generado para la evaluación.
5. Elija Ejecutar.

   Para revisar el informe de evaluación, seleccione Evaluaciones en su aplicación. Para obtener más información, consulte the section called “Revisar los informes de evaluación”.

Para ejecutar una evaluación de resiliencia desde la pestaña Evaluaciones

Puede realizar una nueva evaluación de resiliencia cuando su aplicación o política de resiliencia cambien.

1. En el menú de navegación a la izquierda, elija Aplicaciones.
2. Seleccione una aplicación de la tabla Aplicaciones.
3. Seleccione la pestaña Asignaciones.
4. Seleccione Ejecutar una evaluación de resiliencia.
5. En el cuadro de diálogo Ejecutar una evaluación de la resiliencia, puede introducir un nombre único o utilizar el nombre generado para la evaluación.
6. Elija Ejecutar.

   Para revisar el informe de evaluación, seleccione Evaluaciones en su aplicación. Para obtener más información, consulte the section called “Revisar los informes de evaluación”.

Revisar los informes de evaluación

Encontrará los informes de evaluación en la vista Evaluaciones de su aplicación.

Para encontrar un informe de evaluación

1. En el menú de navegación a la izquierda, elija Aplicaciones.
2. En Aplicaciones, abra una aplicación.
3. En la pestaña Evaluaciones, elija un informe de evaluación de la sección Evaluaciones de resiliencia.

Cuando abra el informe, podrá visualizar lo siguiente:

- Información general acerca del informe de evaluación
- Recomendaciones para mejorar la resiliencia.
- Recomendaciones para configurar alarmas SOPs y pruebas
- ¿Cómo crear y administrar etiquetas para buscar y filtrar sus AWS recursos

Informes de evaluación

En esta sección se proporciona una visión general del informe de evaluación. AWS Resilience Hub enumera cada tipo de interrupción y el componente de aplicación asociado. También enumera sus políticas de RTO y RPO actuales y determina si el componente de aplicación puede satisfacer los objetivos de la política.

Información general

Muestra el nombre de la aplicación, el nombre de la política de resiliencia y la fecha de creación del informe.

Desviaciones de recursos detectadas

En esta sección se enumeran todos los recursos que se agregaron o eliminaron después de incluirlos en la última versión de la aplicación publicada. Seleccione Reimportar fuentes de entrada para volver a importar todas las fuentes de entrada (que contienen recursos desviados) en la pestaña Fuentes de entrada. Elija Publicar y evaluar para incluir los recursos actualizados en la aplicación y recibir una evaluación de resiliencia precisa.

Puede identificar los orígenes de entrada desviados de la siguiente manera:

- ID lógico: indica el ID lógico del recurso. Un identificador lógico es un nombre que se utiliza para identificar los recursos de su AWS CloudFormation pila, del archivo de estado de Terraform, de la aplicación MyApplications o. Grupos de recursos de AWS
- Cambio: indica si se agregó o eliminó un recurso de entrada.
- Nombre del origen: indica el nombre del recurso. Seleccione un nombre de origen para ver sus detalles en la aplicación correspondiente. En el caso de los orígenes de entrada añadidos manualmente, el enlace no estará disponible. Por ejemplo, si elige el nombre de origen que se importa de una AWS CloudFormation pila, se le redirigirá a la página de detalles de la pila en AWS CloudFormation.

- Tipo de recurso: indica el tipo de recurso.
- Cuenta: indica la AWS cuenta propietaria del recurso físico.
- Región: indica la región de AWS en la que se encuentra el recurso.

RTO

Muestra una representación gráfica de si se estima que la aplicación cumple los objetivos de la política de resiliencia. Esto se basa en el tiempo que una aplicación puede permanecer inactiva sin causar un daño significativo a la organización. La evaluación proporciona un RTO estimado de la carga de trabajo.

RPO

Muestra una representación gráfica de si se estima que la aplicación cumple los objetivos de la política de resiliencia. Esto se basa en el tiempo que pueden perderse los datos antes de que se produzca un daño significativo para la empresa. La evaluación proporciona un RPO estimado de carga de trabajo.

Detalles

Proporciona descripciones detalladas de cada tipo de interrupción mediante las pestañas Todos los resultados y Desviaciones de cumplimiento de la aplicación. La pestaña Todos los resultados muestra todas las interrupciones, incluidas las desviaciones de cumplimiento, mientras que la pestaña Desviaciones de cumplimiento de la aplicación muestra solo las desviaciones de cumplimiento. El tipo de interrupción incluye la Aplicación, la infraestructura de nube (Infraestructura y Zona de disponibilidad) y la Región, y proporciona la siguiente información al respecto:

- AppComponent

  Los recursos que componen la aplicación. Por ejemplo, la aplicación puede tener una base de datos o un componente de procesamiento.

- RTO estimado

  Indica si la configuración de la política se ajusta a los requisitos de la política. Proporcionamos dos valores: nuestro RTO estimado y su RTO objetivo. Por ejemplo, si ve un valor de 2 h en el RTO fijado como objetivo y 40 min en el RTO estimado de la carga de trabajo, significa que proporcionamos un RTO estimado de la carga de trabajo de 40 minutos, mientras que el RTO

actual de su aplicación es de dos horas. Para calcular el RTO estimado de la carga de trabajo, nos basamos en la configuración, no en la política. Como resultado, una base de datos de zonas de disponibilidad múltiple tendrá el mismo RTO estimado de carga de trabajo en caso de fallo en una zona de disponibilidad, independientemente de la política que seleccione.

- Desviación del RTO

  Indica el tiempo durante el cual su aplicación se ha desviado del RTO estimado de la carga de trabajo de la última evaluación satisfactoria. Proporcionamos dos valores: nuestro RTO estimado y nuestra Desviación del RTO. Por ejemplo, si ve un valor de 2 h en el RTO estimado y 40 min en la Desviación del RTO significa que su aplicación se desvía en 40 minutos del RTO estimado de la carga de trabajo de la última evaluación satisfactoria.

- RPO estimado

  Muestra la política de RPO estimado de la carga de trabajo real que AWS Resilience Hub estima, en función de la política de RPO fijado como objetivo que haya establecido para cada componente de la aplicación. Por ejemplo, es posible que haya establecido en una hora el objetivo de RPO en su política de resiliencia para errores en las zonas de disponibilidad. El resultado estimado podría calcularse cerca de cero. Esto supone que Amazon Aurora, donde confirmamos todas las transacciones, se realiza correctamente en cuatro de los seis nodos, que abarcan varias zonas de disponibilidad. La point-in-time restauración puede tardar cinco minutos.

  El único objetivo de RTO y RPO que puede optar por no suministrar es región. En el caso de algunas aplicaciones, resulta útil planificar la recuperación cuando existe una dependencia crucial de un servicio de AWS, que podría dejar de estar disponible en toda la región.

  Si elige esta opción, por ejemplo, si establece objetivos de RTO o RPO para la región, recibirá un tiempo de recuperación estimado y recomendaciones operativas para este tipo de errores.

- Desviación del RPO

  Indica el tiempo durante el cual su aplicación se ha desviado del RPO estimado de la carga de trabajo de la última evaluación satisfactoria. Proporcionamos dos valores: nuestro RPO estimado y nuestra Desviación de RPO. Por ejemplo, si ve un valor de 2 h en el RPO estimado y 40 min en la Desviación del RPO significa que su aplicación se desvía en 40 minutos del RPO estimado de la carga de trabajo de la última evaluación satisfactoria.

Revisar las recomendaciones de resiliencia

Las recomendaciones de resiliencia evalúan los componentes de la aplicación y recomiendan cómo optimizar el RTO estimado de la carga de trabajo y el RPO estimado de la carga de trabajo, los costos y los cambios mínimos.

Con AWS Resilience Hub, puede optimizar la resiliencia mediante una de las siguientes opciones recomendadas en Por qué debe elegir esta opción:

> **Note**
>
> - AWS Resilience Hub ofrece hasta tres opciones AWS Resilience Hub recomendadas.
> - Si establece objetivos de RTO y RPO regionales, AWS Resilience Hub mostrará Optimize for Region RTO/RPO en las opciones recomendadas. Si no se han establecido los objetivos de RTO y RPO regionales, aparece Optimize for Availability Zone (AZ) RTO/RPO. Para obtener más información sobre cómo establecer RTO/RPO objetivos regionales y, al mismo tiempo, crear políticas de resiliencia, consulte. Crear políticas de resiliencia
> - Los valores del RTO de la carga de trabajo estimada y el RPO de la carga de trabajo estimada para las aplicaciones y sus configuraciones se determinan teniendo en cuenta la cantidad de datos y la cantidad individual. AppComponents Sin embargo, estos valores son solo estimaciones. Debe utilizar sus propias pruebas (por ejemplo AWS Fault Injection Service) para comprobar los tiempos de recuperación reales de la aplicación.

Optimice para la zona de disponibilidad (RTO/RPO)

Los tiempos de recuperación de la carga de trabajo (RTO/RPO) estimados más bajos posibles durante una interrupción en la zona de disponibilidad (AZ). Si la configuración no se puede cambiar lo suficiente como para cumplir los objetivos de RTO y RPO, se le informará sobre los tiempos de recuperación de carga de trabajo estimados más bajos para que su configuración se acerque a la posibilidad de cumplir con la política.

Optimice el RTO/RPO para la región

Los tiempos de recuperación de la carga de trabajo (RTO/RPO) estimados más bajos posibles durante una interrupción regional. Si la configuración no se puede cambiar lo suficiente como para cumplir los objetivos de RTO y RPO, se le informará sobre los tiempos de recuperación de la carga de trabajo estimados más bajos para que su configuración se acerque a la posibilidad de cumplir con la política.

Optimice en función de los costes

El costo más bajo en el que puede incurrir y, al mismo tiempo, cumplir con su política de resiliencia. Si la configuración no se puede cambiar lo suficiente como para cumplir los objetivos de optimización, se le informará sobre el costo más bajo en el que puede incurrir para que su configuración se acerque a la posibilidad de cumplir con la política.

Optimizar para cambios mínimos

Los cambios mínimos necesarios para alcanzar los objetivos de su política. Si la configuración no se puede cambiar lo suficiente como para cumplir los objetivos de optimización, se le informará sobre los cambios recomendados que pueden acercar su configuración a la posibilidad de cumplir con la política.

Los siguientes elementos se incluyen en los desgloses de las categorías de optimización:

- Descripción

  Describe las configuraciones sugeridas por AWS Resilience Hub.
- Cambios

  Una lista de cambios de texto que describen las tareas necesarias para cambiar a la configuración sugerida.
- Costo básico

  El costo estimado asociado a los cambios recomendados.

  > **Note**
  >
  > El costo base puede variar en función del uso y no incluye descuentos ni ofertas del Programa de descuentos empresariales (EDP).
- RTO y RPO estimados de la carga de trabajo

  El RTO estimado de la carga de trabajo y el RPO estimado de la carga de trabajo después de los cambios.

AWS Resilience Hub evalúa si un componente de la aplicación (AppComponent) puede cumplir con una política de resiliencia. Si no AppComponent cumple con una política de resiliencia y AWS Resilience Hub no puede hacer ninguna recomendación para facilitar el cumplimiento, es posible

que el tiempo de recuperación de lo seleccionado AppComponent no pueda cumplirse dentro de las limitaciones del AppComponent. Algunos ejemplos de AppComponent restricciones son el tipo de recurso, el tamaño del almacenamiento o la configuración de los recursos.

Para facilitar el cumplimiento de la AppComponent política de resiliencia, cambie el tipo de recurso AppComponent o actualice la política de resiliencia para adaptarla a lo que el recurso puede ofrecer.

Revisar las recomendaciones operativas

Las recomendaciones operativas contienen recomendaciones para configurar alarmas y AWS FIS experimentos mediante AWS CloudFormation plantillas. SOPs

AWS Resilience Hub proporciona archivos AWS CloudFormation de plantilla para descargar y administrar la infraestructura de la aplicación en forma de código. Como resultado, proporcionamos recomendaciones en AWS CloudFormation para que pueda añadirlas al código de su aplicación. Si el tamaño del archivo de AWS CloudFormation plantilla es superior a un MB y contiene más de 500 recursos, AWS Resilience Hub genera más de un archivo de AWS CloudFormation plantilla donde el tamaño de cada archivo no es superior a un MB y contiene hasta 500 recursos. Si el archivo de AWS CloudFormation plantilla está dividido en varios archivos, se añadirán los nombres de los archivos de AWS CloudFormation plantilla`partXofY`, donde se `X` indica el número de archivo de la secuencia y se `Y` indica el número total de archivos en los que está dividido el archivo de AWS CloudFormation plantilla. Por ejemplo, si el archivo de la plantilla de `big-app-template5-Alarm-104849185070-us-west-2.yaml` está dividido en cuatro archivos, los nombres de los archivos serían los siguientes:

- `big-app-template5-Alarm-104849185070-us-west-2-part1of4.yaml`
- `big-app-template5-Alarm-104849185070-us-west-2-part2of4.yaml`
- `big-app-template5-Alarm-104849185070-us-west-2-part3of4.yaml`
- `big-app-template5-Alarm-104849185070-us-west-2-part4of4.yaml`

Sin embargo, en el caso de AWS CloudFormation plantillas grandes, se le solicita que proporcione el URI de Amazon Simple Storage Service en lugar de usarlo CLI/API con un archivo local como entrada.

En AWS Resilience Hub, puede realizar las siguientes acciones:

- Puede aprovisionar las alarmas y SOPs los AWS FIS experimentos seleccionados. Para aprovisionar alarmas y AWS FIS experimentos, seleccione la recomendación adecuada e

introduzca un nombre único. SOPs AWS Resilience Hub crea una plantilla basada en las recomendaciones seleccionadas. En Plantillas, puede acceder a las plantillas que haya creado a través de una URL de Amazon Simple Storage Service (Amazon S3).

- Puede incluir o excluir las alarmas y AWS FIS los experimentos seleccionados que se recomendaron para su aplicación en cualquier momento. SOPs Para obtener más información, consulte, the section called “Incluir o excluir recomendaciones operativas”.
- También puede buscar, crear, añadir, eliminar y administrar las etiquetas de una aplicación y ver todas las etiquetas asociadas a ella.

Incluir o excluir recomendaciones operativas

AWS Resilience Hub ofrece la opción de incluir o excluir las alarmas y AWS FIS los experimentos (pruebas) que se recomendaron para mejorar la puntuación de resiliencia de su aplicación en cualquier momento. SOPs La inclusión y exclusión de las recomendaciones operativas tendrá un impacto en la puntuación de resiliencia de la aplicación solo después de realizar una nueva evaluación. Por lo tanto, le recomendamos que realice una evaluación para obtener la puntuación de resiliencia actualizada y comprender su impacto en su aplicación.

Para obtener más información sobre cómo restringir los permisos para incluir o excluir recomendaciones por aplicación, consulte the section called “Limitar los permisos para incluir o excluir recomendaciones de AWS Resilience Hub ”.

Para incluir o excluir recomendaciones operativas de las aplicaciones

1. En el menú de navegación a la izquierda, elija Aplicaciones.
2. En Aplicaciones, abra una aplicación.
3. Seleccione Evaluaciones y elija una evaluación de la tabla Evaluaciones de resiliencia. Si no tiene una evaluación, complete el procedimiento de the section called “Realizar evaluaciones de resiliencia en AWS Resilience Hub” y, a continuación, vuelva a este paso.
4. Seleccione la pestaña Recomendaciones operativas.
5. Complete los siguientes procedimientos para incluir o excluir recomendaciones operativas:

Para incluir o excluir las alarmas recomendadas de su aplicación

1. Complete los siguientes pasos para excluir las alarmas:

a. En la pestaña Alarmas, en la tabla Alarmas, seleccione todas las alarmas (con el estado No implementado) que desee excluir. Puede identificar el estado de implementación actual de una alarma en la columna Estado.

b. En Acciones, seleccione Excluir seleccionadas.

c. En el cuadro de diálogo Excluir recomendaciones, seleccione uno de los siguientes motivos (opcional) y seleccione Excluir seleccionadas para excluir las alarmas seleccionadas de la aplicación.

- Ya implementadas: elija esta opción si ya ha implementado estas alarmas en un AWS servicio como Amazon CloudWatch o en cualquier otro proveedor de servicios externo.
- No pertinente: seleccione esta opción si las alarmas no se ajustan a los requisitos de su empresa.
- Demasiado complicadas de implementar: seleccione esta opción si cree que estas alarmas son demasiado complicadas de implementar.
- Otros: seleccione esta opción para especificar cualquier otro motivo para excluir la recomendación.

2. Complete los siguientes pasos para incluir alarmas:

a. En la pestaña Alarmas, en la tabla Alarmas, seleccione todas las alarmas (con el estado Excluido) que desee incluir. Puede identificar el estado de implementación actual de la alarma en la columna Estado.

b. En Acciones, seleccione Incluir seleccionadas.

c. En el cuadro de diálogo Incluir recomendaciones, seleccione Incluir seleccionadas para incluir todas las alarmas seleccionadas en la aplicación.

Para incluir o excluir los procedimientos operativos estándar recomendados (SOPs) de su solicitud

1. Para excluir los recomendados SOPs, complete los siguientes pasos:

a. En la pestaña Procedimientos operativos estándar, de la SOPstabla, seleccione todos los SOPs elementos (con el estado Implementado o No implementado) que desee excluir. Puede identificar el estado de implementación actual de un SOP en la columna Estado.

b. En Acciones, elija Excluir lo seleccionado para excluir lo seleccionado SOPs de la aplicación.

c. En el cuadro de diálogo Excluir recomendaciones, seleccione uno de los siguientes motivos (opcional) y elija Excluir los seleccionados para excluir los seleccionados SOPs de la aplicación.

- Ya implementados: elija esta opción si ya los ha implementado SOPs en un AWS servicio o en cualquier otro proveedor de servicios externo.
- No relevante: elija esta opción si SOPs no se ajusta a los requisitos de su empresa.
- Muy complicadas de implementar: elija esta opción si cree que SOPs son demasiado complicadas de implementar.
- Ninguno: seleccione esta opción si no desea especificar el motivo.

2. Para SOPs incluirlos, complete los siguientes pasos:

a. En la pestaña Procedimientos operativos estándar, de la SOPstabla, seleccione todas las alarmas (con el estado Excluido) que desee incluir. Puede identificar el estado de implementación actual de la alarma en la columna Estado.

b. En Acciones, seleccione Incluir seleccionadas.

c. En el cuadro de diálogo Incluir recomendaciones, elija Incluir las seleccionadas para incluir todas las seleccionadas SOPs en la aplicación.

Para incluir o excluir las pruebas recomendadas de su aplicación

1. Complete los siguientes pasos para excluir las pruebas recomendadas:

a. En la pestaña Plantillas de experimentos de inyección de errores, en la tabla Plantillas de experimentos de inyección de errores, seleccione todas las pruebas (con el estado Implementado o No implementado) que desee excluir. Puede identificar el estado de implementación actual de una prueba en la columna Estado.

b. En Acciones, seleccione Excluir seleccionadas.

c. En el cuadro de diálogo Excluir recomendaciones, seleccione uno de los siguientes motivos (opcional) y elija Excluir seleccionados para excluir los experimentos de AWS FIS seleccionados de la aplicación.

- Ya implementadas: elija esta opción si ya ha implementado estas pruebas en un AWS servicio o en cualquier otro proveedor de servicios externo.
- No pertinente: seleccione esta opción si las pruebas no se ajustan a los requisitos de su empresa.

- Demasiado complicadas de implementar: seleccione esta opción si cree que estas pruebas son demasiado complicadas de implementar.
- Ninguno: seleccione esta opción si no desea especificar el motivo.

2. Complete los siguientes pasos para incluir las pruebas recomendadas:

   a. En la pestaña Plantillas de experimentos de inyección de errores, en la tabla Plantillas de experimentos de inyección de errores, seleccione todas las pruebas (con el estado Excluido) que desee incluir. Puede identificar el estado de implementación actual de la prueba en la columna Estado.
   b. En Acciones, seleccione Incluir seleccionadas.
   c. En el cuadro de diálogo Incluir recomendaciones, seleccione Incluir seleccionadas para incluir todas las pruebas seleccionadas en la aplicación.

Eliminar las evaluaciones de resiliencia

Puede eliminar las evaluaciones de resiliencia en la vista Evaluaciones de su aplicación.

Para eliminar una evaluación de resiliencia

1. En el menú de navegación a la izquierda, elija Aplicaciones.
2. En Aplicaciones, abra una aplicación.
3. En Evaluaciones, seleccione un informe de evaluación en la tabla Evaluaciones de resiliencia.
4. Para confirmar la eliminación, elija Eliminar.

   El informe ya no aparece en la tabla Evaluaciones de resiliencia.

Ejecutar y gestionar las evaluaciones de resiliencia desde el widget de resiliencia

AWS Resilience Hub le permite ejecutar evaluaciones para las aplicaciones creadas y administradas en el widget MyApplications in Resiliency. Siempre que realice modificaciones en una aplicación, se recomienda ejecutar una evaluación de resiliencia desde el widget de resiliencia o desde la consola. AWS Resilience Hub Durante esta evaluación, la configuración de cada componente de la aplicación se evalúa en función de las políticas y las mejores prácticas establecidas. Sobre la base de esta evaluación, la evaluación genera recomendaciones para configurar las alarmas, crear procedimientos operativos estándar (SOPs) e implementar estrategias de prueba. La implementación

de estas recomendaciones de configuración puede mejorar la velocidad y la eficiencia de sus procedimientos de recuperación, garantizando una respuesta más rápida a los incidentes y minimizando los posibles tiempos de inactividad.

Las recomendaciones de alarmas le ayudan a configurar alarmas que detecten las interrupciones. Las recomendaciones de SOP proporcionan scripts que administran los procesos de recuperación habituales, como la recuperación a partir de una copia de seguridad. Las recomendaciones de prueba ofrecen sugerencias para comprobar que las configuraciones funcionan correctamente. Por ejemplo, puede comprobar si una aplicación se recupera durante los procesos de recuperación automática, como el escalado automático o el equilibrio de carga, debido a problemas de red. Puede comprobar si las alarmas de la aplicación se activan cuando los recursos alcanzan sus límites. También puede comprobar si SOPs funcionan bien en las condiciones que usted indique.

Temas:

Realizar evaluaciones de resiliencia desde el widget de resiliencia

En el caso de las aplicaciones creadas en el widget MyApplications, ahora puede ejecutar evaluaciones de resiliencia desde el widget y la consola de resiliencia. AWS Resilience Hub Para obtener más información sobre cómo ejecutar las evaluaciones de resiliencia desde AWS Resilience Hub la consola, consulte. Realizar evaluaciones de resiliencia en AWS Resilience Hub

Para realizar una evaluación de resiliencia de una aplicación MyApplications existente desde el widget Resiliency por primera vez

1. Inicie sesión en la Consola de AWS License Manager.
2. Expanda la barra lateral izquierda y elija myApplications.
3. Seleccione la aplicación para la que desee ejecutar la evaluación.

   Como requisito previo, asegúrese de haber agregado el widget de resiliencia a la AWS consola. Para añadir este widget, complete los siguientes pasos.

   a. En la parte superior o inferior derecha del panel de inicio de la consola, selecciona +Añadir widgets.

b. Selecciona el indicador de arrastre, representado por seis puntos verticales en la parte superior izquierda de la barra de título del widget, y arrástralo hasta el panel de inicio de la consola.

4. Selecciona Evaluar la aplicación.
5. Para seleccionar una función de IAM existente que se utilizará para acceder a los recursos de la cuenta actual, seleccione Usar una función de IAM y, a continuación, seleccione una función de IAM en la lista desplegable Seleccionar una función de IAM.

   Si desea utilizar el usuario de IAM actual para descubrir los recursos de su aplicación, elija Usar los permisos de usuario de IAM actuales y seleccione Comprendo que debo configurar manualmente los permisos para habilitar la funcionalidad requerida AWS Resilience Hub en la sección Usar el usuario de IAM actual para descubrir los recursos de la aplicación.
6. Seleccione Evaluar.

   Como alternativa, active la opción Evaluar automáticamente todos los días AWS Resilience Hub para poder evaluar su solicitud a diario sin costes adicionales.

   AWS Resilience Hub realiza las siguientes acciones:

   - Crea una aplicación AWS Resilience Hub y descubre y mapea automáticamente los recursos asociados.
   - Crea y asigna una nueva política de resiliencia con valores predefinidos para el Objetivo de tiempo de recuperación (RTO) y el Objetivo de punto de recuperación (RPO). Es decir, cuatro horas para RTO y una hora para RPO. Tras generar una evaluación, puede modificar la política de resiliencia o asignar una política diferente desde la AWS Resilience Hub consola. Para obtener más información sobre cómo actualizar la política de resiliencia y adjuntar una política diferente, consulte Administración de las políticas de resiliencia.
   - Evalúa la resiliencia de la aplicación frente al RTO y el RPO, supervisa de forma continua los recursos y los cambios de configuración, y publica los resultados.

   > **Note**
   >
   > Antes de iniciar las evaluaciones, es recomendable evaluar los costos potenciales que implica la ejecución de las evaluaciones mediante AWS Resilience Hub. Para obtener información detallada sobre los precios, consulte los AWS Resilience Hub precios.

Para volver a ejecutar una evaluación de resiliencia de una aplicación MyApplications existente desde el widget Resiliency

1. Inicie sesión en la Consola de AWS License Manager.
2. Expanda la barra lateral izquierda y elija myApplications.
3. Seleccione la aplicación que desee volver a evaluar.

   Como requisito previo, asegúrese de haber agregado el widget de resiliencia a la consola. AWS Para añadir este widget, complete los siguientes pasos.

   a. En la parte superior o inferior derecha del panel de inicio de la consola, selecciona +Añadir widgets.
   b. Selecciona el indicador de arrastre, representado por seis puntos verticales en la parte superior izquierda de la barra de título del widget, y arrástralo hasta el panel de inicio de la consola.
4. Selecciona Reevaluar en el widget de resiliencia.

   Como alternativa, active la opción Evaluar automáticamente todos los días AWS Resilience Hub para poder evaluar su solicitud a diario sin costes adicionales.

Revisar el resumen de la evaluación en el widget de resiliencia

El widget de resiliencia muestra una instantánea de los resultados de la evaluación que le proporcionará la información más importante y práctica sobre la resiliencia de la aplicación MyApplications, las posibles vulnerabilidades, los indicadores clave de rendimiento (KPIs) y las medidas de mejora recomendadas. Puede obtener más información sobre la postura de resiliencia de la aplicación a partir de la evaluación más reciente mediante lo siguiente:

- Historial de puntuación de resiliencia: este gráfico muestra la tendencia de la puntuación de resiliencia de la aplicación durante un máximo de un año.
- Puntuación de resiliencia: indica la puntuación de resiliencia de la aplicación evaluada en la evaluación más reciente. Esta puntuación refleja en qué medida su aplicación sigue nuestras recomendaciones para cumplir con la política de resiliencia de la aplicación y para implementar alarmas, procedimientos operativos estándar () y AWS Fault Injection Service (SOPs) experimentos.AWS FIS Elija el número para ver información adicional en la sección de puntuación de resiliencia en la pestaña Resumen de la AWS Resilience Hub consola. Para obtener más información, consulte Informes de evaluación.

- Incumplimientos de políticas: elija el número que aparece a continuación para ver todos los componentes de la aplicación (AppComponents) que infringen las políticas adjuntas a su solicitud en el panel del informe de evaluación de la AWS Resilience Hub consola. Para obtener más información, consulte Informes de evaluación.
- Desviaciones políticas: AppComponents indica qué políticas cumplieron con la política en la evaluación anterior, pero no la cumplieron en la evaluación actual. Elija el número siguiente para verlo AppComponents en el panel del informe de evaluación de la AWS Resilience Hub consola. Para obtener más información, consulte Informes de evaluación.
- Desviaciones de recursos: seleccione el número siguiente para ver todos los recursos derivados de la última evaluación en el panel del informe de evaluación de la AWS Resilience Hub consola. Para obtener más información, consulte Informes de evaluación.
- Vaya a Resilience Hub: elija esta opción para abrir la aplicación en la AWS Resilience Hub consola.

Administración de alarmas

Cuando realizas una evaluación de resiliencia, como parte de las recomendaciones operativas, te AWS Resilience Hub recomienda configurar las CloudWatch alarmas de Amazon para monitorear la resiliencia de tus aplicaciones. Recomendamos estas alarmas en función de los recursos y componentes de la configuración actual de la aplicación. Si los recursos y componentes de tu aplicación cambian, debes realizar una evaluación de resiliencia para asegurarte de que tienes las CloudWatch alarmas de Amazon correctas para tu aplicación actualizada.

Además, AWS Resilience Hub ahora detecta e integra automáticamente cualquier CloudWatch alarma de Amazon ya configurada en sus evaluaciones de resiliencia, lo que proporciona una visión más completa del estado de resiliencia de su aplicación. Esta nueva capacidad combina AWS Resilience Hub las recomendaciones con su configuración de monitoreo actual, lo que optimiza la administración de alarmas y mejora la precisión de la evaluación. Si has implementado una CloudWatch alarma de Amazon y AWS Resilience Hub no la detecta automáticamente, puedes excluirla y seleccionar el motivo como Ya implementada. Para obtener más información sobre cómo excluir una recomendación, consultaIncluir o excluir recomendaciones operativas.

AWS Resilience Hub proporciona un archivo de plantilla (`README.md`) que le permite crear alarmas recomendadas por AWS Resilience Hub dentro AWS (por ejemplo, Amazon CloudWatch) o por fuera AWS. Los valores predeterminados que se proporcionan en las alarmas se basan en las mejores prácticas que se utilizan para crear estas alarmas.

Temas

Crear alarmas a partir de las recomendaciones operativas

AWS Resilience Hub crea una CloudFormation plantilla que contiene detalles para crear las alarmas seleccionadas en Amazon CloudWatch. Una vez generada la plantilla, puede acceder a ella a través de una URL de Amazon S3, descargarla y colocarla en su canal de código o crear una pila a través de la consola de CloudFormation .

Para crear una alarma basada en AWS Resilience Hub las recomendaciones, debes crear una CloudFormation plantilla para las alarmas recomendadas e incluirlas en tu base de código.

Para crear alarmas en las recomendaciones operativas

1. En el menú de navegación a la izquierda, elija Aplicaciones.
2. En Aplicaciones, seleccione su aplicación.
3. Seleccione la pestaña Evaluaciones.

   En la tabla Evaluaciones de resiliencia, puede identificar sus evaluaciones con la siguiente información:

   - Nombre: nombre de la evaluación que proporcionó en el momento de la creación.
   - Estado: indica el estado de ejecución de la evaluación.
   - Estado de conformidad: indica si la evaluación cumple con la política de resiliencia.
   - Estado de desviación de la resiliencia: indica si su aplicación se ha desviado o no de la última evaluación satisfactoria.
   - Versión de la aplicación: versión de su aplicación.
   - Invocador: indica el rol que invocó la evaluación.
   - Hora de inicio: indica la hora de inicio de la evaluación.
   - Hora de finalización: indica la hora de finalización de la evaluación.
   - ARN: el nombre de recurso de Amazon (ARN) de la evaluación.
4. Seleccione una evaluación de la tabla Evaluaciones de resiliencia. Si no tiene una evaluación, complete el procedimiento de the section called “Realizar evaluaciones de resiliencia en AWS Resilience Hub” y, a continuación, vuelva a este paso.

5. Seleccione Recomendaciones operativas.
6. Si no está seleccionada de forma predeterminada, seleccione la pestaña Alarmas.

   En la tabla Alarmas, puede identificar las alarmas recomendadas mediante lo siguiente:

   - Nombre: nombre de la alarma que ha configurado para su aplicación.
   - Descripción: describe el objetivo de la alarma.
   - Estado: indica el estado de implementación actual de las CloudWatch alarmas de Amazon.

     Esta columna muestra uno de los siguientes valores:

     - Implementado: indica que las alarmas recomendadas por él AWS Resilience Hub están implementadas en su aplicación. Al elegir el número siguiente, se filtrará la tabla Alarmas para mostrar todas las alarmas recomendadas que están implementadas en su aplicación.
     - No implementadas: indica que las alarmas recomendadas por la aplicación AWS Resilience Hub están incluidas, pero no están implementadas, en la aplicación. Al elegir el número siguiente, se filtrará la tabla Alarmas para mostrar todas las alarmas recomendadas que no están implementadas en la aplicación.
     - Excluidas: indica que las alarmas recomendadas por AWS Resilience Hub están excluidas de la aplicación. Al elegir el número siguiente, se filtrará la tabla Alarmas para mostrar todas las alarmas recomendadas que están excluidas de la aplicación. Para obtener más información sobre cómo incluir y excluir las alarmas recomendadas, consulte Incluir o excluir recomendaciones operativas.
     - Inactivo: indica que las alarmas están desplegadas en Amazon CloudWatch, pero el estado está establecido en INSUFFICIENT_DATA en Amazon. CloudWatch Si selecciona el número siguiente, se filtrará la tabla Alarmas para mostrar todas las alarmas implementadas e inactivas.

   - Configuración: indica si hay alguna dependencia de configuración pendiente que deba abordarse.
   - Tipo: indica el tipo de alarma.
   - AppComponent— Indica los componentes de la aplicación (AppComponents) que están asociados a esta alarma.
   - ID de referencia: indica el identificador lógico del evento de AWS CloudFormation pila en AWS CloudFormation.
   - ID de recomendación: indica el identificador lógico del recurso de AWS CloudFormation pila en AWS CloudFormation.

7. En la pestaña Alarmas, para filtrar las recomendaciones de la tabla Alarmas en función de un estado específico, seleccione un número inferior al mismo.
8. Seleccione las alarmas recomendadas que desee configurar para su aplicación y elija Crear CloudFormation plantilla.
9. En el cuadro de diálogo Crear CloudFormation plantilla, puede utilizar el nombre generado automáticamente o puede introducir un nombre para la CloudFormation plantilla en el cuadro de nombre de la CloudFormation plantilla.
10. Seleccione Crear. La creación de la AWS CloudFormation plantilla puede tardar unos minutos.

    Complete el siguiente procedimiento para incluir las recomendaciones en la base de código.

Para incluir las AWS Resilience Hub recomendaciones, su código base

1. Seleccione la pestaña Plantillas para ver la plantilla que acaba de crear. Puede identificar las plantillas de la siguiente manera:

   - Nombre: nombre de la evaluación que proporcionó en el momento de la creación.
   - Estado: indica el estado de ejecución de la evaluación.
   - Tipo: indica el tipo de recomendación operativa.
   - Formato: indica el formato (JSON/texto) en el que se crea la plantilla.
   - Hora de inicio: indica la hora de inicio de la evaluación.
   - Hora de finalización: indica la hora de finalización de la evaluación.
   - ARN: el ARN de la plantilla
2. En Detalles de la plantilla, seleccione el enlace situado debajo de la Ruta de plantillas S3 para abrir el objeto de plantilla en la consola de Amazon S3.
3. En la consola Amazon S3, en la tabla Objetos, elija el enlace a la carpeta Alarmas.
4. Para copiar la ruta de Amazon S3, seleccione la casilla situada delante del archivo JSON y seleccione Copiar URL.
5. Cree una AWS CloudFormation pila desde la AWS CloudFormation consola. Para obtener más información sobre la creación de una AWS CloudFormation pila, consultehttps://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html.

   Al crear la AWS CloudFormation pila, debe proporcionar la ruta de Amazon S3 que copió del paso anterior.

Visualizar alarmas

Puede ver todas las alarmas activas que ha configurado para supervisar la resiliencia de sus aplicaciones. AWS Resilience Hub utiliza CloudFormation una plantilla para almacenar los detalles de las alarmas que, a su vez, se utiliza para crear las alarmas en Amazon CloudWatch. Puede acceder a la CloudFormation plantilla mediante la URL de Amazon S3 y descargarla y colocarla en su canalización de código o crear una pila a través de la CloudFormation consola.

Para ver las alarmas desde el panel de control, seleccione Panel de control en el menú de navegación de la izquierda. En la tabla de alarmas implementadas, puede identificar las alarmas implementadas con la siguiente información:

- Aplicación afectada: nombre de las aplicaciones que han implementado esta alarma.
- Alarmas activas: indica la cantidad de alarmas activas activadas desde las aplicaciones.
- FIS en curso: indica el AWS FIS experimento que se está ejecutando actualmente para su aplicación.

Para ver las alarmas implementadas en su aplicación

1. En el menú de navegación a la izquierda, elija Aplicaciones.
2. Seleccione una aplicación de la tabla Aplicaciones.
3. En la página de resumen de la aplicación, en la tabla Alarmas implementadas se muestran todas las alarmas recomendadas que están implementadas en la aplicación.

   Para buscar una alarma específica en la tabla Alarmas implementadas, en el cuadro Buscar alarmas por texto, propiedad o valor, seleccione uno de los siguientes campos, elija una operación y, a continuación, escriba un valor.

   - Nombre de alarma: nombre de la alarma que ha configurado para la aplicación.
   - Descripción: describe el objetivo de la alarma.
   - Estado: indica el estado de implementación actual de la CloudWatch alarma de Amazon.

     Esta columna muestra uno de los siguientes valores:

     - Implementado: indica que las alarmas recomendadas por AWS Resilience Hub están implementadas en su aplicación. Seleccione el número siguiente para ver todas las alarmas recomendadas e implementadas en la pestaña Recomendaciones operativas.

- No implementadas: indica que las alarmas recomendadas por la aplicación AWS Resilience Hub están incluidas, pero no están implementadas, en la aplicación. Seleccione el número siguiente para ver todas las alarmas recomendadas y no implementadas en la pestaña Recomendaciones operativas.
- Excluidas: indica que las alarmas recomendadas por AWS Resilience Hub están excluidas de la aplicación. Seleccione el número siguiente para ver todas las alarmas recomendadas y excluidas en la pestaña Recomendaciones operativas. Para obtener más información sobre cómo incluir y excluir las alarmas recomendadas, consulte Incluir o excluir recomendaciones operativas.
- Inactivo: indica que las alarmas están desplegadas en Amazon CloudWatch, pero el estado está establecido en INSUFFICIENT_DATA en Amazon. CloudWatch Seleccione el número siguiente para ver todas las alarmas implementadas e inactivas en la pestaña Recomendaciones operativas.

- Plantilla de origen: proporciona el nombre de recurso de Amazon (ARN) de la AWS CloudFormation pila que contiene los detalles de la alarma.
- Recurso: muestra los recursos a los que está asociada esta alarma y para los que se implementó.
- Métrica: muestra la CloudWatch métrica de Amazon asignada a la alarma. Para obtener más información sobre CloudWatch las métricas de Amazon, consulta Amazon CloudWatch Metrics.
- Último cambio: muestra la fecha y la hora en que se modificó por última vez una alarma.

Para ver las alarmas recomendadas a partir de las evaluaciones

1. En el menú de navegación a la izquierda, elija Aplicaciones.
2. Seleccione una aplicación de la tabla Aplicaciones.

   Para buscar una aplicación, introduzca el nombre de la aplicación en el cuadro Buscar aplicaciones.
3. Seleccione la pestaña Evaluaciones.

   En la tabla Evaluaciones de resiliencia, puede identificar sus evaluaciones con la siguiente información:

   - Nombre: nombre de la evaluación que proporcionó en el momento de la creación.

- Estado: indica el estado de ejecución de la evaluación.
- Estado de conformidad: indica si la evaluación cumple con la política de resiliencia.
- Estado de desviación de la resiliencia: indica si su aplicación se ha desviado o no de la última evaluación satisfactoria.
- Versión de la aplicación: versión de su aplicación.
- Invocador: indica el rol que invocó la evaluación.
- Hora de inicio: indica la hora de inicio de la evaluación.
- Hora de finalización: indica la hora de finalización de la evaluación.
- ARN: el nombre de recurso de Amazon (ARN) de la evaluación.

4. Seleccione una evaluación de la tabla Evaluaciones de resiliencia.
5. Seleccione la pestaña Recomendaciones operativas.
6. Si no está seleccionada de forma predeterminada, seleccione la pestaña Alarmas.

   En la tabla Alarmas, puede identificar las alarmas recomendadas mediante lo siguiente:

   - Nombre: nombre de la alarma que ha configurado para su aplicación.
   - Descripción: describe el objetivo de la alarma.
   - Estado: indica el estado de implementación actual de las CloudWatch alarmas de Amazon.

     Esta columna muestra uno de los siguientes valores:

     - Implementada: indica que la alarma está implementada en su aplicación. Al elegir el número siguiente, se filtrará la tabla Alarmas para mostrar todas las alarmas recomendadas que están implementadas en su aplicación.
     - No implementada: indica que la alarma no está implementada ni incluida en la aplicación. Al elegir el número siguiente, se filtrará la tabla Alarmas para mostrar todas las alarmas recomendadas que no están implementadas en la aplicación.
     - Excluida: indica que la alarma está excluida de la aplicación. Al elegir el número siguiente, se filtrará la tabla Alarmas para mostrar todas las alarmas recomendadas que están excluidas de la aplicación. Para obtener más información sobre cómo incluir y excluir las alarmas recomendadas, consulte the section called “Incluir o excluir recomendaciones operativas”.
     - Inactivo: indica que las alarmas están desplegadas en Amazon CloudWatch, pero el estado está establecido en INSUFFICIENT_DATA en Amazon. CloudWatch Si selecciona el

número siguiente, se filtrará la tabla Alarmas para mostrar todas las alarmas implementadas e inactivas.

- Configuración: indica si hay alguna dependencia de configuración pendiente que deba abordarse.
- Tipo: indica el tipo de alarma.
- AppComponent— Indica los componentes de la aplicación (AppComponents) que están asociados a esta alarma.
- ID de referencia: indica el identificador lógico del evento de AWS CloudFormation pila en AWS CloudFormation.
- ID de recomendación: indica el identificador lógico del recurso de AWS CloudFormation pila en AWS CloudFormation.

Gestión de los procedimientos operativos estándar

Un procedimiento operativo estándar (SOP) es un conjunto prescriptivo de pasos diseñado para recuperar la aplicación de manera eficiente en caso de una interrupción o alarma. Prepárese, pruebe y mida sus datos con SOPs antelación para garantizar una recuperación oportuna en caso de que se produzca una interrupción operativa.

En función de los componentes de su aplicación, SOPs le AWS Resilience Hub recomienda que se prepare. AWS Resilience Hub trabaja con Systems Manager para automatizar sus pasos SOPs al proporcionar una serie de documentos SSM que puede utilizar como base para ellos SOPs.

Por ejemplo, AWS Resilience Hub puede recomendar un SOP para añadir espacio en disco basándose en un documento de automatización de SSM existente. Para ejecutar este documento SSM, necesita una función de IAM específica con los permisos correctos. AWS Resilience Hub crea metadatos en la aplicación que indican qué documento de automatización de SSM se debe ejecutar en caso de escasez de disco y qué función de IAM se requiere para ejecutar ese documento de SSM. A continuación, estos metadatos se guardan en un parámetro SSM.

Además de configurar la automatización de SSM, también se recomienda probarla con un experimento de AWS FIS . Por lo tanto, AWS Resilience Hub también incluye un AWS FIS experimento denominado documento de automatización SSM. De esta forma, puede probar su aplicación de forma proactiva para asegurarse de que el SOP que ha creado cumple con el objetivo previsto.

AWS Resilience Hub proporciona sus recomendaciones en forma de CloudFormation plantilla que puede añadir a la base de código de la aplicación. Esta plantilla proporciona:

- El rol de IAM con los permisos necesarios para ejecutar el SOP.
- Un AWS FIS experimento que puede utilizar para probar el SOP.
- Un parámetro de SSM que contiene metadatos de la aplicación que indican qué documento SSM y qué rol de IAM se van a ejecutar como SOP y en qué recurso. Por ejemplo: `$(DocumentName) for SOP $(HandleCrisisA) on $(ResourceA)`.

La creación de un SOP puede requerir un poco de prueba y error. Realizar una evaluación de resiliencia en función de tu aplicación y generar una CloudFormation plantilla a partir de las AWS Resilience Hub recomendaciones es un buen comienzo. Utilice la CloudFormation plantilla para generar una CloudFormation pila y, a continuación, utilice los parámetros del SSM y sus valores predeterminados en el SOP. Ejecute el SOP y compruebe qué mejoras necesita realizar.

Como todas las aplicaciones tienen requisitos diferentes, la lista predeterminada de documentos SSM que AWS Resilience Hub proporciona no será suficiente para todas sus necesidades. Sin embargo, puede copiar los documentos SSM predeterminados y utilizarlos como base para crear sus propios documentos personalizados adaptados a su aplicación. También puede crear sus propios documentos SSM completamente nuevos. Si crea sus propios documentos SSM en lugar de modificar los valores predeterminados, debe asociarlos a los parámetros SSM para que se llame al documento SSM correcto cuando se ejecute el SOP.

Cuando haya finalizado el SOP creando los documentos SSM necesarios y actualizando las asociaciones de parámetros y documentos según sea necesario, añada los documentos SSM directamente a su base de código y realice allí los cambios o personalizaciones posteriores. De esta forma, cada vez que despliegues tu aplicación, también desplegarás la mayor parte up-to-date del SOP.

Temas

Creación de un SOP en función de las recomendaciones AWS Resilience Hub

Para crear un SOP basado en AWS Resilience Hub las recomendaciones, se necesita una AWS Resilience Hub aplicación que vaya acompañada de una política de resiliencia y se debe haber realizado una evaluación de la resiliencia en función de esa aplicación. La evaluación de resiliencia genera las recomendaciones para su SOP.

Para crear un SOP basado en AWS Resilience Hub las recomendaciones, debe crear una CloudFormation plantilla para las recomendadas SOPs e incluirlas en su base de código.

Cree una CloudFormation plantilla para las recomendaciones del SOP

1. Abre la AWS Resilience Hub consola.
2. En el panel de navegación, elija Aplicaciones.
3. En la lista de aplicaciones, seleccione la aplicación para la que desee crear un SOP.
4. Seleccione la pestaña Evaluaciones.
5. Seleccione una evaluación de la tabla Evaluaciones de resiliencia. Si no tiene una evaluación, complete el procedimiento de the section called “Realizar evaluaciones de resiliencia en AWS Resilience Hub” y, a continuación, vuelva a este paso.
6. En Recomendaciones operativas, seleccione Procedimientos operativos estándar.
7. Seleccione todas las recomendaciones del SOP que desee incluir.
8. Selecciona Crear CloudFormation plantilla. La creación de la AWS CloudFormation plantilla puede tardar unos minutos.

   Complete el siguiente procedimiento para incluir las recomendaciones del SOP en la base de código.

Para incluir las AWS Resilience Hub recomendaciones en su base de código

1. En Recomendaciones operativas, seleccione Plantillas.
2. En la lista de plantillas, seleccione el nombre de la plantilla de SOP que acaba de crear.

   Puede identificar las SOPs que están implementadas en su aplicación con la siguiente información:

   - Nombre del SOP: nombre del SOP que ha definido para la aplicación.
   - Descripción: describe el objetivo del SOP.

- Documento SSM: URL de Amazon S3 del documento SSM que contiene la definición de SOP.
- Ejecución de prueba: URL de Amazon S3 del documento que contiene los resultados de la última prueba.
- Plantilla de origen: proporciona el nombre de recurso de Amazon (ARN) de la AWS CloudFormation pila que contiene los detalles del SOP.

3. En Detalles de la plantilla, seleccione el enlace de la ruta S3 de las plantillas para abrir el objeto de plantilla en la consola de Amazon S3.
4. En la consola de Amazon S3, en la tabla Objetos, seleccione el enlace a la carpeta SOP.
5. Para copiar la ruta de Amazon S3, seleccione la casilla situada delante del archivo JSON y seleccione Copiar URL.
6. Cree una AWS CloudFormation pila desde AWS CloudFormation la consola. Para obtener más información sobre cómo crear una pila AWS CloudFormation , consulte https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html.

   Al crear la AWS CloudFormation pila, debe proporcionar la ruta de Amazon S3 que copió del paso anterior.

Crear un documento SSM personalizado

Para automatizar completamente la recuperación de la aplicación, es posible que necesite crear un documento SSM personalizado para el SOP en la consola de Systems Manager. Puede modificar un documento SSM existente como base o puede crear un documento SSM nuevo.

Para obtener información detallada sobre el uso de Systems Manager para crear un documento SSM, consulte Tutorial: Uso de Document Builder para crear un manual de procedimientos personalizado.

Para obtener información sobre la sintaxis de los documentos SSM, consulte Sintaxis de los documentos SSM.

Para obtener información sobre la automatización de acciones de documentos SSM, consulte la referencia de acciones de automatización de Systems Manager.

Uso de un documento SSM personalizado en lugar del predeterminado

Para reemplazar el documento SSM AWS Resilience Hub sugerido para su SOP por un documento personalizado que haya creado, trabaje directamente en su base de código. Además de añadir su nuevo documento de automatización de SSM personalizado, también podrá:

1. Añadir los permisos de IAM necesarios para ejecutar la automatización.
2. Agrega un AWS FIS experimento para probar tu documento SSM.
3. Añadir un parámetro SSM que apunte al documento de automatización que desee utilizar como SOP.

Por lo general, lo más eficaz es trabajar con los valores predeterminados sugeridos AWS Resilience Hub y personalizarlos según sea necesario. Por ejemplo, añada o elimine los permisos necesarios para la función de IAM, cambie la configuración del AWS FIS experimento para que apunte al nuevo documento SSM o cambie el parámetro SSM para que apunte al nuevo documento SSM.

¿Probando SOPs

Como se ha mencionado anteriormente, la mejor práctica consiste en añadir AWS FIS experimentos a tus CI/CD canalizaciones para probarlas SOPs periódicamente; de esta forma, te asegurarás de que estén listas para funcionar en caso de que se produzca una interrupción.

Realice pruebas tanto AWS Resilience Hub proporcionadas como personalizadas. SOPs

Visualización de los procedimientos operativos estándar

Para ver lo implementado SOPs desde las aplicaciones

1. En el menú de navegación a la izquierda, elija Aplicaciones.
2. En Aplicaciones, abra una aplicación.
3. Seleccione la pestaña Procedimientos operativos estándar.

   En la sección de resumen de los procedimientos operativos estándar, la tabla de procedimientos operativos estándar implementados muestra la lista de los SOPs que se generan a partir de las recomendaciones del SOP.

   Puede identificarlos de SOPs la siguiente manera:

   - Nombre del SOP: nombre del SOP que ha definido para la aplicación.
   - Documento SSM: URL de S3 del documento de Amazon EC2 Systems Manager que contiene la definición del SOP.
   - Descripción: describe el objetivo del SOP.
   - Ejecución de la prueba: URL de S3 del documento que contiene los resultados de la última prueba.

- ID de referencia: identificador de la recomendación del SOP a la que se hace referencia.
- ID de recurso: identificador del recurso para el que se implementa la recomendación del SOP.

Para ver las SOPs evaluaciones recomendadas

1. En el menú de navegación a la izquierda, elija Aplicaciones.
2. Seleccione una aplicación de la tabla Aplicaciones.

   Para buscar una aplicación, introduzca el nombre de la aplicación en el cuadro Buscar aplicaciones.
3. Seleccione la pestaña Evaluaciones.

   En la tabla Evaluaciones de resiliencia, puede identificar sus evaluaciones con la siguiente información:

   - Nombre: nombre de la evaluación que proporcionó en el momento de la creación.
   - Estado: indica el estado de ejecución de la evaluación.
   - Estado de conformidad: indica si la evaluación cumple con la política de resiliencia.
   - Estado de desviación de la resiliencia: indica si su aplicación se ha desviado o no de la última evaluación satisfactoria.
   - Versión de la aplicación: versión de su aplicación.
   - Invocador: indica el rol que invocó la evaluación.
   - Hora de inicio: indica la hora de inicio de la evaluación.
   - Hora de finalización: indica la hora de finalización de la evaluación.
   - ARN: el nombre de recurso de Amazon (ARN) de la evaluación.
4. Seleccione una evaluación de la tabla Evaluaciones de resiliencia.
5. Seleccione la pestaña Recomendaciones operativas.
6. Seleccione la pestaña Procedimientos operativos estándar.

   En la tabla de procedimientos operativos estándar, puede obtener más información sobre lo recomendado SOPs utilizando la siguiente información:

   - Nombre: nombre del SOP recomendado.
   - Descripción: describe el objetivo del SOP.

- Estado: indica el estado de implementación actual del SOP. Es decir, Implementado, No implementado y Excluido.
- Configuración: indica si hay alguna dependencia de configuración pendiente que deba abordarse.
- Tipo: indica el tipo de SOP.
- AppComponent— Indica los componentes de la aplicación (AppComponents) que están asociados a este SOP. Para obtener más información acerca de los recursos compatibles AppComponents, consulte Agrupación de recursos en un. AppComponent
- ID de referencia: indica el identificador lógico del evento de AWS CloudFormation pila en AWS CloudFormation.
- ID de recomendación: indica el identificador lógico del recurso de la pila de AWS CloudFormation en AWS CloudFormation.

Administración AWS Fault Injection Service experimentos

En esta sección se describe cómo gestionar AWS Fault Injection Service (AWS FIS) los experimentos en AWS Resilience Hub. Realiza AWS FIS experimentos para medir la resiliencia de sus AWS recursos y el tiempo que lleva recuperarse de los incidentes relacionados con las aplicaciones, la infraestructura, las zonas de disponibilidad y las AWS regiones.

Para medir la resiliencia, estos AWS FIS experimentos simulan interrupciones en sus recursos. AWS Entre los ejemplos de interrupciones se incluyen los errores de no disponibilidad de la red, las conmutaciones por error, la interrupción de procesos en Amazon EC2 o AWS ASG, la recuperación del arranque en Amazon RDS y los problemas con la zona de disponibilidad. Cuando finalice el AWS FIS experimento, podrá estimar si una aplicación puede recuperarse de los tipos de interrupciones definidos en el objetivo de RTO de la política de resiliencia.

Todos los experimentos se AWS Resilience Hub crean utilizando acciones AWS FIS y las ejecutan AWS FIS . AWS FIS los experimentos utilizan solo acciones de AWS FIS automatización personalizadas para AWS servicios específicos (como la acción de Amazon EKS). Para obtener más información sobre AWS FIS las acciones, consulte la referencia a AWS FIS las acciones.

Puede usar los AWS FIS experimentos en su estado predeterminado o personalizarlos según sus necesidades. Para obtener más información sobre la administración de AWS FIS experimentos desde una AWS Resilience Hub AWS FIS consola y una consola, consulte los siguientes temas:

- AWS Resilience Hub consola

  - Visualización AWS FIS experimentos
    - Para ver la lista de implementados AWS FIS experimentos a partir de aplicaciones
    - Para ver las recomendadas AWS FIS experimentos a partir de evaluaciones
  - the section called “Realización de AWS FIS experimentos”
  - the section called “AWS Fault Injection Service failures/status comprobación del experimento”
- AWS FIS consola
  - Gestionar tus AWS FIS experimentos
  - Trabajando con la biblioteca de AWS FIS escenarios
  - Administrar plantillas de AWS FIS experimentos

Iniciar, crear y ejecutar AWS FIS experimentos

AWS Resilience Hub simplifica los AWS FIS experimentos al integrarse con AWS FIS los experimentos. Proporciona recomendaciones personalizadas y permite iniciar AWS FIS experimentos con plantillas rellenadas previamente asignadas a los componentes de la aplicación (AppComponents), lo que permite realizar pruebas de resiliencia eficientes.

Para iniciar un AWS FIS experimentar a partir de recomendaciones operativas

1. Abra la AWS Resilience Hub consola.
2. En el panel de navegación, elija Aplicaciones.
3. En la lista de aplicaciones, seleccione la aplicación para la que desee crear una prueba.
4. Seleccione la pestaña Evaluaciones.
5. Seleccione una evaluación de la tabla Evaluaciones de resiliencia. Si no tiene una evaluación, complete el procedimiento de the section called “Realizar evaluaciones de resiliencia en AWS Resilience Hub” y, a continuación, vuelva a este paso.
6. Seleccione la pestaña Recomendaciones operativas.
7. Elija la flecha derecha antes de los experimentos de Fault Injection.

   En esta sección se enumeran todos los AWS FIS experimentos recomendados por su aplicación AWS Resilience Hub para realizar pruebas de esfuerzo y mejorar su resiliencia. Según su implementación, los AWS FIS experimentos se clasifican en los siguientes estados:

- Implementado: indica que los experimentos recomendados por AWS Resilience Hub están implementados en su aplicación. Elija el número que aparece a continuación para ver todos los experimentos implementados en la tabla Experimentos.
- Implementado parcialmente: indica que los experimentos recomendados por AWS Resilience Hub se implementaron parcialmente en su aplicación. Elija el número que aparece a continuación para ver todos los experimentos implementados parcialmente en la tabla Experimentos.
- No implementado: indica que los experimentos recomendados por no AWS Resilience Hub están implementados en su aplicación. Elija el número que aparece a continuación para ver todos los experimentos no implementados en la tabla Experimentos.
- Excluido: indica que los experimentos recomendados por AWS Resilience Hub están excluidos de su aplicación. Elija el número siguiente para ver todos los experimentos excluidos en la tabla Experimentos. Para obtener más información sobre cómo incluir y excluir los experimentos recomendados, consulte Incluir o excluir recomendaciones operativas.

La tabla Experimentos muestra todos los experimentos de AWS FIS implementados que afectan a la puntuación de resiliencia de la aplicación. Puede identificar los AWS FIS experimentos con la siguiente información:

- Nombre de la acción: indica la AWS FIS acción recomendada para la aplicación. Elige el nombre de la acción para ver todas las recomendaciones AppComponents en la página de detalles del AWS FIS experimento. Cuando el Estado se establece en No se puede rastrear, indica que el experimento de AWS FIS es un escenario. Elija el nombre del escenario para ver sus detalles en la página de la Biblioteca de escenarios de la consola de AWS FIS .
- Estado: indica el estado actual de implementación del AWS FIS experimento. Es decir, Implementado, Implementado parcialmente, No implementado y Excluido.

> **Note**
>
> AWS FIS El escenario es una función exclusiva de la consola con varias acciones predefinidas. Por lo tanto, AWS Resilience Hub no puede rastrearlo y establecerá el estado en No rastreable.

- Descripción: describe el objetivo de la AWS FIS acción.

8. Seleccione una AWS FIS acción para la que desee iniciar un experimento.

En la sección de recomendaciones de AWS FIS experimentos, puedes obtener más información sobre los experimentos que necesitas implementar AppComponents utilizando la siguiente información:

- Nombre: nombre del grupo AppComponent en el que se agrupan los recursos.
- Estado: indica el estado actual de implementación de la AWS FIS acción. Es decir, Implementado, Implementado parcialmente, No implementado y Excluido.

> **Note**
>
> AWS FIS El escenario es una función exclusiva de la consola con varias acciones predefinidas. Por lo tanto, AWS Resilience Hub no puede rastrearlo y establecerá el estado en No rastreable.

- Selección de objetivos: indica cómo se incluirán los recursos en el experimento al elegir Iniciar experimento. Si AWS Resilience Hub no determina automáticamente los recursos objetivo, coloca el cursor sobre el campo de selección de objetivos correspondiente para obtener información sobre cómo agregarlos.
- Recursos: indica la cantidad de recursos agrupados en. AppComponent Elija el número para ver estos recursos en el cuadro de diálogo Recursos. Puede identificar los recursos mediante lo siguiente:
  - ID lógico: indica el ID lógico del recurso. Un identificador lógico es un nombre que se utiliza para identificar los recursos de su archivo de estado de Terraform AWS CloudFormation, de su aplicación MyApplications, de un Grupos de recursos de AWS recurso o de un clúster de Amazon Elastic Kubernetes Service.
  - ID físico: indica el identificador real asignado al recurso, como un ID de instancia de Amazon EC2 o un nombre de bucket de Amazon S3.
  - Tipo: indica el tipo de recurso.
  - Región: indica la región de AWS en la que se encuentra el recurso.

9. Seleccione uno AppComponent y elija Incluir o Excluir para incluirlo o excluirlo AppComponent en el experimento, respectivamente. AWS FIS
10. Seleccione Iniciar experimento.

    AWS Resilience Hub lo redirigirá a la página Especificar detalles de la plantilla en la AWS FIS consola y la abrirá en una pestaña nueva.

11. Para crear una plantilla de experimento, siga los pasos descritos en Para crear una plantilla de experimento con la consola.

    Además, después de introducir los detalles de la plantilla y elegir Siguiente en la página Especificar detalles de la plantilla de la AWS FIS consola, siga los pasos que se indican en Para crear una plantilla de experimento mediante la consola, AWS Resilience Hub intentará asignar automáticamente las acciones y los objetivos a los tipos de recursos en la página Acciones y objetivos. Sin embargo, para mejorar la cobertura, puede agregar acciones y objetivos manualmente seleccionando Agregar acción y Agregar objetivo, respectivamente, y completar el resto del procedimiento para crear el experimento.

Ejecutar AWS FIS experimentos

Tras crear un experimento en la AWS FIS consola, sigue los pasos que se indican en Iniciar un experimento a partir de una plantilla para ejecutar un experimento en AWS FIS la consola. Si quieres AWS Resilience Hub detectar los experimentos más recientes en los que has AWS FIS realizado, debes realizar una nueva evaluación. Para obtener más información sobre cómo ejecutar evaluaciones, consulte Realizar evaluaciones de resiliencia en AWS Resilience Hub.

Visualización AWS FIS experimentos

En AWS Resilience Hub, consulta los AWS FIS experimentos que configuraste para medir la resiliencia de tus AWS recursos y el tiempo que lleva recuperarse de las aplicaciones, la infraestructura, la zona de disponibilidad y Región de AWS los incidentes.

Para ver la lista de AWS FIS experimentos activos en el panel de control, seleccione Panel de control en el menú de navegación de la izquierda.

En la tabla Experimentos implementados, puede identificar los AWS FIS experimentos con la siguiente información:

- ID del experimento: identificador del experimento de AWS FIS .
- Acción: indica la AWS FIS acción asociada al AWS FIS experimento. Además, si hay más de una acción, resalta el número de AWS FIS acciones asociadas al AWS FIS experimento. Puede identificar los detalles pasando el cursor sobre ellos o navegando hasta ellos.
- ID de plantilla de experimento: identificador de la plantilla de AWS FIS experimento que se utilizó para crear el AWS FIS experimento.

Para ver la lista de implementados AWS FIS experimentos a partir de aplicaciones

1. En el menú de navegación a la izquierda, elija Aplicaciones.
2. Seleccione una aplicación de la tabla Aplicaciones.

   Para buscar una aplicación, introduzca el nombre de la aplicación en el cuadro Buscar aplicaciones.
3. Seleccione Experimentos de inyección de errores.

   En la tabla Experimentos implementados, puede identificar los AWS FIS experimentos implementados en su aplicación mediante la siguiente información:

   - ID del experimento: identificador del experimento de AWS FIS .
   - Acción: indica la AWS FIS acción asociada al AWS FIS experimento. Además, si hay más de una acción, resalta el número de AWS FIS acciones asociadas al AWS FIS experimento. Puede identificar los detalles pasando el cursor sobre ellos o navegando hasta ellos.
   - ID de la plantilla de experimentos: identificador de la plantilla de experimentos de AWS FIS utilizada para crear el experimento de AWS FIS .

Para ver las recomendadas AWS FIS experimentos a partir de evaluaciones

1. En el menú de navegación a la izquierda, elija Aplicaciones.
2. Seleccione una aplicación de la tabla Aplicaciones.

   Para buscar una aplicación, introduzca el nombre de la aplicación en el cuadro Buscar aplicaciones.
3. Seleccione la pestaña Evaluaciones.

   En la tabla Evaluaciones, puede identificar sus evaluaciones con la siguiente información:

   - Nombre: nombre de la evaluación que proporcionó en el momento de la creación.
   - Estado: indica el estado de ejecución de la evaluación.
   - Estado de conformidad: indica si la evaluación cumple con la política de resiliencia.
   - Resiliencia: indica si su aplicación se ha desviado de los objetivos de RTO y RPO definidos en la política de resiliencia adjunta o no con respecto a la evaluación satisfactoria anterior.
   - Versión de la aplicación: versión de la aplicación que se evaluó.
   - Invocador: indica el rol que invocó la evaluación.

- Hora de inicio: indica la hora de inicio de la evaluación.
- Hora de finalización: indica la hora de finalización de la evaluación.
- ARN: el nombre de recurso de Amazon (ARN) de la evaluación.

4. Seleccione una evaluación de la tabla Evaluaciones.
5. Seleccione Recomendaciones operativas.
6. Seleccione la flecha derecha antes de los experimentos de Fault Injection.

En esta sección se enumeran todos los AWS FIS experimentos recomendados por su aplicación AWS Resilience Hub para realizar pruebas de esfuerzo y mejorar su resiliencia. Según su implementación, los AWS FIS experimentos se clasifican en los siguientes estados:

- Implementado: indica que los experimentos recomendados por AWS Resilience Hub están implementados en su aplicación. Elija el número que aparece a continuación para ver todos los experimentos implementados en la tabla Experimentos.
- Implementado parcialmente: indica que los experimentos recomendados por AWS Resilience Hub se implementaron parcialmente en su aplicación. Elija el número que aparece a continuación para ver todos los experimentos implementados parcialmente en la tabla Experimentos.
- No implementado: indica que los experimentos recomendados por no AWS Resilience Hub están implementados en su aplicación. Elija el número que aparece a continuación para ver todos los experimentos no implementados en la tabla Experimentos.
- Excluido: indica que los experimentos recomendados por AWS Resilience Hub están excluidos de su aplicación. Elija el número siguiente para ver todos los experimentos excluidos en la tabla Experimentos. Para obtener más información sobre cómo incluir y excluir los experimentos recomendados, consulte Incluir o excluir recomendaciones operativas.

La tabla Experimentos muestra todos los experimentos de AWS FIS implementados que afectan a la puntuación de resiliencia de la aplicación. Puede identificar los AWS FIS experimentos con la siguiente información:

- Nombre de la acción: indica la AWS FIS acción recomendada para la aplicación. Cuando el Estado se establece en No se puede rastrear, indica que el experimento de AWS FIS es un escenario. Elija el nombre del escenario para ver sus detalles en la página de la Biblioteca de escenarios de la consola de AWS FIS .

- Estado: indica el estado actual de implementación del AWS FIS experimento. Es decir, Implementado, Implementado parcialmente, No implementado y Excluido.

> **Note**
>
> AWS FIS El escenario es una función exclusiva de la consola con varias acciones predefinidas. Por lo tanto, AWS Resilience Hub no puede rastrearlo y establecerá el estado en No rastreable.

- Descripción: describe el objetivo de la AWS FIS acción.

AWS Fault Injection Service failures/status comprobación del experimento

AWS Resilience Hub le permite realizar un seguimiento del estado del experimento que ha iniciado. Para obtener más información, consulte el Para ver las recomendadas AWS FIS experimentos a partir de evaluaciones procedimiento.

Temas

- Analizando AWS FIS ejecución del experimento usando AWS Systems Manager
- AWS FIS experimente errores al probar los pods de Kubernetes que se ejecutan en sus clústeres de Amazon Elastic Kubernetes Service

Analizando AWS FIS ejecución del experimento usando AWS Systems Manager

Tras ejecutar un AWS FIS experimento, puede ver los detalles de la ejecución en el administrador de AWS sistemas.

1. Vaya a CloudTrail > Historial de eventos.
2. Filtre los eventos por Nombre de usuario mediante el ID del experimento.
3. Ver la StartAutomationExecution entrada. El ID de solicitud es el ID de automatización de SSM.
4. Vaya a AWS Systems Manager > Automatización.
5. Filtre por ID de ejecución mediante el ID de automatización de SSM y vea la información relativa a la automatización.

   Puede analizar la ejecución con cualquier automatización de Systems Manager. Para obtener más información, consulte la Guía del usuario de Automatización de AWS Systems Manager.

Los parámetros de entrada de la ejecución aparecen en la sección Parámetros de entrada de los detalles de la ejecución e incluyen parámetros opcionales que no aparecen en el AWS FIS experimento.

Puede encontrar información sobre el estado de los pasos y otra información de los pasos si profundiza en los pasos específicos de los pasos de ejecución.

Errores comunes

Los siguientes son errores comunes que se producen al ejecutar un informe de evaluación:

- La plantilla de alarma no se implementó antes de que se ejecutara el Test/SOP experimento. Esto provoca un mensaje de error durante el paso de automatización.
  - Mensaje de error: `The following parameters were not found: [/ResilienceHub/Alarm/3dee49a1-9877-452a-bb0c-a958479a8ef2/nat-gw-alarm-bytes-out-to-source-2020-09-21_nat-02ad9bc4fbd4e6135]. Make sure all the SSM parameters in automation document are created in SSM Parameter Store.`
  - Solución: asegúrese de emitir la alarma correspondiente e implementar la plantilla resultante antes de volver a ejecutar el experimento de inyección de errores.
- Faltan permisos en el rol de ejecución. Este mensaje de error aparece si al rol de ejecución proporcionado le falta un permiso y aparece en la información relativa al paso.
  - Mensaje de error: `An error occurred (Unauthorized Operation) when calling the DescribeInstanceStatus operation: You are not authorized to perform this operation. Please Refer to Automation Service Troubleshooting Guide for more diagnosis details.`
  - Solución: compruebe que ha proporcionado el rol de ejecución correcto. Si lo ha hecho, añada el permiso necesario y vuelva a ejecutar la evaluación.
- La ejecución se realizó correctamente, pero no obtuvo el resultado esperado. Esto se debe a parámetros incorrectos o a un problema de automatización interna.
  - Mensaje de error: la ejecución se ha realizado correctamente, por lo que no se muestra ningún mensaje de error.
  - Solución: compruebe los parámetros de entrada y observe los pasos ejecutados, tal como se explica en el artículo Analice la ejecución del AWS FIS experimento, antes de examinar los pasos individuales para determinar las entradas y salidas esperadas.

AWS FIS experimente errores al probar los pods de Kubernetes que se ejecutan en sus clústeres de Amazon Elastic Kubernetes Service

A continuación, se muestran los errores más comunes de Amazon Elastic Kubernetes Service (Amazon EKS) que se producen al probar los pods de Kubernetes que se ejecutan en los clústeres de Amazon EKS:

- Configuración incorrecta de las funciones de IAM para los AWS FIS experimentos o la cuenta de servicio de Kubernetes.
  - Mensajes de error:
    - `Error resolving targets. Kubernetes API returned ApiException with error code 401`.
    - `Error resolving targets. Kubernetes API returned ApiException with error code 403`.
    - `Unable to inject AWS FIS Pod: Kubernetes API returned status code 403. Check Amazon EKS logs for more details`.
  - Solución: compruebe lo siguiente.
    - Asegúrese de haber seguido las instrucciones descritas en Utilizar las acciones de AWS FIS`aws:eks:pod`.
    - Asegúrese de haber creado y configurado una cuenta de servicio de Kubernetes con los permisos RBAC necesarios y el espacio de nombres correcto.
    - Asegúrese de haber asignado la función de IAM proporcionada (consulte el resultado de la CloudFormation pila de la prueba) al usuario de Kubernetes.
- No se puede iniciar el AWS FIS pod: se ha alcanzado el número máximo de contenedores fallidos en el sidecar. Esto suele ocurrir cuando la memoria no es suficiente para ejecutar el contenedor del AWS FIS sidecar.
  - Mensaje de error: `Unable to heartbeat FIS Pod: Max failed sidecar containers reached`.
  - Solución: una opción para evitar este error es reducir el porcentaje de carga objetivo para alinearlo con la memoria o la CPU disponibles.
- La afirmación de la alarma falló al principio del experimento. Este error se produce porque la alarma relacionada no tiene ningún punto de datos.
  - Mensaje de error: `Assertion failed for the following alarms`. Muestra todas las alarmas en las que se ha producido un error en la afirmación.

- Solución: asegúrese de que Container Insights esté correctamente instalado para las alarmas y que la alarma no esté activada (en estado `ALARM`).

Comprender las puntuaciones de resiliencia

En esta sección se describe cómo se AWS Resilience Hub cuantifica la preparación de las aplicaciones en diferentes escenarios de interrupción.

AWS Resilience Hub proporciona una puntuación de resiliencia que representa la postura de resiliencia de la aplicación. Esta puntuación refleja en qué medida la aplicación sigue nuestras recomendaciones para cumplir con la política de resiliencia, las alarmas, los procedimientos operativos estándar (SOPs) y las pruebas de la aplicación. Según el tipo de recursos que utilice la aplicación, AWS Resilience Hub recomienda alarmas y un conjunto de pruebas para cada tipo de interrupción. SOPs

La puntuación máxima de resiliencia es de 100 puntos. Para lograr la mejor puntuación posible o la máxima puntuación, debe implementar todas las alarmas y pruebas recomendadas en su aplicación. SOPs Por ejemplo, AWS Resilience Hub recomienda una prueba con una alarma y un SOP. La prueba se ejecuta, activa la alarma e inicia el SOP asociado. Si funcionan correctamente y si la aplicación cumple con la política de resiliencia, recibirá una puntuación de resiliencia cercana o igual a 100 puntos.

Tras ejecutar la primera evaluación, AWS Resilience Hub ofrece la opción de excluir las recomendaciones operativas de la aplicación. Para comprender la repercusión de las recomendaciones excluidas en la puntuación de resiliencia, debe realizar una nueva evaluación. Sin embargo, siempre puede incluir las recomendaciones excluidas en su aplicación y realizar una nueva evaluación. Para obtener más información sobre cómo incluir y excluir las recomendaciones de alarmas, SOP y pruebas, consulte the section called “Incluir o excluir recomendaciones operativas”.

Acceder a la puntuación de resiliencia de sus aplicaciones

Para ver la puntuación de resiliencia de su aplicación, seleccione Panel de control o Aplicaciones en el menú de navegación.

Acceder a la puntuación de resiliencia desde el panel

1. En el menú de navegación izquierdo, elija Panel.
2. En Puntuación de resiliencia de las aplicaciones a lo largo del tiempo, seleccione una o más aplicaciones en la lista desplegable Elegir hasta 4 aplicaciones.

3. En el gráfico Puntuación de resiliencia se muestra la puntuación de resiliencia de todas las aplicaciones elegidas.

Acceder a la puntuación de resiliencia desde las aplicaciones

1. En el menú de navegación a la izquierda, elija Aplicaciones.
2. En Aplicaciones, abra una aplicación.
3. Seleccione Resumen.

   El gráfico de puntuación de resiliencia muestra la tendencia de la puntuación de resiliencia de su aplicación durante un máximo de un año. AWS Resilience Hub muestra las medidas a tomar, las infracciones de las políticas de resiliencia y las recomendaciones operativas que deben abordarse para mejorar y lograr la máxima puntuación de resiliencia posible, utilizando lo siguiente:

   - Para ver los elementos de acción que deben completarse para mejorar y lograr la máxima puntuación de resiliencia posible, seleccione la pestaña Elementos de acción. Cuando se selecciona, AWS Resilience Hub muestra lo siguiente:
     - RTO/RPO: indica el número de tiempos de recuperación (RTO/RPOs) that need to be fixed to resolve the breaches in your application's resiliency policy. Choose the value to view the RTO/RPOdetalles) en el informe de evaluación de su aplicación.
     - Alarmas: indica el número de CloudWatch alarmas de Amazon recomendadas que deben implementarse en tu aplicación. Elija el valor para ver las CloudWatch alarmas de Amazon que deben corregirse en el informe de evaluación de su aplicación.
     - SOPs— Indica el número de recomendaciones SOPs que deben implementarse en su aplicación. Elija el valor para ver los SOPs que deben fijarse en el informe de evaluación de su solicitud.
     - FIS: indica el número de pruebas recomendadas que deben implementarse en la aplicación. Seleccione el valor para ver las pruebas que deben corregirse en el informe de evaluación de su aplicación.
   - Para ver la puntuación de cada componente que afecta a su puntuación de resiliencia, seleccione Desglose de puntuaciones. Cuando se selecciona esta opción, AWS Resilience Hub muestra lo siguiente:
     - Cumplimiento de RTO/RPO: indica el grado de conformidad de los componentes de la aplicación (AppComponents) con los tiempos estimados de recuperación de la carga de trabajo y los tiempos de recuperación objetivo que se definen en la política de resiliencia de

la aplicación. Elija el valor para ver las RTO/RPO estimaciones en el informe de evaluación de su aplicación.

- Alarmas implementadas: indica la contribución real de las CloudWatch alarmas de Amazon implementadas en comparación con su contribución máxima posible a la puntuación de resiliencia de su aplicación. Elija el valor para ver las CloudWatch alarmas de Amazon implementadas en el informe de evaluación de su aplicación.
- SOPs implementada: indica la contribución real de la aplicación implementada SOPs en comparación con su contribución máxima posible a la puntuación de resiliencia de su aplicación. Elija el valor para ver lo implementado SOPs en el informe de evaluación de su aplicación.
- Experimentos del FIS implementados: indica la contribución real de las pruebas implementadas en comparación con su contribución máxima posible a la puntuación de resiliencia de su aplicación. Seleccione el valor para ver las pruebas implementadas en el informe de evaluación de su aplicación.

- Para ver las infracciones de la política de resiliencia y las recomendaciones operativas, seleccione la flecha derecha para ampliar la sección Desglose de las recomendaciones operativas y de incumplimiento de la política. Cuando se expande, AWS Resilience Hub muestra lo siguiente:
  - Incumplimientos de la política de resiliencia: indica la cantidad de componentes de la aplicación que infringen la política de resiliencia de la aplicación. Seleccione el valor situado junto a RTO/RPO para ver los datos relativos en la pestaña Recomendaciones de resiliencia del informe de evaluación de su aplicación.
  - Recomendaciones operativas: indica las recomendaciones operativas que no se han implementado o ejecutado para mejorar la resiliencia de su aplicación mediante las pestañas Pendientes y Excluidas. Las recomendaciones operativas incluyen todas las recomendaciones que están inactivas y las que no se han implementado.

    Para ver las recomendaciones operativas que deben implementarse, seleccione la pestaña Pendientes. Cuando se selecciona, AWS Resilience Hub muestra lo siguiente:
    - Alarmas: indica el número de CloudWatch alarmas de Amazon recomendadas que deben implementarse.
    - SOPs— Indica el número de recomendaciones SOPs que deben implementarse.
    - FIS: indica la cantidad de pruebas recomendadas que deben implementarse.

Para ver las recomendaciones operativas que están excluidas de la aplicación, seleccione la pestaña Excluidas. Cuando se selecciona, AWS Resilience Hub muestra lo siguiente:

- Alarmas: indica el número de CloudWatch alarmas de Amazon recomendadas que están excluidas de tu aplicación.
- SOPs— Indica el número de recomendaciones SOPs que están excluidas de su solicitud.
- FIS: indica el número de pruebas recomendadas que están excluidas de la aplicación.

Calcular las puntuaciones de resiliencia

En las tablas de esta sección se explican las fórmulas que se utilizan AWS Resilience Hub para determinar los componentes de puntuación de cada tipo de recomendación y la puntuación de resiliencia de la aplicación. Todos los valores resultantes determinados AWS Resilience Hub por los componentes de calificación de cada tipo de recomendación y la puntuación de resiliencia de su solicitud se redondean al punto más cercano. Por ejemplo, si se implementaran dos de cada tres alarmas, la puntuación sería de 13,33 ((2/3) * 20) puntos. Este valor se redondeará a 13 puntos. Para obtener más información sobre las ponderaciones utilizadas en las fórmulas de las tablas, consulte la sección the section called “Ponderación AppComponents y tipos de interrupciones”.

Algunos de los componentes de puntuación solo se pueden obtener a través de la API `ScoringComponentResiliencyScore`. Para obtener más información acerca esta API, consulte ScoringComponentResiliencyScore.

Tablas

- Fórmulas para calcular el componente de puntuación de cada tipo de recomendación
- Fórmula para calcular la puntuación de resiliencia
- Fórmulas para calcular la puntuación de resiliencia y los tipos de disrupción AppComponents

En la siguiente tabla se explican las fórmulas utilizadas AWS Resilience Hub para calcular el componente de puntuación de cada tipo de recomendación.

Fórmulas para calcular el componente de puntuación de cada tipo de recomendación

Componente de puntuación	Description (Descripción)	Formula	Ejemplo
Cobertura de las pruebas (T)	Una puntuación normalizada (de 0 a 100 puntos) basada en el número de pruebas que se implementaron y excluyeron correctamente, del número total de pruebas AWS Resilience Hub recomendadas. **Note** Para calcular la puntuación de resiliencia, las pruebas recomendadas deben haberse realizado correctamente en los últimos 30 días AWS Resilience Hub para que se consideren implementadas.	`T = ((Total number of tests implemented) + (Total number of tests excluded)) / (Total number of tests recommended)` Algunas partes de la fórmula son las siguientes: • Número total de pruebas configuradas: indica el número total de pruebas configuradas cuando se crea la AWS CloudFormation plantilla y se carga en la AWS CloudFormation consola. • Número total de pruebas recomendadas: indica las pruebas recomendadas en AWS Resilience Hub función de los recursos de la aplicación. • Número total de pruebas excluidas: indica el número de pruebas recomendadas que ha excluido de la aplicación.	Si ha implementado 10 pruebas y excluido 5 de las 20 pruebas AWS Resilience Hub recomendadas, la cobertura de las pruebas se calcula de la siguiente manera: `T = (10 + 5) / 20` Es decir, `T = .75 or 75 points`

Componente de puntuación	Description (Descripción)	Formula	Ejemplo
Cobertura de alarmas (A)	Una puntuación normalizada (0 a 100 puntos) basada en el número de CloudWatch alarmas de Amazon que se han implementado y excluido correctamente, del número total de alarmas de AWS Resilience Hub Amazon CloudWatch recomendadas. **Note** Para calcular la puntuación de resiliencia, las alarmas recomendadas deben estar en estado Listo para que AWS Resilience Hub las considere implementadas.	`A = ((Total number of alarms implemented) + (Total number of alarms excluded)) / (Total number of alarms recommended)` Algunas partes de la fórmula son las siguientes: • Número total de alarmas configuradas: indica el número total de CloudWatch alarmas de Amazon configuradas al crear y cargar la AWS CloudFormation plantilla en la AWS CloudFormation consola. • Número total de alarmas recomendadas: indica las CloudWatch alarmas de Amazon recomendadas en AWS Resilience Hub función de los recursos de la aplicación. • Número total de alarmas excluidas: indica el número de CloudWatch alarmas de Amazon recomendadas que has	Si has implementado 10 alarmas de Amazon y has excluido 5 de las 20 CloudWatch alarmas AWS Resilience Hub recomendadas por Amazon CloudWatch , la cobertura de CloudWatch las alarmas de Amazon se calcula de la siguiente manera: `A = (10 + 5) / 20` Es decir, `A = .75 or 75 points`

Componente de puntuación	Description (Descripción)	Formula	Ejemplo
		excluido de la aplicación.	

Componente de puntuación	Description (Descripción)	Formula	Ejemplo
Cobertura SOP (S)	Una puntuación normalizada (de 0 a 100 puntos) basada en el número de los SOPs que se han implementado y excluido satisfactoriamente, del número total de los recomendados. AWS Resilience Hub SOPs	`S = ((Total number of SOPs implemented) + (Total number of SOPs excluded)) / (Total number of SOPs recommended)` Algunas partes de la fórmula son las siguientes: • Número total de SOPs configurados: indica el número total de SOPs configurados al crear y cargar la AWS CloudFormation plantilla en la AWS CloudFormation consola. • Número total de SOPs recomendados: indica el número SOPs recomendado en AWS Resilience Hub función de los recursos de la aplicación. • Número total de SOPs excluidos: indica el número de productos recomendados SOPs que se han excluido de la solicitud.	Si ha implementado 10 y excluido 5 SOPs de los 20 AWS Resilience Hub recomendados SOPs, la cobertura del SOP se calcula de la siguiente manera: `S = (10 + 5) / 20` Es decir, `S = .75 or 75 points`

Componente de puntuación	Description (Descripción)	Formula	Ejemplo
Conformidad con RTO/RPO (P)	Una puntuación normaliza da (0 a 100 puntos) basada en el cumplimiento de la política de resiliencia por parte de la aplicación.	`P = Total weights of disruption types meeting the application's resiliency policy / Total weights of all disruption types .`	Si la política de resiliencia de su aplicación solo se ajusta a los tipos de zona de disponibilidad (AZ) e interrupción de la infraestructura, la puntuación de la política de resilienc ia (P) se calcula de la siguiente manera: • Si ha establecido objetivos de RTO y RPO regionale s, P se calcula de la siguiente manera: `P = (20 + 30)/ 100` Es decir, `P = .5 or 50 points` • Si no ha establecido objetivos de RTO y RPO regionale s, P se calcula de la siguiente manera:

Componente de puntuación	Description (Descripción)	Formula	Ejemplo
			`P = (22.22 + 33.33)/ 99.9` Es decir, `P = .55 or 55 points`

En la siguiente tabla se explica la fórmula utilizada AWS Resilience Hub para calcular la puntuación de resiliencia de toda la aplicación.

Fórmula para calcular la puntuación de resiliencia

Componente de puntuación	Description (Descripción)	Formula	Ejemplo

Puntuación de resiliencia por aplicación (RS)	Una puntuación de resiliencia normalizada (de 0 a 100 puntos) basada en el cumplimiento de la política de resiliencia por parte de la aplicación. La puntuación de resilienc ia por aplicación es el promedio ponderado de todos los tipos de recomendaciones. Es decir: `RS = Weighted Average (T, A, S, P)`	La puntuación de resilienc ia por aplicación se calcula con la siguiente fórmula: `RS = (T * Weight(T) +`
		
		`A * Weight(A) +`
		
		`S * Weight(S) +`
		
		`P * Weight(P)) /`
		
		`(Weight(T) + Weight(A) + Weight(S) + Weight(P))`
			Las fórmulas para calcular la cobertura de cada tabla de tipos de recomendación son las siguientes:
			
			• `Test coverage (T) = .75`
			• `Alarms (A) = .75`
			• `SOPs (S) = .75`
			• `Meeting resiliency policy (P) = .5`

Componente de puntuación	Description (Descripción)	Formula	Ejemplo
			La puntuación de resiliencia por aplicación se calcula de la siguiente forma: `RS = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) /(.2 + .2 + .2 + .4)` Es decir, `RS = .65 or 65 points`

En la siguiente tabla se explican las fórmulas que se utilizan AWS Resilience Hub para calcular la puntuación de resiliencia para los componentes de la aplicación (AppComponents) y los tipos de interrupciones. Sin embargo, solo puede obtener la puntuación de resiliencia AppComponents y los tipos de interrupciones a través del siguiente centro APIs de resiliencia de AWS:

- DescribeAppAssessmentpara obtener `RSo`
- ListAppComponentCompliancesobtener `RSao` y `RSA`

Fórmulas para calcular la puntuación de resiliencia AppComponents y los tipos de disrupción

Componente de puntuación	Description (Descripción)	Formula	Ejemplo
Puntuación de resilienc ia por tipo de	Una puntuació n normaliza da (de 0 a	La puntuación de resiliencia por tipo de interrupción AppCompon	Las suposiciones `RSao` para todos los tipos de

Componente de puntuación	Description (Descripción)	Formula	Ejemplo
interrupción AppComponent y por tipo () RSao	100 puntos) basada en el AppComponent cumplimiento de su política de resiliencia por tipo de interrupción. La puntuación de resiliencia por tipo de interrupción AppComponent y por tipo es la media ponderada de todos los tipos de recomendaciones. Es decir: RSao = Weighted Average (T, A, S, P) Los valores de T, A, S, P se calculan para todas las pruebas y alarmas recomendadas y para cumplir	ent y por tipo se calcula mediante la siguiente fórmula: RSao = (T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))	recomendaciones son las siguientes: • Test coverage (T) = .75 • Alarms (A) = .75 • SOPs (S) = .75 • Meeting resiliency policy (P) = .5 La puntuación de resiliencia por tipo de interrupción AppComponent y por tipo de interrupción se calcula de la siguiente manera: RSao = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4) Es decir, RSao = .65 or 65 points

Componente de puntuación	Description (Descripción)	Formula	Ejemplo
	con la política de resilienc ia del tipo AppCompon ent de interrupción. SOPs		

Componente de puntuación	Description (Descripción)	Formula	Ejemplo
Puntuación de resiliencia por () AppComponent RSa	Una puntuación normalizada (de 0 a 100 puntos) basada en el cumplimiento de su política de resiliencia. La puntuación de resiliencia por AppComponent es la media ponderada de todos los tipos de recomendaciones. Es decir: RSa = Weighted Average (T, A, S, P) Los valores de T, A, S, P se calculan para todas las pruebas y alarmas recomendadas y para cumplir con la política de resilienc ia del. SOPs	La puntuación de resiliencia per AppComponent se calcula mediante la siguiente fórmula: RSa = (T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))	Las suposiciones RSa para todos los tipos de recomendaciones son las siguientes: • Test coverage (T) = .75 • Alarms (A) = .75 • SOPs (S) = .75 • Meeting resiliency policy (P) = .5 La puntuación de resiliencia por AppComponent se calcula de la siguiente manera: RSa = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4) Es decir, RSa = .65 or 65 points

Componente de puntuación	Description (Descripción)	Formula	Ejemplo
	AppComponent		

Componente de puntuación	Description (Descripción)	Formula	Ejemplo

Puntuación de resilienc ia por tipo de interrupción (RSo)	Una puntuació n normaliza da (de 0 a 100 puntos) basada en el cumplimiento de su política de resiliencia. La puntuació n de resilienc ia por tipo de interrupción es el promedio ponderado de todos los tipos de recomenda ciones. Es decir: `RSo = Weighted Average (T, A, S, P)`
	
	Los valores de `T, A, S, P` se calculan para todas las pruebas y alarmas recomendadas y para cumplir con la política de resilienc ia del tipo de
		La puntuación de resiliencia por tipo de interrupción se calcula con la siguiente fórmula:
		
		`RSo = (T * Weight(T) + A * Weight(A) +`
		
		`S * Weight(S) + P * Weight(P)) /`
		
		`(Weight(T) + Weight(A) + Weight(S) + Weight(P))`
			Las suposiciones `RSo` para todos los tipos de recomendaciones son las siguientes:
			
			• `Test coverage (T) = .75`
			• `Alarms (A) = .75`
			• `SOPs (S) = .75`
			• `Meeting resiliency policy (P) = .5`
			
			La puntuación de resiliencia por tipo de interrupción se calcula de la siguiente forma:
			
			`RSo = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 *.4)) /`
			
			`(.2 + .2 + .2 + .4)`
			
			Es decir, `RSo = .65 or 65 points`

Componente de puntuación	Description (Descripción)	Formula	Ejemplo
	interrupción. SOPs		

Ponderaciones

AWS Resilience Hub asigna una ponderación a cada tipo de recomendación para la puntuación de resiliencia total.

En las siguientes tablas se muestra la importancia de las alarmas, las pruebas SOPs, la política de resiliencia de las reuniones y los tipos de interrupciones. Los tipos de interrupciones incluyen aplicación, infraestructura, zona de disponibilidad y región.

> **Note**
>
> Si decide no definir los objetivos regionales de RTO o RPO para su política, las ponderaciones para los demás tipos de interrupciones se incrementarán en consecuencia, como se muestra en la columna Ponderación cuando la región no está definida.

Ponderaciones para las alarmas SOPs, las pruebas y el objetivo de la política

Tipo de recomendación	Peso
Alarmas	20 puntos
SOPs	20 puntos
Tests	20 puntos
Cumplimiento de la política de resiliencia	40 puntos

Ponderaciones por tipo de interrupción

Tipo de interrupción	Peso cuando se define la región	Peso cuando la región no está definida
Aplicación	40 puntos	44,44 puntos
Infraestructura	30 puntos	33,33 puntos
Zona de disponibilidad	20 puntos	22,22 puntos
Region	10 puntos	N/A

Integrar las recomendaciones operativas en su aplicación con CloudFormation

Tras seleccionar Crear CloudFormation plantilla en la página de recomendaciones operativas, AWS Resilience Hub crea una CloudFormation plantilla que describe la alarma, el procedimiento operativo estándar (SOP) o el AWS FIS experimento específicos para su aplicación. La CloudFormation plantilla se almacena en un bucket de Amazon S3 y puede comprobar la ruta de S3 a la plantilla en la pestaña Detalles de la plantilla de la página de recomendaciones operativas.

Por ejemplo, en la siguiente lista se muestra una CloudFormation plantilla con formato JSON que describe una recomendación de alarma proporcionada por. AWS Resilience Hub Es una alarma de limitación de lectura para una tabla de DynamoDB llamada `Employees`.

La sección `Resources` de la plantilla describe la alarma de `AWS::CloudWatch::Alarm` que se activa cuando el número de eventos de limitación de lectura de la tabla de DynamoDB supera 1. Además, los dos `AWS::SSM::Parameter` recursos definen los metadatos que permiten AWS Resilience Hub identificar los recursos instalados sin tener que escanear la aplicación real.

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",
  "Parameters" : {
    "SNSTopicARN" : {
      "Type" : "String",
      "Description" : "The ARN of the Amazon SNS topic to which alarm status changes
 are to be sent. This must be in the same Region being deployed.",
```

```
      "AllowedPattern" : "^arn:(aws|aws-cn|aws-iso|aws-iso-[a-z]{1}|aws-us-gov):sns:
([a-z]{2}-((iso[a-z]{0,1}-)|(gov-)){0,1}[a-z]+-[0-9]):[0-9]{12}:[A-Za-z0-9/][A-Za-
z0-9:_/+=,@.-]{1,256}$"
    }
  },
  "Resources" : {

 "ReadthrottleeventsthresholdexceededEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm" :
 {
      "Type" : "AWS::CloudWatch::Alarm",
      "Properties" : {
        "AlarmDescription" : "An Alarm by AWS Resilience Hub that alerts when the
 number of read-throttle events are greater than 1.",
        "AlarmName" : "ResilienceHub-ReadThrottleEventsAlarm-2020-04-01_Employees-ON-
DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9",
        "AlarmActions" : [ {
          "Ref" : "SNSTopicARN"
        } ],
        "MetricName" : "ReadThrottleEvents",
        "Namespace" : "AWS/DynamoDB",
        "Statistic" : "Sum",
        "Dimensions" : [ {
          "Name" : "TableName",
          "Value" : "Employees-ON-DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9"
        } ],
        "Period" : 60,
        "EvaluationPeriods" : 1,
        "DatapointsToAlarm" : 1,
        "Threshold" : 1,
        "ComparisonOperator" : "GreaterThanOrEqualToThreshold",
        "TreatMissingData" : "notBreaching",
        "Unit" : "Count"
      },
      "Metadata" : {
        "AWS::ResilienceHub::Monitoring" : {
          "recommendationId" : "dynamodb:alarm:health-read_throttle_events:2020-04-01"
        }
      }
    },

 "dynamodbalarmhealthreadthrottleevents20200401EmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm
 {
      "Type" : "AWS::SSM::Parameter",
      "Properties" : {
```

```
        "Name" : "/ResilienceHub/Alarm/3f904525-4bfa-430f-96ef-58ec9b19aa73/dynamodb-
alarm-health-read-throttle-events-2020-04-01_Employees-ON-DEMAND-0-DynamoDBTable-
PXBZQYH3DCJ9",
        "Type" : "String",
        "Value" : {
          "Fn::Sub" :
 "${ReadthrottleeventsthresholdexceededEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm}"
        },
        "Description" : "SSM Parameter for identifying installed resources."
      }
    },

 "dynamodbalarmhealthreadthrottleevents20200401EmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm
 {
      "Type" : "AWS::SSM::Parameter",
      "Properties" : {
        "Name" : "/ResilienceHub/Info/Alarm/3f904525-4bfa-430f-96ef-58ec9b19aa73/
dynamodb-alarm-health-read-throttle-events-2020-04-01_Employees-ON-DEMAND-0-
DynamoDBTable-PXBZQYH3DCJ9",
        "Type" : "String",
        "Value" : {
          "Fn::Sub" : "{\"alarmName\":
\"${ReadthrottleeventsthresholdexceededEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm}\",
\"referenceId\":\"dynamodb:alarm:health_read_throttle_events:2020-04-01\",
\"resourceId\":\"Employees-ON-DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9\",\"relatedSOPs\":
[\"dynamodb:sop:update_provisioned_capacity:2020-04-01\"]}"
        },
        "Description" : "SSM Parameter for identifying installed resources."
      }
    }
  }
}
```

Modificar la CloudFormation plantilla

La forma más sencilla de integrar una alarma, un SOP o un AWS FIS recurso en la aplicación principal consiste simplemente en añadirlos como otro recurso en la plantilla que describe la plantilla de la aplicación. El archivo con formato JSON que se proporciona a continuación proporciona un esquema básico de cómo se describe una tabla de DynamoDB en una plantilla. CloudFormation Es probable que una aplicación real incluya varios recursos más, como tablas adicionales.

```
{
   "AWSTemplateFormatVersion": "2010-09-09T00:00:00.000Z",
```

```
    "Description": "Application Stack with Employees Table",
    "Outputs": {
       "DynamoDBTable": {
          "Description": "The DynamoDB Table Name",
          "Value": {"Ref": "Employees"}
       }
    },
    "Resources": {
       "Employees": {
          "Type": "AWS::DynamoDB::Table",
          "Properties": {
             "BillingMode": "PAY_PER_REQUEST",
             "AttributeDefinitions": [
                {
                   "AttributeName": "USER_ID",
                   "AttributeType": "S"
                },
                {
                   "AttributeName": "RANGE_ATTRIBUTE",
                   "AttributeType": "S"
                }
             ],
             "KeySchema": [
                {
                   "AttributeName": "USER_ID",
                   "KeyType": "HASH"
                },
                {
                   "AttributeName": "RANGE_ATTRIBUTE",
                   "KeyType": "RANGE"
                }
             ],
             "PointInTimeRecoverySpecification": {
                "PointInTimeRecoveryEnabled": true
             },
             "Tags": [
                {
                   "Key": "Key",
                   "Value": "Value"
                }
             ],
             "LocalSecondaryIndexes": [
                {
                   "IndexName": "resiliencehub-index-local-1",
```

```
                  "KeySchema": [
                     {
                        "AttributeName": "USER_ID",
                        "KeyType": "HASH"
                     },
                     {
                        "AttributeName": "RANGE_ATTRIBUTE",
                        "KeyType": "RANGE"
                     }
                  ],
                  "Projection": {
                     "ProjectionType": "ALL"
                  }
               }
            ],
            "GlobalSecondaryIndexes": [
               {
                  "IndexName": "resiliencehub-index-1",
                  "KeySchema": [
                     {
                        "AttributeName": "USER_ID",
                        "KeyType": "HASH"
                     }
                  ],
                  "Projection": {
                     "ProjectionType": "ALL"
                  }
               }
            ]
         }
      }
   }
}
```

Para poder implementar el recurso de alarma con su aplicación, ahora tiene que reemplazar los recursos codificados por una referencia dinámica en las pilas de la aplicación.

Por lo tanto, en la definición del recurso de `AWS::CloudWatch::Alarm`, cambie lo siguiente:

```
"Value" : "Employees-ON-DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9"
```

a lo siguiente:

```
"Value" : {"Ref": "Employees"}
```

Y en la parte inferior de la definición del recurso de `AWS::SSM::Parameter`, cambie lo siguiente:

```
"Fn::Sub" : "{\"alarmName\":
\"${ReadthrottleeventsthresholdexceededDynamoDBEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm
\"referenceId\":\"dynamodb:alarm:health_read_throttle_events:2020-04-01\",
\"resourceId\":\"Employees-ON-DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9\",\"relatedSOPs\":
[\"dynamodb:sop:update_provisioned_capacity:2020-04-01\"]}"
```

a lo siguiente:

```
"Fn::Sub" : "{\"alarmName\":
\"${ReadthrottleeventsthresholdexceededEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm}\",
\"referenceId\":\"dynamodb:alarm:health_read_throttle_events:2020-04-01\",\"resourceId
\":\"${Employees}\",\"relatedSOPs\":
[\"dynamodb:sop:update_provisioned_capacity:2020-04-01\"]}"
```

Al modificar CloudFormation plantillas SOPs y AWS FIS realizar experimentos, adoptará el mismo enfoque: sustituirá las referencias codificadas por referencias dinámicas que seguirán funcionando IDs incluso después de cambios de hardware.

Al utilizar una referencia a la tabla de DynamoDB, CloudFormation permite hacer lo siguiente:

- Cree primero la tabla de la base de datos.
- Utilice siempre el ID real del recurso generado en la alarma y actualice la alarma de forma dinámica si es CloudFormation necesario reemplazar el recurso.

> **Note**
>
> Puede elegir métodos más avanzados para administrar los recursos de su aplicación CloudFormation , como anidar pilas o consultar las salidas de recursos en una pila independiente CloudFormation. (Sin embargo, si desea mantener la pila de recomendaciones separada de la pila principal, debe configurar una forma de pasar la información entre las dos pilas).
> Además, también se pueden utilizar herramientas de terceros, como Terraform by HashiCorp, para aprovisionar Infrastructure as Code (IaC).

Utilización AWS Resilience Hub APIs para describir y gestionar la aplicación

Como alternativa para describir y administrar aplicaciones mediante AWS Resilience Hub la consola, AWS Resilience Hub permite describir y administrar aplicaciones mediante AWS Resilience Hub API. En este capítulo se explica cómo crear una aplicación mediante AWS Resilience Hub las API. También define la secuencia en la que debe ejecutar las API y los valores de los parámetros que debe proporcionar con los ejemplos adecuados. Para obtener más información, consulte los temas siguientes:

- the section called “Preparación de la aplicación”
- the section called “Ejecutar y analizar la aplicación”
- the section called “Modificar su aplicación”

Preparación de la aplicación

Para preparar una aplicación, primero debe crearla, asignar una política de resiliencia y, a continuación, importar los recursos de la aplicación desde sus orígenes de entrada. Para obtener más información sobre las AWS Resilience Hub API que se utilizan para preparar una aplicación, consulte los siguientes temas:

- the section called “Creación de una aplicación de ”
- the section called “Crear una política de resiliencia”
- the section called “Importe el recurso de la aplicación y supervise el estado de la importación”
- the section called “Publique su aplicación y asigne una política de resiliencia”

Creación de una aplicación de

Para crear una nueva aplicación AWS Resilience Hub, debe llamar a la `CreateApp` API y proporcionar un nombre de aplicación único. Para obtener más información acerca esta API, consulte https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateApp.html.

El siguiente ejemplo muestra cómo crear una nueva aplicación `newApp` en AWS Resilience Hub mediante una API `CreateApp`.

Solicitud

```
aws resiliencehub create-app --name newApp
```

Respuesta

```
{
    "app": {
        "appArn": "<App_ARN>",
        "name": "newApp",
        "creationTime": "2022-10-26T19:48:00.434000+03:00",
        "status": "Active",
        "complianceStatus": "NotAssessed",
        "resiliencyScore": 0.0,
        "tags": {},
        "assessmentSchedule": "Disabled"
    }
}
```

Creación de una política de resiliencia

Tras crear la aplicación, debe crear una política de resiliencia que le permita comprender la postura de resiliencia de la aplicación mediante una API `CreateResiliencyPolicy`. Para obtener más información acerca esta API, consulte https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateResiliencyPolicy.html.

El siguiente ejemplo muestra cómo crear `newPolicy` para su aplicación AWS Resilience Hub mediante la `CreateResiliencyPolicy` API.

Solicitud

```
aws resiliencehub create-resiliency-policy \
--policy-name newPolicy --tier NonCritical \
--policy '{"AZ": {"rtoInSecs": 172800,"rpoInSecs": 86400}, \
"Hardware": {"rtoInSecs": 172800,"rpoInSecs": 86400}, \
"Software": {"rtoInSecs": 172800,"rpoInSecs": 86400}}'
```

Respuesta

```
{
    "policy": {
```

```
        "policyArn": "<Policy_ARN>",
        "policyName": "newPolicy",
        "policyDescription": "",
        "dataLocationConstraint": "AnyLocation",
        "tier": "NonCritical",
        "estimatedCostTier": "L1",
        "policy": {
            "AZ": {
                "rtoInSecs": 172800,
                "rpoInSecs": 86400
            },
            "Hardware": {
                "rtoInSecs": 172800,
                "rpoInSecs": 86400
            },
            "Software": {
                "rtoInSecs": 172800,
                "rpoInSecs": 86400
            }
        },
        "creationTime": "2022-10-26T20:48:05.946000+03:00",
        "tags": {}
    }
}
```

Importación de recursos desde un origen de entrada y supervisión del estado de la importación

AWS Resilience Hub proporciona las siguientes API para importar recursos a su aplicación:

- `ImportResourcesToDraftAppVersion`: esta API le permite importar recursos a la versión preliminar de su aplicación desde diferentes orígenes de entrada. Para obtener más información acerca esta API, consulte https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_ImportResourcesToDraftAppVersion.html.
- `PublishAppVersion`— Esta API publica una nueva versión de la aplicación junto con la versión actualizada AppComponents. Para obtener más información acerca esta API, consulte https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_PublishAppVersion.html.
- `DescribeDraftAppVersionResourcesImportStatus`: esta API le permite supervisar el estado de importación de sus recursos a una versión de la aplicación. Para obtener más información acerca esta API, consulte https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeDraftAppVersionResourcesImportStatus.html.

En el siguiente ejemplo, se muestra cómo importar recursos a su aplicación en AWS Resilience Hub mediante una API `ImportResourcesToDraftAppVersion`.

Solicitud

```
aws resiliencehub import-resources-to-draft-app-version \
--app-arn <App_ARN> \
--terraform-sources '[{"s3StateFileUrl": <S3_URI>}]'
```

Respuesta

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "sourceArns": [],
    "status": "Pending",
    "terraformSources": [
        {
            "s3StateFileUrl": <S3_URI>
        }
    ]
}
```

En el siguiente ejemplo, se muestra cómo añadir recursos manualmente a su aplicación en AWS Resilience Hub mediante una API `CreateAppVersionResource`.

Solicitud

```
aws resiliencehub create-app-version-resource \
--app-arn <App_ARN> \
--resource-name "backup-efs" \
--logical-resource-id '{"identifier": "backup-efs"}' \
--physical-resource-id '<Physical_resource_id_ARN>' \
--resource-type AWS::EFS::FileSystem \
--app-components '["new-app-component"]'
```

Respuesta

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
```

```
    "physicalResource": {
        "resourceName": "backup-efs",
        "logicalResourceId": {
            "identifier": "backup-efs"
        },
        "physicalResourceId": {
            "identifier": "<Physical_resource_id_ARN>",
            "type": "Arn"
        },
        "resourceType": "AWS::EFS::FileSystem",
        "appComponents": [
            {
                "name": "new-app-component",
                "type": "AWS::ResilienceHub::StorageAppComponent",
                "id": "new-app-component"
            }
        ]
    }
}
```

En el siguiente ejemplo, se muestra cómo supervisar el estado de la importación de sus recursos en AWS Resilience Hub mediante una API `DescribeDraftAppVersionResourcesImportStatus`.

Solicitud

```
aws resiliencehub describe-draft-app-version-resources-import-status \
--app-arn <App_ARN>
```

Respuesta

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "status": "Success",
    "statusChangeTime": "2022-10-26T19:55:18.471000+03:00"
}
```

Publicar la versión preliminar de su aplicación y asignar una política de resiliencia

Antes de realizar una evaluación, primero debe publicar la versión preliminar de la aplicación y asignar una política de resiliencia a la versión publicada de la aplicación.

Para publicar la versión preliminar de su aplicación y asignar una política de resiliencia

1. Para publicar la versión preliminar de su aplicación, utilice la API `PublishAppVersion`. Para obtener más información acerca esta API, consulte https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_PublishAppVersion.html.

   El siguiente ejemplo muestra cómo publicar la versión preliminar de la aplicación AWS Resilience Hub mediante la `PublishAppVersion` API.

   Solicitud

   ```
   aws resiliencehub publish-app-version \
    --app-arn <App_ARN>
   ```

   Respuesta

   ```
   {
       "appArn": "<App_ARN>",
       "appVersion": "release"
   }
   ```

2. Aplique una política de resiliencia a la versión publicada de su aplicación mediante una API `UpdateApp`. Para obtener más información acerca esta API, consulte https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_UpdateApp.html.

   El siguiente ejemplo muestra cómo aplicar una política de resiliencia a la versión publicada de una aplicación AWS Resilience Hub mediante la `UpdateApp` API.

   Solicitud

   ```
   aws resiliencehub update-app \
   --app-arn <App_ARN> \
   --policy-arn <Policy_ARN>
   ```

   Respuesta

```
{
    "app": {
        "appArn": "<App_ARN>",
        "name": "newApp",
        "policyArn": "<Policy_ARN>",
        "creationTime": "2022-10-26T19:48:00.434000+03:00",
        "status": "Active",
        "complianceStatus": "NotAssessed",
        "resiliencyScore": 0.0,
        "tags": {
            "resourceArn": "<App_ARN>"
        },
        "assessmentSchedule": "Disabled"
    }
}
```

Ejecutar y administrar AWS Resilience Hub evaluaciones de resiliencia

Después de publicar una nueva versión de la aplicación, debe realizar una nueva evaluación de la resiliencia y analizar los resultados para asegurarse de que la aplicación cumple con el RTO de carga de trabajo y el RPO estimados que se definen en su política de resiliencia. La evaluación compara la configuración de cada componente de la aplicación con la política y formula recomendaciones de alarma, SOP y pruebas.

Para obtener más información, consulte los temas siguientes:

- the section called “Ejecute y supervise una evaluación de resiliencia”
- the section called “Crear una política de resiliencia”

Ejecución y supervisión AWS Resilience Hub evaluaciones de resiliencia

Para realizar evaluaciones de resiliencia AWS Resilience Hub y monitorear su estado, debe usar las siguientes API:

- `StartAppAssessment`: esta API crea una nueva evaluación para una aplicación. Para obtener más información acerca esta API, consulte https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_StartAppAssessment.html.

- `DescribeAppAssessment`: esta API describe una evaluación de la aplicación y proporciona el estado de finalización de la evaluación. Para obtener más información acerca esta API, consulte https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeAppAssessment.html.

En el siguiente ejemplo, se muestra cómo comenzar a ejecutar una nueva evaluación en AWS Resilience Hub mediante API `StartAppAssessment`.

Solicitud

```
aws resiliencehub start-app-assessment \
--app-arn <App_ARN> \
--app-version release \
--assessment-name first-assessment
```

Respuesta

```
{
    "assessment": {
        "appArn": "<App_ARN>",
        "appVersion": "release",
        "invoker": "User",
        "assessmentStatus": "Pending",
        "startTime": "2022-10-27T08:15:10.452000+03:00",
        "assessmentName": "first-assessment",
        "assessmentArn": "<Assessment_ARN>",
        "policy": {
            "policyArn": "<Policy_ARN>",
            "policyName": "newPolicy",
            "dataLocationConstraint": "AnyLocation",
            "policy": {
                "AZ": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                },
                "Hardware": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                },
                "Software": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
```

```
                }
            }
        },
        "tags": {}
    }
}
```

En el siguiente ejemplo, se muestra cómo supervisar el estado de la evaluación en AWS Resilience Hub mediante API `DescribeAppAssessment`. Puede extraer el estado de la evaluación a partir de la variable `assessmentStatus`.

Solicitud

```
aws resiliencehub describe-app-assessment \
--assessment-arn <Assessment_ARN>
```

Respuesta

```
{
    "assessment": {
        "appArn": "<App_ARN>",
        "appVersion": "release",
        "cost": {
            "amount": 0.0,
            "currency": "USD",
            "frequency": "Monthly"
        },
        "resiliencyScore": {
            "score": 0.27,
            "disruptionScore": {
                "AZ": 0.42,
                "Hardware": 0.0,
                "Region": 0.0,
                "Software": 0.38
            }
        },
        "compliance": {
            "AZ": {
                "achievableRtoInSecs": 0,
                "currentRtoInSecs": 4500,
                "currentRpoInSecs": 86400,
                "complianceStatus": "PolicyMet",
                "achievableRpoInSecs": 0
```

```
            },
            "Hardware": {
                "achievableRtoInSecs": 0,
                "currentRtoInSecs": 2595601,
                "currentRpoInSecs": 2592001,
                "complianceStatus": "PolicyBreached",
                "achievableRpoInSecs": 0
            },
            "Software": {
                "achievableRtoInSecs": 0,
                "currentRtoInSecs": 4500,
                "currentRpoInSecs": 86400,
                "complianceStatus": "PolicyMet",
                "achievableRpoInSecs": 0
            }
        },
        "complianceStatus": "PolicyBreached",
        "assessmentStatus": "Success",
        "startTime": "2022-10-27T08:15:10.452000+03:00",
        "endTime": "2022-10-27T08:15:31.883000+03:00",
        "assessmentName": "first-assessment",
        "assessmentArn": "<Assessment_ARN>",
        "policy": {
            "policyArn": "<Policy_ARN>",
            "policyName": "newPolicy",
            "dataLocationConstraint": "AnyLocation",
            "policy": {
                "AZ": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                },
                "Hardware": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                },
                "Software": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                }
            }
        },
        "tags": {}
    }
```

```
}
```

Examen de los resultados de la evaluación

Una vez que la evaluación se haya completado correctamente, puede examinar los resultados de la evaluación mediante las siguientes API.

- `DescribeAppAssessment`: esta API le permite hacer un seguimiento del estado actual de su aplicación en relación con la política de resiliencia. Además, también puede extraer el estado de conformidad de la variable `complianceStatus` y la puntuación de resiliencia de cada tipo de interrupción a partir de la estructura `resiliencyScore`. Para obtener más información acerca esta API, consulte https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeAppAssessment.html.
- `ListAlarmRecommendations`: esta API le permite obtener las recomendaciones de alarma utilizando el nombre de recurso de Amazon (ARN) de la evaluación. Para obtener más información acerca esta API, consulte https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_ListAlarmRecommendations.html.

> **Note**
>
> Para obtener las recomendaciones de las pruebas SOP y FIS, utilice `ListSopRecommendations` y las API `ListTestRecommendations`.

En el siguiente ejemplo, se muestra cómo obtener las recomendaciones de alarma utilizando el nombre de recurso de Amazon (ARN) de la evaluación mediante API `ListAlarmRecommendations`.

> **Note**
>
> Para obtener las recomendaciones de las pruebas SOP y FIS, sustitúyalas por `ListSopRecommendations` o `ListTestRecommendations`.

Solicitud

```
aws resiliencehub list-alarm-recommendations \
--assessment-arn <Assessment_ARN>
```

Respuesta


```
{
    "alarmRecommendations": [
        {
            "recommendationId": "78ece7f8-c776-499e-baa8-b35f5e8b8ba2",
            "referenceId": "app_common:alarm:synthetic_canary:2021-04-01",
            "name": "AWSResilienceHub-SyntheticCanaryInRegionAlarm_2021-04-01",
            "description": "A monitor for the entire application, configured to
 constantly verify that the application API/endpoints are available",
            "type": "Metric",
            "appComponentName": "appcommon",
            "items": [
                {
                    "resourceId": "us-west-2",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ],
            "prerequisite": "Make sure Amazon CloudWatch Synthetics is setup to monitor
 the application (see the <a href=\"https://docs.aws.amazon.com/AmazonCloudWatch/
latest/monitoring/CloudWatch_Synthetics_Canaries.html\" target=\"_blank\">docs</a>).
 \nMake sure that the Synthetics Name passed in the alarm dimension matches the name of
 the Synthetic Canary. It Defaults to the name of the application.\n"
        },
        {
            "recommendationId": "d9c72c58-8c00-43f0-ad5d-0c6e5332b84b",
            "referenceId": "efs:alarm:percent_io_limit:2020-04-01",
            "name": "AWSResilienceHub-EFSHighIoAlarm_2020-04-01",
            "description": "An alarm by AWS Resilience Hub that reports when Amazon EFS
 I/O load is more than 90% for too much time",
            "type": "Metric",
            "appComponentName": "storageappcomponent-rlb",
            "items": [
                {
                    "resourceId": "fs-0487f945c02f17b3e",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
```

```
            "recommendationId": "09f340cd-3427-4f66-8923-7f289d4a3216",
            "referenceId": "efs:alarm:mount_failure:2020-04-01",
            "name": "AWSResilienceHub-EFSMountFailureAlarm_2020-04-01",
            "description": "An alarm by AWS Resilience Hub that reports when volume
 failed to mount to EC2 instance",
            "type": "Metric",
            "appComponentName": "storageappcomponent-rlb",
            "items": [
                {
                    "resourceId": "fs-0487f945c02f17b3e",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ],
            "prerequisite": "* Make sure Amazon EFS utils are installed(see the <a
 href=\"https://github.com/aws/efs-utils#installation\" target=\"_blank\">docs</a>).
\n* Make sure cloudwatch logs are enabled in efs-utils (see the <a href=\"https://
github.com/aws/efs-utils#step-2-enable-cloudwatch-log-feature-in-efs-utils-config-
file-etcamazonefsefs-utilsconf\" target=\"_blank\">docs</a>).\n* Make sure that
 you've configured `log_group_name` in `/etc/amazon/efs/efs-utils.conf`, for example:
 `log_group_name = /aws/efs/utils`.\n* Use the created `log_group_name` in the
 generated alarm. Find `LogGroupName: REPLACE_ME` in the alarm and make sure the
 `log_group_name` is used instead of REPLACE_ME.\n"
        },
        {
            "recommendationId": "b0f57d2a-1220-4f40-a585-6dab1e79cee2",
            "referenceId": "efs:alarm:client_connections:2020-04-01",
            "name": "AWSResilienceHub-EFSHighClientConnectionsAlarm_2020-04-01",
            "description": "An alarm by AWS Resilience Hub that reports when client
 connection number deviation is over the specified threshold",
            "type": "Metric",
            "appComponentName": "storageappcomponent-rlb",
            "items": [
                {
                    "resourceId": "fs-0487f945c02f17b3e",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "15f49b10-9bac-4494-b376-705f8da252d7",
```

```
            "referenceId": "rds:alarm:health-storage:2020-04-01",
            "name": "AWSResilienceHub-RDSInstanceLowStorageAlarm_2020-04-01",
            "description": "Reports when database free storage is low",
            "type": "Metric",
            "appComponentName": "databaseappcomponent-hji",
            "items": [
                {
                    "resourceId": "terraform-20220623141426115800000001",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "c1906101-cea8-4f77-be7b-60abb07621f5",
            "referenceId": "rds:alarm:health-connections:2020-04-01",
            "name": "AWSResilienceHub-RDSInstanceConnectionSpikeAlarm_2020-04-01",
            "description": "Reports when database connection count is anomalous",
            "type": "Metric",
            "appComponentName": "databaseappcomponent-hji",
            "items": [
                {
                    "resourceId": "terraform-20220623141426115800000001",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "f169b8d4-45c1-4238-95d1-ecdd8d5153fe",
            "referenceId": "rds:alarm:health-cpu:2020-04-01",
            "name": "AWSResilienceHub-RDSInstanceOverUtilizedCpuAlarm_2020-04-01",
            "description": "Reports when database used CPU is high",
            "type": "Metric",
            "appComponentName": "databaseappcomponent-hji",
            "items": [
                {
                    "resourceId": "terraform-20220623141426115800000001",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
```

```
            ]
        },
        {
            "recommendationId": "69da8459-cbe4-4ba1-a476-80c7ebf096f0",
            "referenceId": "rds:alarm:health-memory:2020-04-01",
            "name": "AWSResilienceHub-RDSInstanceLowMemoryAlarm_2020-04-01",
            "description": "Reports when database free memory is low",
            "type": "Metric",
            "appComponentName": "databaseappcomponent-hji",
            "items": [
                {
                    "resourceId": "terraform-20220623141426115800000001",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "67e7902a-f658-439e-916b-251a57b97c8a",
            "referenceId": "ecs:alarm:health-service_cpu_utilization:2020-04-01",
            "name": "AWSResilienceHub-ECSServiceHighCpuUtilizationAlarm_2020-04-01",
            "description": "An alarm by AWS Resilience Hub that triggers when CPU
utilization of ECS tasks of Service exceeds the threshold",
            "type": "Metric",
            "appComponentName": "computeappcomponent-nrz",
            "items": [
                {
                    "resourceId": "aws_ecs_service_terraform-us-east-1-demo",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "fb30cb91-1f09-4abd-bd2e-9e8ee8550eb0",
            "referenceId": "ecs:alarm:health-service_memory_utilization:2020-04-01",
            "name": "AWSResilienceHub-ECSServiceHighMemoryUtilizationAlarm_2020-04-01",
            "description": "An alarm by AWS Resilience Hub for Amazon ECS that
indicates if the percentage of memory that is used in the service, is exceeding
specified threshold limit",
            "type": "Metric",
            "appComponentName": "computeappcomponent-nrz",
```

```
            "items": [
                {
                    "resourceId": "aws_ecs_service_terraform-us-east-1-demo",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "1bd45a8e-dd58-4a8e-a628-bdbee234efed",
            "referenceId": "ecs:alarm:health-service_sample_count:2020-04-01",
            "name": "AWSResilienceHub-ECSServiceSampleCountAlarm_2020-04-01",
            "description": "An alarm by AWS Resilience Hub for Amazon ECS that triggers
 if the count of tasks isn't equal Service Desired Count",
            "type": "Metric",
            "appComponentName": "computeappcomponent-nrz",
            "items": [
                {
                    "resourceId": "aws_ecs_service_terraform-us-east-1-demo",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ],
            "prerequisite": "Make sure the Container Insights on Amazon ECS is enabled:
 (see the <a href=\"https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/
deploy-container-insights-ECS-cluster.html\" target=\"_blank\">docs</a>)."
        }
    ]
}
```

El siguiente ejemplo muestra cómo obtener las recomendaciones de configuración (recomendaciones sobre cómo mejorar su resiliencia actual) mediante la API `ListAppComponentRecommendations`.

Solicitud

```
aws resiliencehub list-app-component-recommendations \
--assessment-arn <Assessment_ARN>
```

Respuesta


```
{
    "componentRecommendations": [
        {
            "appComponentName": "computeappcomponent-nrz",
            "recommendationStatus": "MetCanImprove",
            "configRecommendations": [
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                },
                    "appComponentName": "computeappcomponent-nrz",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        }
                    },
```

```
                    "optimizationType": "LeastCost",
                    "description": "Current Configuration",
                    "suggestedChanges": [],
                    "haArchitecture": "BackupAndRestore",
                    "referenceId": "original"
                },
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "computeappcomponent-nrz",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        }
                    },
                    "optimizationType": "LeastChange",
                    "description": "Current Configuration",
```

```
                    "suggestedChanges": [],
                    "haArchitecture": "BackupAndRestore",
                    "referenceId": "original"
                },
                {
                    "cost": {
                        "amount": 14.74,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "computeappcomponent-nrz",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 0,
                            "expectedRtoDescription": "No expected downtime. You're
launching using EC2, with DesiredCount > 1 in multiple AZs and CapacityProviders with
MinSize > 1",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "ECS Service state is saved on
Amazon EFS file system. No data loss is expected as objects are be stored in multiple
AZs."
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 0,
                            "expectedRtoDescription": "No expected downtime. You're
launching using EC2, with DesiredCount > 1 and CapacityProviders with MinSize > 1",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "ECS Service state is saved on
Amazon EFS file system. No data loss is expected as objects are be stored in multiple
AZs."
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        }
                    },
                    "optimizationType": "BestAZRecovery",
```

```
                    "description": "Stateful Amazon ECS service with launch type Amazon
EC2 and Amazon EFS storage, deployed in multiple AZs. AWS Backup is used to backup
Amazon EFS and copy snapshots in-Region.",
                    "suggestedChanges": [
                        "Add AWS Auto Scaling Groups and Capacity Providers in multiple
AZs",
                        "Change desired count of the setup",
                        "Remove Amazon EBS volume"
                    ],
                    "haArchitecture": "BackupAndRestore",
                    "referenceId": "ecs:config:ec2-multi_az-efs-backups:2022-02-16"
                }
            ]
        },
        {
            "appComponentName": "databaseappcomponent-hji",
            "recommendationStatus": "MetCanImprove",
            "configRecommendations": [
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "databaseappcomponent-hji",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
an RDS backup. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
snapshot. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
```

```
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
snapshot. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        }
                    },
                    "optimizationType": "LeastCost",
                    "description": "Current Configuration",
                    "suggestedChanges": [],
                    "haArchitecture": "BackupAndRestore",
                    "referenceId": "original"
                },
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "databaseappcomponent-hji",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
an RDS backup. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
```

```
                            "expectedRtoDescription": "Estimated time to restore from
snapshot. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
snapshot. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        }
                    },
                    "optimizationType": "LeastChange",
                    "description": "Current Configuration",
                    "suggestedChanges": [],
                    "haArchitecture": "BackupAndRestore",
                    "referenceId": "original"
                },
                {
                    "cost": {
                        "amount": 76.73,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "databaseappcomponent-hji",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 120,
                            "expectedRtoDescription": "Estimated time to promote a
secondary instance.",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "Aurora data is automatically
replicated across multiple Availability Zones in a Region."
                        },
                        "Hardware": {
```

```
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 120,
                            "expectedRtoDescription": "Estimated time to promote a
secondary instance.",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "Aurora data is automatically
replicated across multiple Availability Zones in a Region."
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 900,
                            "expectedRtoDescription": "Estimate time to backtrack to a
stable state.",
                            "expectedRpoInSecs": 300,
                            "expectedRpoDescription": "Estimate for latest restorable
time for point in time recovery."
                        }
                    },
                    "optimizationType": "BestAZRecovery",
                    "description": "Aurora database cluster with one read replica, with
backtracking window of 24 hours.",
                    "suggestedChanges": [
                        "Add read replica in the same Region",
                        "Change DB instance to a supported class (db.t3.small)",
                        "Change to Aurora",
                        "Enable cluster backtracking",
                        "Enable instance backup with retention period 7"
                    ],
                    "haArchitecture": "WarmStandby",
                    "referenceId": "rds:config:aurora-backtracking"
                }
            ]
        },
        {
            "appComponentName": "storageappcomponent-rlb",
            "recommendationStatus": "BreachedUnattainable",
            "configRecommendations": [
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "storageappcomponent-rlb",
```

```
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 0,
                            "expectedRtoDescription": "No data loss in your system",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "No data loss in your system"
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyBreached",
                            "expectedRtoInSecs": 2592001,
                            "expectedRtoDescription": "No recovery option configured",
                            "expectedRpoInSecs": 2592001,
                            "expectedRpoDescription": "No recovery option configured"
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 900,
                            "expectedRtoDescription": "Time to recover Amazon EFS from
backup. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Recovery Point Objective for
Amazon EFS from backups, derived from backup frequency"
                        }
                    },
                    "optimizationType": "BestAZRecovery",
                    "description": "Amazon EFS with backups configured",
                    "suggestedChanges": [
                        "Add additional availability zone"
                    ],
                    "haArchitecture": "MultiSite",
                    "referenceId": "efs:config:with_backups:2020-04-01"
                },
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "storageappcomponent-rlb",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 0,
```

```
                            "expectedRtoDescription": "No data loss in your system",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "No data loss in your system"
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyBreached",
                            "expectedRtoInSecs": 2592001,
                            "expectedRtoDescription": "No recovery option configured",
                            "expectedRpoInSecs": 2592001,
                            "expectedRpoDescription": "No recovery option configured"
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 900,
                            "expectedRtoDescription": "Time to recover Amazon EFS from
 backup. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Recovery Point Objective for
 Amazon EFS from backups, derived from backup frequency"
                        }
                    },
                    "optimizationType": "BestAttainable",
                    "description": "Amazon EFS with backups configured",
                    "suggestedChanges": [
                        "Add additional availability zone"
                    ],
                    "haArchitecture": "MultiSite",
                    "referenceId": "efs:config:with_backups:2020-04-01"
                }
            ]
        }
    ]
}
```

Modificación de la aplicación

AWS Resilience Hub le permite modificar los recursos de la aplicación editando una versión preliminar de la aplicación y publicando los cambios en una versión nueva (publicada). AWS Resilience Hub utiliza la versión publicada de la aplicación, que incluye los recursos actualizados, para realizar las evaluaciones de resiliencia.

Para obtener más información, consulte los temas siguientes:

- the section called “Agregue recursos manualmente”
- the section called “Agrupar los recursos en un único componente de aplicación”
- the section called “Excluir un recurso de un AppComponent”

Agregar recursos manualmente a la aplicación

Si el recurso no se implementa como parte de una fuente de entrada, te AWS Resilience Hub permite añadir el recurso manualmente a tu aplicación mediante la `CreateAppVersionResource` API. Para obtener más información acerca esta API, consulte https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateAppVersionResource.html.

Debe proporcionar los siguientes parámetros a esta API:

- Nombre de recurso de Amazon (ARN) de la aplicación
- ID lógico del recurso
- ID física del recurso
- AWS CloudFormation escriba

En el siguiente ejemplo, se muestra cómo añadir recursos manualmente a su aplicación en AWS Resilience Hub mediante una API `CreateAppVersionResource`.

Solicitud

```
aws resiliencehub create-app-version-resource \
--app-arn <App_ARN> \
--resource-name "backup-efs" \
--logical-resource-id '{"identifier": "backup-efs"}' \
--physical-resource-id '<Physical_resource_id_ARN>' \
--resource-type AWS::EFS::FileSystem \
--app-components '["new-app-component"]'
```

Respuesta

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "physicalResource": {
```

```
        "resourceName": "backup-efs",
        "logicalResourceId": {
            "identifier": "backup-efs"
        },
        "physicalResourceId": {
            "identifier": "<Physical_resource_id_ARN>",
            "type": "Arn"
        },
        "resourceType": "AWS::EFS::FileSystem",
        "appComponents": [
            {
                "name": "new-app-component",
                "type": "AWS::ResilienceHub::StorageAppComponent",
                "id": "new-app-component"
            }
        ]
    }
}
```

Agrupar los recursos en un único componente de aplicación

Un componente de aplicación (AppComponent) es un grupo de AWS recursos relacionados que funcionan y fallan como una sola unidad. Por ejemplo, cuando tiene cargas de trabajo entre regiones que se utilizan como implementaciones en espera. AWS Resilience Hub tiene reglas que rigen qué AWS recursos pueden pertenecer a qué tipo de. AppComponent AWS Resilience Hub permite agrupar los recursos en uno solo AppComponent mediante las siguientes API de administración de recursos.

- `UpdateAppVersionResource`: esta API actualiza los detalles de los recursos de una aplicación. Para obtener más información acerca esta API, consulte UpdateAppVersionResource.
- `DeleteAppVersionAppComponent`— Esta API los elimina AppComponent de la aplicación. Para obtener más información acerca esta API, consulte DeleteAppVersionAppComponent.

El siguiente ejemplo muestra cómo actualizar los detalles de los recursos de su aplicación AWS Resilience Hub mediante la `DeleteAppVersionAppComponent` API.

Solicitud

```
aws resiliencehub delete-app-version-app-component \
--app-arn <App_ARN> \
```

```
--id new-app-component
```

Respuesta

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "appComponent": {
        "name": "new-app-component",
        "type": "AWS::ResilienceHub::StorageAppComponent",
        "id": "new-app-component"
    }
}
```

El siguiente ejemplo muestra cómo eliminar el vacío AppComponent que se creó en los ejemplos anteriores al AWS Resilience Hub usar la `UpdateAppVersionResource` API.

Solicitud

```
aws resiliencehub delete-app-version-app-component \
--app-arn <App_ARN> \
--id new-app-component
```

Respuesta

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "appComponent": {
        "name": "new-app-component",
        "type": "AWS::ResilienceHub::StorageAppComponent",
        "id": "new-app-component"
    }
}
```

Excluir un recurso de un AppComponent

AWS Resilience Hub permite excluir los recursos de las evaluaciones mediante la `UpdateAppVersionResource` API. Estos recursos no se tendrán en cuenta al calcular la resiliencia de la aplicación. Para obtener más información acerca esta API, consulte https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_UpdateAppVersionResource.html.

> **Note**
>
> Solo puede excluir los recursos que se importaron de un origen de entrada.

El siguiente ejemplo muestra cómo excluir un recurso de su aplicación en AWS Resilience Hub mediante la API `UpdateAppVersionResource`.

Solicitud

```
aws resiliencehub update-app-version-resource \
--app-arn <App_ARN> \
--resource-name "ec2instance-nvz" \
--excluded
```

Respuesta

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "physicalResource": {
        "resourceName": "ec2instance-nvz",
        "logicalResourceId": {
            "identifier": "ec2",
            "terraformSourceName": "test.state.file"
        },
        "physicalResourceId": {
            "identifier": "i-0b58265a694e5ffc1",
            "type": "Native",
            "awsRegion": "us-west-2",
            "awsAccountId": "123456789101"
        },
        "resourceType": "AWS::EC2::Instance",
        "appComponents": [
            {
                "name": "computeappcomponent-nrz",
                "type": "AWS::ResilienceHub::ComputeAppComponent"
            }
        ]
    }
}
```

Seguridad en AWS Resilience Hub

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 https://aws.amazon.com/compliance/shared-responsibility-model/ describe estos conceptos 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. Third-party los auditores comprueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los programas de AWS cumplimiento, los programas de . Para obtener más información sobre los programas de cumplimiento aplicables AWS Resilience Hub, 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 la normativa aplicables.

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

Contenido

Protección de datos en AWS Resilience Hub

El modelo de responsabilidad compartida de AWS se aplica a la protección de datos en AWS Resilience Hub. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos los Nube de AWS. Eres responsable de mantener el control

sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre privacidad de datos y los . Para obtener más información sobre la protección de datos en Europa, consulte el Centro del Reglamento General de Protección de Datos (RGPD).

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

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

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con Resilience Hub u otro dispositivo Servicios de AWS mediante la consola, la API o los SDK. AWS CLI AWS Cualquier dato que introduzca en etiquetas o campos de formato libre utilizados para los nombres se pueden emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya la información de las credenciales en la URL para validar la solicitud para ese servidor.

Cifrado en reposo

AWS Resilience Hub cifra sus datos en reposo. Los datos en reposo AWS Resilience Hub se cifran mediante un cifrado transparente del lado del servidor. Esto ayuda a reducir la carga y la complejidad operativas que conlleva la protección de información confidencial. Con el cifrado en reposo, puede crear aplicaciones sensibles a la seguridad que cumplen los requisitos de cifrado y normativos.

Cifrado en tránsito

AWS Resilience Hub cifra los datos en tránsito entre el servicio y otros servicios integrados. AWS Todos los datos que pasan entre los servicios integrados AWS Resilience Hub y los servicios integrados se cifran mediante Transport Layer Security (TLS). AWS Resilience Hub proporciona acciones preconfiguradas para tipos específicos de objetivos en todos los AWS servicios y respalda las acciones para los recursos objetivo.

Identity and Access Management para AWS Centro de resiliencia

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

Temas

- Habilitación AWS Resilience Hub para publicar en tus temas de Amazon Simple Notification Service
- Limitar los permisos para incluir o excluir AWS Resilience Hub recomendaciones

Público

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

- Usuario del servicio: solicite permisos al administrador si no puede acceder a las características (consulte Resolución de problemas AWS Identidad y acceso a Resilience Hub).
- Administrador del servicio: determine el acceso de los usuarios y envíe las solicitudes de permiso (consulte Cómo AWS Resilience Hub funciona con IAM).
- Administrador de IAM: escribe las políticas para administrar el acceso (consulte Identity-based ejemplos de políticas para AWS Centro de resiliencia).

Autenticación con identidades

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

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

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

Cuenta de AWS usuario raíz

Al crear una Cuenta de AWS, se comienza con una identidad de inicio de sesión denominada usuario Cuenta de AWS raíz, que tiene acceso completo a todos los Servicios de AWS recursos. Se recomiendaencarecidamente que no utilice el usuario raíz para las tareas diarias. Para ver las tareas que requieren credenciales de usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio empresarial, del proveedor de identidades web o al Directory Service que se accede Servicios de AWS mediante credenciales de una fuente de identidad. Las identidades federadas asumen roles que proporcionan credenciales temporales.

Para una administración de acceso centralizada, se recomienda AWS IAM Identity Center. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad con permisos específicos para una sola persona o aplicación. Recomendamos el uso de credenciales temporales en lugar de usuarios de IAM con credenciales de larga duración. Para obtener más información, consulte Exigir a los usuarios humanos que utilicen la federación con un proveedor de identidad para acceder AWS mediante credenciales temporales en la Guía del usuario de IAM.

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

Roles de IAM

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

Los roles de IAM son útiles para el acceso de usuario federado, los permisos de usuario de IAM temporales, el acceso entre cuentas, el acceso entre servicios y las aplicaciones que se ejecutan en Amazon EC2. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Administración del acceso con políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política define los permisos cuando están asociados a una identidad o un recurso. AWS evalúa estas

políticas cuando un director hace una solicitud. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre los documentos de políticas de JSON, consulte Información general de políticas de JSON en la Guía del usuario de IAM.

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

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

Identity-based políticas

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

Identity-based las políticas pueden ser políticas integradas (integradas directamente en una sola identidad) o políticas administradas (políticas independientes asociadas a varias identidades). Para obtener información sobre cómo elegir entre políticas administradas e insertadas, consulte Selección entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Resource-based políticas

Resource-based las políticas son documentos de políticas de JSON que se adjuntan a un recurso. Los ejemplos incluyen las Políticas de confianza de roles de IAM y las Políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Debe especificar una entidad principal en una política basada en recursos.

Resource-based las políticas son políticas en línea que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Otros tipos de políticas

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

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

Varios tipos de políticas

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

Cómo AWS Resilience Hub funciona con IAM

Antes de usar IAM para administrar el acceso a AWS Resilience Hub, conozca qué funciones de IAM están disponibles para usar con AWS Resilience Hub.

Funciones de IAM que puede utilizar con AWS Centro de resiliencia

Característica de IAM	AWS Soporte para Resilience Hub
Identity-based políticas	Sí
Resource-based políticas	No
Acciones de políticas	Sí
Recursos de políticas	Sí

Característica de IAM	AWS Soporte para Resilience Hub
Claves de condición de política (específicas del servicio)	Sí
ACL	No
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí
Sesiones de acceso directo (FAS)	Sí
Roles de servicio	Sí

Para obtener una visión general de cómo funcionan AWS Resilience Hub y otros AWS servicios con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Identity-based políticas para AWS Centro de resiliencia

Compatibilidad con las políticas basadas en identidad: sí

Identity-based las políticas son documentos de política de permisos de JSON que puedes adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de la política de JSON de IAM en la Guía del usuario de IAM.

Identity-based ejemplos de políticas para AWS Centro de resiliencia

Para ver ejemplos de políticas basadas en la identidad de AWS Resilience Hub, consulte. Identity-based ejemplos de políticas para AWS Centro de resiliencia

Resource-based políticas dentro AWS Centro de resiliencia

Admite políticas basadas en recursos: no

Resource-based las políticas son documentos de políticas de JSON que se adjuntan a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. 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 basada en recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Acciones políticas para AWS Centro de resiliencia

Compatibilidad con las acciones de políticas: sí

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

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

Para ver una lista de las acciones de AWS Resilience Hub, consulte las acciones definidas por AWS Resilience Hub en la Referencia de autorización de servicios.

Las acciones políticas de AWS Resilience Hub utilizan el siguiente prefijo antes de la acción:

```
resiliencehub
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "resiliencehub:action1",
      "resiliencehub:action2"
```

```
        ]
```

Para ver ejemplos de políticas basadas en la identidad de AWS Resilience Hub, consulte. Identity-based ejemplos de políticas para AWS Centro de resiliencia

Recursos de políticas para AWS Centro de resiliencia

Compatibilidad con los recursos de políticas: sí

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

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

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

Para ver una lista de los tipos de recursos de AWS Resilience Hub y sus ARN, consulte los recursos definidos por AWS Resilience Hub en la Referencia de autorización de servicios. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte Acciones definidas por AWS Resilience Hub.

Para ver ejemplos de políticas basadas en la identidad de AWS Resilience Hub, consulte. Identity-based ejemplos de políticas para AWS Centro de resiliencia

Claves de condición de la política para AWS Centro de resiliencia

Compatibilidad con claves de condición de políticas específicas del servicio: sí

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

El elemento `Condition` especifica cuándo se ejecutan las instrucciones en función de criterios definidos. Puede crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de las claves de condición de AWS Resilience Hub, consulte las claves de condición de AWS Resilience Hub en la Referencia de autorización de servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Acciones definidas por AWS Resilience Hub.

Para ver ejemplos de políticas basadas en la identidad de AWS Resilience Hub, consulte. Identity-based ejemplos de políticas para AWS Centro de resiliencia

ACL en AWS Centro de resiliencia

Compatibilidad con ACL: no

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

ABAC con AWS Centro de resiliencia

Compatibilidad con ABAC (etiquetas en las políticas): parcial

Attribute-based el control de acceso (ABAC) es una estrategia de autorización que define los permisos en función de unos atributos denominados etiquetas. Puede adjuntar etiquetas a las entidades y AWS los recursos de IAM y, a continuación, diseñar políticas de ABAC para permitir las operaciones cuando la etiqueta del director coincida con la etiqueta del recurso.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Utilizar credenciales temporales con AWS Centro de resiliencia

Compatibilidad con credenciales temporales: sí

Las credenciales temporales proporcionan acceso a AWS los recursos a corto plazo y se crean automáticamente cuando se utiliza la federación o se cambia de rol. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM y Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Sesiones de acceso directo para AWS Centro de resiliencia

Admite sesiones de acceso directo (FAS): sí

Las sesiones de acceso directo (FAS) utilizan los permisos de la persona principal que llama Servicio de AWS, junto con la solicitud, Servicio de AWS para realizar solicitudes a los servicios descendentes. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Sesiones de acceso directo.

Funciones de servicio para AWS Centro de resiliencia

Compatible con roles de servicio: sí

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Crear un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de AWS Resilience Hub. Edite las funciones de servicio solo cuando AWS Resilience Hub le dé instrucciones para hacerlo.

Identity-based ejemplos de políticas para AWS Centro de resiliencia

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos de AWS Resilience Hub. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por AWS Resilience Hub, incluido el formato de los ARN de cada uno de los tipos de recursos, consulte las acciones, los recursos y las claves de condición de AWS Resilience Hub en la Referencia de autorización de servicios.

Temas

Prácticas recomendadas sobre las políticas

Identity-based las políticas determinan si alguien puede crear, acceder o eliminar los recursos de AWS Resilience Hub de su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.

- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

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

Uso de AWS Consola Resilience Hub

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

No necesita conceder permisos mínimos de consola a los usuarios que solo realizan llamadas a la API AWS CLI o a la AWS API. En su lugar, permita el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la consola de AWS Resilience Hub, adjunte también el AWS Resilience Hub `ConsoleAccess` o la política `ReadOnly` AWS gestionada a las entidades. Para obtener más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

La siguiente política otorga a los usuarios el permiso para enumerar y ver todos los recursos de la AWS Resilience Hub consola, pero no para crearlos, actualizarlos ni eliminarlos.

JSON

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

Cómo permitir a los usuarios consultar sus propios permisos

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
```

```
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Listado disponible AWS Resilience Hub aplicaciones

La siguiente política concede a los usuarios el permiso para enumerar las aplicaciones de AWS Resilience Hub disponibles.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:ListApps"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Inicio de una evaluación de la solicitud

La siguiente política otorga a los usuarios el permiso para iniciar una evaluación para una AWS Resilience Hub aplicación específica.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:StartAppAssessment"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}
```

Eliminar la evaluación de una aplicación

La siguiente política otorga a los usuarios el permiso para eliminar una evaluación de una AWS Resilience Hub aplicación específica.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:DeleteAppAssessment"
      ],
      "Resource": [
```

```
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}
```

Crear una plantilla de recomendación para una aplicación específica

La siguiente política otorga a los usuarios el permiso para crear una plantilla de recomendación para una AWS Resilience Hub aplicación específica.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:CreateRecommendationTemplate"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}
```

Eliminar una plantilla de recomendaciones para una aplicación específica

La siguiente política otorga a los usuarios el permiso para eliminar una plantilla de recomendación para una AWS Resilience Hub aplicación específica.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
```

```
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:DeleteRecommendationTemplate"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}
```

Actualizar una aplicación con una política de resiliencia específica

La siguiente política concede a los usuarios el permiso para actualizar una aplicación de AWS Resilience Hub con una política de resiliencia específica.

Configuración de roles y permisos de IAM

AWS Resilience Hub le permite configurar las funciones de IAM que le gustaría utilizar al ejecutar las evaluaciones de su aplicación. Hay varias formas de configurar AWS Resilience Hub para obtener acceso de solo lectura a los recursos de la aplicación. Sin embargo, AWS Resilience Hub recomienda lo siguiente:

- Acceso basado en roles: este rol se define y usa en la cuenta corriente. AWS Resilience Hub asumirá este rol para acceder a los recursos de su aplicación.

  Para proporcionar un acceso basado en roles, el rol debe incluir lo siguiente:

  - Read-only permiso para leer sus recursos (se AWS Resilience Hub recomienda utilizar la política `AWSResilienceHubAsssessmentExecutionPolicy` gestionada).
  - Confíe en la política para asumir esta función, que permite al director de AWS Resilience Hub servicio asumir esta función. Si no tienes esa función configurada en tu cuenta, AWS Resilience Hub se mostrarán las instrucciones para crearla. Para obtener más información, consulte the section called “Configuración de permisos”.

> **Note**
>
> Si solo proporciona el nombre del rol de invocador y si sus recursos están ubicados en otra cuenta, AWS Resilience Hub utilizará este nombre de rol en las demás cuentas para

acceder a los recursos multicuenta. Si lo desea, puede configurar los ARN del rol para otras cuentas, que se utilizarán en lugar del nombre del rol del invocador.

- Acceso de usuario de IAM actual: AWS Resilience Hub utilizará el usuario de IAM actual para acceder a los recursos de la aplicación. Cuando sus recursos estén en una cuenta diferente, AWS Resilience Hub asumirá las siguientes funciones de IAM para acceder a los recursos:
  - `AwsResilienceHubAdminAccountRole` en la cuenta actual
  - `AwsResilienceHubExecutorAccountRole` en otras cuentas

  Además, cuando configure una evaluación programada, AWS Resilience Hub asumirá esa `AwsResilienceHubPeriodicAssessmentRole` función. Sin embargo, no `AwsResilienceHubPeriodicAssessmentRole` se recomienda su uso porque hay que configurar manualmente las funciones y los permisos, y es posible que algunas funcionalidades (como la notificación de derivación) no funcionen como se esperaba.

Resolución de problemas AWS Identidad y acceso a Resilience Hub

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas habituales que pueden surgir al trabajar con AWS Resilience Hub e IAM.

Temas

No estoy autorizado a realizar ninguna acción en AWS Centro de resiliencia

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `resiliencehub:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 resiliencehub:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `resiliencehub:`*`GetWidget`*.

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

No estoy autorizado a realizar tareas como: PassRole

Si recibe un mensaje de error que indica que no está autorizado a realizar la `iam:PassRole` acción, sus políticas deben actualizarse para que pueda transferir una función a AWS Resilience Hub.

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

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

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

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

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

Quiero permitir que personas ajenas a mi Cuenta de AWS para acceder a mi AWS Recursos del Resilience Hub

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para obtener más información, consulte lo siguiente:

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

AWS Resilience Hub referencia de permisos de acceso

Puede usar AWS Identity and Access Management (IAM) para administrar el acceso a los recursos de la aplicación y crear políticas de IAM que se apliquen a los usuarios, grupos o roles.

Todas las AWS Resilience Hub aplicaciones se pueden configurar para que utilicen the section called “Rol de invocador” (una función de IAM) o los permisos de usuario de IAM actuales (junto con un conjunto de funciones predefinidas para la evaluación multicuenta y programada). En esta función, puede adjuntar una política que defina los permisos necesarios AWS Resilience Hub para acceder a otros AWS recursos o recursos de la aplicación. La función de invocador debe tener una política de confianza que se añada a AWS Resilience Hub Service Principal.

Para administrar los permisos de su aplicación, le recomendamos que utilice the section called “AWS políticas gestionadas”. Puede usar estas políticas administradas sin ninguna modificación, o puede usarlas como punto de partida para escribir sus propias políticas restrictivas. Las políticas pueden restringir los permisos de los usuarios a nivel de recursos para diferentes acciones mediante el uso de condiciones opcionales adicionales.

Si los recursos de la aplicación están en cuentas diferentes (secondary/resourcecuentas), debe configurar un nuevo rol en cada cuenta que contenga los recursos de la aplicación.

> **Note**
>
> Si define puntos de enlace de VPC para sus recursos de carga de trabajo, asegúrese de que las políticas de puntos de enlace de VPC proporcionen acceso de solo lectura para acceder a los recursos. AWS Resilience Hub Para obtener más información, consulte Controlar el acceso a puntos de conexión de VPC con políticas de punto de conexión.

Temas

- the section called “Uso un rol de IAM”
- the section called “Usar permisos de usuario de IAM actuales”

Uso un rol de IAM

AWS Resilience Hub utilizará un rol de IAM predefinido y existente para acceder a los recursos de la cuenta o cuenta principal. secondary/resources Esta es la opción de permiso recomendada para acceder a sus recursos.

Temas

- the section called “Rol de invocador”
- the section called “Funciones en diferentes AWS cuentas para el acceso entre cuentas”

Rol de invocador

La función de AWS Resilience Hub invocador es una función AWS Identity and Access Management (IAM) que se AWS Resilience Hub asume para acceder a los AWS servicios y recursos. Por ejemplo, puede crear un rol de invocador que tenga permiso para acceder a su plantilla CFN y al recurso que crea. Esta página proporciona información sobre cómo crear, ver y administrar un rol de invocador de aplicaciones.

Al crear una aplicación, se proporciona un rol de invocador. AWS Resilience Hub asume este rol para acceder a sus recursos cuando importe recursos o inicie una evaluación. AWS Resilience Hub Para asumir correctamente la función de invocador, la política de confianza de la función debe especificar que el principal del AWS Resilience Hub servicio (resiliencehub.amazonaws.com) es un servicio de confianza.

Para ver el rol de invocador de la aplicación, seleccione Aplicaciones en el panel de navegación y, a continuación, seleccione Actualizar permisos en el menú Acciones de la página Aplicación.

Puede añadir o eliminar permisos de un rol de invocador de aplicación en cualquier momento, o configurar la aplicación para que utilice un rol diferente para acceder a los recursos de la aplicación.

Temas

- the section called “Crear un rol invocador en la consola de IAM”
- the section called “Administración de roles con la API de IAM”
- the section called “Definir la política de confianza mediante un archivo JSON”

Crear un rol invocador en la consola de IAM

Para poder acceder AWS Resilience Hub a los AWS servicios y recursos, debe crear un rol de invocador en la cuenta principal mediante la consola de IAM. Para obtener más información sobre la creación de funciones mediante la consola de IAM, consulte Creación de una función para un AWS servicio (consola).

Para crear un rol de invocador en la cuenta principal mediante la consola de IAM

1. Abra la consola de IAM en `https://console.aws.amazon.com/iam/`.
2. En el panel de navegación, seleccione Roles y, a continuación, seleccione Crear rol.
3. Seleccione Política de confianza personalizada, copie la siguiente política en la ventana Política de confianza personalizada y, a continuación, seleccione Siguiente.

> **Note**
>
> Si sus recursos están en cuentas diferentes, debe crear un rol en cada una de esas cuentas y usar la política de confianza de la cuenta secundaria para las demás cuentas.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. En la sección Políticas de permisos de la página Añadir permisos, introduzca `AWSResilienceHubAsssessmentExecutionPolicy` en el cuadro Filtre las políticas por propiedad o nombre de política y pulse Entrar.
5. Seleccione la política y elija Siguiente.
6. En la sección Información del rol, introduzca un nombre de rol único (por ejemplo, `AWSResilienceHubAssessmentRole`) en el cuadro Nombre del rol.

   Este campo solo acepta caracteres alfanuméricos y «`+=,.@-_/`».
7. (Opcional) Introduzca una descripción sobre el rol en el cuadro Descripción.
8. Elija Crear rol.

   Para editar los casos de uso y los permisos, en el paso 6, elija el botón Editar que se encuentra a la derecha de las secciones Paso 1: seleccionar entidades de confianza o Paso 2: agregar permisos.

Tras crear el rol de invocador y el rol de recurso (si procede), puede configurar su aplicación para que utilice estos roles.

> **Note**
>
> Debe tener un `iam:passRole` permiso en su IAM actual user/role para el rol de invocador al crear o actualizar la aplicación. Sin embargo, no necesita este permiso para ejecutar una evaluación.

Administración de roles con la API de IAM

La política de confianza de un rol otorga a la entidad principal especificada permiso para asumir el rol. Para crear los roles mediante AWS Command Line Interface (AWS CLI), utilice el `create-role` comando. Al usar este comando, puede especificar las políticas de confianza en línea. El

siguiente ejemplo muestra cómo conceder al AWS Resilience Hub servicio el permiso principal para que asuma su función.

> **Note**
>
> El requisito de estar por fuera de las comillas (' ') en la cadena JSON puede variar en función de la versión de intérprete de comandos.

Ejemplo de **`create-role`**

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-role-policy-
document '{
  "Version": "2012-10-17",       "Statement":
  [
    {
      "Effect": "Allow",
      "Principal": {"Service": "resiliencehub.amazonaws.com"},
      "Action": "sts:AssumeRole"
    }
  ]
}'
```

Definir la política de confianza mediante un archivo JSON

Puede definir la política de confianza para el rol utilizando un archivo JSON independiente y luego ejecutar el comando `create-role`. En el siguiente ejemplo, se muestra un archivo **`trust-policy.json`** que contiene la política de confianza en el directorio actual. Esta política se asocia a un rol mediante la ejecución del comando **`create-role`**. El resultado del comando **`create-role`** se muestra en el Ejemplo de salida. Para añadir permisos al rol, use el comando attach-policy-to-role y empiece por añadir la política administrada por `AWSResilienceHubAsssessmentExecutionPolicy`. Para obtener más información sobre esta política administrada, consulte the section called “AWSResilienceHubAsssessmentExecutionPolicy”.

Ejemplo de **`trust-policy.json`**

JSON

```
{
```

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

Ejemplo de **`create-role`**

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-
role-policy-document file://trust-policy.json
```

Resultados de ejemplo

Ejemplo de **`attach-policy-to-role`**

```
aws iam attach-role-policy --role-name AWSResilienceHubAssessmentRole --
policy-arn arn:aws:iam::aws:policy/
AWSResilienceHubAsssessmentExecutionPolicy
```

Funciones en diferentes AWS cuenta para el acceso entre cuentas (opcional)

Cuando sus recursos estén ubicados en secondary/resource cuentas, debe crear funciones en cada una de estas cuentas AWS Resilience Hub para poder evaluar correctamente su solicitud. El procedimiento de creación de roles es similar al proceso de creación de roles del invocador, excepto en lo que respecta a la configuración de la política de confianza.

> **Note**
>
> Debe crear los roles en las cuentas secundarias donde se encuentran los recursos.

Temas

- the section called “Crear un rol en la consola de IAM para las cuentas secondary/resource”
- the section called “Administración de roles con la API de IAM”
- the section called “Definir la política de confianza mediante un archivo JSON”

Crear un rol en la consola de IAM para las cuentas secondary/resource

Para poder acceder AWS Resilience Hub a AWS los servicios y recursos de otras AWS cuentas, debe crear roles en cada una de estas cuentas.

Para crear un rol en la consola de IAM para secondary/resource las cuentas mediante la consola de IAM

1. Abra la consola de IAM en `https://console.aws.amazon.com/iam/`.
2. En el panel de navegación, seleccione Roles y, a continuación, seleccione Crear rol.
3. Seleccione Política de confianza personalizada, copie la siguiente política en la ventana Política de confianza personalizada y, a continuación, seleccione Siguiente.

   > **Note**
   >
   > Si sus recursos están en cuentas diferentes, debe crear un rol en cada una de esas cuentas y usar la política de confianza de la cuenta secundaria para las demás cuentas.

4. En la sección Políticas de permisos de la página Añadir permisos, introduzca `AWSResilienceHubAsssessmentExecutionPolicy` en el cuadro Filtre las políticas por propiedad o nombre de política y pulse Entrar.
5. Seleccione la política y elija Siguiente.
6. En la sección Información del rol, introduzca un nombre de rol único (por ejemplo, `AWSResilienceHubAssessmentRole`) en el cuadro Nombre del rol.
7. (Opcional) Introduzca una descripción sobre el rol en el cuadro Descripción.
8. Elija Crear rol.

   Para editar los casos de uso y los permisos, en el paso 6, elija el botón Editar que se encuentra a la derecha de las secciones Paso 1: seleccionar entidades de confianza o Paso 2: agregar permisos.

Además, también debe añadir el permiso de `sts:assumeRole` al rol de invocador para que pueda asumir los roles de sus cuentas secundarias.

Añada la siguiente política a su rol de invocador para cada uno de los roles secundarios que haya creado:

```
{
```

```
    "Effect": "Allow",
    "Resource": [
      "arn:aws:iam::secondary_account_id_1:role/RoleInSecondaryAccount_1",
      "arn:aws:iam::secondary_account_id_2:role/RoleInSecondaryAccount_2",
      ...
      ],
      "Action": [
        "sts:AssumeRole"
      ]
}
```

Administración de roles con la API de IAM

La política de confianza de un rol otorga a la entidad principal especificada permiso para asumir el rol. Para crear los roles mediante AWS Command Line Interface (AWS CLI), utilice el `create-role` comando. Al usar este comando, puede especificar las políticas de confianza en línea. En el siguiente ejemplo, se muestra cómo conceder al director del AWS Resilience Hub servicio el permiso para que asuma su función.

> **Note**
>
> El requisito de estar por fuera de las comillas (`'  '`) en la cadena JSON puede variar en función de la versión de intérprete de comandos.

Ejemplo de **`create-role`**

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-role-policy-
document '{"Version": "2012-10-17",       "Statement": [{"Effect": "Allow","Principal":
 {"AWS": ["arn:aws:iam::primary_account_id:role/InvokerRoleName"]},"Action":
 "sts:AssumeRole"}]}'
```

También puede definir la política de confianza para el rol con un archivo JSON aparte. En el siguiente ejemplo, `trust-policy.json` es un archivo que se encuentra en el directorio actual.

Definir la política de confianza mediante un archivo JSON

Puede definir la política de confianza para el rol utilizando un archivo JSON independiente y luego ejecutar el comando `create-role`. En el siguiente ejemplo, se muestra un archivo **`trust-policy.json`** que contiene la política de confianza en el directorio actual. Esta política se asocia a un rol mediante la ejecución del comando **`create-role`**. El resultado

del comando **`create-role`** se muestra en el Ejemplo de salida. Para añadir permisos a un rol, use el comando attach-policy-to-role y empiece por añadir la política administrada por `AWSResilienceHubAsssessmentExecutionPolicy`. Para obtener más información sobre esta política administrada, consulte the section called “AWSResilienceHubAsssessmentExecutionPolicy”.

Ejemplo de **`trust-policy.json`**

Ejemplo de **`create-role`**

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-role-policy-
document file://trust-policy.json
```

Resultados de ejemplo

Ejemplo de **`attach-policy-to-role`**

`aws iam attach-role-policy --role-name AWSResilienceHubAssessmentRole --policy-arn arn:aws:iam::aws:policy/AWSResilienceHubAsssessmentExecutionPolicy`.

Usar permisos de usuario de IAM actuales

Utilice este método si quiere usar sus permisos de usuario de IAM actuales para crear y ejecutar una evaluación. Puede adjuntar la política administrada por `AWSResilienceHubAsssessmentExecutionPolicy` a su usuario de IAM o un rol asociado a su usuario.

Configuración de cuenta única

El uso de la política administrada mencionada anteriormente es suficiente para ejecutar una evaluación en una aplicación que se administra en la misma cuenta que el usuario de IAM.

Configuración de la evaluación programada

Debe crear un nuevo rol de `AwsResilienceHubPeriodicAssessmentRole` para que AWS Resilience Hub pueda realizar las tareas relacionadas con la evaluación programada.

> **Note**
>
> - Si utiliza el acceso basado en roles (con el rol de invocador mencionado anteriormente), este paso no es obligatorio.

- El nombre de rol debe ser `AwsResilienceHubPeriodicAssessmentRole`.

Para habilitar AWS Resilience Hub para realizar tareas programadas relacionadas con la evaluación

1. Asocie la política administrada por `AWSResilienceHubAsssessmentExecutionPolicy` al rol.
2. Añada la siguiente política, donde `primary_account_id` se encuentra la AWS cuenta en la que se define la aplicación y en la que se ejecutará la evaluación. Además, debe agregar la política de confianza asociada a la función de la evaluación programada, (`AwsResilienceHubPeriodicAssessmentRole`), que otorga permisos para que el AWS Resilience Hub servicio asuma la función de la evaluación programada.

   Política de confianza para el rol de evaluación programada (**`AwsResilienceHubPeriodicAssessmentRole`**)

   JSON

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

Cross-account configuración

Las siguientes políticas de permisos de IAM son obligatorias si utiliza AWS Resilience Hub con varias cuentas. Es posible que cada AWS cuenta necesite permisos diferentes según su caso de uso. Al configurar AWS Resilience Hub para el acceso entre cuentas, se tienen en cuenta las siguientes cuentas y roles:

- Cuenta principal: cuenta de AWS en la que desea crear la aplicación y ejecutar las evaluaciones.
- Secondary/Resource cuentas: AWS cuentas en las que se encuentran los recursos.

> **Note**
>
> - Si utiliza el acceso basado en roles (con el rol de invocador mencionado anteriormente), este paso no es obligatorio.
> - Para obtener más información sobre la configuración de permisos para acceder a Amazon Elastic Kubernetes Service, consulte the section called “Habilitar el AWS Resilience Hub acceso a su clúster de Amazon EKS”.

Configuración de cuenta principal

Debe crear un nuevo rol `AwsResilienceHubAdminAccountRole` en la cuenta principal y permitir el AWS Resilience Hub acceso para asumirlo. Esta función se utilizará para acceder a otra función de su AWS cuenta que contenga sus recursos. No debe tener permisos para leer los recursos.

> **Note**
>
> - El nombre de rol debe ser `AwsResilienceHubAdminAccountRole`.
> - Debe crearse en la cuenta principal.
> - Su IAM actual user/role debe tener el `iam:assumeRole` permiso para asumir esta función.
> - Sustituya `secondary_account_id_1/2/...` por los identificadores de cuenta secundarios correspondientes.

La siguiente política proporciona permisos de ejecutor a tu rol para acceder a los recursos de otro rol de tu AWS cuenta:

La política de confianza del rol de administrador (`AwsResilienceHubAdminAccountRole`) es la siguiente:

Secondary/Resource configuración de cuentas

En cada una de sus cuentas secundarias, debe crear un nuevo `AwsResilienceHubExecutorAccountRole` y habilitar el rol de administrador creado anteriormente para asumir este rol. Dado que esta función se utilizará AWS Resilience Hub para analizar y evaluar los recursos de la aplicación, también necesitará los permisos adecuados.

Sin embargo, debe asociar la política administrada por `AWSResilienceHubAsssessmentExecutionPolicy` al rol y la política del rol de ejecutor.

La política de confianza del rol de ejecutor es la siguiente:

AWS políticas gestionadas para AWS Resilience Hub

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

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

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

Para obtener más información, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

AWSResilienceHubAsssessmentExecutionPolicy

Puede adjuntar la `AWSResilienceHubAsssessmentExecutionPolicy` a las identidades de IAM. Al ejecutar una evaluación, esta política otorga permisos de acceso a otros AWS servicios para ejecutar las evaluaciones.

Detalles del permiso

Esta política proporciona los permisos adecuados para publicar alarmas AWS FIS y plantillas de SOP en su bucket de Amazon Simple Storage Service (Amazon S3). El nombre del bucket de Amazon S3 debe comenzar por `aws-resilience-hub-artifacts-`. Si desea publicar en otro bucket de Amazon S3, puede hacerlo mientras llama a la API `CreateRecommendationTemplate`. Para obtener más información, consulte CreateRecommendationTemplate.

Esta política incluye los permisos siguientes:

- Amazon CloudWatch (CloudWatch): obtiene todas las alarmas implementadas que configuraste en Amazon CloudWatch para monitorear la aplicación. Además, publicamos CloudWatch las métricas de la puntuación de resiliencia de la aplicación en el `ResilienceHub` espacio de nombres. `cloudwatch:PutMetricData`
- Amazon Data Lifecycle Manager: obtiene y proporciona `Describe` permisos para los recursos de Amazon Data Lifecycle Manager asociados a su AWS cuenta.
- Amazon DevOps Guru: muestra los recursos de Amazon DevOps Guru asociados a su AWS cuenta y proporciona `Describe` permisos para ellos.
- Amazon DocumentDB: muestra los recursos de Amazon DocumentDB asociados a su cuenta y proporciona `Describe` permisos para ellos. AWS
- Amazon DynamoDB (DynamoDB): enumera y proporciona permisos de `Describe` para los recursos de Amazon DynamoDB asociados a su cuenta de AWS .
- Amazon ElastiCache (ElastiCache): proporciona `Describe` permisos para ElastiCache los recursos asociados a tu AWS cuenta.
- Amazon ElastiCache (Redis OSS) Serverless (ElastiCache (Redis OSS) Serverless): proporciona `Describe` permisos para las configuraciones sin servidor ElastiCache (Redis OSS) asociadas a su cuenta. AWS
- Amazon Elastic Compute Cloud (Amazon EC2): enumera y proporciona permisos de `Describe` para los recursos de Amazon EC2 asociados a su cuenta de AWS .
- Amazon Elastic Container Registry (Amazon ECR): proporciona `Describe` permisos para los recursos de Amazon ECR asociados a su cuenta. AWS
- Amazon Elastic Container Service (Amazon ECS): `Describe` proporciona permisos para los recursos de Amazon ECS asociados AWS a su cuenta.
- Amazon Elastic File System (Amazon EFS): proporciona `Describe` permisos para los recursos de Amazon EFS asociados a su AWS cuenta.

- Amazon Elastic Kubernetes Service (Amazon EKS): enumera y proporciona permisos de `Describe` para los recursos de Amazon EKS asociados a su cuenta de AWS .
- Amazon EC2 Auto Scaling: muestra y `Describe` proporciona permisos para los recursos de Amazon EC2 Auto Scaling que están asociados a su cuenta. AWS
- Amazon EC2 Systems Manager (SSM): `Describe` proporciona permisos para los recursos de SSM asociados a su cuenta. AWS
- AWS Fault Injection Service (AWS FIS): enumera los experimentos y las plantillas de AWS FIS experimentos que están asociados a su cuenta y proporciona `Describe` permisos para ellos. AWS
- Amazon FSx for Windows File Server (Amazon FSx): muestra los recursos de Amazon FSx asociados a su cuenta y proporciona `Describe` permisos para ellos. AWS
- Amazon RDS: muestra los recursos de Amazon RDS asociados a su AWS cuenta y proporciona `Describe` permisos para ellos.
- Amazon Route 53 (Route 53): enumera y proporciona permisos de `Describe` para los recursos de Route 53 asociados a su cuenta de AWS .
- Amazon Route 53 Resolver — Enumera los Amazon Route 53 Resolver recursos asociados a su AWS cuenta y proporciona `Describe` permisos para ellos.
- Amazon Simple Notification Service (Amazon SNS): enumera y proporciona permisos de `Describe` para los recursos de Amazon SNS asociados a su cuenta de AWS .
- Amazon Simple Queue Service (Amazon SQS): enumera y proporciona permisos de `Describe` para los recursos de Amazon SQS asociados a su cuenta de AWS .
- Amazon Simple Storage Service (Amazon S3): enumera y `Describe` proporciona permisos para los recursos de Amazon S3 que están asociados AWS a su cuenta.

> **Note**
>
> Mientras realiza una evaluación, si falta algún permiso que deba actualizarse desde las políticas administradas, AWS Resilience Hub completará correctamente la evaluación utilizando s3: GetBucketLogging permission. Sin embargo, AWS Resilience Hub mostrará un mensaje de advertencia con una lista de los permisos faltantes y proporcionará un período de gracia para añadirlos. Si no agrega los permisos que faltan dentro del período de gracia especificado, la evaluación fallará.

- AWS Backup — Muestra y obtiene `Describe` los permisos para los recursos de Amazon EC2 Auto Scaling asociados a AWS su cuenta.

- AWS CloudFormation — Enumera los recursos de las AWS CloudFormation pilas asociadas a su AWS cuenta y obtiene los `Describe` permisos correspondientes.
- AWS DataSync — Muestra los AWS DataSync recursos asociados a tu AWS cuenta y proporciona `Describe` permisos para ellos.
- Directory Service — Enumera los Directory Service recursos que están asociados a su AWS cuenta y proporciona `Describe` permisos para ellos.
- AWS Elastic Disaster Recovery (Elastic Disaster Recovery): proporciona `Describe` permisos para los recursos de Elastic Disaster Recovery asociados a su AWS cuenta.
- AWS Lambda (Lambda): muestra los recursos de Lambda asociados a su cuenta y proporciona `Describe` permisos para ellos. AWS
- Grupos de recursos de AWS (Resource Groups): muestra los recursos de Resource Groups asociados a su AWS cuenta y proporciona `Describe` permisos para ellos.
- AWS Service Catalog (Service Catalog): muestra y proporciona `Describe` permisos para los recursos del Service Catalog que están asociados a su AWS cuenta.
- AWS Step Functions — Muestra los AWS Step Functions recursos que están asociados a su AWS cuenta y proporciona `Describe` permisos para ellos.
- Elastic Load Balancing: muestra y proporciona `Describe` permisos para los recursos de Elastic Load Balancing que están asociados a su AWS cuenta.
- `ssm:GetParametersByPath`— Usamos este permiso para administrar CloudWatch las alarmas, las pruebas o los SOP configurados para su aplicación.

La siguiente política de IAM es necesaria para que una AWS cuenta añada permisos para los usuarios, grupos de usuarios y funciones que proporcionen los permisos necesarios para que su equipo pueda acceder a los AWS servicios mientras realiza las evaluaciones.

AWS Resilience Hub actualizaciones de AWS políticas administradas

Vea los detalles sobre las actualizaciones de las políticas AWS administradas AWS Resilience Hub desde que este servicio comenzó a rastrear estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial del AWS Resilience Hub documento.

Cambio	Descripción	Fecha
AWSResilienceHubAssessmentExecutionPolicy: cambio	AWS Resilience Hub actualizó `AWSResilienceHubAssessmentExecutionPolicy` la concesión `List` y `Get` los permisos para permitirle acceder a los experimentos AWS FIS mientras se ejecutan las evaluaciones.	17 de diciembre de 2024
AWSResilienceHubAssessmentExecutionPolicy: cambio	AWS Resilience Hub actualizó el `AWSResilienceHubAssessmentExecutionPolicy` para conceder `Describe` permisos que le permitan acceder a los recursos y configuraciones en Amazon ElastiCache (Redis OSS) Serverless mientras ejecuta las evaluaciones.	25 de septiembre de 2024
AWSResilienceHubAssessmentExecutionPolicy: cambio	AWS Resilience Hub la actualizó `AWSResilienceHubAsssessmentExecutionPolicy` para conceder `Describe` permisos que le permitieran acceder a los recursos y las configuraciones en Amazon DocumentDB, Elastic Load Balancing y AWS Lambda al ejecutar las evaluaciones.	1 de agosto de 2024

Cambio	Descripción	Fecha
AWSResilienceHubAssessmentExecutionPolicy: cambio	AWS Resilience Hub actualizó el `AWSResilienceHubAssessmentExecutionPolicy` para conceder `Describe` permisos que le permitieran leer la configuración de Amazon FSx for Windows File Server mientras se ejecutan las evaluaciones.	26 de marzo de 2024
AWSResilienceHubAssessmentExecutionPolicy: cambio	AWS Resilience Hub actualizó el `AWSResilienceHubAssessmentExecutionPolicy` para conceder `Describe` permisos que le permitieran leer la AWS Step Functions configuración mientras se ejecutan las evaluaciones.	30 de octubre de 2023
AWSResilienceHubAssessmentExecutionPolicy: cambio	AWS Resilience Hub actualizó el `AWSResilienceHubAssessmentExecutionPolicy` para conceder `Describe` permisos que le permitan acceder a los recursos de Amazon RDS mientras ejecuta las evaluaciones.	5 de octubre de 2023
AWSResilienceHubAssessmentExecutionPolicy—Nuevo	Esta AWS Resilience Hub política proporciona acceso a otros AWS servicios para realizar evaluaciones.	26 de junio de 2023

Cambio	Descripción	Fecha
AWS Resilience Hub comenzó a rastrear los cambios	AWS Resilience Hub comenzó a realizar un seguimiento de los cambios de sus políticas AWS gestionadas.	15 de junio de 2023

AWS Resilience Hub referencia de personas y permisos de IAM

Puedes conceder los permisos de IAM a las personas con las que es necesario trabajar AWS Resilience Hub mediante una política `AWSResilienceHubAsssessmentExecutionPolicy` AWS gestionada y una de las siguientes políticas específicas para cada persona. Para obtener más información sobre la política AWS gestionada, consulte. the section called “AWSResilienceHubAsssessmentExecutionPolicy”

Políticas para personas sugeridas por AWS Resilience Hub:

- Permisos de IAM para el personaje de administrador de aplicaciones de infraestructura
- Permisos de IAM para el personaje de administrador de continuidad empresarial
- Permisos de IAM para la persona propietaria de la aplicación
- Permisos de IAM para conceder acceso de solo lectura

Permisos de IAM para el personaje de administrador de aplicaciones de infraestructura

La siguiente política otorga los permisos necesarios para el personaje de administrador de aplicaciones de infraestructura.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "InfrastructureApplicationManager",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:AddDraftAppVersionResourceMappings",
        "resiliencehub:CreateAppVersionAppComponent",
```

```
        "resiliencehub:CreateAppVersionResource",
        "resiliencehub:CreateRecommendationTemplate",
        "resiliencehub:DeleteAppAssessment",
        "resiliencehub:DeleteAppInputSource",
        "resiliencehub:DeleteAppVersionAppComponent",
        "resiliencehub:DeleteAppVersionResource",
        "resiliencehub:DeleteRecommendationTemplate",
        "resiliencehub:Describe*",
        "resiliencehub:List*",
        "resiliencehub:PublishAppVersion",
        "resiliencehub:PutDraftAppVersionTemplate",
        "resiliencehub:RemoveDraftAppVersionResourceMappings",
        "resiliencehub:ResolveAppVersionResources",
        "resiliencehub:StartAppAssessment",
        "resiliencehub:TagResource",
        "resiliencehub:UntagResource",
        "resiliencehub:UpdateAppVersion",
        "resiliencehub:UpdateAppVersionAppComponent",
        "resiliencehub:UpdateAppVersionResource"
      ],
      "Resource": "*"
    }
  ]
}
```

Permisos de IAM para el personaje de administrador de continuidad empresarial

La siguiente política otorga los permisos necesarios para el personaje de gerente de continuidad empresarial.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "BusinessContinuityManager",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:CreateResiliencyPolicy",
        "resiliencehub:DeleteResiliencyPolicy",
        "resiliencehub:Describe*",
```

```
        "resiliencehub:List*",
        "resiliencehub:ResolveAppVersionResources",
        "resiliencehub:TagResource",
        "resiliencehub:UntagResource",
        "resiliencehub:UpdateAppVersion",
        "resiliencehub:UpdateAppVersionAppComponent",
        "resiliencehub:UpdateAppVersionResource",
        "resiliencehub:UpdateResiliencyPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Permisos de IAM para la persona propietaria de la aplicación

La siguiente política otorga los permisos necesarios para la persona propietaria de la aplicación.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "ApplicationOwner",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:AddDraftAppVersionResourceMappings",
        "resiliencehub:BatchUpdateRecommendationStatus",
        "resiliencehub:CreateApp",
        "resiliencehub:CreateAppVersionAppComponent",
        "resiliencehub:CreateAppVersionResource",
        "resiliencehub:CreateRecommendationTemplate",
        "resiliencehub:CreateResiliencyPolicy",
        "resiliencehub:DeleteApp",
        "resiliencehub:DeleteAppAssessment",
        "resiliencehub:DeleteAppInputSource",
        "resiliencehub:DeleteAppVersionAppComponent",
        "resiliencehub:DeleteAppVersionResource",
        "resiliencehub:DeleteRecommendationTemplate",
        "resiliencehub:DeleteResiliencyPolicy",
        "resiliencehub:Describe*",
```

```
        "resiliencehub:ImportResourcesToDraftAppVersion",
        "resiliencehub:List*",
        "resiliencehub:PublishAppVersion",
        "resiliencehub:PutDraftAppVersionTemplate",
        "resiliencehub:RemoveDraftAppVersionResourceMappings",
        "resiliencehub:ResolveAppVersionResources",
        "resiliencehub:StartAppAssessment",
        "resiliencehub:TagResource",
        "resiliencehub:UntagResource",
        "resiliencehub:UpdateApp",
        "resiliencehub:UpdateAppVersion",
        "resiliencehub:UpdateAppVersionAppComponent",
        "resiliencehub:UpdateAppVersionResource",
        "resiliencehub:UpdateResiliencyPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Permisos de IAM para conceder acceso de solo lectura

La siguiente política concede los permisos necesarios para el acceso de solo lectura.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "ReadOnly",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:Describe*",
        "resiliencehub:List*",
        "resiliencehub:ResolveAppVersionResources"
      ],
      "Resource": "*"
    }
  ]
}
```

Importación del archivo de estado de Terraform a AWS Resilience Hub

AWS Resilience Hub admite la importación de archivos de estado de Terraform cifrados mediante cifrado del lado del servidor (SSE) con claves administradas de Amazon Simple Storage Service (SSE-S3) o con claves AWS Key Management Service administradas (). SSE-KMS Si sus archivos de estado de Terraform se cifran con claves de cifrado proporcionadas por el cliente (SSE-C), no podrá importarlos con ellas. AWS Resilience Hub

La importación de archivos de estado de Terraform a archivos de estado AWS Resilience Hub requiere las siguientes políticas de IAM, según la ubicación del archivo de estado.

Importar archivos de estado de Terraform desde un bucket de Amazon S3 ubicado en la cuenta principal

Se requieren las siguientes políticas de bucket de Amazon S3 y de IAM para permitir a AWS Resilience Hub el acceso de solo lectura a los archivos de estado de Terraform ubicados en un bucket de Amazon S3 de la cuenta principal.

- Política de bucket: política de bucket en el bucket de Amazon S3 de destino, que se encuentra en la cuenta principal. Para obtener más información, consulte el siguiente ejemplo.
- Política de identidad: la política de identidad asociada a la función de invocador definida para esta aplicación o a la función de IAM AWS actual de AWS Resilience Hub la cuenta principal. AWS Para obtener más información, consulte el siguiente ejemplo.

  JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<s3-bucket-name>/<path-to-state-file>"
    },
    {
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<s3-bucket-name>"
    }
  ]
}
```

> **Note**
>
> Si utiliza la política administrada por `AWSResilienceHubAsssessmentExecutionPolicy`, no se requiere permiso de `ListBucket`.

> **Note**
>
> Si sus archivos de estado de Terraform están cifrados mediante KMS, debe añadir el siguiente permiso de `kms:Decrypt`.

```
{
      "Effect": "Allow",
      "Action": [
              "kms:Decrypt",
      ],
      "Resource": "<arn_of_kms_key>"
}
```

Importar archivos de estado de Terraform desde un bucket de Amazon S3 ubicado en una cuenta secundaria

- Política de bucket: política de bucket en el bucket de Amazon S3 de destino, que se encuentra en una de las cuentas secundarias. Para obtener más información, consulte el siguiente ejemplo.
- Política de identidad: la política de identidad asociada al rol de AWS cuenta, que se ejecuta AWS Resilience Hub en la cuenta principal AWS . Para obtener más información, consulte el siguiente ejemplo.

> **Note**
>
> Si utiliza la política administrada por `AWSResilienceHubAsssessmentExecutionPolicy`, no se requiere permiso de `ListBucket`.

> **Note**
>
> Si sus archivos de estado de Terraform están cifrados mediante KMS, debe añadir el siguiente permiso de `kms:Decrypt`.

```
{
      "Effect": "Allow",
      "Action": [
              "kms:Decrypt",
      ],
      "Resource": "<arn_of_kms_key>"
}
```

Habilitación AWS Resilience Hub acceso a su clúster de Amazon Elastic Kubernetes Service

AWS Resilience Hub evalúa la resiliencia de un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) mediante el análisis de la infraestructura de su clúster de Amazon EKS. AWS Resilience Hub utiliza la configuración de control de acceso basado en roles (RBAC) de Kubernetes para evaluar otras cargas de trabajo de Kubernetes (K8), que se implementan como parte del clúster de Amazon EKS. AWS Resilience Hub Para consultar su clúster de Amazon EKS para analizar y evaluar la carga de trabajo, debe completar lo siguiente:

- Cree o utilice un rol AWS Identity and Access Management (IAM) existente en la misma cuenta que el clúster de Amazon EKS.
- Permitir el acceso de los roles y usuarios de IAM a su clúster de Amazon EKS y conceder permisos adicionales de solo lectura a los recursos de K8 incluidos en el clúster de Amazon EKS. Para obtener más información sobre cómo habilitar el acceso de los roles y usuarios de IAM a su clúster de Amazon EKS, consulte Habilitar el acceso de roles y usuarios de IAM a su clúster: Amazon EKS.

El acceso al clúster Amazon EKS mediante las entidades de AWS IAM está habilitado por el Autenticador de IAM para Kubernetes, que se ejecuta en el plano de control de Amazon EKS. El autenticador obtiene la información de la configuración de `aws-auth ConfigMap`.

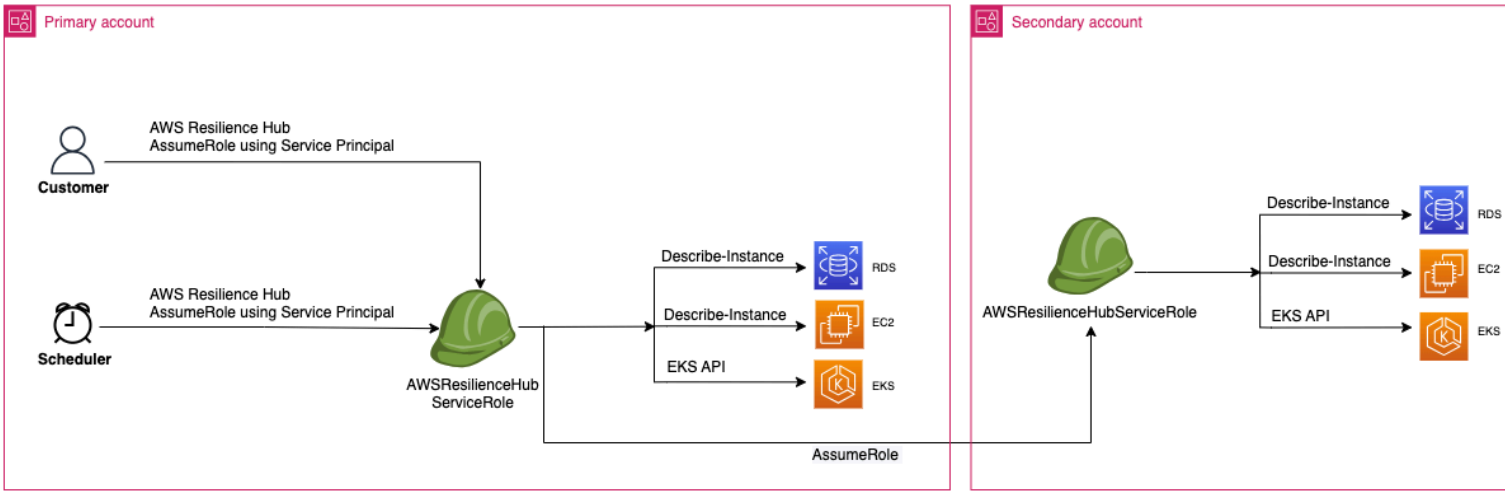
> **Note**
>
> - Para obtener más información sobre todos los `aws-auth ConfigMap` ajustes, consulte Formato de configuración completo en GitHub.
> - Para obtener más información acerca de las diferentes identidades de IAM, consulte Identidades (usuarios, grupos y roles) en la Guía del usuario de IAM.
> - Para obtener más información sobre la configuración del control de acceso basado en roles (RBAC) de Kubernetes, consulte Uso de la autorización de RBAC.

AWS Resilience Hub consulta los recursos de su clúster de Amazon EKS mediante un rol de IAM en su cuenta. Para acceder AWS Resilience Hub a los recursos de su clúster de Amazon EKS, la función de IAM utilizada por AWS Resilience Hub debe asignarse a un grupo de Kubernetes con suficientes permisos de solo lectura para los recursos de su clúster de Amazon EKS.

AWS Resilience Hub permite acceder a los recursos de su clúster de Amazon EKS mediante una de las siguientes opciones de rol de IAM:

- Si su aplicación está configurada para utilizar el acceso basado en roles para acceder a los recursos, el rol de invocador o el rol de cuenta secundaria transferido a AWS Resilience Hub al crear una aplicación se utilizarán para acceder a su clúster de Amazon EKS durante la evaluación.

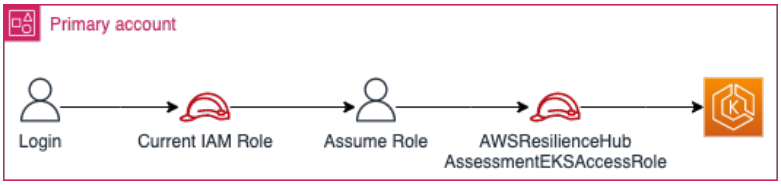
  El siguiente diagrama conceptual muestra cómo AWS Resilience Hub accede a los clústeres de Amazon EKS cuando la aplicación está configurada como una aplicación basada en roles.



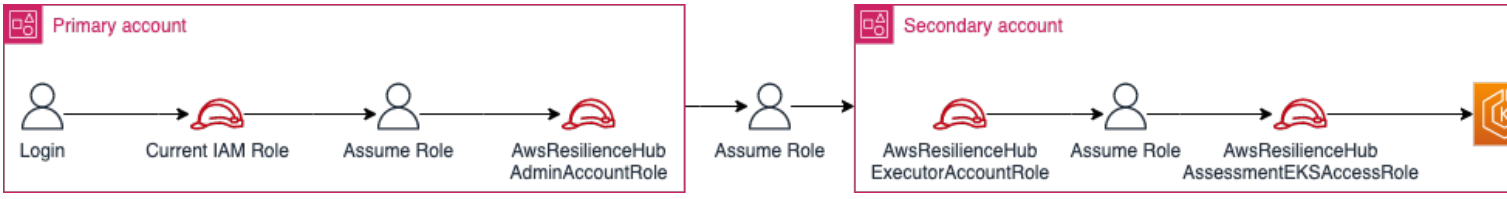
- Si su aplicación está configurada para utilizar el usuario de IAM actual para acceder al recurso, debe crear un nuevo rol de IAM con el nombre

`AwsResilienceHubAssessmentEKSAccessRole` en la misma cuenta que el del clúster de Amazon EKS. Este rol de IAM se utilizará entonces para acceder a su clúster de Amazon EKS.

El siguiente diagrama conceptual muestra cómo AWS Resilience Hub accede a los clústeres de Amazon EKS implementados en su cuenta principal cuando la aplicación está configurada para usar los permisos de usuario de IAM actuales.



El siguiente diagrama conceptual muestra cómo se AWS Resilience Hub accede a los clústeres de Amazon EKS implementados en una cuenta secundaria cuando la aplicación está configurada para usar los permisos de usuario de IAM actuales.



Concesión AWS Resilience Hub acceso a los recursos de su clúster de Amazon EKS

AWS Resilience Hub le permite acceder a los recursos ubicados en los clústeres de Amazon EKS siempre que haya configurado los permisos necesarios.

Para conceder los permisos necesarios a AWS Resilience Hub para descubrir y evaluar los recursos del clúster Amazon EKS

1. Configure un rol de IAM para acceder al clúster de Amazon EKS.

   Si ha configurado la aplicación mediante el acceso basado en roles, puede omitir este paso y continuar con el paso 2 y usar el rol que utilizó para crear la aplicación. Para obtener más información acerca de cómo AWS Resilience Hub utiliza roles de IAM, consulte the section called “Cómo AWS Resilience Hub funciona con IAM”.

   Si ha configurado la aplicación con los permisos de usuario de IAM actuales, debe crear el rol de IAM `AwsResilienceHubAssessmentEKSAccessRole` en la misma cuenta que la del clúster de Amazon EKS. Este rol de IAM se utilizará entonces al acceder a su clúster de Amazon EKS.

Al importar y evaluar su aplicación, AWS Resilience Hub utiliza una función de IAM para acceder a los recursos de su clúster de Amazon EKS. Esta función debe crearse en la misma cuenta que su clúster de Amazon EKS y se asignará a un grupo de Kubernetes que incluya los permisos necesarios AWS Resilience Hub para evaluar su clúster de Amazon EKS.

Si su clúster de Amazon EKS está en la misma cuenta que la cuenta de AWS Resilience Hub llamada, el rol debe crearse mediante la siguiente política de confianza de IAM. En esta política de confianza de IAM, `caller_IAM_role` se utiliza en la cuenta corriente para solicitar las API. AWS Resilience Hub

> **Note**
>
> `caller_IAM_role`Es el rol que está asociado a su cuenta AWS de usuario.

Si su clúster de Amazon EKS está en una cuenta cruzada (una cuenta diferente AWS Resilience Hub a la cuenta de llamada), debe crear el rol de `AwsResilienceHubAssessmentEKSAccessRole` IAM mediante la siguiente política de confianza de IAM:

> **Note**
>
> Como requisito previo, para acceder al clúster de Amazon EKS que está desplegado en una cuenta diferente a la cuenta del AWS Resilience Hub usuario, debe configurar el acceso a varias cuentas. Para obtener más información, consulte

2. Cree `ClusterRole` `ClusterRoleBinding` (o`RoleBinding`) roles para la AWS Resilience Hub aplicación.

   Creando `ClusterRole` y `ClusterRoleBinding` concediendo los permisos de solo lectura necesarios AWS Resilience Hub para analizar y evaluar los recursos que forman parte de determinados espacios de nombres de su clúster de Amazon EKS.

   AWS Resilience Hub le permite limitar su acceso a sus espacios de nombres para generar evaluaciones de resiliencia realizando una de las siguientes acciones:

   a. Conceder a la aplicación de AWS Resilience Hub acceso de lectura a todos los espacios de nombres.

AWS Resilience Hub Para evaluar la resiliencia de los recursos en todos los espacios de nombres de un clúster de Amazon EKS, debe crear los siguientes y. `ClusterRole` `ClusterRoleBinding`

- `resilience-hub-eks-access-cluster-role`(`ClusterRole`): define los permisos necesarios AWS Resilience Hub para evaluar su clúster de Amazon EKS.
- `resilience-hub-eks-access-cluster-role-binding` (`ClusterRoleBinding`): define un grupo denominado `resilience-hub-eks-access-group` en su clúster de Amazon EKS que concede a sus usuarios los permisos necesarios para ejecutar evaluaciones de resiliencia en AWS Resilience Hub.

La plantilla para conceder a la aplicación de AWS Resilience Hub acceso de lectura en todos los espacios de nombres es la siguiente:

```
cat << EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: resilience-hub-eks-access-cluster-role
rules:
- apiGroups:
    - ""
  resources:
    - pods
    - replicationcontrollers
    - nodes
  verbs:
    - get
    - list
- apiGroups:
    - apps
  resources:
    - deployments
    - replicasets
  verbs:
    - get
    - list
- apiGroups:
    - policy
```

```
  resources:
    - poddisruptionbudgets
  verbs:
    - get
    - list
- apiGroups:
    - autoscaling.k8s.io
  resources:
    - verticalpodautoscalers
  verbs:
    - get
    - list
- apiGroups:
    - autoscaling
  resources:
    - horizontalpodautoscalers
  verbs:
    - get
    - list
- apiGroups:
    - karpenter.sh
  resources:
    - provisioners
    - nodepools
  verbs:
    - get
    - list
- apiGroups:
    - karpenter.k8s.aws
  resources:
    - awsnodetemplates
    - ec2nodeclasses
  verbs:
    - get
    - list
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: resilience-hub-eks-access-cluster-role-binding
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
```

```
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-cluster-role
  apiGroup: rbac.authorization.k8s.io
---
EOF
```

b. AWS Resilience Hub Otorga el acceso para leer espacios de nombres específicos.

Puede limitar el acceso AWS Resilience Hub a los recursos dentro de un conjunto específico de espacios de nombres utilizando. `RoleBinding` Para ello, debe crear los siguientes roles:

- `ClusterRole`— Para acceder AWS Resilience Hub a los recursos en espacios de nombres específicos dentro de un clúster de Amazon EKS y evaluar su resiliencia, debe crear las siguientes funciones. `ClusterRole`
  - `resilience-hub-eks-access-cluster-role`: especifica los permisos necesarios para evaluar los recursos dentro de espacios de nombres específicos.
  - `resilience-hub-eks-access-global-cluster-role`— Especifica los permisos necesarios para evaluar los recursos con ámbito de clúster, que no están asociados a un espacio de nombres específico, dentro de sus clústeres de Amazon EKS. AWS Resilience Hub requiere permisos para acceder a los recursos del ámbito del clúster (como los nodos) de su clúster de Amazon EKS a fin de evaluar la resiliencia de la aplicación.

  La plantilla para crear el rol de `ClusterRole` es la siguiente:

```
cat << EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: resilience-hub-eks-access-cluster-role
rules:
  - apiGroups:
      - ""
    resources:
      - pods
      - replicationcontrollers
    verbs:
      - get
```

```
      - list
  - apiGroups:
      - apps
    resources:
      - deployments
      - replicasets
    verbs:
      - get
      - list
  - apiGroups:
      - policy
    resources:
      - poddisruptionbudgets
    verbs:
      - get
      - list
  - apiGroups:
      - autoscaling.k8s.io
    resources:
      - verticalpodautoscalers
    verbs:
      - get
      - list
  - apiGroups:
      - autoscaling
    resources:
      - horizontalpodautoscalers
    verbs:
      - get
      - list

---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: resilience-hub-eks-access-global-cluster-role
rules:
  - apiGroups:
      - ""
    resources:
      - nodes
    verbs:
      - get
      - list
```

```
  - apiGroups:
      - karpenter.sh
    resources:
      - provisioners
      - nodepools
    verbs:
      - get
      - list
  - apiGroups:
      - karpenter.k8s.aws
    resources:
      - awsnodetemplates
      - ec2nodeclasses
    verbs:
      - get
      - list

---
EOF
```

- `RoleBinding`rol: este rol otorga los permisos necesarios para acceder AWS Resilience Hub a los recursos dentro de espacios de nombres específicos. Es decir, debes crear un `RoleBinding` rol en cada espacio de nombres para poder acceder AWS Resilience Hub a los recursos dentro del espacio de nombres determinado.

  > **Note**
  >
  > Si utiliza `ClusterAutoscaler` para el ajuste de escala automático, también debe crear `RoleBinding` en el `kube-system`. Esto es necesario para evaluar su `ClusterAutoscaler`, que forma parte del espacio de nombres de `kube-system`.
  > De este modo, concederá AWS Resilience Hub los permisos necesarios para evaluar los recursos dentro del espacio de `kube-system` nombres mientras evalúa su clúster de Amazon EKS.

  La plantilla para crear el rol de `RoleBinding` es la siguiente:

```
cat << EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
```

```
kind: RoleBinding
metadata:
  name: resilience-hub-eks-access-cluster-role-binding
  namespace: <namespace>
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-cluster-role
  apiGroup: rbac.authorization.k8s.io

---
EOF
```

- `ClusterRoleBinding`rol: este rol otorga los permisos necesarios para acceder AWS Resilience Hub a los recursos del ámbito del clúster.

  La plantilla para crear el rol de `ClusterRoleBinding` es la siguiente:

```
cat << EOF | kubectl apply -f -
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: resilience-hub-eks-access-global-cluster-role-binding
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-global-cluster-role
  apiGroup: rbac.authorization.k8s.io

---
EOF
```

3. Actualice `aws-auth ConfigMap` para asignar el `resilience-hub-eks-access-group` al rol de IAM utilizado para acceder al clúster de Amazon EKS.

Este paso crea una asignación entre el rol de IAM utilizado en el paso 1 y el grupo de Kubernetes creado en el paso 2. Esta asignación otorga permisos a los roles de IAM para acceder a los recursos del clúster de Amazon EKS.

> **Note**
>
> - `ROLE-NAME` hace referencia al rol de IAM que se utiliza para acceder al clúster de Amazon EKS.
>   - Si la aplicación está configurada para usar el acceso basado en roles, el rol debe ser el rol de invocador o el rol de cuenta secundaria al que se transfiere al crear la aplicación. AWS Resilience Hub
>   - Si su aplicación está configurada para utilizar el usuario de IAM actual para acceder a los recursos, debe ser el de `AwsResilienceHubAssessmentEKSAccessRole`.
> - `ACCOUNT-ID`debe ser el ID de AWS cuenta del clúster de Amazon EKS.

Puede crear el `aws-auth ConfigMap` utilizando una de las siguientes maneras:

- Uso de `eksctl`

  Use el siguiente comando para actualizar el `aws-auth ConfigMap`:

  ```
  eksctl create iamidentitymapping \
   --cluster <cluster-name> \
   --region=<region-code> \
   --arn arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>\
   --group resilience-hub-eks-access-group \
   --username AwsResilienceHubAssessmentEKSAccessRole
  ```

- Puede editar manualmente `aws-auth ConfigMap` añadiendo los datos del rol de IAM a la sección `mapRoles` de los datos secundarios de `ConfigMap`. Utilice el siguiente comando para editar el archivo `aws-auth ConfigMap`.

  ```
  kubectl edit -n kube-system configmap/aws-auth
  ```

  La sección `mapRoles` consta de los siguientes parámetros:

- `rolearn`: el nombre de recurso de Amazon (ARN) del rol de IAM que se agregará.
  - Sintaxis del ARN: `arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>`.
- `username`: nombre del usuario de Kubernetes al que se mapea el rol de IAM (`AwsResilienceHubAssessmentEKSAccessRole`).
- `groups`: los nombres de los grupos deben coincidir con los nombres de los grupos creados en el Paso 2 (`resilience-hub-eks-access-group`).

> **Note**
>
> Si la sección `mapRoles` no existe, debe añadirla manualmente.

Utilice la siguiente plantilla para añadir la información del rol de IAM a la sección `mapRoles` de los datos secundarios de `ConfigMap`.

```
- groups:
  - resilience-hub-eks-access-group
  rolearn: arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>
  username: AwsResilienceHubAssessmentEKSAccessRole
```

Habilitación AWS Resilience Hub para publicar en tus temas de Amazon Simple Notification Service

En esta sección se explica cómo AWS Resilience Hub habilitar la publicación de notificaciones sobre la aplicación en los temas del Amazon Simple Notification Service (Amazon SNS). Para enviar notificaciones a un tema de Amazon SNS, asegúrese de tener lo siguiente:

- Una AWS Resilience Hub aplicación activa.
- Un tema de Amazon SNS existente al que se AWS Resilience Hub deben enviar notificaciones. Para obtener más información sobre la creación de un tema de Amazon SNS, consulte Creación de un tema de Amazon SNS.

AWS Resilience Hub Para habilitar la publicación de notificaciones en su tema de Amazon SNS, debe actualizar la política de acceso del tema de Amazon SNS con lo siguiente:

> **Note**
>
> Cuando publicas AWS Resilience Hub mensajes de regiones con suscripción voluntaria en temas ubicados en regiones que están habilitadas de forma predeterminada, debes modificar la política de recursos creada para el tema de Amazon SNS. Cambie el valor de la entidad principal de `resiliencehub.amazonaws.com` a `resiliencehub.<opt-in-region>.amazonaws.com`.

Si utiliza un tema de Amazon SNS cifrado del servidor (SSE), debe asegurarse de que AWS Resilience Hub tiene el acceso `Decrypt` y `GenerateDataKey*` a la clave de cifrado de Amazon SNS.

Para proporcionar `Decrypt GenerateDataKey*` acceso a él AWS Resilience Hub, debe incluir la siguiente política de permisos de AWS Key Management Service acceso.

Limitar los permisos para incluir o excluir AWS Resilience Hub recomendaciones

AWS Resilience Hub permite restringir los permisos para incluir o excluir recomendaciones por aplicación. Puede restringir los permisos para incluir o excluir recomendaciones por aplicación mediante la siguiente política de confianza de IAM. En esta política de confianza de IAM, `caller_IAM_role` (asociada a su cuenta de AWS usuario) se utiliza en la cuenta corriente para AWS Resilience Hub solicitar las API.

Seguridad de la infraestructura en AWS Resilience Hub

Como servicio gestionado, AWS Resilience Hub está protegido por los procedimientos de seguridad de la red AWS global que se describen en el white paper Amazon Web Services: Overview of Security Processes.

Utiliza las llamadas a la API AWS publicadas para acceder a AWS Resilience Hub través de la red. Los clientes deben ser compatibles con Transport Layer Security (TLS) 1.2 o con una versión posterior. Recomendamos TLS 1.3 o una versión posterior. Los clientes también deben admitir conjuntos de cifrado con perfecto secreto directo (PFS), como Ephemeral (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Diffie-Hellman La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puedes utilizar AWS

Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Controles de resiliencia para AWS servicios

En este capítulo se proporcionan los detalles de las diversas comprobaciones de resiliencia realizadas AWS Resilience Hub por AWS los servicios compatibles para garantizar que las posturas de resiliencia de las aplicaciones no se vean afectadas. Estas comprobaciones estiman el objetivo de tiempo de recuperación (RTO) y el objetivo del punto de recuperación (RPO) en función de los valores definidos en la política de resiliencia para cada componente de la aplicación (). AppComponent Las evaluaciones abarcan diferentes tipos de interrupciones, es decir, las fallas en las aplicaciones, la infraestructura, las interrupciones en las zonas de disponibilidad y las fallas regionales. Sin embargo, para realizar estas comprobaciones, debe proporcionar los permisos de IAM pertinentes AWS Resilience Hub para que pueda acceder a sus recursos. Para obtener más información sobre los permisos de IAM necesarios para acceder AWS Resilience Hub a sus recursos y realizar las comprobaciones de resiliencia de este capítulo, consulte. AWS políticas gestionadas para AWS Resilience Hub

AWS servicios

- Amazon Elastic File System
- Amazon Relational Database Service y Amazon Aurora
- Amazon Simple Storage Service
- Amazon DynamoDB
- Amazon Elastic Compute Cloud
- Amazon EBS
- AWS Lambda
- Amazon Elastic Kubernetes Service
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- Amazon Elastic Container Service
- Elastic Load Balancing
- Amazon API Gateway
- Amazon DocumentDB
- Puerta de enlace NAT

- Amazon Route 53
- Controlador de recuperación de aplicaciones (ARC) de Amazon
- Amazon FSx para Windows File Server
- AWS Step Functions
- Amazon ElastiCache (Redis OSS)

Amazon Elastic File System

En esta sección se enumeran todas las comprobaciones y recomendaciones de resiliencia específicas de Amazon Elastic File System. Para obtener más información sobre Amazon Elastic File System, consulte la documentación de Amazon Elastic File System.

Tipo de sistema de archivos

AWS Resilience Hub comprueba el tipo de sistema de archivos: regional o de una sola zona. El tipo de sistema de archivos afecta a su capacidad de recuperación en caso de que se produzcan interrupciones en la infraestructura o en la zona de disponibilidad. Para obtener más información sobre los tipos de sistemas de archivos, consulte Disponibilidad y durabilidad de los sistemas de archivos de Amazon EFS.

Backup del sistema de archivos

AWS Resilience Hub comprueba si se ha definido un AWS Backup plan para el sistema de archivos desplegado. Además, verifica si la opción de `Cross-Region` copia de seguridad está habilitada, lo que garantiza la cobertura en caso de que su póliza lo exija en caso Region-level de que así lo exija.

Replicación de los datos

AWS Resilience Hub comprueba si se ha definido una replicación de datos de Amazon EFS dentro o entre regiones para el sistema de archivos implementado. La replicación de datos de Amazon EFS ayuda a mejorar el RTO estimado y el RPO estimado a nivel de aplicación, infraestructura, zona de disponibilidad y región. Además, AWS Resilience Hub comprueba si se combina con un sistema IN Region AWS Backup para permitir la resiliencia del sistema de archivos en caso de que se interrumpa la aplicación.

Amazon Relational Database Service y Amazon Aurora

En esta sección se enumeran todas las comprobaciones y recomendaciones de resiliencia específicas de Amazon Relational Database Service y Amazon Aurora. Para obtener más información sobre Amazon Relational Database Service y Amazon Aurora, consulte la documentación de Amazon Relational Database Service.

Single-AZ despliegue

AWS Resilience Hub comprueba si la base de datos está desplegada como una sola instancia y, si se determina, indica que no admite la instancia secundaria ni la réplica de lectura.

Multi-AZ despliegue

AWS Resilience Hub comprueba si la base de datos se implementa con una instancia secundaria o con réplicas de lectura. Si la base de datos se implementa con una réplica de lectura, AWS Resilience Hub valida si se implementa en una zona de disponibilidad diferente para permitir la conmutación por error en caso de que se produzca una interrupción en la zona de disponibilidad.

Copia de seguridad

AWS Resilience Hub comprueba si las siguientes capacidades de copia de seguridad se aplican a una instancia de base de datos implementada.

- AWS Backup planifique con la opción de copia de seguridad automática
- AWS Backup planifique con una copia de seguridad para todas las regiones si así lo exige su póliza
- Instantáneas manuales para sistemas de respaldo de terceros

Cross-Region conmutación por error

AWS Resilience Hub comprueba los objetivos de RTO y RPO definidos en la política de resiliencia para recuperarse de una disrupción regional. Además, AWS Resilience Hub puede identificar las siguientes arquitecturas interregionales para cubrir las disrupciones regionales:

- Una copia de seguridad regional con una copia de una instantánea entre regiones
- Una réplica de lectura en otra región

- Una base de datos global de Amazon Aurora con un clúster secundario en otra región
- Una base de datos global de Amazon Aurora con un clúster secundario independiente en otra región

Conmutación por error en la región más rápida

AWS Resilience Hub comprueba los objetivos de RTO y RPO definidos en la política de resiliencia durante las interrupciones en la infraestructura o en las zonas urbanizadas. Además, AWS Resilience Hub puede identificar las siguientes arquitecturas regionales para cubrir las interrupciones en las aplicaciones, la infraestructura y las zonas de disponibilidad:

- ¿Una copia de seguridad In-Region
- Una réplica de lectura en una zona de disponibilidad diferente
- Un cúmulo de Aurora con una réplica de lectura en otra AZ
- Una Multi-AZ instancia de Amazon Relational Database Service (Amazon RDS)
- Un clúster de Amazon RDS Multi-AZ
- Una sola instancia de Amazon RDS con una réplica de lectura en otra zona de disponibilidad

Amazon Simple Storage Service

En esta sección se enumeran todas las comprobaciones y recomendaciones de resiliencia específicas de Amazon Simple Storage Service (Amazon S3). Para obtener más información sobre Amazon S3, consulte la documentación de Amazon S3.

Control de versiones

AWS Resilience Hub verifica si un bucket de Amazon S3 está configurado con el control de versiones activado.

Copia de seguridad programada

AWS Resilience Hub comprueba si se ha definido un AWS Backup plan para el bucket de Amazon Simple Storage Service (Amazon S3) desplegado. Además, también comprueba si la opción de copia de seguridad entre regiones está habilitada si su póliza requiere cobertura en caso de Region-level interrupciones.

Point-in-time recuperación

AWS Resilience Hub comprueba si el objetivo de RPO de su política de resiliencia exige una recuperación puntual (PITR). Sin embargo, el PITR no admite copias de seguridad entre regiones. Por lo tanto, puede utilizar un AWS Backup plan programado existente con la opción de copia de seguridad entre regiones habilitada o crear uno nuevo.

Replicación de los datos

AWS Resilience Hub comprueba si se han definido una replicación en la misma región (SRR) y una replicación entre regiones (CRR) para el bucket de Amazon S3 implementado. La replicación de datos de Amazon S3 mejora el RTO de la carga de trabajo estimada y el RPO de la carga de trabajo estimada a nivel de aplicación, infraestructura, zona de disponibilidad y región. Además, también protege contra la eliminación física del objeto, ya que la eliminación de una versión del objeto no se replica en el bucket de Amazon S3 de destino. Además, en función de los objetivos de RTO definidos en su política de resiliencia, AWS Resilience Hub comprueba si Amazon S3 Replication Time Control (S3 RTC) debe estar habilitado o no. Esta función facturable replica el 99,99 por ciento de los objetos del bucket de origen en 15 minutos.

- AWS Backup planifique con la opción de copia de seguridad automática
- AWS Backup planifique con una copia de seguridad para todas las regiones si así lo exige su póliza
- Instantáneas manuales para sistemas de respaldo de terceros

Amazon DynamoDB

En esta sección se enumeran todas las comprobaciones de resiliencia y las recomendaciones específicas de Amazon DynamoDB. Para obtener más información sobre Amazon DynamoDB, consulte la documentación de Amazon DynamoDB.

Copia de seguridad programada

AWS Resilience Hub comprueba si ya hay una copia de seguridad definida para la tabla implementada. Además, también comprueba si la copia de seguridad entre regiones debe configurarse para su póliza si requiere cobertura en caso de Region-level interrupciones.

Point-in-time recuperación

AWS Resilience Hub comprueba si se requiere una recuperación puntual (PITR) de acuerdo con el objetivo de RPO de su política de resiliencia. Sin embargo, el PITR no admite copias de seguridad entre regiones. Por lo tanto, puede utilizar un AWS Backup plan programado existente con la opción de copia de seguridad entre regiones habilitada o crear uno nuevo.

Tabla global

AWS Resilience Hub comprueba si la tabla de Amazon DynamoDB desplegada está definida como una tabla global con una o más réplicas en otras regiones. La configuración de la tabla global mejora el RTO de la carga de trabajo estimada y el RPO de la carga de trabajo estimada a nivel regional, y también permite trabajar en modos multirregionales activo-activo o activo-pasivo. AWS Backup o Amazon DynamoDB PITR se puede utilizar en una de las regiones para gestionar las interrupciones de las aplicaciones.

Amazon Elastic Compute Cloud

En esta sección se enumeran todas las comprobaciones y recomendaciones de resiliencia específicas de Amazon Elastic Compute Cloud. Para obtener más información sobre Amazon Elastic Compute Cloud, consulte la documentación de Amazon Elastic Compute Cloud.

Instancia con estado

AWS Resilience Hub identifica una instancia de Amazon EC2 como instancia con estado si se cumple uno de los siguientes criterios:

- Si el `DeleteOnTermination` atributo está establecido en false para al menos un volumen de Amazon Elastic Block Store (Amazon EBS) adjunto a esta instancia.
- Si Amazon Data Lifecycle Manager o un AWS Backup plan están adjuntos a la instancia de Amazon EC2 o al menos a un volumen de Amazon EBS.
- AWS Elastic Disaster Recovery Se utiliza para replicar los volúmenes de almacenamiento de sus instancias Amazon EC2.

> **Note**
>
> Si una instancia de Amazon EC2 no cumple ninguno de los criterios anteriores, la considerará una AWS Resilience Hub instancia Amazon EC2 sin estado.

Grupos de escalado automático

AWS Resilience Hub comprueba si hay un grupo de instancias Amazon EC2 sin estado. Si se descubre, se recomienda orquestar lo mismo utilizando grupos de Auto Scaling (ASG) con Multi-AZ configuración. Si se identifica un ASG existente, ARH verificará si está configurado en varias zonas de disponibilidad. Si ASG también se define utilizando únicamente instancias Amazon EC2 puntuales, se recomienda aumentar su capacidad con instancias Amazon EC2 bajo demanda para mejorar la resiliencia cuando las instancias puntuales de Amazon EC2 no estén disponibles.

Flota de Amazon EC2

AWS Resilience Hub identifica la flota de Amazon EC2 y verifica si está definida como Multi-AZ implementación y también si solo utiliza instancias puntuales de Amazon EC2. Definir una flota de Amazon EC2 como Multi-AZ despliegue mejorará su resiliencia en caso de que se produzca una interrupción en la zona de disponibilidad. Aumentar la flota de Amazon EC2 con instancias bajo demanda mejorará su resiliencia cuando las instancias puntuales no estén disponibles.

Amazon EBS

En esta sección se enumeran todas las comprobaciones y recomendaciones de resiliencia específicas de Amazon EBS. Para obtener más información sobre Amazon EBS, consulte la documentación de Amazon EBS.

Copia de seguridad programada

AWS Resilience Hub comprueba si uno o ambos de los siguientes elementos están definidos para sus volúmenes de Amazon EBS.

- Una regla de respaldo para un volumen de Amazon EBS específico adjunto a su instancia de Amazon EC2.
- Una regla de respaldo para crear una EBS-backed AMI de Amazon en su instancia de Amazon EC2.
- Instantáneas manuales para sistemas de respaldo de terceros.

Además, si tu póliza requiere una cobertura en caso de Region-level interrupciones, AWS Resilience Hub comprueba si tu regla de copia de seguridad tiene habilitada la opción de copia de seguridad entre regiones.

Respaldo y replicación de datos

AWS Resilience Hub identifica que un volumen de Amazon EBS se considera un volumen con estado si se cumple uno de los siguientes criterios:

- Si el `DeleteOnTermination` atributo está establecido en false para este volumen de Amazon EBS.
- Si Amazon Data Lifecycle Manager o un AWS Backup plan están asociados a este volumen de Amazon EBS o a la instancia de Amazon EC2 a la que está conectado.
- AWS Elastic Disaster Recovery Se utiliza para replicar los volúmenes de almacenamiento de sus instancias Amazon EC2.

AWS Lambda

En esta sección se enumeran todas las comprobaciones de resiliencia y las recomendaciones específicas de AWS Lambda. Para obtener más información al respecto AWS Lambda, consulte AWS Lambda la documentación.

Acceso de clientes a Amazon VPC

AWS Resilience Hub identifica una AWS Lambda función conectada a la VPC. La conexión AWS Lambda a subredes en diferentes zonas de disponibilidad de su Amazon VPC permite la resiliencia de las funciones en caso de que se produzca una interrupción en la zona de disponibilidad.

Dead-letter cola

AWS Resilience Hub comprueba si una AWS Lambda función tiene una cola de letras muertas (DLQ) adjunta para almacenar las solicitudes fallidas. Adjuntar un DLQ a una AWS Lambda función permite evitar la pérdida de datos de las solicitudes y volver a intentar procesar las solicitudes fallidas en una etapa posterior.

Amazon Elastic Kubernetes Service

En esta sección se enumeran todas las comprobaciones y recomendaciones de resiliencia específicas de Amazon Elastic Kubernetes Service (Amazon EKS). Para obtener más información sobre Amazon EKS, consulte la documentación de Amazon EKS.

Multi-AZ despliegue

AWS Resilience Hub identifica si el despliegue del módulo se está ejecutando en varios nodos de trabajo en varias zonas de disponibilidad. Se requiere un clúster de Amazon EKS adicional en otra región si su política de resiliencia requiere cobertura en caso de una interrupción regional. Este clúster adicional de Amazon EKS también se verifica para las implementaciones de pods que se distribuyen entre varios nodos de trabajo en varias zonas de disponibilidad.

Implementación frente a ReplicaSet

AWS Resilience Hub comprueba si está utilizando objetos ReplicaSets o agrupando objetos en lugar de desplegarlos. Sustituir ReplicaSets los objetos del pod por objetos de despliegue simplifica las actualizaciones del pod a una nueva versión del software e incluye otras funciones útiles.

Implementación y mantenimiento

AWS Resilience Hub comprueba si se utilizan las siguientes prácticas recomendadas para la implementación:

- Uso de Pod Disruption Budget (PDB): el uso de PDB permite mejorar la disponibilidad al establecer un límite en la cantidad de pods de la carga de trabajo que pueden interrumpirse en un momento dado.
- Sustitución de los grupos de nodos autogestionados por grupos de nodos gestionados por Amazon EKS: esta sustitución simplifica las actualizaciones de las imágenes de los nodos de trabajo durante el mantenimiento.
- Admite solicitudes dinámicas de CPU y memoria por implementación: estas solicitudes ayudan a Kubernetes a seleccionar un nodo que se adapte a las necesidades de un pod.
- Configuración de las sondas de actividad y preparación para todos los contenedores: la configuración de las sondas de actividad ayuda a mejorar la resiliencia al reiniciar los módulos que no funcionan. La configuración de las sondas de preparación permite mejorar la disponibilidad al desviar el tráfico de los módulos más concurridos.
- Configuración de Karpenter, Cluster Autoscaler o AWS Fargate : estas configuraciones permiten que la infraestructura del clúster de Amazon EKS crezca y satisfaga las demandas de carga de trabajo.
- Configuración del escalador automático de pods horizontales: esta configuración ayuda al clúster de Amazon EKS a escalar automáticamente la carga de trabajo para satisfacer la demanda de procesamiento de solicitudes.

Amazon Simple Notification Service

En esta sección se enumeran todas las comprobaciones y recomendaciones de resiliencia específicas de Amazon Simple Notification Service (Amazon SNS). Para obtener más información sobre Amazon SNS, consulte la documentación de Amazon SNS.

Suscripciones temáticas

AWS Resilience Hub comprueba si el tema de Amazon SNS tiene al menos 1 suscripción adjunta para garantizar que los mensajes entrantes no se pierdan.

Amazon Simple Queue Service

En esta sección se enumeran todas las comprobaciones de resiliencia y las recomendaciones específicas de Amazon Simple Queue Service (Amazon SQS). Para obtener más información sobre Amazon SQS, consulte la documentación de Amazon SQS.

Dead-letter cola

AWS Resilience Hub comprueba si la cola de Amazon SQS tiene un DLQ asociado para gestionar los mensajes que no se pueden entregar correctamente a los suscriptores.

Amazon Elastic Container Service

En esta sección se enumeran todas las comprobaciones y recomendaciones de resiliencia específicas de Amazon Elastic Container Service (Amazon ECS). Para obtener más información sobre Amazon ECS, consulte la documentación de Amazon ECS.

Multi-AZ despliegue

AWS Resilience Hub comprueba si las tareas o los servicios de Amazon ECS se ejecutan en varias zonas de disponibilidad en función de Amazon EC2 o del tipo de AWS Fargate lanzamiento. Se requiere un clúster de Amazon ECS adicional en otra región si su póliza necesita cobertura por una interrupción regional. También se verifica la ejecución de tareas o servicios en varias zonas de disponibilidad del clúster adicional.

Elastic Load Balancing

En esta sección, se enumeran todas las comprobaciones y recomendaciones de resiliencia específicas de Elastic Load Balancing. Para obtener más información sobre Elastic Load Balancing, consulte la documentación de Elastic Load Balancing.

Multi-AZ despliegue

AWS Resilience Hub comprueba si Elastic Load Balancing se está ejecutando en varias zonas de disponibilidad.

Se requiere un Elastic Load Balancing adicional en una región diferente si tu póliza necesita cobertura para una disrupción regional. El Elastic Load Balancing adicional, ubicado en una región diferente, también se verifica para su despliegue en varias zonas de disponibilidad.

Amazon API Gateway

En esta sección se enumeran todas las comprobaciones y recomendaciones de resiliencia específicas de Amazon API Gateway. Para obtener más información sobre Amazon API Gateway, consulte la documentación de Amazon API Gateway.

Cross-Region despliegue

Si su política debe tener en cuenta la disrupción regional, AWS Resilience Hub comprobará si hay un despliegue adicional del recurso de API de Amazon API Gateway en otra región.

Multi-AZ Despliegue de API privadas

AWS Resilience Hub comprueba si su API está definida como privada en Amazon API Gateway. Las API privadas deben recibir tráfico a través del punto de enlace de la interfaz de Amazon VPC que se implementa en varias zonas de disponibilidad.

Amazon DocumentDB

En esta sección se enumeran todas las comprobaciones y recomendaciones específicas de Amazon DocumentDB. Para obtener más información sobre Amazon DocumentDB, consulte la documentación de Amazon DocumentDB.

Multi-AZ despliegue

AWS Resilience Hub comprueba si el clúster de Amazon DocumentDB está implementado en varias zonas de disponibilidad. Se requiere un clúster secundario de Amazon DocumentDB adicional en una región diferente si su póliza requiere cobertura por una interrupción regional. El clúster adicional de Amazon DocumentDB, ubicado en una región diferente, también se verifica para su ejecución en varias zonas de disponibilidad.

Clúster e Multi-AZ implementación elásticos

AWS Resilience Hub comprueba si los fragmentos de clústeres elásticos de Amazon DocumentDB utilizan réplicas de lectura que se implementan en diferentes zonas de disponibilidad.

Instantáneas manuales y de Elastic Cluster

AWS Resilience Hub comprueba si las instantáneas manuales se crean con regularidad para un clúster elástico de Amazon DocumentDB. Las instantáneas manuales permiten una mayor persistencia y ofrecen flexibilidad a la hora de configurar la frecuencia de las instantáneas para adaptarla a las necesidades de su empresa.

Puerta de enlace NAT

En esta sección se enumeran todas las comprobaciones y recomendaciones específicas de NAT Gateway. Para obtener más información sobre las puertas de enlace NAT, consulte Puertas de enlace NAT.

Multi-AZ despliegue

AWS Resilience Hub comprueba si la puerta de enlace NAT está desplegada en varias zonas de disponibilidad. Es necesario implementar una puerta de enlace NAT adicional en una región diferente si su póliza requiere cobertura en caso de interrupción regional. La puerta de enlace NAT adicional, ubicada en una región diferente, también está verificada para su despliegue en varias zonas de disponibilidad.

Amazon Route 53

En esta sección se enumeran todas las comprobaciones y recomendaciones específicas de Amazon Route 53. Para obtener más información sobre Amazon Route 53, consulte la documentación de Amazon Route 53.

Multi-AZ despliegue

AWS Resilience Hub comprueba si el registro de zonas alojadas de Amazon Route 53 está definido con varios destinos en la misma región y si estos objetivos están desplegados en varias zonas de disponibilidad. Si su política requiere cobertura en caso de interrupción regional, AWS Resilience Hub compruebe si el registro de zonas alojadas de Amazon Route 53 está definido en varias regiones con varios objetivos por región y si estos objetivos están desplegados en varias zonas de disponibilidad.

Controlador de recuperación de aplicaciones (ARC) de Amazon

En esta sección se enumeran todas las comprobaciones y recomendaciones específicas de Amazon Application Recovery Controller (ARC) (ARC). Para obtener más información sobre ARC, consulte la documentación de ARC.

Multi-AZ despliegue

AWS Resilience Hub comprueba si se están desplegando recursos similares en varias regiones y recomienda, como práctica óptima, definir las comprobaciones de preparación para el ARC a fin de aumentar su disponibilidad y preparación en caso de que se produzca una interrupción regional. Se le notificará que se le cobrarán cargos adicionales por hora.

Amazon FSx para Windows File Server

En esta sección se enumeran todas las comprobaciones y recomendaciones específicas de Amazon FSx for Windows File Server. Para obtener más información acerca de Amazon FSx for Windows File Server, consulte la documentación de Amazon FSx for Windows File Server.

Tipo de sistema de archivos

AWS Resilience Hub comprueba el tipo de sistema de archivos: o. `Regional` `One Zone` El tipo de sistema de archivos afecta a su capacidad de recuperación en caso de que se produzcan interrupciones en la infraestructura o en la zona de disponibilidad. Para obtener más información sobre los tipos de sistemas de archivos, consulte Amazon EFS.

Backup del sistema de archivos

AWS Resilience Hub comprueba si AWS Backup se ha definido una para el sistema de archivos desplegado. Además, también comprueba si la `cross-Region backup` opción está habilitada si tu póliza requiere cobertura en caso de Region-level interrupciones.

Replicación de los datos

AWS Resilience Hub comprueba si se ha definido una tarea de replicación de AWS DataSync datos programada dentro o entre regiones para el sistema de archivos implementado.

AWS DataSync la tarea de replicación de datos programada puede mejorar el RTO de la carga de trabajo estimada y el RPO de la carga de trabajo estimada a nivel de infraestructura, zona y región. Además, podría combinarse con un sistema IN Region AWS Backup para recuperarse en caso de que se interrumpa una aplicación.

AWS Step Functions

En esta sección se enumeran todas las comprobaciones y recomendaciones específicas de AWS Step Functions. Para obtener más información al respecto AWS Step Functions, consulte AWS Step Functions la documentación.

Control de versiones y alias

AWS Resilience Hub comprueba si el AWS Step Functions flujo de trabajo utiliza el control de versiones y los alias para mejorar el tiempo de reimplementación.

Cross-Region despliegue

AWS Resilience Hub comprueba si un AWS Step Functions flujo de trabajo del mismo tipo de flujo de trabajo está desplegado en una región diferente para recuperarlo en caso de una interrupción regional.

Amazon ElastiCache (Redis OSS)

En esta sección se enumeran todas las comprobaciones y recomendaciones específicas de Amazon ElastiCache (Redis OSS).

Para obtener más información sobre Amazon ElastiCache (Redis OSS), consulte la ElastiCache documentación de Amazon.

Single-AZ despliegue

AWS Resilience Hub comprueba si el clúster de Amazon ElastiCache (Redis OSS) está desplegado como un único nodo o con todos sus nodos en una única zona de disponibilidad.

Single-AZ despliegue

AWS Resilience Hub valida si el clúster de Amazon ElastiCache (Redis OSS) se implementa como un grupo de replicación (tanto para los clústeres con el modo de clúster como con el modo de clúster deshabilitado) en varias zonas de disponibilidad para permitir la conmutación por error en caso de que se interrumpa la zona de disponibilidad.

Cross-Region conmutación por error

AWS Resilience Hub comprueba los objetivos de RTO y RPO definidos en la política de resiliencia para recuperarse de una interrupción regional. Además, AWS Resilience Hub puede identificar los

clústeres de almacenes de datos globales de Amazon ElastiCache (Redis OSS) implementados en varias regiones.

Copia de seguridad

AWS Resilience Hub comprueba si las siguientes capacidades de copia de seguridad se aplican en un clúster de Amazon ElastiCache (Redis OSS) desplegado o de diseño propio:

- Copia de seguridad automática
- Copia de seguridad manual para sistemas de copia de seguridad de terceros

AWS Resilience Hub no recomendará la copia de seguridad como método de recuperación si no está utilizando la copia de seguridad. Sin embargo, puede restablecer la capa de caché en caso de incoherencia en los datos y volver a crear los datos desde el almacenamiento principal.

Conmutación por error en la región más rápida

AWS Resilience Hub comprueba los objetivos de RTO y RPO definidos en la política de resiliencia durante las interrupciones en la infraestructura o en las zonas de disponibilidad. Además, AWS Resilience Hub puede identificar las siguientes arquitecturas regionales para recuperarse de las interrupciones en la infraestructura y la zona de disponibilidad:

- Instancia de nodo en espera secundaria en una zona de disponibilidad diferente para el tipo de clúster de Amazon ElastiCache (Redis OSS) deshabilitado en modo de clúster.
- Instancia de nodo en espera secundaria en una zona de disponibilidad diferente por cada fragmento para el tipo de clúster de Amazon ElastiCache (Redis OSS) habilitado para el modo de clúster.

Trabajar con otros servicios de

En esta sección se describen AWS los servicios con AWS Resilience Hub los que se interactúa.

Temas

AWS CloudFormation

AWS Resilience Hub está integrado con AWS CloudFormation un servicio que le ayuda a modelar y configurar sus AWS recursos para que pueda dedicar menos tiempo a crear y administrar sus recursos e infraestructura. Crea una plantilla que describe todos los AWS recursos que desea (por ejemplo, AWS::ResilienceHub:::ResiliencyPolicy y AWS::ResilienceHub:::App), y CloudFormation aprovisiona y configura esos recursos por usted.

Cuando la utilice CloudFormation, podrá reutilizar la plantilla para configurar los AWS Resilience Hub recursos de forma coherente y repetida. Describa sus recursos una vez y, a continuación, aprovisione los mismos recursos repetidamente en varias AWS cuentas y regiones.

AWS Resilience Hub y CloudFormation plantillas

Para aprovisionar y configurar recursos AWS Resilience Hub y servicios relacionados, debe conocer CloudFormation las plantillas. Las plantillas son archivos de texto con formato JSON o YAML. Estas plantillas describen los recursos que desea aprovisionar en sus CloudFormation pilas. Si no estás familiarizado con JSON o YAML, puedes usar CloudFormation Designer para ayudarte a empezar con CloudFormation las plantillas. Para obtener más información, consulte ¿Qué es Designer de CloudFormation ? en la Guía del usuario de AWS CloudFormation .

AWS Resilience Hub admite la creación AWS::ResilienceHub:::ResiliencyPolicy y el ingreso AWS::ResilienceHub:::App. CloudFormation Para obtener más información, incluidos ejemplos de plantillas JSON y YAML para AWS::ResilienceHub:::ResiliencyPolicy y AWS::ResilienceHub:::App, consulta la referencia sobre los tipos de AWS Resilience Hub recursos en la Guía del AWS CloudFormation usuario.

Puedes usar CloudFormation pilas para definir AWS Resilience Hub aplicaciones. Una pila le permite administrar los recursos relacionados como una sola unidad. Una pila puede contener todos los recursos necesarios para ejecutar una aplicación web, como, por ejemplo, un servidor web o reglas de red.

Obtenga más información sobre CloudFormation

Para obtener más información CloudFormation, consulte los siguientes recursos:

- AWS CloudFormation
- AWS CloudFormation Guía del usuario

- CloudFormation Referencia de la API
- Guía del usuario de la interfaz de la línea de comandos de AWS CloudFormation

AWS CloudTrail

AWS Resilience Hub está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en AWS Resilience Hub. CloudTrail captura todas las llamadas a la API AWS Resilience Hub como eventos. Las llamadas que se capturan incluyen las llamadas desde la AWS Resilience Hub consola y las llamadas en código a las operaciones de la AWS Resilience Hub API. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos para AWS Resilience Hub. 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 Resilience Hub, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales.

Para obtener más información al respecto CloudTrail, consulte la Guía AWS CloudTrail del usuario.

AWS Systems Manager

AWS Resilience Hub trabaja con Systems Manager para automatizar los pasos de sus SOP proporcionando una serie de documentos SSM que puede utilizar como base para dichos SOP.

AWS Resilience Hub le proporciona CloudFormation plantillas que contienen las funciones de IAM necesarias para ejecutar diferentes documentos de Systems Manager, una función por documento con los permisos necesarios para el documento específico. Tras crear una pila con la CloudFormation plantilla, configurará las funciones de IAM y guardará los metadatos en el parámetro Systems Manager para que el documento de automatización de Systems Manager se ejecute en diferentes procedimientos de recuperación.

Para obtener más información acerca del uso de SOP, consulte Gestión de los procedimientos operativos estándar.

AWS Trusted Advisor

AWS Trusted Advisor es un sitio centralizado con recomendaciones de AWS mejores prácticas que le ayudan a identificar, priorizar y optimizar su implementación. AWS AWS Trusted Advisor inspecciona su AWS entorno y, a continuación, hace recomendaciones comprobando si existen

oportunidades para ahorrar dinero, mejorar la disponibilidad y el rendimiento del sistema o ayudar a cerrar las brechas de seguridad. Estas comprobaciones se dividen en varias categorías en función de su finalidad. Para obtener más información sobre las diferentes categorías de registros AWS Trusted Advisor, consulte la Guía del AWS Supportusuario.

AWS Trusted Advisor proporciona varias recomendaciones de resiliencia de alto nivel mediante comprobaciones de resiliencia para cada aplicación incluida en la AWS Resilience Hub categoría de tolerancia a errores. La categoría de tolerancia a fallos enumera todas las comprobaciones que ponen a prueba sus aplicaciones para determinar su resiliencia y fiabilidad. Estas comprobaciones le avisan cuando se producen AppComponent fallos o incumplimientos de las políticas que pueden provocar riesgos de resiliencia y afectar a la disponibilidad de las aplicaciones para la continuidad empresarial. También proporciona recomendaciones de resiliencia que mejorarán las posibilidades de reducir estos riesgos en la sección de medidas recomendadas, que debe abordarse en esta sección. AWS Resilience Hub Para obtener más información sobre las recomendaciones para cada aplicación de la AWS Trusted Advisor, le recomendamos que consulte las recomendaciones detalladas que se proporcionan en la AWS Resilience Hub.

AWS Trusted Advisor proporciona las siguientes comprobaciones para cada solicitud en AWS Resilience Hub:

- AWS Resilience Hub puntuaciones de resiliencia de las aplicaciones: comprueba la puntuación de resiliencia de sus aplicaciones a partir de su última evaluación AWS Resilience Hub y le avisa si sus puntuaciones de resiliencia están por debajo de un valor específico.

  Criterios de alerta

  - Verde: indica que la aplicación tiene una puntuación de resiliencia igual o superior a 70.
  - Amarillo: indica que la aplicación tiene una puntuación de resiliencia entre 40 y 69.
  - Rojo: indica que la aplicación tiene una puntuación de resiliencia inferior a 40.

  Acción recomendada

  Para mejorar la postura de resiliencia y obtener la mejor puntuación de resiliencia posible para su aplicación, realice una evaluación con la versión actualizada más reciente de los recursos de la aplicación y, si corresponde, implemente las recomendaciones operativas sugeridas. Para obtener más información sobre la ejecución, revisión e implementación de las evaluaciones, las recomendaciones including/excluding operativas y de revisión y su implementación, consulte los siguientes temas:

  - the section called “Realizar evaluaciones de resiliencia en AWS Resilience Hub”

  - the section called “Revisar los informes de evaluación”
  - the section called “Revisar las recomendaciones de resiliencia”
  - the section called “Incluir o excluir recomendaciones operativas”
- AWS Resilience Hub incumplimiento de la política de aplicación: comprueba si las AWS Resilience Hub aplicaciones cumplen los objetivos de RTO y RPO que ha establecido para una aplicación y le avisa si la aplicación no cumple los objetivos de RTO y RPO.

  Criterios de alerta

  - Verde: indica que la aplicación tiene una política y que el RTO de carga de trabajo estimado y el RPO de carga de trabajo estimada cumplen los objetivos de RTO y RPO.
  - Amarillo: indica que la aplicación tiene una política y no se ha evaluado.
  - Rojo: indica que la aplicación tiene una política y que el RTO y el RPO de carga de trabajo estimados no cumplen los objetivos de RTO y RPO.

  Acción recomendada

  Para garantizar que el RTO de la carga de trabajo estimado y el RPO de la carga de trabajo estimada de su aplicación sigan cumpliendo los objetivos de RTO y RPO definidos, ejecute evaluaciones periódicas con la versión actualizada más reciente de los recursos de la aplicación. Además, si quiere asegurarse de que no se infrinja la política de resiliencia de su aplicación, le recomendamos que revise el informe de evaluación e implemente las recomendaciones de resiliencia sugeridas. Para obtener más información sobre cómo permitir realizar evaluaciones AWS Resilience Hub a diario en tu nombre, realizar evaluaciones, revisar las recomendaciones de resiliencia e implementarlas, consulta los siguientes temas:

  - the section called “Edición de recursos de aplicaciones”(AWS Resilience Hub Para poder realizar evaluaciones diarias en su nombre, complete los pasos de Para editar la configuración de las notificaciones de error del procedimiento de solicitud y active la casilla de verificación Evaluar automáticamente todos los días).
  - the section called “Realizar evaluaciones de resiliencia en AWS Resilience Hub”
  - the section called “Revisar los informes de evaluación”
  - the section called “Revisar las recomendaciones de resiliencia”
  - the section called “Incluir o excluir recomendaciones operativas”
- AWS Resilience Hub antigüedad de la evaluación de la solicitud: comprueba la última vez desde que realizó una evaluación para cada una de sus solicitudes AWS Resilience Hub. Le avisa si no ha realizado una evaluación durante el número especificado de días.

Criterios de alerta

- Verde: indica que ha realizado una evaluación de su solicitud en los últimos 30 días.
- Amarillo: indica que no ha realizado ninguna evaluación para su solicitud en los últimos 30 días.

Acción recomendada

Realice evaluaciones con regularidad para gestionar y mejorar la resiliencia de sus aplicaciones AWS. Si desea evaluar su solicitud AWS Resilience Hub a diario en su nombre, puede activarla marcando la casilla de verificación Evaluar automáticamente esta solicitud a diario en las notificaciones AWS Resilience Hub de error. Para seleccionar la casilla de verificación Evaluar automáticamente esta solicitud a diario, complete la casilla Para editar la notificación de desvío del procedimiento de solicitud que aparece en???.

> **Note**
>
> Esta verificación determina la edad de evaluación solo de las solicitudes que se han evaluado al menos una vez. AWS Resilience Hub

- AWS Resilience Hub comprobación de componentes de la aplicación: comprueba si un componente de la aplicación (AppComponent) de la aplicación es irrecuperable. Es decir, si AppComponent no se recupera en caso de una interrupción, es posible que se produzca una pérdida de datos desconocida y un tiempo de inactividad del sistema. Si el criterio de alerta está establecido en rojo, indica que AppComponent es irrecuperable.

  Acción recomendada

  Para garantizar que la suya AppComponent sea recuperable, revise e implemente las recomendaciones de resiliencia y, a continuación, realice una nueva evaluación. Para obtener más información sobre la revisión de las recomendaciones de resiliencia, consulte. the section called “Revisar las recomendaciones de resiliencia”

Para obtener más información sobre su uso AWS Trusted Advisor, consulte la Guía del AWS Support usuario.

Historial de documentos del AWS Resilience Hub Guía del usuario de

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

- Versión de la API: la más reciente
- Última actualización de la documentación: 17 de diciembre de 2024

Cambio	Descripción	Fecha
Se agregaron eventos EventBridge de notificación	La próxima generación de Resilience Hub ahora emite eventos a Amazon EventBridge para evaluar el ciclo de vida, encontrar la resolución del modo de error y descubrir nuevas dependencias. Puede crear EventBridge reglas para automatizar las respuestas a estos eventos. Para obtener más información, consulte EventBridge las notificaciones.	9 de julio de 2026
Campos de estado de descubrimiento de dependencias documentados	Se agregó documentación para los `message` campos `eligibleResourceCount` y en la estructura de `DependencyDiscoveryConfig` respuestas. Estos campos permiten supervisar el estado del descubrimiento de dependencias mediante las operaciones de la `ListServices` API `GetService` y.	30 de junio de 2026

Se agregaron los permisos de IAM para las pruebas de resiliencia	Se agregaron las políticas de confianza y permisos para las funciones de ejecución de IAM, que AWS Fault Injection Service suponen la ejecución de pruebas de resiliencia, tanto para las pruebas de una sola cuenta como para las de varias cuentas.	15 de junio de 2026
Se agregaron pruebas de resiliencia	Se agregó documentación para las pruebas de resilienc ia, que le permite validar la recuperación del servicio mediante pruebas preconfig uradas AWS Fault Injection Service integradas.	4 de junio de 2026
Versión inicial de la guía del usuario de Resilience Hub de próxima generación	Publicación inicial de la guía del usuario de Resilience Hub de próxima generación.	19 de mayo de 2026

AWS Resilience Hub integra las CloudWatch alarmas de Amazon ya implementadas	AWS Resilience Hub ahora detecta e integra automáticamente CloudWatch las alarmas de Amazon ya configuradas en sus evaluaciones de resiliencia, lo que proporciona una visión más completa del estado de resiliencia de su aplicación. Esta nueva capacidad combina AWS Resilience Hub las recomendaciones con su configuración de monitoreo actual para agilizar la administración de alarmas y mejorar la precisión de las evaluaciones. Para obtener más información, consulte Administración de alarmas.	17 de diciembre de 2024

AWS Resilience Hub ha permitido disponer de capacidades adicionales para proporcionar pruebas de resiliencia simplificadas con AWS Fault Injection Service experimentos personalizados	AWS Resilience Hub ahora admite una integración mejorada con AWS Fault Injection Service (AWS FIS) para ofrecer recomendaciones personalizadas mediante AWS FIS acciones y escenario s basados en el contexto específico de la aplicació n para mejorar la postura de resiliencia. Realizar los experimentos recomendados o realizar tus propias pruebas mejorará tu puntuación de resiliencia, lo que te permitirá hacer un seguimiento de los cambios a lo largo del tiempo. Para obtener más información, consulte los temas siguientes: • AWSResilienceHubAs ssessmentExecutionPolicy • Administración AWS Fault Injection Service experimen tos • AWS Resilience Hub — Pruebas de resiliencia	17 de diciembre de 2024

AWS Resilience Hub presenta una vista resumida	AWS Resilience Hub La nueva vista resumida ofrece una representación visual de alto nivel de la resiliencia de las aplicaciones a través de tablas y gráficos claros, lo que le permite visualizar el estado de su cartera de aplicaciones y gestionar y mejorar de manera eficiente la capacidad de sus aplicaciones para resistir las interrupciones y recuperar se de ellas. Además de la nueva vista resumida, puede exportar los datos que utilizan la vista resumida para crear informes personalizados para la comunicación con las partes interesadas. Para obtener más informaci ón, consulte the section called “AWS Resilience Hub resumen”.	21 de noviembre de 2024

AWS Resilience Hub presenta el widget de resiliencia en el panel de control de MyApplications	El nuevo widget de resiliencia del panel de control de MyApplications agiliza la evaluación y el monitoreo del estado de resiliencia de sus aplicaciones. Le permite evaluar rápidamente la resiliencia de las aplicaciones definidas en MyApplications sin tener que replicarlas manualmente en. AWS Resilience Hub Para obtener más información, consulte los temas siguientes: • the section called “AWS Resilience Hub y MyApplications” • the section called “Gestión de las evaluaciones de resiliencia desde el widget de resiliencia”	22 de octubre de 2024

AWS Resilience Hub amplía el soporte para Amazon ElastiCache (Redis OSS) Serverless	AWS Resilience Hub ahora evalúa las aplicaciones que utilizan Amazon ElastiCache (Redis OSS), incluidos los almacenes de datos globales y sin servidor de Amazon ElastiCache (Redis OSS), y ofrece recomendaciones para mejorar la resiliencia. Estas incluyen directrices para las configuraciones regionales y multirregionales, así como estrategias para las implement aciones, la agrupación de recursos y las copias de Multi-AZ seguridad. Además, para ofrecer un mejor control sobre la capacidad de recuperación de las aplicaciones, Amazon AWS Resilience Hub ofrece CloudWatch alarmas personali zadas para Amazon ElastiCac he (Redis OSS). Para obtener más información, consulte los temas siguientes: • the section called “Gestión de los componentes de la aplicación” • the section called “ AWS Resilience Hub Recursos compatibles” • the section called “AWSResilienceHubA sssessmentExecutionPolicy”	25 de septiembre de 2024

AWS Resilience Hub introduce recomendaciones de agrupamiento	AWS Resilience Hub presenta una nueva opción de agrupación inteligente para agrupar los recursos en componentes de la aplicació n (AppComponents) mientras se incorporan las aplicaciones. Cuando realices evaluaciones de resiliencia AWS Resilienc e Hub, es importante que tus recursos se agrupen de forma precisa y adecuada AppComponents para recibir recomendaciones optimizad as y prácticas. Esta opción es ideal para aplicaciones complejas o interregionales a fin de reducir el tiempo necesario para incorporar las aplicaciones, y complementa el flujo de trabajo de incorpora ción de aplicaciones existente que está disponible en la actualidad. Para obtener más información, consulte los temas siguientes: • the section called “Gestión de los componentes de la aplicación” • the section called “AWS Resilience Hub recomenda ciones de agrupamiento de recursos”	1 de agosto de 2024

AWS Resilience Hub presenta un nuevo widget de resumen de las evaluaciones	AWS Resilience Hub presenta un nuevo widget de resumen de las evaluaciones que utiliza las capacidades de inteligencia artificial generativa de Amazon Bedrock para transformar datos complejos sobre resilienc ia en información muy útil. Estos resúmenes de evaluació n extraen los hallazgos fundamentales, priorizan los riesgos y recomiendan medidas para mejorar la resiliencia. Al centrarse en los elementos más impactant es, puede comprender las evaluaciones con mucha más facilidad, lo que le ayuda a obtener información de alto impacto que se centra en los elementos más críticos de su postura de resiliencia. Para obtener más informaci ón, consulte the section called “Resumen de la evaluación”.	1 de agosto de 2024

AWS Resilience Hub amplía el soporte para Amazon DocumentDB	Esta AWS Resilience Hub política le permite conceder `Describe` permisos para acceder a los recursos y configuraciones de Amazon DocumentDB y Elastic Load Balancing, así como AWS Lambda durante la ejecución de las evaluaciones. Para obtener más informaci ón sobre la política AWS administrada, consultethe section called “AWSResil ienceHubAsssessmen tExecutionPolicy”.	1 de agosto de 2024

AWS Resilience Hub amplía la resiliencia de las aplicaciones y las capacidades de detección de desviaciones	AWS Resilience Hub ha ampliado sus capacidades de detección de desviaciones al introducir un nuevo tipo de detección de desviaciones: las desviaciones de los recursos de las aplicaciones. Esta mejora detecta cambios, como la adición o eliminación de recursos en las fuentes de entrada de la aplicación. Puede habilitar los servicios de evaluación AWS Resilience Hub programada y notificación de desviaciones y recibir una notificación cada vez que se produzca una desviación. La evaluación de resiliencia más reciente identifica las deficiencias y presenta medidas correctivas para que la aplicación vuelva a cumplir con su política de resiliencia. Para obtener más información, consulte los temas siguientes: • the section called “Detección de desviaciones” • the section called “Configure la evaluación programada y la notificación de desviaciones”	8 de mayo de 2024

AWS Trusted Advisor mejoras	AWS Resilience Hub ha ampliado el soporte AWS Trusted Advisor añadiendo una comprobación para identificar los componentes de la aplicación irrecuperables ()AppComponents. Para obtener más informaci ón, consulte the section called “AWS Trusted Advisor”.	28 de marzo de 2024
AWS Resilience Hub amplía el soporte para las alarmas recomendadas	AWS Resilience Hub ha actualizado el archivo de `README.md` plantilla con valores que permiten crear alarmas AWS Resilience Hub internas AWS (como Amazon CloudWatch) o externas AWS. Para obtener más informaci ón, consulte the section called “Administración de alarmas”.	26 de marzo de 2024

AWS Resilience Hub amplía la compatibilidad con Amazon FSx para Windows File Server	AWS Resilience Hub amplía el soporte de evaluación de los recursos de Amazon FSx para servidores de archivos Windows y, al mismo tiempo, evalúa la resiliencia de su aplicación. En el caso de las aplicaciones que utilizan Amazon FSx para Windows File Server, AWS Resilienc e Hub proporciona un nuevo conjunto de recomenda ciones de resiliencia que abarcan la zona de disponibi lidad (AZ) y Multi-AZ las implementaciones, los planes de respaldo y la replicación de datos. AWS Resilience Hub admite Amazon FSx para el servidor de archivos de Windows, incluida la dependencia del sistema de archivos de Microsoft Active Directory, tanto para las implementaciones dentro de la región como entre regiones. Para obtener más información, consulte los temas siguientes: • the section called “ AWS Resilience Hub Recursos compatibles” • the section called “AWSResilienceHubA sssessmentExecutionPolicy”	26 de marzo de 2024

	• the section called “Agrupación de recursos en un componente de aplicación”	
AWS Resilience Hub proporciona información adicional sobre la puntuación de resiliencia	AWS Resilience Hub ha actualizado la experiencia de usuario con la puntuación de resiliencia para ayudarlo a navegar y comprender fácilmente las acciones necesarias para mejorar la postura de resiliencia de sus aplicaciones. Para obtener más información, consulte the section called “Comprender las puntuaciones de resiliencia”.	9 de noviembre de 2023

AWS Resilience Hub amplía el soporte para aplicaciones que incluyen recursos de Amazon Elastic Kubernetes Service (Amazon EKS)	AWS Resilience Hub amplía el soporte para las aplicaciones que incluyen recursos de Amazon EKS para incluir nuevas recomendaciones operativas. Mientras realizamos una evaluación que incluye recursos de los clústeres de Amazon EKS, ahora recomendaremos que se ejecuten pruebas y alarmas para ayudar a mejorar la resiliencia de las aplicaciones. Para obtener más información, consulte the section called “Administración AWS Fault Injection Service experimentos”.	9 de noviembre de 2023

AWS Resilience Hub proporciona información adicional a nivel de aplicación	AWS Resilience Hub proporciona información adicional a nivel de aplicación sobre el RTO estimado de la carga de trabajo y el RPO estimado de la carga de trabajo. Esta información adicional indica el máximo RTO de carga de trabajo estimado posible y el RPO de carga de trabajo estimado de su aplicación a partir de la última evaluación exitosa. Este valor es el RTO máximo estimado de la carga de trabajo y el RPO estimado de la carga de trabajo de todos los tipos de interrupciones. Para obtener más información, consulte the section called “Administración de las aplicaciones de ”.	30 de octubre de 2023

AWS Resilience Hub amplía el soporte de evaluación de los recursos AWS Step Functions	AWS Resilience Hub amplía el soporte de evaluación de los AWS Step Functions recursos y, al mismo tiempo, evalúa la resiliencia de su aplicación. AWS Resilienc e Hub analiza la AWS Step Functions configuración, incluido el tipo de máquina de estado (flujos de trabajo estándar o exprés). Además, también AWS Resilience Hub proporcionará recomenda ciones que le ayudarán a cumplir los objetivos de tiempo de recuperación (RTO) estimados de la carga de trabajo y los objetivos de punto de recuperación (RPO) estimados de la carga de trabajo. Para evaluar las aplicaciones, incluidos AWS Step Functions los recursos, debe configurar los permisos necesarios, ya sea mediante una política AWS gestionada o añadiendo manualmente el permiso específico para AWS Resilience Hub poder leer la AWS Step Functions configur ación. Para obtener más informaci ón acerca de cómo editar los permisos asociados, consulte the section called “AWSResil	30 de octubre de 2023

ienceHubAsssessmen
tExecutionPolicy”.

AWS Resilience Hub permite excluir las recomendaciones operativas	AWS Resilience Hub añade la posibilidad de excluir las recomendaciones operativas, incluidas las alarmas, los procedimientos operativos estándar (SOP) y las pruebas AWS Fault Injection Service (AWS FIS). Al realizar una evaluación AWS Resilience Hub, se le proporcionan tiempos de recuperación estimados y recomendaciones sobre cómo aumentar la resiliencia de la aplicación evaluada. Con el flujo de trabajo de exclusión de recomendaciones, ahora podrá excluir las alarmas, los procedimientos operativos estándar y AWS FIS las pruebas recomendados que no sean relevantes para ellos. El flujo de trabajo de exclusión es beneficioso si utiliza una plataforma distinta a la sugerida o si ya ha implementado la recomendación con un método alternativo. Para obtener más información, consulte los temas siguientes: • the section called “Incluir o excluir recomendaciones operativas” • the section called “Limitar los permisos para incluir o	9 de agosto de 2023

	excluir recomendaciones de AWS Resilience Hub ”	
Mejorar el diseño de permisos para AWS Resilience Hub	AWS Resilience Hub introduce un nuevo diseño de permisos para ofrecer flexibilidad a la hora de configurar AWS Identity and Access Management (IAM) las funciones de AWS Resilienc e Hub. También consolida los permisos en un solo rol, con la posibilidad de crear nombres de rol personalizados que sean significativos para usted y sus equipos. Una nueva política gestionada le AWS Resilience Hub permitirá disponer de los permisos adecuados para los servicios compatibles. Si se siente cómodo con el método actual de configuración de permisos, seguiremos admitiendo la configuración manual. Para obtener más informaci ón sobre la política AWS administrada, consultethe section called “AWSResil ienceHubAsssessmen tExecutionPolicy”.	2 de agosto de 2023

Detección de variaciones en la resiliencia de las aplicaciones con AWS Resilience Hub	AWS Resilience Hub le permite detectar y comprender de forma proactiva las acciones necesarias para resolver la resiliencia de las aplicaciones. Permitir que Amazon Simple Notification Service (Amazon SNS) reciba notificaciones cuando el objetivo de tiempo de recuperación (RTO) de la carga de trabajo o el objetivo de punto de recuperación (RPO) de la carga de trabajo estimado hayan pasado de cumplir el objetivo a dejar de cumplir los objetivos empresariales de la organización. Pasar de detectar problemas de resiliencia de forma reactiva al ejecutar una evaluación de forma manual a recibir notificaciones proactivas a través de los temas de Amazon SNS le permitirá anticipar las posibles interrupciones con antelación y le proporcionará una mayor confianza en el logro de los objetivos de recuperación. Para obtener más información, consulte los temas siguientes: • the section called “Configure la evaluación programada	2 de agosto de 2023

y la notificación de desviaciones”

- the section called “Edición de recursos de aplicaciones”

AWS Resilience Hub mejora el soporte para Amazon Relational Database Service y Amazon Aurora	AWS Resilience Hub amplía el soporte de evaluación para el proxy de Amazon Relational Database Service y las configuraciones de bases de datos headless y Amazon Aurora DB. Además, al evaluar las aplicaciones que incluyen Amazon RDS, ahora distinguiremos entre los diferentes motores de bases de datos para proporcionar objetivos de tiempo de recuperación de la carga de trabajo (RTO) estimados con mayor precisión. AWS Resilience Hub También proporcionará acciones adicionales para implementar las mejores prácticas de resiliencia en su AWS entorno. Las mejores prácticas pueden incluir información sobre el rendimiento con DevOps Guru para Amazon RDS, una supervisión mejorada y la automatización de la blue/green implementación en los motores de bases de datos compatibles. Para obtener más información sobre los permisos necesarios AWS Resilience Hub para incluir recursos de todos los servicios compatibles en	2 de agosto de 2023

	su evaluación, consultethe section called “AWSResilienceHubAsssessmentExecutionPolicy”.	
AWS Resilience Hub amplía el soporte para las instantáneas de Amazon Elastic Block Store	AWS Resilience Hub amplía el soporte de evaluación de Amazon Elastic Block Store (Amazon EBS) para reconocer las instantáneas de Amazon EBS que se toman dentro de la misma región de Amazon EBS mediante API directas. El soporte ampliado se suma al soporte actual para los clientes que utilizan Amazon Data Lifecycle Manager (Amazon Data Lifecycle Manager) o Amazon Backup. AWS Para obtener más información, consulte Amazon Elastic Block Store (Amazon EBS).	2 de agosto de 2023

Mejoras de Amazon Elastic Compute Cloud	AWS Resilience Hub ha ampliado el soporte para Amazon Elastic Compute Cloud (Amazon EC2). Para aplicaciones de diferentes tamaños, AWS permite a sus clientes que utilizan Amazon EC2 seleccionar la configura ción adecuada para su caso de uso. AWS Resilience Hub admite la evaluación de las siguientes configuraciones de Amazon EC2: • On-demand instancias. • Respaldo de instancias por AWS Backup y AWS Elastic Disaster Recovery. • Soporte para escalar grupos automáticamente con Amazon Application Recovery Controller (ARC) (ARC) A partir de ahora, el soporte de evaluación se ampliará para incluir instancias de spot, hosts dedicados, instancia s dedicadas, grupos de ubicación y flotas. Para obtener más informaci ón, consulte the section called “AWS Resilience Hub referencia de permisos de acceso”.	27 de junio de 2023

AWS actualizaciones de políticas administradas	Se agregó una nueva política que brinda acceso a otros AWS servicios para ejecutar evaluaciones. Para obtener más informaci ón, consulte the section called “AWSResilienceHubA sssessmentExecutionPolicy”.	26 de junio de 2023
Nuevas alarmas de recomendación operativa de Amazon DynamoDB	Para las aplicaciones que utilizan Amazon DynamoDB, AWS Resilience Hub ahora ofrece un nuevo conjunto de alarmas que lo alertan sobre los riesgos de resilienc ia derivados de los modos de capacidad aprovisionada y bajo demanda y de las tablas globales. Para acceder a las nuevas alarmas, es posible que deba actualizar la política AWS Identity and Access Management (IAM) del rol que está utilizando. Para obtener más informaci ón, consulte the section called “AWS Resilience Hub referencia de permisos de acceso”.	2 de mayo de 2023

AWS Trusted Advisor mejoras	AWS Resilience Hub ha ampliado el soporte para AWS Trusted Advisor las aplicaciones que utilizan Amazon DynamoDB. Al usar AWS Trusted Advisor con AWS Resilience Hub, ahora puede recibir una notificación cuando una solicitud no se haya evaluado en los últimos 30 días. Esta notificación le pide que vuelva a evaluar la aplicación para saber si hay algún cambio que pueda afectar a su capacidad de recuperación. Para obtener más informaci ón sobre la verificación de la antigüedad de la evaluació n AWS Resilience Hub , consulte the section called “AWS Trusted Advisor”.	2 de mayo de 2023

Soporte adicional para Amazon Simple Storage Service	Además del soporte actual de Amazon Simple Storage Service (Amazon S3) para la Cross-Region replicación (Amazon S3 CRR) y la Same-Region replicación de Amazon S3 (SRR), el control de versiones y el AWS respaldo, ahora AWS Resilience Hub evaluará Amazon S3 para la configuración de puntos de acceso multirregionales, control del tiempo de replicación de Amazon S3 (Amazon S3 RTC) y recuperación puntual de AWS respaldo (PITR). Para obtener más información, consulte los temas siguientes: • the section called “AWS Resilience Hub referencia de permisos de acceso” • Gestionar el almacenamiento de Amazon S3	21 de marzo de 2023

Soporte adicional para Amazon Elastic Kubernetes Service	AWS Resilience Hub ha agregado el clúster Amazon EKS como recurso compatible para definir, validar y rastrear la resiliencia de las aplicaciones. Los clientes pueden añadir clústeres de Amazon EKS a aplicaciones nuevas o existentes y recibir evaluaciones y recomendaciones para mejorar la resiliencia. Los clientes pueden agregar recursos de aplicaciones mediante Terraform AWS CloudFormation y Grupos de recursos de AWS MyApplications. Además, los clientes pueden agregar uno o más clústeres de Amazon EKS directamente en una o más regiones con uno o más espacios de nombres en cada clúster. Esto permite AWS Resilience Hub ofrecer evaluaciones y recomendaciones únicas y transregionales. Además de examinar las implementaciones, las réplicas y los pods ReplicationControllers, AWS Resilience Hub analizaremos la resiliencia general de los clústeres. AWS Resilience Hub admite cargas de trabajo de clústeres de Amazon EKS sin estado. Las nuevas funciones están	21 de marzo de 2023

	disponibles en todas las AWS regiones en las que AWS Resilience Hub está disponibl e. Para obtener más información, consulte los temas siguientes: • the section called “Administ re los recursos de su aplicación” • the section called “Añadir clústeres de EKS” • the section called “AWS Resilience Hub referencia de permisos de acceso” • AWS Servicios regionales	
Soporte adicional para Amazon Elastic File System	Además del soporte actual para las copias de seguridad de Amazon Elastic File System (Amazon EFS), ahora AWS Resilience Hub evaluaremos Amazon EFS para la replicación de Amazon EFS y la configuración AZ. Para obtener más información, consulte los temas siguientes: • the section called “ AWS Resilience Hub Recursos compatibles” • ¿Qué es Amazon Elastic File System?	21 de marzo de 2023

Soporte para orígenes de entrada de aplicaciones	AWS Resilience Hub ahora ofrece transparencia sobre las fuentes de sus aplicaciones. Le ayuda a añadir, eliminar y volver a importar los orígenes de entrada de la aplicación, así como a publicar una nueva versión de la aplicación. Para obtener más informaci ón, consulte the section called “Edición de recursos de aplicaciones”.	21 de febrero de 2023

Soporte para los parámetros de configuración de la aplicación	AWS Resilience Hub ahora proporciona un mecanismo de entrada para recopilar información adicional sobre los recursos asociados a sus aplicaciones. Con esta información, AWS Resilience Hub obtendrá una comprensión más profunda de sus recursos y proporcionará mejores recomendaciones de resiliencia. Para obtener más información, consulte los temas siguientes: • the section called “Parámetros de configuración de la aplicación” • the section called “Configure los parámetros de configuración de la aplicación” • the section called “Actualizar los parámetros de configuración de la aplicación”	21 de febrero de 2023

Soporte adicional para Amazon Elastic Block Store	Además del soporte actual de los volúmenes de Amazon Elastic Block Store (Amazon EBS), ahora AWS Resilienc e Hub evaluará las instantán eas de Amazon EBS mediante Amazon Data Lifecycle Manager y la restauración rápida de instantáneas (FSR) de Amazon EBS. Para obtener más información, consulte los temas siguientes: • the section called “AWS Resilience Hub referencia de permisos de acceso” • Amazon Elastic Block Store (Amazon EBS)	21 de febrero de 2023

Integración con AWS Trusted Advisor	AWS Trusted Advisor los usuarios podrán ver las aplicaciones asociadas a su cuenta que hayan sido evaluadas por AWS Resilienc e Hub. AWS Trusted Advisor muestra la puntuación de resiliencia más reciente y proporciona un estado que indica si la política de resilienc ia objetivo (RTO y RPO) se ha cumplido o no. Cada vez que se ejecuta una evaluación, se AWS Resilience Hub actualiza AWS Trusted Advisor con los resultados más recientes . AWS Trusted Advisor es un servicio que analiza tus AWS cuentas de forma continua y ofrece recomendaciones para ayudarte a seguir las AWS mejores prácticas y AWS Well-Architected directrices. Para obtener más informaci ón, consulte the section called “AWS Trusted Advisor”.	18 de noviembre de 2022

Soporte para Amazon Simple Notification Service (Amazon SNS)	AWS Resilience Hub ahora evalúa las aplicaciones que utilizan Amazon SNS analizando la configuración de Amazon SNS, incluidos los suscriptores, y ofrece recomendaciones para cumplir los objetivos de recuperac ión de la carga de trabajo estimados de la organización (RTO estimado de la carga de trabajo y RPO estimado de la carga de trabajo) para las aplicaciones. Amazon SNS es un servicio administrado que envía mensajes de los editores (productores) a los suscriptores (consumidores). Para obtener más información, consulte los temas siguientes: • the section called “ AWS Resilience Hub Recursos compatibles” • the section called “Gestión de identidad y acceso” • the section called “Agrupaci ón de recursos en un componente de aplicación”	16 de noviembre de 2022

Soporte adicional para Amazon Application Recovery Controller (ARC) (Amazon ARC)	AWS Resilience Hub ahora evalúa Amazon ARC para Elastic Load Balancing y Amazon Relational Database Service (Amazon RDS), lo que incluye asesorar sobre cuándo Amazon ARC sería beneficioso. Ampliando AWS Resilience Hub el soporte de evaluación de Amazon ARC más allá de AWS Auto Scaling Group (AWS ASG) y Amazon DynamoDB. Amazon ARC proporciona una alta disponibilidad para su aplicación, lo que le permite conmutar rápidamente toda la aplicación a una región de conmutación por error. Para obtener más información, consulte los temas siguientes: • the section called “ AWS Resilience Hub Recursos compatibles” • the section called “Gestión de identidad y acceso”	16 de noviembre de 2022

Soporte adicional para copias de seguridad AWS	AWS Resilience Hub ahora evalúa Amazon ARC para Elastic Load Balancing y Amazon Relational Database Service (Amazon RDS), lo que incluye asesorar sobre cuándo Amazon ARC sería beneficioso. Ampliando AWS Resilience Hub el soporte de evaluación de Amazon ARC más allá de AWS Auto Scaling Group (AWS ASG) y Amazon DynamoDB. Amazon ARC proporciona una alta disponibi lidad para su aplicación, lo que le permite conmutar rápidamente toda la aplicació n a una región de conmutación por error. Para obtener más información, consulte los temas siguientes: • the section called “ AWS Resilience Hub Recursos compatibles” • the section called “Gestión de identidad y acceso”	16 de noviembre de 2022
Contenido actualizado: se han añadido nuevos recursos para los componentes de la aplicación	Se agregaron Route53 y AWS Backup a la lista de recursos de componentes de aplicacio nes compatibles en la sección de agrupamiento. AppCompon ent	1 de julio de 2022

Contenido nuevo: concepto de estado de conformidad de las aplicaciones	Se agregó el tipo de estado Cambios detectados.	2 de junio de 2022
Presentamos AWS Resilience Hub	AWS Resilience Hub ya está disponible. Esta guía describe cómo utilizarla AWS Resilience Hub para analizar su infraestructura, obtener recomendaciones para mejorar la resiliencia de sus AWS aplicaciones, revisar las puntuaciones de resiliencia y mucho más.	10 de noviembre de 2021

Resilience Hub de próxima generación

Resilience Hub de próxima generación es un servicio de gestión de la resiliencia que utiliza evaluaciones en modo de GenAI-powered fallo, el descubrimiento automático de dependencias, las pruebas de resiliencia y políticas de resiliencia componibles para ayudarlo a evaluar, probar y mejorar de forma proactiva la postura de resiliencia de sus aplicaciones. AWS

Temas

¿Qué es el Centro de Resiliencia de Próxima Generación?

El Resilience Hub de última generación es un servicio de gestión de la resiliencia que le ayuda a definir los objetivos de resiliencia, modelar sus aplicaciones, descubrir dependencias, poner a prueba la resiliencia y evaluar su posición de resiliencia en relación con esos objetivos. La próxima generación de Resilience Hub utiliza evaluaciones en modo de GenAI-powered fallo basadas en el

AWS Well-Architected Marco para identificar posibles puntos débiles y ofrecer recomendaciones prácticas. AWS Las pruebas de resiliencia recomendadas validan la forma en que sus servicios responden a escenarios de fallos específicos y se recuperan de ellos en función de los límites y las dependencias de los fallos.

Las capacidades clave de un vistazo

La próxima generación de Resilience Hub ofrece las siguientes capacidades clave:

- Modelado de aplicaciones: modele sus aplicaciones utilizando una jerarquía que coincida con la forma en que su organización piensa de ellas. Los sistemas representan las aplicaciones empresariales, los recorridos de los usuarios describen las rutas críticas de los usuarios finales dentro de un sistema y los servicios son los componentes básicos que componen AWS los recursos que respaldan los recorridos de los usuarios. Usted define dónde encontrar sus AWS recursos (AWS CloudFormation pilas, archivos de estado de Terraform, etiquetas de recursos o clústeres de Amazon EKS) y Resilience Hub los descubre automáticamente y los mapea en una topología que muestra cómo se conectan los recursos.
- Descubrimiento de dependencias: descubre y mapea de forma continua las dependencias de sus servicios, incluidos los servicios, los puntos de conexión internos y AWS los de terceros.
- Evaluaciones de modos de falla (GenAI-powered): analiza sus servicios comparándolos con las políticas de resiliencia y las AWS Well-Architected mejores prácticas para identificar los posibles modos de falla y recomendar mejoras.
- Pruebas de resiliencia: evalúa sus servicios para verificar que se cumplen los objetivos de recuperación y que las dependencias se comportan según lo esperado, como el deterioro de la zona de disponibilidad, el deterioro regional y el error de dependencia.
- Políticas de resiliencia: requisitos modulares y componibles para la disponibilidad (SLO), la recuperación Multi-Region ante desastres, la recuperación ante desastres y el Multi-AZ objetivo de recuperación de datos.
- AWS Integración de las organizaciones: gobierno centralizado en varias cuentas con soporte delegado de administradores y políticas de resiliencia para toda la organización.

Para las implementaciones a escala empresarial, el Resilience Hub de próxima generación se integra con AWS las organizaciones para ofrecer una gestión centralizada de la resiliencia en toda la organización desde una única cuenta de administrador delegado. Obtiene visibilidad en toda la organización sobre la postura de resiliencia y los paneles agregados sin tener que iniciar sesión en cuentas individuales.

Regiones compatibles y disponibilidad

La próxima generación de Resilience Hub está disponible en los siguientes Región de AWS s.

Nombre de región	Código de región
Este de EE. UU. (Norte de Virginia)	us-east-1
Este de EE. UU. (Ohio)	us-east-2
Oeste de EE. UU. (Oregón)	us-west-2
Canadá (centro)	ca-central-1
Europa (Irlanda)	eu-west-1
Europa (Londres)	eu-west-2
Europa (Fráncfort)	eu-central-1
Europa (París)	eu-west-3
Europa (Estocolmo)	eu-north-1
Asia-Pacífico (Bombay)	ap-south-1
Asia Pacífico (Singapur)	ap-southeast-1
Asia-Pacífico (Sídney)	ap-southeast-2
Asia-Pacífico (Tokio)	ap-northeast-1
Asia-Pacífico (Seúl)	ap-northeast-2
América del Sur (São Paulo)	sa-east-1

Para obtener la información más reciente sobre Región de AWS los dispositivos disponibles, consulte los puntos finales y las cuotas de la próxima generación de Resilience Hub en la Referencia AWS general.

Información general sobre precios

La próxima generación de Resilience Hub utiliza un modelo de precios basado en los servicios. En la siguiente tabla se resumen los componentes de los precios.

Componente	Precio
Tarifa de servicio (incluye hasta 150 recursos y 2 evaluaciones en modo de fallo al mes)	15 USD por servicio al mes
Se incluyen recursos adicionales por encima de 150€ y cada evaluación posterior	0,10 USD por recurso por cada evaluación del modo de fallo
Descubrimiento de dependencias (compleme nto opcional)	10$ por servicio al mes
Pruebas de resiliencia (opcionales)	0,10 USD por minuto de acción del servicio de inyección de fallos (FIS)

La tarifa de servicio incluye dos evaluaciones de modo de fallo al mes para servicios con hasta 150 recursos. En el caso de los servicios con más de 150 recursos, cada evaluación del modo de fallo incluida conlleva un cargo adicional de 0,10 USD por recurso por encima del umbral de 150 recursos. En el caso de las evaluaciones adicionales a las dos incluidas, el costo es de 0,10 USD por recurso evaluable con un mínimo de 50 recursos.

La detección de dependencias es un complemento opcional que proporciona una identificación continua y automatizada de todas las dependencias a las que llama su servicio.

Las pruebas de resiliencia funcionan con AWS Fault Injection Service ()AWS FIS. Se te cobrarán 0,10 USD por minuto de acción más 0,10 USD por minuto de acción por cada cuenta de destino adicional. Para obtener información detallada sobre los precios, consulta los precios. AWS FIS Los informes de las pruebas de resiliencia generados por la próxima generación de Resilience Hub se incluyen sin costo adicional.

Para obtener información detallada sobre los precios, consulta los precios de la próxima generación de Resilience Hub.

Servicios relacionados

Los siguientes AWS servicios se integran con la próxima generación de Resilience Hub o la complementan:

- AWS Fault Injection Service (AWS FIS) — Las pruebas de resiliencia se utilizan AWS FIS para inyectar fallos controlados en su servicio, a fin de ayudarlo a validar que funciona y se recupera según lo esperado. Para obtener más información, consulte Pruebas de resiliencia.
- AWS Controlador de recuperación de aplicaciones (ARC): proporciona comprobaciones de disponibilidad, controles de enrutamiento y funciones de cambio zonal que complementan la próxima generación de Resilience Hub.
- AWS Well-Architected Marco: las evaluaciones del modo de fallo aprovechan las Well-Architected mejores prácticas para evaluar su arquitectura de servicios.
- AWS Organizaciones: permite la gestión de la resiliencia en múltiples cuentas a través de la próxima generación de Resilience Hub desde una única cuenta de administrador delegado.
- Amazon EventBridge: utilice Amazon EventBridge para recibir notificaciones de eventos de la próxima generación de Resilience Hub con el fin de completar la evaluación, encontrar soluciones y descubrir dependencias. Puede usar estos eventos para crear flujos de trabajo de automatización basados en eventos.

Configuración de Resilience Hub de próxima generación

Antes de poder usar la próxima generación de Resilience Hub, debes completar los pasos de configuración que se describen en esta sección.

Temas

Requisitos previos

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

- Un activo Cuenta de AWS.
- Permisos de IAM para crear funciones y políticas en tu cuenta.
- (Opcional) AWS Organizaciones configuradas si planeas usar la gobernanza multicuenta.
- (opcional) AWS los recursos implementados mediante Terraform AWS CloudFormation, etiquetas de recursos o Amazon Elastic Kubernetes Service que desea evaluar.
- (Opcional) Una función de ejecución de IAM para las pruebas de resiliencia. Para obtener más información, consulte Funciones de ejecución de IAM para las pruebas de resiliencia.

Permisos y funciones de IAM necesarios

AWS política administrada

Puede adjuntar la `AWSResilienceHubV2AssessmentExecutionPolicy` a las identidades de IAM. Al ejecutar una evaluación, esta política otorga permisos de acceso de solo lectura a otros AWS servicios para el descubrimiento, la evaluación y la administración de la resiliencia. Para obtener más detalles acerca de los permisos incluidos en esta política, consulte AWSResilienceHubV2AssessmentExecutionPolicy.

> **Note**
>
> `AWSResilienceHubV2AssessmentExecutionPolicy`Sustituye al anterior `AWSResilienceHubAsssessmentExecutionPolicy` para su uso por el de la próxima generación de Resilience Hub.

Si utilizas pruebas de resiliencia, adjunta también la política `AWSResilienceHubResilienceTestingPolicy` gestionada. Esta política otorga a Resilience Hub los AWS Fault Injection Service (AWS FIS) permisos necesarios para iniciar y gestionar experimentos en tu nombre. Para obtener más detalles acerca de los permisos incluidos en esta política, consulte AWSResilienceHubResilienceTestingPolicy.

> **Note**
>
> Si la política gestionada no está disponible en tu cuenta, crea una política integrada con los mismos permisos. Para ver el contenido de la política, consulteAWSResilienceHubResilienceTestingPolicy.

El papel de la IAM en la evaluación y las pruebas de resiliencia

Para realizar una evaluación o una prueba de resiliencia, la próxima generación de Resilience Hub debe asumir una función de IAM con los permisos necesarios. Este rol descubre y lee la configuración de sus AWS recursos y, cuando las pruebas de resiliencia están habilitadas, inicia y administra AWS FIS los experimentos en su nombre.

Hay dos maneras de crear o configurar este rol:

- Crear un nuevo rol de servicio (recomendado): al crear o editar un servicio en la consola de próxima generación de Resilience Hub, puede elegir Crear nuevo rol en el modelo de permisos. La consola crea automáticamente un rol de IAM con la política de confianza correcta y adjunta la política `AWSResilienceHubV2AssessmentExecutionPolicy` administrada.
- Use un rol de servicio existente: si ya tiene un rol configurado o si prefiere crear roles fuera de la consola, elija Usar un rol de servicio existente. A continuación, elija el rol de la lista y asegúrese de que tenga la política de confianza y los permisos necesarios que se describen a continuación.

Crear el rol manualmente

Para crear el rol manualmente, abra la consola de IAM. Elija una política de confianza personalizada y utilice una política de confianza como la siguiente:

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

```
    }
  ]
}
```

Para los permisos, adjunte la política `AWSResilienceHubV2AssessmentExecutionPolicy` gestionada. Si utilizas pruebas de resiliencia, adjunta también la política `AWSResilienceHubResilienceTestingPolicy` gestionada.

Función de IAM Service-Linked

La próxima generación de Resilience Hub crea automáticamente un Service-Linked rol con la política `AWSResilienceHubServiceRolePolicy` administrada.

Permisos de acceso a los archivos estatales de Terraform

Si va a incluir los archivos de estado de Terraform en su servicio Resilience Hub de próxima generación, conceda permisos para leer los archivos de Terraform desde su bucket de Amazon S3 con una política como la siguiente:

```
{
  "Version": "2012-10-17"       ,
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::s3-bucket-name/path-to-state-file"
    },
    {
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::s3-bucket-name"
    }
  ]
}
```

Permisos de Amazon EKS

Si va a incluir clústeres de Amazon EKS en su servicio de Resilience Hub de próxima generación, siga el siguiente proceso de 3 pasos para conceder permisos a Resilience Hub de próxima

generación para leer los datos de configuración de sus clústeres de Amazon EKS mediante el control de acceso basado en roles (RBAC) de Kubernetes.

Paso 1: aplique lo siguiente a su clúster de Amazon EKS

Esto otorga a Resilience Hub de última generación acceso de solo lectura a los recursos de Kubernetes que necesita en todos los espacios de nombres:

```
cat << EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: resilience-hub-eks-access-cluster-role
rules:
- apiGroups:
    - ""
  resources:
    - pods
    - replicationcontrollers
    - nodes
    - services
  verbs:
    - get
    - list
- apiGroups:
    - apps
  resources:
    - deployments
    - replicasets
  verbs:
    - get
    - list
- apiGroups:
    - policy
  resources:
    - poddisruptionbudgets
  verbs:
    - get
    - list
- apiGroups:
    - autoscaling.k8s.io
  resources:
```

```
    - verticalpodautoscalers
  verbs:
    - get
    - list
- apiGroups:
    - autoscaling
  resources:
    - horizontalpodautoscalers
  verbs:
    - get
    - list
- apiGroups:
    - karpenter.sh
  resources:
    - provisioners
    - nodepools
  verbs:
    - get
    - list
- apiGroups:
    - karpenter.k8s.aws
  resources:
    - awsnodetemplates
    - ec2nodeclasses
  verbs:
    - get
    - list
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: resilience-hub-eks-access-cluster-role-binding
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-cluster-role
  apiGroup: rbac.authorization.k8s.io
---
EOF
```

Paso 2: Asigne la función de IAM al grupo de Kubernetes

Asigne el rol de IAM que creó al grupo de Kubernetes. `resilience-hub-eks-access-group` Puede utilizar las entradas de acceso de Amazon EKS (recomendado) o las. `aws-auth` ConfigMap

Opción A: usar las entradas de acceso de EKS (recomendado)

Las entradas de acceso EKS son el método preferido para administrar la autenticación de clústeres. El clúster debe utilizar el modo de `API_AND_CONFIG_MAP` autenticación `API` o.

```
aws eks create-access-entry \
  --cluster-name cluster-name \
  --principal-arn arn:aws:iam::ACCOUNT-ID:role/ResilienceHubRole \
  --type STANDARD \
  --kubernetes-groups '["resilience-hub-eks-access-group"]'
```

Opción B: usar aws-auth ConfigMap

Si su clúster usa el modo de `API_AND_CONFIG_MAP` autenticación `CONFIG_MAP` o, puede editar el aws-auth en su lugar: ConfigMap

Con eksctl:

```
eksctl create iamidentitymapping \
  --cluster cluster-name \
  --region region \
  --arn arn:aws:iam::ACCOUNT-ID:role/ResilienceHubRole \
  --group resilience-hub-eks-access-group \
  --username AwsResilienceHubAssessmentEKSAccessRole
```

O edite manualmente: ConfigMap

```
kubectl edit -n kube-system configmap/aws-auth
```

Añada esto `mapRoles` en la sección de datos:

```
- groups:
    - resilience-hub-eks-access-group
  rolearn: arn:aws:iam::ACCOUNT-ID:role/ResilienceHubRole
  username: AwsResilienceHubAssessmentEKSAccessRole
```

Paso 3: Verificar

Confirme que los recursos de RBAC existen y que la asignación de funciones está establecida:

```
kubectl get clusterrole resilience-hub-eks-access-cluster-role
kubectl describe clusterrolebinding resilience-hub-eks-access-cluster-role-binding
```

Si utiliza entradas de acceso (opción A):

```
aws eks describe-access-entry \
  --cluster-name cluster-name \
  --principal-arn arn:aws:iam::ACCOUNT-ID:role/ResilienceHubRole
```

Si usa aws-auth ConfigMap (opción B):

```
kubectl get configmap aws-auth -n kube-system -o yaml | grep -A 3 "ResilienceHubRole"
```

AWS políticas gestionadas para el Centro de resiliencia de próxima generación

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

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen

todos los AWS clientes. Se recomienda definir políticas administradas por el cliente de 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 se lance un nuevo AWS servicio o cuando haya nuevas operaciones de API disponibles para los servicios existentes.

Temas

- AWSResilienceHubV2AssessmentExecutionPolicy
- AWSResilienceHubResilienceTestingPolicy
- AWSResilienceHubServiceRolePolicy
- La próxima generación de Resilience Hub se actualiza a AWS políticas administradas

AWSResilienceHubV2AssessmentExecutionPolicy

Puede adjuntar la `AWSResilienceHubV2AssessmentExecutionPolicy` a las identidades de IAM. Al ejecutar una evaluación, esta política otorga permisos de acceso de solo lectura a otros AWS servicios para el descubrimiento, la evaluación y la administración de la resiliencia.

Detalles del permiso

Esta política otorga permisos de solo lectura con caracteres comodín que pueden incluir información confidencial en los resultados.

Esta política incluye los permisos siguientes:

- Amazon CloudWatch (CloudWatch): proporciona `Describe` y otorga `List` permisos para los CloudWatch recursos asociados a su cuenta. `Get` AWS
- AWS CloudFormation — Proporciona `Describe` y `Get` otorga `List` permisos para los AWS CloudFormation recursos que están asociados a su AWS cuenta.
- Amazon Elastic Compute Cloud (Amazon EC2): proporciona `Describe` permisos específicos para los recursos de Amazon EC2 asociados a su AWS cuenta.
- Amazon Elastic Container Service (Amazon ECS): proporciona `Describe` y otorga `List` permisos para los recursos de Amazon ECS asociados a su AWS cuenta.

- Amazon Elastic Kubernetes Service (Amazon EKS): proporciona `Describe` y otorga `List` permisos para los recursos de Amazon EKS que están asociados a su cuenta. AWS
- Amazon Elastic Container Registry (Amazon ECR): proporciona `Describe` permisos para los recursos de Amazon ECR asociados a su cuenta. AWS
- Amazon Elastic File System (Amazon EFS): proporciona `Describe` permisos para los recursos de Amazon EFS que están asociados a su AWS cuenta.
- Amazon ElastiCache (ElastiCache): proporciona `Describe` permisos para ElastiCache los recursos que están asociados a su AWS cuenta.
- Elastic Load Balancing: proporciona `Describe` permisos para los recursos de Elastic Load Balancing que están asociados a su AWS cuenta.
- Amazon DynamoDB (DynamoDB): proporciona `List` permisos para `Describe` los recursos de DynamoDB asociados a su cuenta. AWS
- Amazon RDS: proporciona `Describe` permisos para los recursos de Amazon RDS que están asociados a su cuenta. AWS
- Amazon DocumentDB: proporciona `List` permisos para `Describe` los recursos de Amazon DocumentDB asociados a su cuenta. AWS
- AWS Lambda (Lambda): proporciona `List` permisos `Get` y especificaciones para los recursos de Lambda que están asociados a su cuenta. AWS
- AWS Step Functions — Proporciona `Describe` y otorga `List` permisos para AWS Step Functions los recursos que están asociados a su AWS cuenta.
- IAM: proporciona `List` permisos `Get` y especificaciones para los recursos de IAM asociados a su AWS cuenta.
- Amazon Simple Notification Service (Amazon SNS): proporciona `List` permisos para `Get` los recursos de Amazon SNS asociados a su cuenta. AWS
- Amazon Simple Queue Service (Amazon SQS): proporciona `List` permisos para `Get` los recursos de Amazon SQS asociados a su cuenta. AWS
- Amazon Simple Storage Service (Amazon S3): proporciona `Get` `List` permisos para los recursos de Amazon S3 asociados a su cuenta. AWS Los permisos de Amazon S3 del `AWSResilienceHubS3AccessStatement` están restringidos a los recursos de la misma cuenta mediante el uso de la clave de `aws:ResourceAccount` condición.
- Amazon Route 53 (Route 53): proporciona `Get` y otorga `List` permisos para los recursos de Route 53, incluidos los recursos del controlador de recuperación de aplicaciones de Route 53, que están asociados a su AWS cuenta.

- Amazon EC2 Systems Manager (SSM): proporciona `Describe` y otorga `Get` permisos para los recursos de SSM asociados a su cuenta. AWS
- Amazon EC2 Auto Scaling: proporciona `Describe` permisos para los recursos de Amazon EC2 Auto Scaling asociados a su cuenta. AWS
- AWS Backup — Proporciona `Describe` y otorga `List` permisos para los AWS Backup recursos que están asociados a su AWS cuenta. `Get`
- AWS Elastic Disaster Recovery (Elastic Disaster Recovery): proporciona `Describe` permisos para los recursos de Elastic Disaster Recovery que están asociados a su AWS cuenta.
- AWS Fault Injection Service (AWS FIS) — Proporciona `Get` `List` permisos para los AWS FIS experimentos y las plantillas de experimentos que están asociados a su AWS cuenta.
- Amazon FSx para Windows File Server (Amazon FSx): proporciona `Describe` permisos para los recursos de Amazon FSx asociados a su cuenta. AWS
- Amazon Data Lifecycle Manager: proporciona `Get` permisos para los recursos de Amazon Data Lifecycle Manager que están asociados a su cuenta. AWS
- AWS DataSync — Proporciona `Describe` y otorga `List` permisos para AWS DataSync los recursos que están asociados a su AWS cuenta.
- Grupos de recursos de AWS (Grupos de recursos): proporciona `Get` y otorga `List` permisos para los recursos de los grupos de recursos que están asociados a su AWS cuenta.
- AWS Service Catalog (Catálogo de servicios): proporciona `Get` `List` permisos para los recursos del catálogo de servicios que están asociados a su AWS cuenta.
- Amazon API Gateway: proporciona `GET` permisos limitados a patrones de ARN de recursos específicos para las API REST, las API HTTP, los planes de uso y los nombres de dominio.
- Amazon Kinesis: proporciona `List` permisos para `Describe` los recursos de Kinesis asociados a su cuenta. AWS
- Amazon Kinesis Data Firehose: proporciona `List` permisos para `Describe` los recursos de Kinesis Data Firehose asociados a su cuenta. AWS
- Amazon EventBridge : proporciona `Describe` y otorga `List` permisos para los EventBridge recursos que están asociados a su cuenta. AWS
- Amazon MSK: proporciona `Describe` y otorga `List` permisos para los recursos de Amazon MSK y MSK Connect asociados a su cuenta. `Get` AWS
- Amazon MemoryDB: proporciona `Describe` permisos para los recursos de MemoryDB asociados a su cuenta. AWS

- Amazon Redshift: proporciona `Describe` permisos para los recursos de Redshift que están asociados a su cuenta. AWS
- AWS Global Accelerator: proporciona `Describe` `List` permisos para los recursos de Global Accelerator asociados a su AWS cuenta.
- AWS Firewall de red: proporciona `Describe` `List` permisos para los recursos del Firewall de red asociados a su AWS cuenta.
- AWS Shield: proporciona `Describe` `List` permisos para los recursos de Shield que están asociados a su AWS cuenta.
- AWS WAF V2: proporciona `Get` `List` permisos para los recursos del WAF V2 asociados a su AWS cuenta.
- AWS Administrador de acceso a los recursos: proporciona `Get` `List` permisos para los recursos de RAM asociados a su AWS cuenta.
- Amazon VPC Lattice: proporciona `List` permisos para `Get` los recursos de VPC Lattice que están asociados a su cuenta. AWS
- AWS Configuración: proporciona `Describe` y otorga `List` permisos para los recursos de configuración asociados a su cuenta. AWS
- Amazon CloudFront : proporciona `Get` y otorga `List` permisos para CloudFront los recursos que están asociados a su AWS cuenta.
- AWS Secrets Manager: proporciona `Describe` `List` permisos para los recursos de Secrets Manager que están asociados a su AWS cuenta.
- AWS Servicio de directorio: proporciona `Describe` permisos para los recursos del servicio de directorio que están asociados a su AWS cuenta.
- Amazon DSQL: proporciona `List` permisos para `Get` los recursos de DSQL asociados a su AWS cuenta.
- Amazon QLDB: proporciona `List` permisos para `Describe` los recursos de QLDB asociados a su cuenta. AWS
- AWS Gestor de certificados: proporciona `Describe` y otorga `List` permisos para los recursos de ACM asociados a su cuenta. `Get` AWS
- Application Auto Scaling: proporciona `Describe` permisos para los recursos de Application Auto Scaling que están asociados a su AWS cuenta.
- Incidentes de SSM: proporciona `Get` `List` permisos para los recursos de incidentes de SSM asociados a su AWS cuenta.

- Etiqueta: otorga `GetResources` permiso para consultar los recursos etiquetados que están asociados a su cuenta. AWS

La política AWS gestionada `AWSResilienceHubV2AssessmentExecutionPolicy` proporciona estos permisos. Adjunte la política administrada en lugar de copiar el documento de la política para que sus permisos permanezcan actualizados a medida que se AWS actualiza. Para ver el documento completo de la política, consulte AWSResilienceHubV2AssessmentExecutionPolicy la Guía de referencia de políticas AWS administradas.

AWSResilienceHubResilienceTestingPolicy

Puede adjuntar la `AWSResilienceHubResilienceTestingPolicy` a las identidades de IAM. Esta política otorga a Resilience Hub los AWS Fault Injection Service (AWS FIS) permisos necesarios para iniciar y gestionar experimentos en tu nombre durante las pruebas de resiliencia. Los experimentos iniciados por Resilience Hub se etiquetan con`managedBy: resiliencehub`.

Detalles del permiso

Esta política incluye los permisos siguientes:

- AWS Fault Injection Service (AWS FIS) — Proporciona permisos para crear y administrar las plantillas de experimentos y los experimentos que Resilience Hub ejecuta en tu nombre: crear y eliminar plantillas de experimentos, iniciar y detener los experimentos, supervisar el estado de los experimentos, enumerar los recursos de clientes a los que va dirigido un experimento, etiquetar los recursos al crearlos y configurar objetivos con varias cuentas. Estas acciones se refieren a los recursos etiquetados con ellos. `managedBy: resiliencehub`
- IAM: permite `iam:PassRole` transferir la función de ejecución de la prueba y permitir `iam:CreateServiceLinkedRole` crear la función vinculada AWS FIS al servicio que necesita para ejecutar los experimentos. AWS FIS
- AWS Conmutador regional del controlador de recuperación de aplicaciones (ARC): proporciona `List Get` permisos para supervisar las ejecuciones del plan del conmutador regional que se ejecutan como parte de un experimento.
- Amazon CloudWatch (CloudWatch): permite `DescribeAlarmHistory` evaluar las alarmas de los clientes como parte del flujo de trabajo posterior al experimento durante las pruebas de resiliencia.

```
{
  "Version": "2012-10-17"       ,
```

```
  "Statement": [
    {
      "Sid": "AWSResilienceHubFISActionStatement",
      "Effect": "Allow",
      "Action": "fis:CreateExperimentTemplate",
      "Resource": "arn:aws:fis:*:*:action/*"
    },
    {
      "Sid": "AWSResilienceHubFISCreateExperimentTemplateStatement",
      "Effect": "Allow",
      "Action": "fis:CreateExperimentTemplate",
      "Resource": "arn:aws:fis:*:*:experiment-template/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/managedBy": "resiliencehub"
        }
      }
    },
    {
      "Sid": "AWSResilienceHubFISStartExperimentFromTemplateStatement",
      "Effect": "Allow",
      "Action": "fis:StartExperiment",
      "Resource": "arn:aws:fis:*:*:experiment-template/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/managedBy": "resiliencehub"
        }
      }
    },
    {
      "Sid": "AWSResilienceHubFISStartExperimentStatement",
      "Effect": "Allow",
      "Action": "fis:StartExperiment",
      "Resource": "arn:aws:fis:*:*:experiment/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/managedBy": "resiliencehub"
        }
      }
    },
    {
      "Sid": "AWSResilienceHubFISExperimentStatement",
      "Effect": "Allow",
      "Action": [
```

```
        "fis:GetExperiment",
        "fis:StopExperiment",
        "fis:ListExperimentResolvedTargets"
      ],
      "Resource": "arn:aws:fis:*:*:experiment/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/managedBy": "resiliencehub"
        }
      }
    },
    {
      "Sid": "AWSResilienceHubFISExperimentTemplateStatement",
      "Effect": "Allow",
      "Action": [
        "fis:CreateTargetAccountConfiguration",
        "fis:DeleteExperimentTemplate"
      ],
      "Resource": "arn:aws:fis:*:*:experiment-template/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/managedBy": "resiliencehub"
        }
      }
    },
    {
      "Sid": "AWSResilienceHubFISPassRoleStatement",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::*:role/*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "fis.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AWSResilienceHubFISTagResourceStatement",
      "Effect": "Allow",
      "Action": "fis:TagResource",
      "Resource": [
        "arn:aws:fis:*:*:experiment-template/*",
        "arn:aws:fis:*:*:experiment/*"
      ],
```

```
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/managedBy": "resiliencehub"
        }
      }
    },
    {
      "Sid": "AWSResilienceHubRegionSwitchStatement",
      "Effect": "Allow",
      "Action": [
        "arc-region-switch:ListPlanExecutions",
        "arc-region-switch:GetPlanExecution"
      ],
      "Resource": "arn:aws:arc-region-switch::*:plan/*:*"
    },
    {
      "Sid": "AWSResilienceHubFISCreateSLRStatement",
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "fis.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AWSResilienceHubCloudWatchAlarmStatement",
      "Effect": "Allow",
      "Action": "cloudwatch:DescribeAlarmHistory",
      "Resource": "*"
    }
  ]
}
```

AWSResilienceHubServiceRolePolicy

`AWSResilienceHubServiceRolePolicy`Se trata de una política de roles vinculados al servicio (SLR). No puede adjuntar esta política a sus entidades de IAM. La próxima generación de Resilience Hub crea automáticamente este rol vinculado al servicio cuando habilitas el soporte de la AWS organización para la gestión de la resiliencia de varias cuentas. Este rol confía en el director del servicio. `resiliencehub.amazonaws.com`

Para obtener más información sobre los roles vinculados a servicios para AWS Resilience Hub, consulte Uso de roles vinculados a servicios para Resilience Hub. AWS

Detalles del permiso

Con esta política, Next Generation Resilience Hub puede acceder a la información de AWS las organizaciones de solo lectura para gestionar la resiliencia con múltiples cuentas.

Esta política incluye los permisos siguientes:

- AWS Organizaciones: proporciona `Describe` y otorga `List` permisos a los recursos de las organizaciones. Estos permisos descubren la estructura de la organización, identifican a los administradores delegados y verifican el estado de acceso confiable.

La siguiente política de IAM proporciona los permisos necesarios para que el Resilience Hub de próxima generación acceda a los recursos de la AWS organización para la gestión de la resiliencia de varias cuentas.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSResilienceHubOrganizationsReadStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListChildren",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListDelegatedServicesForAccount",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListRoots",
                "organizations:ListTagsForResource"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

La próxima generación de Resilience Hub se actualiza a AWS políticas administradas

Consulta los detalles sobre las actualizaciones de las políticas AWS gestionadas para la próxima generación de Resilience Hub desde que este servicio comenzó a hacer un seguimiento de estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial de documentos de Next Generation Resilience Hub.

Cambio	Descripción	Fecha
AWSResilienceHubResilienceTestingPolicy: política nueva	AWS se ha añadido una nueva política para la próxima generación de Resilience Hub para conceder los AWS Fault Injection Service (AWS FIS) permisos necesarios para iniciar y gestionar experimentos en tu nombre durante las pruebas de resiliencia.	31 de julio de 2026
AWSResilienceHubServiceRolePolicy: actualización de una política actual	La próxima generación de Resilience Hub agregó permisos de AWS organización de solo lectura al. `AWSResilienceHubServiceRolePolicy` Estos permisos permiten la gestión de la resiliencia de varias cuentas, lo que incluye descubrir la estructura de la organización, identificar a los administradores delegados y verificar el estado de acceso confiable.	7 de julio de 2026

Cambio	Descripción	Fecha
AWSResilienceHubV2 AssessmentExecutionPolicy: política nueva	La próxima generación de Resilience Hub agregó una nueva política para otorgar permisos de acceso de solo lectura a otros AWS servicios para el descubrimiento, la evaluación y la administración de la resiliencia.	18 de junio de 2026
La próxima generación de Resilience Hub comenzó a rastrear los cambios	La próxima generación de Resilience Hub comenzó a hacer un seguimiento de los cambios en sus políticas AWS gestionadas.	18 de junio de 2026

Configuración AWS Integración de organizaciones (opcional)

Si usas AWS Organizations, puedes configurar opcionalmente la próxima generación de Resilience Hub para proporcionar una gobernanza centralizada en toda tu organización. El siguiente es un resumen rápido de la configuración:

1. La cuenta de administración permite el acceso confiable para `resiliencehub.amazonaws.com`.
2. Service-Linked Los roles (`AWSServiceRoleForResilienceHub`) se crean automáticamente en todas las cuentas de los miembros.
3. La cuenta de administración registra a un administrador delegado.
4. El administrador delegado selecciona una región de origen para la agregación de datos.

Los propietarios de servicios individuales de las cuentas de los miembros siguen creando sus propias funciones de invocador para sus servicios. La SLR proporciona al administrador delegado una visibilidad multicuenta de solo lectura.

Configuración de una región de origen

Si usas AWS Organizaciones, el administrador delegado selecciona una región de origen en la que se agregan los datos a nivel de la organización. La región de origen es Región de AWS donde se

recopilan todos los datos resumidos a nivel de la organización para centralizar los informes y los paneles.

Al seleccionar una región de origen, elija una región que:

- Está cerca de tu equipo de operaciones principal.
- Cumple con sus requisitos de residencia de datos.

Los datos resumidos del servicio (identificadores, puntajes de cumplimiento, estado) se replican desde todas las regiones y cuentas a la región de origen para realizar consultas rápidas y centralizadas. Los detalles completos, como la topología, los hallazgos y las dependencias, permanecen en sus regiones de origen y se puede acceder a ellos a pedido.

Para obtener instrucciones detalladas para la configuración, consulte AWS Integración de organizaciones.

Multi-account configuración (sin AWS Organizaciones)

Si los recursos de tu servicio abarcan varias AWS cuentas y no utilizas AWS Organizaciones, necesitas funciones multicuenta además de la función de invocador.

Paso 1: Crea funciones multicuenta

En cada cuenta que contenga recursos para tu servicio, crea un rol con:

- `ReadOnlyAccess`política adjunta.
- Una política de confianza que permite al invocador asumirla, utilizando una `ExternalId` para evitar ataques confusos de subalternos. Utilice un `ExternalId` valor único por combinación de servicio y cuenta:

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

```
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::123456789012:role/AWSResilienceHubAssessmentRole"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "sts:ExternalId": "ngrh-my-service-111122223333"
      }
    }
  }]
}
```

Paso 2: Conceda permiso al rol de invocador para que asuma funciones multicuenta

Agregue una política integrada a su función de invocador que le permita asumir las funciones multicuenta:

```
{
  "Effect": "Allow",
  "Action": "sts:AssumeRole",
  "Resource": [
    "arn:aws:iam::111122223333:role/NGRHResourceRole",
    "arn:aws:iam::444455556666:role/NGRHResourceRole"
  ]
}
```

Paso 3: Configura los roles multicuenta en tu servicio

Especifique los ARN y los ID externos de los roles multicuenta al crear el servicio:

```
aws resiliencehubv2 create-service \
  --name "my-service" \
  --regions '["us-east-1"]' \
  --permission-model '{
    "invokerRoleName": "AWSResilienceHubAssessmentRole",
    "crossAccountRoles": [
      {
        "crossAccountRoleArn": "arn:aws:iam::111122223333:role/NGRHResourceRole",
        "externalId": "ngrh-my-service-111122223333"
      },
      {
```

```
        "crossAccountRoleArn": "arn:aws:iam::444455556666:role/NGRHResourceRole",
        "externalId": "ngrh-my-service-444455556666"
      }
    ]
  }'
```

Puede configurar hasta 5 ARN de roles multicuenta por servicio.

Customer-managed claves (opcional)

La próxima generación de Resilience Hub admite AWS KMS claves administradas por el cliente (CMK) para cifrar sus datos. Para usar una CMK, asegúrate de que tu política de IAM incluya los siguientes permisos: AWS KMS

- `kms:DescribeKey`
- `kms:GenerateDataKey`
- `kms:Encrypt`
- `kms:Decrypt`

Para las evaluaciones programadas o de larga duración, incluya también. `kms:CreateGrant`

No es necesario cambiar la función de invocador para el cifrado CMK. La próxima generación de Resilience Hub utiliza la identidad de la persona que llama para las operaciones sincrónicas y AWS KMS concede para las operaciones asincrónicas.

Cómo empezar con Resilience Hub de próxima generación

Este tutorial lo guía a través del flujo de trabajo integral para usar la próxima generación de Resilience Hub, desde la creación de su primer servicio hasta la revisión de los resultados del modo de falla.

Temas

- Paso 5: Habilitar el descubrimiento de dependencias (opcional)
- Paso 6: Realiza tu primera prueba de resiliencia (opcional)

Descripción general del tutorial y requisitos previos

Este tutorial lo guía a través del flujo de trabajo integral para crear su primer sistema y servicio, realizar una evaluación del modo de falla y revisar los resultados. Al final, dispondrá de una evaluación de resiliencia válida para una de sus aplicaciones.

Paso	Qué harás	Tiempo estimado
1	Configure una política de resiliencia	3 minutos
2	Cree su primer sistema y servicio	5 minutos
3	Ejecute su primera evaluación del modo de fallo	De 5 a 15 minutos (asincrón ico)
4	Revise las conclusiones y recomendaciones	10 minutos
5	Habilite el descubrimiento de dependencias (opcional)	5 minutos
6	Realice su primera prueba de resiliencia (opcional)	10 minutos

Tiempo total: aproximadamente de 40 a 50 minutos.

Antes de comenzar este tutorial, asegúrese de lo siguiente:

- Tiene un conjunto de recursos Cuenta de AWS implementados (AWS CloudFormation pila, recursos etiquetados o clúster de Amazon EKS).
- Tiene una función de servicio de IAM para la próxima generación de Resilience Hub. Puedes dejar que la consola cree uno automáticamente al crear tu servicio, o crear uno manualmente de antemano. Para obtener más información, consulte Permisos y funciones de IAM necesarios.

- Tienes permisos de IAM para llamar a la próxima generación de API de Resilience Hub.

Paso 1: Configurar una política de resiliencia

Una política de resiliencia define los objetivos de resiliencia de su servicio, como los objetivos de SLO de disponibilidad, los objetivos de tiempo de recuperación (RTO) y los objetivos de punto de recuperación (RPO). En este paso, crea una política y la aplica a su servicio.

Consola:

1. Seleccione Políticas > Crear política.
2. Introduzca un nombre (por ejemplo,`Standard Availability`).
3. Habilite el SLO de disponibilidad y configúrelo en`99.9%`.
4. (Opcional) Habilite la Multi-Region DR si su aplicación abarca varias regiones.
5. Seleccione Crear.
6. Diríjase a su servicio y aplique la política.

AWS CLI:

```
# Create the policy
aws resiliencehubv2 create-policy \
  --name "standard-availability" \
  --availability-slo '{"target": 99.9}'

# Apply the policy to your service
aws resiliencehubv2 update-service \
  --service-arn "arn:aws:resiliencehub:us-east-1:123456789012:service/api-
service:def456" \
  --policy-arn "arn:aws:resiliencehub:us-east-1:123456789012:policy/standard-
availability:ghi789"
```

Para obtener más información acerca de las políticas de , consulte Políticas de resiliencia.

Paso 2: Cree su primer sistema y servicio

Un sistema de la próxima generación de Resilience Hub representa una aplicación empresarial. Un servicio representa un componente desplegable dentro de ese sistema. En este paso, se crea el primer sistema y se le asocia un servicio.

Crea un sistema

Consola:

1. Abra la consola Resilience Hub de próxima generación.
2. Seleccione Sistemas > Crear sistema.
3. Introduzca un nombre (por ejemplo`My Application`) y una descripción opcional.
4. Seleccione Crear.

AWS CLI:

```
aws resiliencehubv2 create-system \
  --name "my-application" \
  --description "My first application in Resilience Hub"
```

Crear un servicio

Un servicio representa un componente desplegable. Al crear un servicio, lo asocias a tu sistema y especificas dónde debe buscar tus AWS recursos la próxima generación de Resilience Hub (fuentes de entrada).

Consola:

1. Seleccione Servicios > Crear servicio.
2. Introduzca un nombre (por ejemplo,`api-service`).
3. Seleccione su sistema.
4. En Modelo de permisos, realice una de las siguientes acciones:
   - Para permitir que la consola cree automáticamente el rol requerido, elija Crear nuevo rol.
   - Si ya tiene un rol, elija Usar un rol de servicio existente y elíjalo de la lista.
5. En Fuentes de entrada, agrega el ARN de la AWS CloudFormation pila, las etiquetas de recursos o la ubicación del archivo de estado de Terraform.
6. Seleccione Crear.

AWS CLI:

```
aws resiliencehubv2 create-service \
```

```
  --name "api-service" \
  --regions '["us-east-1"]' \
  --associated-systems '[{"systemArn": "arn:aws:resiliencehub:us-
east-1:123456789012:system/my-application:abc123"}]' \
  --permission-model '{"invokerRoleName": "AWSResilienceHubAssessmentRole"}'
```

Asocie el servicio al sistema

Tras crear el sistema y el servicio, asocie el servicio al sistema creando un recorrido de usuario.

Consola:

1. Elija Sistemas y seleccione el nombre de su sistema.
2. Seleccione Crear recorrido de usuario.
3. Introduzca un nombre para el recorrido del usuario (por ejemplo,`checkout process`).
4. Seleccione el servicio que creó para asociarlo a este recorrido del usuario.
5. Elige Crear recorrido de usuario.

Paso 3: Realice su primera evaluación del modo de fallo

Una vez creado un servicio y aplicada una política, ahora puede ejecutar una evaluación del modo de fallo. Durante la evaluación, la próxima generación de Resilience Hub descubre automáticamente sus recursos y crea una topología antes de analizar los modos de falla.

Consola:

1. Navega hasta tu servicio.
2. Seleccione la guía del modo de error y añada cualquier afirmación sobre su servicio. Para obtener más información, consulte Guía del modo de error.
3. Seleccione Ejecutar la evaluación del modo de fallo.
4. Espere a que finalice la evaluación. Esto suele tardar entre 5 y 15 minutos.

AWS CLI:

```
aws resiliencehubv2 start-failure-mode-assessment \
  --service-arn "arn:aws:resiliencehub:us-east-1:123456789012:service/api-
service:def456"
```

Para comprobar el estado de la evaluación:

```
aws resiliencehubv2 list-failure-mode-assessments \
  --service-arn "arn:aws:resiliencehub:us-east-1:123456789012:service/api-
service:def456"
```

Qué ocurre durante la evaluación

Mientras se ejecuta la evaluación, la próxima generación de Resilience Hub realiza los siguientes pasos en segundo plano:

1. la próxima generación de Resilience Hub asume su función de invocador.
2. Lee los recursos de las fuentes de entrada configuradas (etiquetas AWS CloudFormation, Terraform, Amazon EKS).
3. Identifica las relaciones entre padres e hijos (por ejemplo, del grupo de Auto Scaling a las instancias EC2).
4. Resilience Hub crea una topología de su servicio.
5. Crea una topología que muestra el flujo y la contención de los datos.
6. Un sistema de IA multiagente analiza la arquitectura en busca de modos de fallo comparándolos con su política de resiliencia y AWS Well-Architected sus mejores prácticas.

Una vez finalizada la generación de la topología, puede ver los resultados en la consola:

- Vista gráfica: mapa visual de los recursos y las conexiones.
- Vista de tabla: lista de todos los recursos descubiertos con metadatos.
- Exportación a JSON: descargue la topología completa para un análisis externo.

Paso 4: Revise las conclusiones y recomendaciones del modo de falla

Una vez finalizada la evaluación, revise los resultados para comprender los posibles modos de falla de su servicio y las mejoras recomendadas.

Consola:

1. Navegue hasta su servicio y seleccione la pestaña Modos de error.
2. Revise los hallazgos ordenados por gravedad.
3. Elige cualquier resultado para ver el razonamiento detallado y las recomendaciones.

AWS CLI:

```
aws resiliencehubv2 list-failure-mode-findings \
  --service-arn "arn:aws:resiliencehub:us-east-1:123456789012:service/api-
service:def456"
```

Comprender sus hallazgos

Cada hallazgo le indica:

- Cuál es el modo de error (por ejemplo, "base de datos Single-AZ RDS»).
- Por qué es importante para su arquitectura.
- Cómo solucionarlo, con recomendaciones que incluyen consideraciones de costo y complejidad.
- Con qué requisito de política se refiere.

Tomar medidas

Para cada hallazgo, puedes hacer lo siguiente:

- Motivo: piense en el modo de falla en detalle y razone en la probabilidad y el impacto de que ocurra.
- Solucionarlo: implemente la recomendación si la probabilidad y el impacto lo justifican y, a continuación, vuelva a ejecutar la evaluación para verificarla.
- Marcar como irrelevante: suprima la conclusión si no se aplica a su caso de uso. Los hallazgos suprimidos permanecerán suprimidos en futuras evaluaciones.
- Priorizar: utilice la gravedad para decidir qué es lo que debe abordarse primero.

Paso 5: Habilitar el descubrimiento de dependencias (opcional)

La detección de dependencias identifica automáticamente los AWS servicios, los puntos finales internos y los puntos finales de terceros a los que llama su servicio. Utiliza el análisis del registro de consultas del DNS con un período retrospectivo de 35 días y un sondeo continuo para identificar las dependencias que quizás no conozcas, incluidas las llamadas interregionales inesperadas o las dependencias críticas de terceros.

La detección de dependencias es un complemento opcional. Para habilitarlo, vaya a su servicio en la consola y elija Habilitar la detección de dependencias. Una vez habilitada, la próxima generación de

Resilience Hub comienza a descubrir las dependencias y las muestra en la pestaña Dependencias de su servicio.

Para obtener más información, consulte Detección de dependencias.

Paso 6: Realiza tu primera prueba de resiliencia (opcional)

Las pruebas de resiliencia ayudan a validar que tu servicio funcione y se recupere según lo esperado mediante la inyección de errores controlados mediante (). AWS Fault Injection Service AWS FIS En este paso, eliges una plantilla de prueba, creas una prueba para tu servicio e inicias una ejecución de prueba.

Consola

1. Navega hasta tu servicio y elige la pestaña Pruebas. Verás las pruebas de resiliencia recomendadas en función de la arquitectura y la política de resiliencia de tu servicio.
2. Seleccione una plantilla de prueba (por ejemplo, Zona de disponibilidad: recuperación). Seleccione Ver detalles para obtener más información sobre la prueba recomendada.
3. Seleccione Editar la configuración de la prueba, especifique los parámetros necesarios y guarde. De este modo, se crea la prueba a partir de la plantilla; la configuración se guarda y se reutiliza para futuras ejecuciones. Puede editar la configuración de prueba en cualquier momento.
4. Seleccione Iniciar prueba para iniciar una ejecución de prueba.
5. Supervise la ejecución y compruebe si se han cumplido sus objetivos de recuperación.

AWS CLI

```
# List the available test templates
aws resiliencehubv2 list-test-templates --region us-east-1

# Create a test for your service from a template
aws resiliencehubv2 create-test \
  --test-template-arn "arn:aws:resiliencehub:us-east-1:aws:test-template/aws-az-
recovery:rtaz001" \
  --target-identifier "arn:aws:resiliencehub:us-east-1:123456789012:service/api-
service:def456" \
  --parameters '{"availabilityZone": ["us-east-1a"]}'

# Start a test run
aws resiliencehubv2 start-test-run --test-id "test-id"
```

```
# Check the status and results of the test run
aws resiliencehubv2 get-test-run --test-run-id "test-run-id"
```

Para obtener más información, consulte Pruebas de resiliencia.

Sistemas, recorridos de usuarios y servicios

El modelado de aplicaciones es la base de la próxima generación de Resilience Hub. Usted modela sus aplicaciones utilizando una jerarquía de sistemas, recorridos de usuario y servicios que coincide con la forma en que su organización piensa acerca de sus aplicaciones empresariales.

Temas

- Descripción general: los sistemas, los recorridos de los usuarios y la jerarquía de servicios
- Creación y administración de sistemas
- Creación y gestión de los recorridos de los usuarios
- Creación y administración de servicios
- Agregar y eliminar recursos de un servicio
- Importación del contexto de la aplicación desde registros externos
- Visualización de la topología del servicio
- Ejemplo: modelar una aplicación multicuenta

Descripción general: los sistemas, los recorridos de los usuarios y la jerarquía de servicios

La jerarquía de modelado de aplicaciones de la próxima generación de Resilience Hub consta de tres niveles:

- Sistemas: el contenedor de nivel superior que representa una aplicación empresarial (por ejemplo, una plataforma de comercio electrónico o un sistema comercial).
- Trayectorias de los usuarios: rutas empresariales fundamentales dentro de un sistema (por ejemplo, la «ruta de compra» o la «tramitación de los pedidos»).
- Servicios: los componentes básicos que comprenden AWS los recursos, el código y la capacidad de observación que respaldan el recorrido de los usuarios. Un servicio pertenece exactamente a un sistema, pero puede soportar múltiples recorridos de usuario.

El siguiente ejemplo muestra la jerarquía de una plataforma de comercio electrónico:

```
System (e.g., "E-commerce Platform")
### User Journey: "Path to purchase"
#   ### Service: "Auth Service"
#   ### Service: "Checkout Service"
#   ### Service: "Payment Service"
### User Journey: "Order fulfillment"
#   ### Service: "Order Management Service"
#   ### Service: "Shipping Service"
### Shared Service: "EKS Platform Service"
    (supports multiple user journeys)
```

Usted define dónde encontrar sus AWS recursos (AWS CloudFormation pilas, archivos de estado de Terraform, etiquetas de recursos o clústeres de Amazon EKS) y la próxima generación de Resilience Hub los descubre automáticamente y los mapea en una topología que muestra cómo se conectan los recursos.

Cómo funciona el modelado de aplicaciones

Para modelar su aplicación en la próxima generación de Resilience Hub, siga estos pasos:

1. Cree una política de resiliencia: defina sus objetivos de disponibilidad, recuperación ante desastres y recuperación de datos. Consulte the section called “Políticas de resiliencia”.
2. Cree un sistema: defina la aplicación empresarial de nivel superior. Consulte the section called “Cree un sistema”.
3. Cree recorridos de usuario: defina las rutas comerciales críticas dentro de su sistema. Consulte the section called “Creación y gestión de los recorridos de los usuarios”.
4. Cree servicios: defina los componentes básicos y especifique las fuentes de entrada para el descubrimiento de recursos. Consulte the section called “Creación y administración de servicios”.
5. Realice una evaluación: inicie una evaluación en modo de falla para identificar las brechas de resiliencia. Consulte the section called “Evaluaciones de modos de falla”.

Creación y administración de sistemas

Un sistema representa una aplicación empresarial que opera su organización. La mayoría de los clientes crean un sistema por cada aplicación empresarial principal.

Cree un sistema

Para crear un sistema (consola)

1. Abra la consola de Resilience Hub de próxima generación en https://console.aws.amazon.com/resiliencehub/v2/home.
2. En el panel de navegación, elija Sistemas.
3. Seleccione Crear sistema.
4. Proporcione los siguientes detalles:
   - Nombre del sistema: introduzca un nombre descriptivo para el sistema. El nombre debe tener entre 1 y 60 caracteres y puede contener letras, números, guiones y guiones bajos.
   - Descripción: (opcional) Ingresa una descripción que ayude a tu equipo a identificar el propósito de este sistema.
   - Cross-account compartir: (opcional) Habilite esta configuración si desea que los servicios de otros Cuenta de AWS usuarios se asocien a este sistema.
   - Cifrado: (opcional) Elija una AWS KMS clave gestionada por el cliente para cifrar los datos del sistema.
   - Etiquetas: (opcional) Agregue una o más etiquetas a su sistema.
5. Seleccione Crear sistema.

Para crear un sistema (AWS CLI)

- Use el siguiente comando:

```
aws resiliencehubv2 create-system \
  --name "system-name" \
  --description "system-description"
```

Cuándo crear varios sistemas

Cree sistemas separados cuando:

- Las aplicaciones o los servicios son gestionados de forma independiente por distintos equipos.

- Quieres un seguimiento independiente de las posturas de resiliencia para cada aplicación.

Utilice un único sistema cuando:

- Varios servicios trabajan en conjunto para ofrecer valor empresarial.
- Desea evaluar en grupo la resiliencia de los servicios relacionados.
- Los servicios comparten la infraestructura (por ejemplo, una plataforma Amazon EKS común).

Enumere y describa los sistemas

Para ver sus sistemas (consola)

1. Abra la consola Resilience Hub de próxima generación.
2. En el panel de navegación, elija Sistemas.
3. La lista de sistemas muestra todos los sistemas de su cuenta con su nombre, número de servicios y fecha de creación.
4. Para ver los detalles de un sistema específico, elige el nombre del sistema.

Para enumerar los sistemas (AWS CLI)

- Ejecute los siguientes comandos :

```
aws resiliencehubv2 list-systems

aws resiliencehubv2 get-system \
  --system-arn "arn:aws:resiliencehub:region:account-id:system/system-name:id"
```

Eliminar un sistema

No se puede eliminar un sistema mientras tenga asociaciones de servicios. Cuando se elimina un sistema mediante la consola, se eliminan automáticamente las asociaciones de servicios. Al utilizar la CLI de AWS, primero debe eliminar todas las asociaciones de servicios y, a continuación, eliminar el sistema.

Para eliminar un sistema (consola)

1. Abra la consola Resilience Hub de próxima generación.
2. En el panel de navegación, elija Sistemas.
3. Seleccione el sistema que desea eliminar.
4. Seleccione Actions (Acciones) y, a continuación, seleccione Delete (Eliminar).
5. En el cuadro de diálogo de confirmación, seleccione la casilla de confirmación de eliminación y elija Eliminar.

Para eliminar un sistema (AWS CLI)

- Use el siguiente comando:

```
aws resiliencehubv2 delete-system \
  --system-arn "arn:aws:resiliencehub:region:account-id:system/system-name:id"
```

Creación y gestión de los recorridos de los usuarios

Los recorridos de los usuarios describen las rutas empresariales críticas dentro de su sistema. Le ayudan a organizar los servicios por capacidad empresarial y a aplicar políticas de resiliencia a nivel empresarial.

Cree un recorrido para el usuario

Para crear un recorrido de usuario (consola)

1. Abra la consola Resilience Hub de próxima generación.
2. En el panel de navegación, selecciona Sistemas y, a continuación, elige el sistema al que quieres añadir un recorrido de usuario.
3. Seleccione la pestaña Trayectorias de usuario.
4. Selecciona Crear recorrido de usuario.
5. Proporcione los siguientes detalles:

- Nombre: introduzca un nombre que describa la capacidad empresarial (por ejemplo, «Ruta de compra» o «Gestión logística de pedidos»). Nombre los viajes del usuario después de lo que hace un usuario final, no después de los componentes técnicos.
- Descripción: (opcional) Introduzca una descripción del recorrido del usuario.
- Servicios asociados: (opcional) Seleccione los servicios que respaldan este recorrido del usuario. Puede agregar servicios más adelante.

6. Elige Crear recorrido de usuario.

Para crear un recorrido de usuario (AWS CLI)

- Use el siguiente comando:

```
aws resiliencehubv2 create-user-journey \
  --system-arn "arn:aws:resiliencehub:region:account-id:system/system-name:id" \
  --name "journey-name" \
  --description "journey-description"
```

Pautas para definir los recorridos de los usuarios

- Nombra los recorridos de los usuarios según las capacidades empresariales, no los componentes técnicos.
- El recorrido de un usuario debe representar algo que hace un usuario final (por ejemplo, «comprobar el saldo», no «leer la base de datos»).
- Comience con sus recorridos de usuario más importantes y añada más con el tiempo.
- Un servicio puede pertenecer a múltiples recorridos de usuario, algo que suelen hacer los servicios de plataformas compartidas.

En la siguiente tabla se muestran ejemplos de sistemas y sus correspondientes recorridos de usuario:

Sistema	Viajes de usuario
E-commerce plataforma	Ruta de compra, descubrimiento de productos, cumplimiento de pedidos, devoluciones
Sistema de negociación	Ejecute operaciones, verifique la cartera, transfiera fondos
Orquestación de conmutación por error	Gestione los planes, ejecute la conmutación por error y ejecute informes

Actualice el recorrido de un usuario

Para actualizar el recorrido de un usuario (consola)

1. Abra la consola Resilience Hub de próxima generación y navegue hasta su sistema.
2. Seleccione la pestaña Trayectorias de los usuarios.
3. Elige el recorrido del usuario que quieres actualizar.
4. Elija Edit (Edición de).
5. Modifique el nombre, la descripción o los servicios asociados según sea necesario.
6. Seleccione Save changes (Guardar cambios).

Eliminar el recorrido de un usuario

Para eliminar el recorrido de un usuario (consola)

1. Abra la consola Resilience Hub de próxima generación y navegue hasta su sistema.
2. Seleccione la pestaña Trayectorias de los usuarios.
3. Selecciona el recorrido del usuario que deseas eliminar.
4. Elija Eliminar.
5. Confirme la eliminación.

Creación y administración de servicios

Los servicios son la entidad principal con la que interactúas en la próxima generación de Resilience Hub. Un servicio representa una unidad desplegable que incluye AWS recursos, código y capacidad de observación.

Crear un servicio

Para crear un servicio (consola)

1. Abra la consola Resilience Hub de próxima generación.
2. En el panel de navegación, elija Servicios.
3. Elija Crear servicio.
4. Proporcione los siguientes detalles:

   - Nombre del servicio: introduzca un nombre descriptivo para su servicio (por ejemplo, `checkout-service` o `payment-service`).
   - Descripción: (opcional) Introduzca una descripción del servicio.
   - Política de resiliencia: seleccione una política de resiliencia para asociarla a este servicio. La política define su SLO y sus RTO/RPO objetivos de disponibilidad.
   - Modelo de permisos: especifique la función de IAM que utilizará la próxima generación de Resilience Hub para la detección de recursos. Elija una de las siguientes opciones:
     - Cree un nuevo rol de servicio (recomendado): la consola crea automáticamente un rol de IAM con la política de confianza correcta y adjunta la política administrada requerida.
     - Usar un rol de servicio existente: elige un rol de IAM existente de la lista. Asegúrese de que el rol tenga la política de confianza y los permisos necesarios. Para obtener más información, consulte Permisos y funciones de IAM necesarios.
     - Cross-account roles: (opcional) Si sus recursos están en otras cuentas, agregue los ARN de los roles multicuenta.
   - Regiones: seleccione las áreas en las Región de AWS que opera su servicio. Puede seleccionar hasta 5 regiones.
   - Descubrimiento de recursos: proporcione fuentes de entrada para permitir el descubrimiento de los recursos utilizados por su servicio. Consulte the section called “Agregue fuentes de entrada a un servicio” para obtener instrucciones sobre cómo agregar fuentes de entrada.

- Detección de dependencias: (opcional) habilite la función de detección de dependencias para este servicio. Consulte the section called “Detección de dependencias” para obtener más información sobre el descubrimiento de dependencias.
- Cifrado de datos: (opcional) Elija una AWS KMS clave gestionada por el cliente para cifrar los datos del servicio. Para obtener más información, consulte the section called “Cifrado de datos”.
- Etiquetas: (opcional) Agregue etiquetas a su servicio.

5. Elija Crear servicio.

Para crear un servicio (AWS CLI)

- Use el siguiente comando:

```
aws resiliencehubv2 create-service \
  --name "service-name" \
  --regions '["region"]' \
  --permission-model '{"invokerRoleName": "role-name"}' \
  --associated-systems '[{"systemArn": "system-arn"}]'
```

En la siguiente tabla se describen los tipos de fuentes de entrada disponibles que puede agregar después de crear el servicio:

Origen de entrada	Usar cuando
AWS CloudFormation pilas	Su infraestructura se define en AWS CloudFormation.
Archivos de estado de Terraform	Terraform (archivo de estado en Amazon S3) administra su infraestructura.
Etiquetas de recursos	El servicio descubre los recursos haciendo coincidir las etiquetas. Una única fuente de entrada basada en etiquetas con varias etiquetas descubre solo los recursos que coinciden con todas las etiquetas especific

Origen de entrada	Usar cuando
	adas. Varias fuentes de entrada basadas en etiquetas descubren los recursos que coinciden con alguna de ellas.
Clústeres de Amazon Elastic Kubernetes Service	Su servicio se ejecuta en Amazon EKS.

Agregue fuentes de entrada a un servicio

Para agregar una fuente de entrada (consola)

1. Abra la consola Resilience Hub de próxima generación y navegue hasta su servicio.
2. Elija la pestaña Configuración.
3. Elija Editar en la sección de detección de recursos del servicio.
4. Seleccione el tipo de fuente de entrada y proporcione la configuración requerida:
   - AWS CloudFormation pila: seleccione una o más AWS CloudFormation pilas. El selector mostrará las pilas correspondientes a las regiones que hayas seleccionado para este servicio.
   - Archivo de estado de Terraform: introduzca la URL de Amazon S3 del archivo de estado.
   - Etiquetas de recursos: introduzca la clave de la etiqueta y los valores que desee que coincidan.
   - Clúster Amazon EKS: introduzca el ARN del clúster y seleccione los espacios de nombres que desee incluir.
5. Elija Añadir.

Para añadir una fuente de entrada (AWS CLI)

- Use el siguiente comando:

```
aws resiliencehubv2 create-input-source \
  --service-arn "service-arn" \
  --resource-configuration '{"cfnStackArn": "stack-arn"}'
```

Ubicación del servicio: misma cuenta frente a cuenta diferente

La misma cuenta que el sistema (sencillo): el sistema y el servicio son los mismos Cuenta de AWS. Un único rol de invocador lo cubre todo. Este enfoque es el mejor para equipos pequeños y cargas de trabajo de una sola cuenta.

Cuenta diferente del sistema (empresa): el sistema está en una cuenta central y los servicios están en cuentas individuales. Este enfoque requiere funciones u AWS organizaciones multicuentas. Es mejor para las grandes organizaciones con propiedad distribuida.

Funciones de servicio

Las funciones de servicio son subconjuntos técnicos de la topología de servicios que representan flujos de trabajo específicos dentro de un servicio.

Por ejemplo, un servicio de autenticación puede tener dos funciones de servicio:

- Inicio de sesión único: incluye al proveedor de identidades, el almacén de sesiones y el servicio de tokens.
- Registro: incluye la base de datos de usuarios, el servicio de correo electrónico y el flujo de verificación.

Las funciones del servicio ayudan a comprender qué recursos participan en qué flujos de trabajo dentro de un solo servicio. La próxima generación de Resilience Hub identifica las funciones de servicio durante la evaluación.

Visualización del registro de eventos de servicio

El registro de eventos del servicio proporciona un historial cronológico de todos los eventos que se han producido en un servicio. Puede usar el registro de eventos para realizar un seguimiento de los cambios, solucionar problemas y auditar la actividad.

Para ver el registro de eventos del servicio (consola)

1. Navegue hasta su servicio.
2. Selecciona el botón Acciones.
3. Selecciona Ver registro de eventos.

Puede filtrar los eventos por tipo de evento e intervalo de tiempo. Se registran los siguientes tipos de eventos:

- Aserción creada: se agregó una aserción al servicio.
- Afirmación eliminada: se eliminó una afirmación del servicio.
- Afirmación actualizada: se modificó una afirmación existente.
- Alcanzabilidad actualizada: se modificó el estado de viabilidad de un componente de la política.
- Servicio creado: se creó el servicio.
- Servicio eliminado: se eliminó el servicio.
- Función creada: se creó una función de servicio.
- Función eliminada: se eliminó una función de servicio.
- Recursos de función agregados: se agregaron recursos a una función de servicio.
- Recursos de funciones eliminados: se eliminaron recursos de una función de servicio.
- Función actualizada: se actualizó una función de servicio.
- Fuentes de entrada actualizadas: se modificaron las fuentes de entrada del servicio.
- Política asociada: se asoció una política de resiliencia al servicio.
- Política disociada: se eliminó una política de resiliencia del servicio.
- Recursos asociados: se descubrieron nuevos recursos y se asociaron al servicio.
- Recursos desasociados: se eliminaron los recursos del servicio.
- Sistema asociado: el servicio estaba asociado a un sistema.
- Sistema desasociado: el servicio se eliminó de un sistema.
- Flujo de trabajo actualizado: se actualizó una configuración de flujo de trabajo.

Cada entrada de evento muestra la marca de tiempo, el tipo de evento y un resumen de lo que ha cambiado. Selecciona Mostrar detalles para ver información adicional sobre un evento específico.

Agregar y eliminar recursos de un servicio

Los recursos se descubren automáticamente a partir de las fuentes de entrada configuradas. Los recursos individuales no se agregan manualmente. La próxima generación de Resilience Hub descubre los recursos de las AWS CloudFormation pilas, los archivos de estado de Terraform, los clústeres de Amazon EKS y las etiquetas de recursos.

Vea los recursos descubiertos

Para ver los recursos (consola)

1. Abra la consola de Resilience Hub de próxima generación y navegue hasta su servicio.
2. Elija la topología del servicio.
3. El gráfico de recursos y la lista de recursos muestran todos los recursos descubiertos con su tipo, región y función de servicio asociada.
4. Use los filtros para filtrar por región o función de servicio.

Para enumerar los recursos (AWS CLI)

- Use el siguiente comando:

```
aws resiliencehubv2 list-resources \
  --service-arn "service-arn"
```

Para filtrar por región:

```
aws resiliencehubv2 list-resources \
  --service-arn "service-arn" \
  --aws-region "region"
```

Actualiza las fuentes de entrada

Para cambiar el lugar en el que la próxima generación de Resilience Hub busca recursos, añada o elimine fuentes de entrada en el servicio. Consulte the section called “Agregue fuentes de entrada a un servicio” para obtener instrucciones sobre cómo agregar fuentes de entrada.

Para eliminar una fuente de entrada (consola)

1. Abra la consola Resilience Hub de próxima generación y navegue hasta su servicio.
2. Elija la pestaña Configuración.

3. Elija Edit (Edición de).
4. Elimine las selecciones de fuentes de entrada existentes.
5. Seleccione Save changes (Guardar cambios).

Para eliminar una fuente de entrada (AWS CLI)

- Use el siguiente comando:

```
aws resiliencehubv2 delete-input-source \
  --service-arn "service-arn" \
  --input-source-id "input-source-id"
```

Importación del contexto de la aplicación desde registros externos

Puede importar el contexto de la aplicación desde registros externos, como los documentos de diseño, para enriquecer su modelo de aplicación en la próxima generación de Resilience Hub. El contexto importado complementa la topología de los recursos con metadatos empresariales que no se capturan en la configuración de los AWS recursos.

Importe documentos de diseño

Los documentos de diseño proporcionan un contexto arquitectónico adicional que la próxima generación de Resilience Hub utiliza durante las evaluaciones en modo de falla. Puede cargar documentos de diseño almacenados en Amazon S3 como fuentes de entrada para su servicio.

Para importar un documento de diseño (consola)

1. Abra la consola Resilience Hub de próxima generación y navegue hasta su servicio.
2. Seleccione la pestaña Asignaciones.
3. Elija la guía del modo de fallo.
4. Seleccione Agregar más desde los archivos de diseño de arquitectura.
5. Introduzca la URL de Amazon S3 de su documento de diseño.
6. Seleccione Guardar archivo de diseño.

Para importar un documento de diseño (AWS CLI)

- Use el siguiente comando:

```
aws resiliencehubv2 create-input-source \
  --service-arn "service-arn" \
  --resource-configuration '{"designFileS3Url": "s3://bucket/path/to/design-doc.pdf"}'
```

Los formatos de documentos de diseño compatibles incluyen archivos PDF, Markdown y de texto sin formato. El motor de evaluación de la IA utiliza estos documentos para comprender la arquitectura prevista e identificar las brechas entre la intención del diseño y la implementación real.

Visualización de la topología del servicio

La consola Resilience Hub de próxima generación ofrece una vista de lienzo visual que muestra la jerarquía de servicios, incluida la topología de los recursos y las funciones de los servicios.

Para ver la topología de los servicios

1. Abra la consola de Resilience Hub de próxima generación y navegue hasta su servicio.
2. Elija la topología del servicio.
3. La vista de topología muestra cómo los recursos descubiertos se conectan entre sí. Los recursos se agrupan por función de servicio y muestran bordes que representan las dependencias.
4. Elija un nodo de recursos para ver sus detalles, incluidos el tipo de recurso, el ARN, la región y la cuenta.

Ejemplo: modelar una aplicación multicuenta

Este ejemplo muestra cómo modelar una gran plataforma de comercio electrónico con 30 servicios en 10 cuentas en Next generation Resilience Hub.

Para modelar una aplicación con varias cuentas

1. Cree el sistema en una cuenta central.

Empieza por crear un sistema único que represente a toda la plataforma de comercio electrónico. Cree el sistema en su cuenta de gobierno central y habilite el uso compartido entre cuentas:

```
aws resiliencehubv2 create-system \
  --name "acme-ecommerce" \
  --description "Acme Corp e-commerce platform" \
  --sharing-enabled
```

2. Cree servicios en sus cuentas respectivas.

   Cada equipo crea su servicio en su propia cuenta, haciendo referencia al ARN del sistema central:

```
# In account A (auth team)
aws resiliencehubv2 create-service \
  --name "auth-service" \
  --regions '["us-east-1", "us-west-2"]' \
  --permission-model '{"invokerRoleName": "AWSResilienceHubAssessmentRole"}' \
  --associated-systems '[{"systemArn": "arn:aws:resiliencehub:us-
east-1:111111111111:system/acme-ecommerce:abc123"}]'

# In account B (checkout team)
aws resiliencehubv2 create-service \
  --name "checkout-service" \
  --regions '["us-east-1", "us-west-2"]' \
  --permission-model '{"invokerRoleName": "AWSResilienceHubAssessmentRole"}' \
  --associated-systems '[{"systemArn": "arn:aws:resiliencehub:us-
east-1:111111111111:system/acme-ecommerce:abc123"}]'
```

3. Agregue fuentes de entrada a cada servicio.

   Cada equipo agrega su configuración de descubrimiento de recursos:

```
# Auth team adds their CloudFormation stack
aws resiliencehubv2 create-input-source \
```

```
  --service-arn "arn:aws:resiliencehub:us-east-1:222222222222:service/auth-
service:def456" \
  --resource-configuration '{"cfnStackArn": "arn:aws:cloudformation:us-
east-1:222222222222:stack/auth-prod/..."}'

# Checkout team adds their EKS cluster
aws resiliencehubv2 create-input-source \
  --service-arn "arn:aws:resiliencehub:us-east-1:333333333333:service/checkout-
service:ghi789" \
  --resource-configuration '{"eks": {"clusterArn": "arn:aws:eks:us-
east-1:333333333333:cluster/checkout-cluster", "namespaces": ["checkout"]}}'
```

4. Defina los recorridos de los usuarios.

   Cree recorridos de usuario en la cuenta central que agrupe los servicios por capacidad empresarial:

```
aws resiliencehubv2 create-user-journey \
  --system-arn "arn:aws:resiliencehub:us-east-1:111111111111:system/acme-
ecommerce:abc123" \
  --name "Path to purchase" \
  --description "Customer browses, adds to cart, and completes checkout"
```

5. Aplica una política de resiliencia.

   Cree una política y asóciela a los servicios:

```
# Create a policy
aws resiliencehubv2 create-policy \
  --name "mission-critical" \
  --availability-slo '{"target": 99.99}' \
  --multi-az '{"rtoInMinutes": 5, "rpoInMinutes": 1, "disasterRecoveryApproach":
 "ACTIVE_ACTIVE"}' \
  --multi-region '{"rtoInMinutes": 30, "rpoInMinutes": 5,
 "disasterRecoveryApproach": "WARM_STANDBY"}'

# Associate with a service
aws resiliencehubv2 update-service \
```

```
  --service-arn "arn:aws:resiliencehub:us-east-1:333333333333:service/checkout-
service:ghi789" \
  --policy-arn "arn:aws:resiliencehub:us-east-1:111111111111:policy/mission-
critical:xyz"
```

6. Ejecute evaluaciones.

   Inicie una evaluación del modo de falla en cada servicio para identificar las brechas de resiliencia:

```
aws resiliencehubv2 start-failure-mode-assessment \
  --service-arn "arn:aws:resiliencehub:us-east-1:333333333333:service/checkout-
service:ghi789"
```

Los servicios se pueden agregar de forma gradual: comience con los servicios más críticos e incorpore más con el tiempo. La vista a nivel de sistema de la consola muestra todos los servicios de todas las cuentas en un único lienzo.

Políticas de resiliencia

Haga coincidir los requisitos de resiliencia de su organización con las políticas de resiliencia. Una política de resiliencia define sus expectativas de resiliencia mediante requisitos modulares y componibles. En lugar de elegir un único tipo de política rígida, las políticas se crean seleccionando los requisitos que son importantes para su aplicación.

Temas

- Comprender las políticas de resiliencia
- Componentes de política
- Crear una política de resiliencia
- Aplicar políticas a la experiencia del usuario y a los niveles de servicio
- Herencia de políticas y evaluación multinivel
- Gestión y actualización de políticas

Comprender las políticas de resiliencia

Las políticas de resiliencia definen los requisitos de resiliencia de su aplicación. Cada política especifica los objetivos que la próxima generación de Resilience Hub evalúa durante las evaluaciones del modo de fallo para determinar si la aplicación cumple sus objetivos de resiliencia.

Las distintas partes interesadas se preocupan por los distintos aspectos de la resiliencia:

- Los equipos centrales de SRE se centran en la recuperación ante desastres (RTO/RPO) y en los objetivos de disponibilidad.
- Los equipos de servicio se centran en el rendimiento operativo (latencia, tasas de error, rendimiento).
- Los equipos de cumplimiento se centran en la protección de datos (RPO para garantizar la durabilidad de los datos).

Las políticas modulares permiten a cada parte interesada definir sus requisitos de forma independiente y, a continuación, aplicarlos en el nivel adecuado de la jerarquía de aplicaciones.

Componentes de política

Las políticas incluyen los siguientes componentes:

Objetivo de nivel de servicio (SLO) de disponibilidad

Defina el SLO objetivo para los servicios asociados a esta política.

Multi-Region recuperación ante desastres

Defina un enfoque multirregional, un objetivo de tiempo de recuperación (RTO) objetivo y un objetivo de punto de recuperación (RPO) para los servicios asociados a esta política.

Multi-AZ recuperación ante desastres

Defina un enfoque multizona, un objetivo de tiempo de recuperación (RTO) objetivo y un objetivo de punto de recuperación (RPO) para los servicios asociados a esta política.

Objetivo de recuperación de datos

Defina la cantidad de tiempo entre las copias de seguridad data/storage de los servicios asociados a esta política.

Crear una política de resiliencia

Puede crear políticas de resiliencia desde la consola o AWS CLI de Resilience Hub de última generación.

Consola:

1. Vaya a Resilience Hub > Políticas.
2. Elija Crear política.
3. Introduzca un nombre de política y una descripción.
4. Seleccione los componentes que necesita:
   - Cambia Multi-Region DR y RTO/RPO configúralo.
   - Cambia el SLO de disponibilidad y establece el porcentaje objetivo.
   - Cambia el objetivo de recuperación de datos y establece el tiempo entre copias de seguridad.
5. Seleccione Crear.

AWS CLI:

```
aws resiliencehubv2 create-policy \
  --name "Critical Service Policy" \
  --multi-region '{"rtoInMinutes": 15, "rpoInMinutes": 5, "disasterRecoveryApproach":
 "WARM_STANDBY"}' \
  --availability-slo '{"target": 99.99}'
```

Aplicar políticas a la experiencia del usuario y a los niveles de servicio

Las políticas se pueden aplicar en dos niveles de la jerarquía de aplicaciones:

Nivel	Cómo aplicarlas	¿Quién suele ser el propietario
Recorrido del usuario	Se aplica al recorrido del usuario dentro del sistema	Equipo central de SRE
Servicio	Aplicado directamente a la entidad de servicio	Equipo de servicio

Para aplicar una política al recorrido de un usuario, utilice el siguiente comando. Todos los servicios incluidos en ese recorrido de usuario se evalúan según esta política:

```
aws resiliencehubv2 update-user-journey \
  --system-arn "arn:aws:resiliencehub:region:account-id:system/system-name:id" \
  --user-journey-id "user-journey-id" \
  --policy-arn "arn:aws:resiliencehub:us-east-1:123456789012:policy/critical-dr:abc123"
```

Para aplicar una política directamente a un servicio, utilice el siguiente comando:

```
aws resiliencehubv2 update-service \
  --service-arn "arn:aws:resiliencehub:..." \
  --policy-arn "arn:aws:resiliencehub:us-east-1:123456789012:policy/high-
performance:def456"
```

Herencia de políticas y evaluación multinivel

Un servicio se evalúa en función de todas las políticas que se le aplican:

- Su política de asignación directa (si la hubiera).
- Políticas heredadas de los recorridos de los usuarios a los que pertenece.

Esto permite separar las preocupaciones:

- Los equipos centrales de SRE establecen las políticas de DR a nivel del recorrido del usuario para su gobernanza.
- Los equipos de servicio establecen políticas de rendimiento a nivel de servicio en función de los requisitos operativos.
- Ambas políticas se aplican simultáneamente a los servicios del recorrido del usuario.

Por ejemplo:

```
User Journey: "Path to Trade"
```

```
  Policy: "Trading Platform DR Policy" (Multi-Region, RTO 15 min, RPO 5 min)
  ### Service: "Order Execution"
        Policy: "Order Execution Performance Policy" (Availability 99.99%, Error <
0.1%, p99 < 50ms)
```

El servicio de «ejecución de órdenes» se evalúa en función de ambas políticas. Debe cumplir los requisitos de DR de la política de experiencia del usuario y los requisitos de rendimiento de su política de servicios específicos.

Resolución de conflictos

Cuando varias políticas contienen requisitos contradictorios para el mismo componente, Next Generation Resilience Hub aplica automáticamente el valor más estricto. El siguiente ejemplo muestra cómo se resuelven los valores de RTO conflictivos:

origen	Componente	Valor
Política de recorrido del usuario	RTO	30 minutos
Política de servicio	RTO	15 minutos
Valor aplicado	RTO	15 minutos (más estricto)

Gestión y actualización de políticas

Puede enumerar, actualizar y eliminar las políticas de resiliencia de la consola o AWS CLI de Resilience Hub de próxima generación.

Para enumerar todas las políticas de su cuenta:

```
aws resiliencehubv2 list-policies
```

Para actualizar una política:

```
aws resiliencehubv2 update-policy \
  --policy-arn "arn:aws:resiliencehub:..." \
  --availability-slo '{"target": 99.99}'
```

Los cambios en una política entran en vigor en la siguiente evaluación del modo de error para todos los servicios que utilizan esa política.

No puede eliminar una política que se aplique actualmente a los servicios o a los viajes de los usuarios. Elimine primero todas las asociaciones.

Evaluación

La próxima generación de Resilience Hub ofrece dos capacidades de evaluación complementarias: la evaluación automática de la dependencia para descubrir y clasificar las dependencias del servicio, y las evaluaciones del modo de fallo para identificar las posibles debilidades de la resiliencia mediante el GenAI-powered análisis.

Temas

- Detección de dependencias
- Evaluaciones de modos de falla

Detección de dependencias

El descubrimiento de dependencias de la próxima generación de Resilience Hub identifica automáticamente todos los AWS servicios, puntos de enlace internos y puntos de enlace de terceros de los que dependen sus servicios y evalúa su ubicación y frecuencia. Utiliza el análisis del registro de consultas del DNS para descubrir dependencias que quizás no conozcas, como las llamadas inesperadas entre regiones, las dependencias críticas de terceros y los servicios a los que se accede con poca frecuencia y que podrían provocar fallos durante los incidentes.

Temas

- Cómo funciona el descubrimiento de dependencias
- Requisitos previos para el descubrimiento de dependencias
- Habilitar la detección de dependencias para un servicio
- Supervisar el estado de descubrimiento

Cómo funciona el descubrimiento de dependencias

El descubrimiento de dependencias analiza los registros de consultas del solucionador de DNS de Route 53 para identificar todos los nombres de dominio que resuelven los recursos informáticos de su servicio. Esto revela el conjunto completo de dependencias externas sin necesidad de agentes, cambios de código ni instrumentación.

Característica	Detalle
Ventana retrospectiva	35 días de datos históricos de consultas de DNS
Supervisión continua	Descubrimiento continuo resumido por hora
Tipos de dependencias compatibles	AWS servicios, puntos finales internos, puntos finales de terceros
Atribución	Las dependencias se atribuyen a recursos informáticos específicos de su servicio
Configuración	No se requieren agentes ni cambios de código: actívelo en cuestión de minutos

Tipos de dependencias compatibles

El descubrimiento de dependencias identifica los siguientes tipos de dependencias:

- AWS puntos de enlace de servicio: Amazon S3, Amazon DynamoDB, SQS AWS y otros servicios a los que recurra su aplicación.
- Puntos finales internos: servicios dentro de su VPC u organización.
- Third-party puntos finales: servicios externos como Stripe o LaunchDarkly Datadog.

- Cross-region llamadas: dependencias que se resuelven en puntos finales de otras regiones. AWS

Cada dependencia descubierta se clasifica por tipo:

Tipo	Description (Descripción)	Ejemplo
AWS servicio	Un punto final AWS de servicio	Amazon S3, Amazon DynamoDB, SQS
Third-party	Un servicio externo AWS y de su organización	LaunchDarkly, Stripe, Datadog
Internal	Un servicio dentro de su organizac ión	Microservicios internos, API compartidas

En qué se diferencia el descubrimiento de dependencias de las herramientas de observabilidad

El descubrimiento de dependencias se centra en la validación de la resiliencia más que en la observabilidad operativa:

Funcionalidad	Herramientas de observabilidad (,) X-Ray CloudWatch	Descubrimiento de dependenc ias de Resilience Hub de próxima generación
Configuración	Requiere instrumentos o agentes del SDK	Sin agentes ni cambios de código, sin agentes
Focus	Supervisión del rendimiento, depuración de la latencia	Validación de resiliencia, pruebas de fallos
Discovery	Reactivo: descubre los fallos durante los incidentes	Proactivo: descubre las dependencias antes de los incidentes
Clasificación	Sin clasificación de criticidad	Hard/soft clasificación
Momento de creación de valor	Días o semanas de instrumen tación	Minutos para habilitarla

Requisitos previos para el descubrimiento de dependencias

Antes de habilitar el descubrimiento de dependencias, asegúrese de que se cumplan los siguientes requisitos:

- El servicio debe tener recursos de cómputo (instancias de Amazon Elastic Compute Cloud, tareas de Amazon Elastic Container Service, pods de Amazon Elastic Kubernetes Service o funciones Lambda vinculadas a VPC) que realicen consultas de DNS a través de resolutores de Route 53.
- Los recursos informáticos deben residir en una VPC configurada para usar resolutores de DNS de Route 53.
- Resilience Hub de última generación descubre instancias de Amazon Elastic Compute Cloud (preferiblemente) o Amazon VPC (alternativa). Esto se puede verificar consultando la topología del servicio en la consola.
- No se requieren permisos de IAM adicionales más allá de la función de invocador estándar: la detección de dependencias utiliza las propias credenciales de servicio de Resilience Hub de próxima generación para acceder a los datos de consulta del DNS.

Habilitar la detección de dependencias para un servicio

Puede habilitar la detección de dependencias desde la consola o mediante la AWS CLI.

Para habilitar la detección de dependencias para un solo servicio (consola)

Navegue hasta su servicio en la consola y elija la pestaña Evaluación. A continuación, selecciona Habilitar el descubrimiento de dependencias.

Para habilitar la detección de dependencias para un solo servicio (CLI)

```
aws resiliencehubv2 update-service \
  --service-arn "arn:aws:resiliencehub:us-east-1:123456789012:service/checkout:abc123"
 \
  --dependency-discovery "ENABLED"
```

Después de habilitar la detección de dependencias, Resilience Hub de próxima generación realiza los siguientes pasos:

1. Consulta 35 días de datos históricos de DNS para los recursos informáticos de su servicio.
2. Identifica, deduplica y atribuye las dependencias a su servicio.

3. Continúa monitoreando cada hora para detectar nuevas dependencias y actualizar las existentes.
4. Muestra los resultados de su servicio en la consola, en la pestaña «Evaluaciones».

Supervisar el estado de descubrimiento

Tras activar la detección de dependencias, el `DependencyDiscoveryConfig` objeto devuelto por las operaciones de la `ListServices` API `GetService` y la API incluye campos que indican si se han encontrado recursos aptos y si el análisis de dependencias sigue en curso.

En la siguiente tabla se describen los campos que indican el estado actual del descubrimiento de dependencias.

Campo	Tipo	Description (Descripción)
`status`	Cadena	El estado actual del descubrimiento de dependencias:`INITIALIZING` ,`ENABLED`, o`DISABLED`.
`eligibleResourceCount`	Entero	La cantidad de recursos informáticos aptos para el descubrimiento de dependencias. Este valor es válido `null` hasta que el proceso de descubrimiento de recursos complete su primera ejecución y se actualice en cada ejecución posterior.
`message`	Cadena	Un mensaje que describe el estado actual del descubrimiento. Este valor se indica `null` cuando se completa el descubrimiento y las dependencias están listas para su visualización.

El `message` campo proporciona un contexto sobre el estado actual de la detección en función del estado y la cantidad de recursos aptos. En la siguiente tabla se muestran los posibles mensajes.

Status	Recuento de recursos aptos	Mensaje
`INITIALIZING`	Aún no está disponible	«Descubriendo recursos»

Status	Recuento de recursos aptos	Mensaje
INITIALIZING	0	«No se descubrió ningún recurso apto»
INITIALIZING	1 o más	«Descubriendo dependencias»
ENABLED	0	«No se descubrió ningún recurso apto»
ENABLED	1 o más	Ninguna. Las dependencias están listas para ser vistas.
DISABLED	Cualquiera	«Habilite el descubrimiento de dependencias para mostrar las dependencias».

El siguiente ejemplo muestra cómo comprobar el estado de detección mediante la AWS CLI.

```
aws resiliencehubv2 get-service \
  --service-arn "arn:aws:resiliencehub:us-east-1:123456789012:service/checkout:abc123"
```

La respuesta incluye el `dependencyDiscovery` objeto:

```
{
  "service": {
    ...
    "dependencyDiscovery": {
      "status": "INITIALIZING",
      "updatedAt": "2026-06-30T10:00:00Z",
      "eligibleResourceCount": 5,
      "message": "Discovering dependencies"
    }
  }
}
```

Cuando el `message` campo es `null` y `status` es`ENABLED`, se completa la detección de dependencias y los resultados están disponibles a través de la `ListDependencies` operación.

> **Note**
>
> Si `eligibleResourceCount` es 0 una vez finalizada la detección, asegúrese de que los recursos informáticos de su servicio cumplen los requisitos previos descritos enRequisitos previos para el descubrimiento de dependencias.

Visualización de las dependencias descubiertas

Después de activar la detección de dependencias, puede ver una tabla de dependencias detectadas con las siguientes columnas:

Columna	Description (Descripción)
Nombre de la dependencia	Nombre o nombre de dominio identificado (por ejemplo, «» o LaunchDarkly «api.stripe.com»)
Tipo	AWS de servicio, de terceros o interno
Ubicación	Dónde está alojada la dependencia (por ejemplo, AWS us-east-1, Azure us-central o RFC1918)
Criticidad	Difícil o flexible: clasificación asignada por el usuario
Frecuencia de consulta	Visualización del volumen de consultas a lo largo del tiempo
Visto por primera vez	Cuando se descubrió la dependencia por primera vez
Visto por última vez	Consulta más reciente a esta dependencia

Cronología de la dependencia

La cronología de las dependencias muestra cuándo se descubrió cada dependencia por primera vez y su actividad a lo largo del tiempo. Seleccione cualquier dependencia para ver los nombres de dominio subyacentes y las direcciones IP de destino. La frecuencia de uso está disponible durante los últimos 35 días y se muestra en detalle por hora para los períodos de un solo día o por día para los períodos semanales.

Calcule la atribución de recursos

La próxima generación de Resilience Hub atribuye las dependencias descubiertas a los recursos informáticos específicos, como las instancias de Amazon EC2, las funciones de Lambda o los contenedores, que realizan consultas de DNS a esas dependencias. Puede filtrar la lista de dependencias por servicio (si la visualiza a nivel de sistema), criticidad (física, parcial o no clasificada), tipo (AWS servicio, externo o interno) o ubicación (AWS externa o interna).

Clasificar las dependencias en rígidas o blandas

Tras revisar las dependencias descubiertas, clasifique cada una de ellas para indicar su impacto en el fallo:

```
aws resiliencehubv2 update-dependency \
  --service-arn "arn:aws:resiliencehub:..." \
  --dependency-id "dependency-id" \
  --criticality "HARD" \
  --comment "Payment processing fails completely without Stripe"
```

Utilice las siguientes pautas para clasificar las dependencias:

Clasifique como	Cuando	Ejemplo
Rígido	Su servicio falla por completo si esta dependencia no está disponible	Base de datos principal, pasarela de pago, servicio de autenticación
Flexible	Su servicio se degrada pero sigue funcionando sin esta dependencia	API de análisis, indicadores de características, motor de recomenda ciones

Cobertura y limitaciones conocidas

El descubrimiento de dependencias cubre todas las consultas de DNS realizadas a través de los resolutores de Route 53 en su VPC, incluidas las consultas de IPv4 e IPv6 y las consultas de Amazon EC2, Amazon ECS, Amazon EKS y Lambda. VPC-connected Se aplican las siguientes limitaciones conocidas:

Limitación	Impact	Solución
Non-VPC Lambda	No se incluyen las funciones Lambda sin conectividad de VPC	Conecte las funciones de Lambda a la VPC
Conexiones IP directas	No se detectan las conexione s realizadas por una dirección IP (no por DNS)	No hay solución alternativa
Dependencias poco frecuente s	Es posible que las dependenc ias a las que se llame menos de una vez por hora no se detecten en el descubrimiento inicial	La mayoría son las llamadas retrospectivas de 35 días; es posible que no aparezcan llamadas muy raras
Tenencia compartida de Kubernetes	Multi-tenant Los clústeres de Amazon EKS pueden atribuir las dependencias al servicio incorrecto	Compruebe que la atribución de recursos de cómputo esté mapeando correctamente los recursos a los servicios

Solución de problemas de detección de dependencias

Si el descubrimiento de dependencias no arroja los resultados esperados, revise los siguientes problemas comunes:

- El descubrimiento no devuelve las dependencias esperadas para las instancias de EC2: compruebe que la dependencia utilice una resolución de DNS (no una IP directa), confirme que los recursos informáticos estén en una VPC con una resolución de Route 53 y compruebe que se haya llamado a la dependencia dentro del período retrospectivo de 35 días.
- El descubrimiento no devuelve las dependencias esperadas para ECS Fargate: compruebe que la topología del servicio incluya la VPC del servicio Fargate de ECS.
- El descubrimiento no devuelve las dependencias esperadas para las funciones de Lambda: compruebe que las funciones de Lambda sí lo VPC-connected son y que la topología del servicio incluye la VPC.

- Dependencias inesperadas entre regiones: las dependencias se marcan automáticamente en la Cross-region consola. Entre las causas más comunes se incluyen los puntos de enlace regionales codificados en el código de la aplicación, los clientes AWS del SDK configurados para una región específica y el enrutamiento de servicios de terceros a puntos de enlace no locales.
- Las dependencias aparecen en el servicio incorrecto: esto suele ocurrir con las VPC compartidas o los clústeres de Amazon EKS. Compruebe que la atribución de recursos de cómputo esté mapeando correctamente los recursos a los servicios.

Para obtener sugerencias adicionales para la solución de problemas, consulte Solución de problemas de Resilience Hub de próxima generación.

Precios

El descubrimiento de dependencias es un complemento opcional:

Componente	Precio
Detección de dependencias	10$ por servicio al mes

Esto permite una identificación automática y continua de todas las dependencias con una retrospectiva de 35 días.

Evaluaciones de modos de falla

Las evaluaciones de los modos de fallo de la próxima generación de Resilience Hub utilizan el GenAI-powered análisis para identificar los posibles modos de fallo en sus servicios y ofrecer recomendaciones prácticas. Las evaluaciones evalúan su arquitectura comparándola con las políticas de resiliencia definidas, las AWS Well-Architected mejores prácticas y el marco de análisis de AWS resiliencia.

Temas

- Cómo funcionan las evaluaciones del modo de falla
- Realizar una evaluación del modo de falla a nivel de servicio
- Visualización de los hallazgos y recomendaciones del modo de falla
- Historial y tendencias de la evaluación
- Precios

Cómo funcionan las evaluaciones del modo de falla

Cuando se ejecuta una evaluación del modo de fallo, el Resilience Hub de próxima generación lleva a cabo los siguientes pasos:

1. Lee el estado actual de los recursos: actualiza la configuración de recursos del servicio desde tu AWS cuenta.
2. Analiza la topología: un sistema de IA multiagente examina cómo se conectan e interactúan sus recursos.
3. Evalúa las políticas mediante el marco de análisis de resiliencia: compara su arquitectura con sus políticas de resiliencia. En primer lugar, realiza una evaluación para determinar si los componentes de la política son alcanzables o no.
4. Aplica las AWS Well-Architected mejores prácticas: comprueba si hay antipatrones de resiliencia comunes.
5. Genera hallazgos: identifica los modos de falla con su gravedad, razonamiento y recomendaciones, y asigna los resultados a sus políticas de resiliencia.

El motor de evaluación utiliza agentes de inteligencia artificial especializados que aplican las mejores prácticas de confiabilidad de AWS Well-Architected Framework y el marco de análisis de AWS resiliencia a su arquitectura específica. Los agentes analizan diferentes aspectos de la resiliencia:

- Disponibilidad: puntos únicos de falla, distribución AZ y redundancia.
- Recuperación ante desastres: Cross-region capacidades, replicación y preparación para la conmutación por error.
- Resiliencia de dependencias: impacto de las fallas de dependencia en su servicio.
- Observabilidad: monitorear las brechas que podrían retrasar la detección de fallas.

La evaluación del modo de falla no consume todos los recursos disponibles. En su lugar, evalúa un subconjunto de recursos conocido como recursos evaluados.

Recurso evaluado: un componente de infraestructura o servicio de alto nivel que se evalúa directamente durante una evaluación de resiliencia. Se evalúa si la configuración de un recurso tiene un impacto significativo en la disponibilidad, la capacidad de recuperación o la tolerancia a errores del servicio. Los recursos que estén fuera de este ámbito no tendrán ningún impacto en la evaluación y no aparecerán en la lista de recursos.

Relación con las políticas de resiliencia

Las evaluaciones del modo de fallo evalúan su aplicación en función de los objetivos definidos en sus políticas de resiliencia. Cada uno de los hallazgos se corresponde con requisitos políticos específicos y muestra exactamente qué objetivos de resiliencia están en riesgo. Por ejemplo:

```
Finding: "RDS database is not configured for Multi-AZ"
  -> Policy requirement: Multi-Region DR (RTO 15 min)
  -> Impact: Regional failover would require manual database restoration,
     exceeding the 15-minute RTO target

Finding: "No health check configured on ALB target group"
  -> Policy requirement: Availability SLO (99.99%)
  -> Impact: Unhealthy instances continue receiving traffic,
     degrading availability below target
```

Guía del modo de error

La orientación sobre los modos de fallo permite orientar a los agentes para que inicien el análisis del modo de fallo.

Aserciones

Las afirmaciones son afirmaciones sobre su aplicación que proporcionan un contexto para las evaluaciones del modo de fallo. Ayudan a los agentes de IA generativos a comprender los aspectos de su arquitectura que no son visibles únicamente desde la configuración de los recursos.

Las afirmaciones pueden ser:

- User-created— Añades aserciones antes de ejecutar una evaluación. Algunos ejemplos son: «La pérdida de datos es inaceptable», «Los picos de tráfico son predecibles» o «El tráfico típico es de 1000 TPS y se convierte en 10 000 TPS».
- System-generated— El motor de evaluación genera afirmaciones durante el análisis que puede revisar, confirmar o ajustar.

Las afirmaciones se clasifican y sirven como puntos de ventaja. Al confirmar o ajustar las afirmaciones, se orienta la evaluación hacia hallazgos más relevantes. Por ejemplo, si la evaluación da por sentado que su solicitud debe aceptar 100 TPS, pero en realidad necesita soportar picos de 10 000 TPS, al ajustar esa afirmación cambiarán los resultados que reciba.

Archivos de diseño de servicios

Puede cargar archivos de diseño que incluyan detalles sobre el diseño técnico que se proporcionarán a los agentes de IA para que realicen el análisis del modo de falla.

Realizar una evaluación del modo de falla a nivel de servicio

Puede ejecutar una evaluación del modo de fallo desde la consola o mediante la AWS CLI. La evaluación se ejecuta de forma asincrónica. El tiempo de finalización típico es de 5 a 15 minutos, según la complejidad del servicio.

Requisitos previos

- La función de invocador del servicio debe estar configurada y ser accesible. Para obtener más información, consulte Permisos y funciones de IAM necesarios.
- El servicio debe tener una topología descubierta válida con una relación de flujo de datos entre al menos dos recursos. Para obtener más información, consulte Requisitos topológicos mínimos.
- Debe aplicarse al menos una política de resiliencia. Las evaluaciones sin políticas siguen ejecutándose, pero producen menos conclusiones específicas.

Requisitos topológicos mínimos

Para ejecutar una evaluación del modo de fallo, el servicio debe tener una topología con una relación de flujo de datos entre al menos dos recursos.

La evaluación del modo de falla analiza cómo se propagan las fallas a través de la arquitectura mediante el examen de las relaciones entre los recursos. Sin una relación de flujo de datos que conecte al menos dos recursos, no hay flujo de datos que analizar. La evaluación no puede producir hallazgos significativos.

Topología válida (la evaluación puede ejecutarse)

Es válida cualquier topología en la que al menos dos recursos estén conectados mediante una relación de flujo de datos. Por ejemplo:

- Un balanceador de carga de aplicaciones que dirige el tráfico a un clúster de Amazon ECS.
- Una función de Lambda que lee una tabla de DynamoDB.
- Una cola de Amazon SQS que envía mensajes a una función de Lambda.

Topología no válida (no se puede ejecutar la evaluación)

Una topología con solo recursos aislados y sin relaciones de flujo de datos entre ellos no es válida. Por ejemplo, un servicio que descubre un único bucket de Amazon S3 o varias instancias de Amazon EC2 desconectadas no tiene ningún flujo de datos para analizarlo en la evaluación.

Para iniciar una evaluación del modo de error (consola)

1. Navegue hasta su servicio.
2. Seleccione la guía del modo de error y añada cualquier afirmación sobre su servicio. Para obtener más información, consulte Guía del modo de error.
3. Seleccione Ejecutar la evaluación del modo de fallo.
4. Espere a que finalice la evaluación (normalmente de 5 a 15 minutos).

Para iniciar una evaluación en modo de error (CLI)

```
aws resiliencehubv2 start-failure-mode-assessment \
  --service-arn "arn:aws:resiliencehub:us-east-1:123456789012:service/checkout:abc123"
```

Para comprobar el estado de la evaluación

```
aws resiliencehubv2 list-failure-mode-assessments \
  --service-arn "arn:aws:resiliencehub:..."
```

Los valores de estado progresan de la siguiente manera: `PENDINGIN_PROGRESS`, luego, `SUCCESS` o`FAILED`.

Durante la evaluación, Next Generation Resilience Hub ejecuta el descubrimiento de recursos en segundo plano:

1. La próxima generación de Resilience Hub asume su función de invocador.
2. Lee los recursos de las fuentes de entrada configuradas (etiquetasCloudFormation, Terraform o Amazon EKS).
3. Identifica las relaciones entre padres e hijos (por ejemplo, entre el grupo de Auto Scaling y las instancias de Amazon EC2).
4. Resilience Hub crea una topología de su servicio.
5. Crea una topología que muestra el flujo y la contención de los datos.

Una vez completada la topología, puede verla en la consola:

- Vista gráfica: mapa visual de los recursos y las conexiones.
- Vista de tabla: lista de todos los recursos descubiertos con metadatos.
- Exportación a JSON: descargue la topología completa para un análisis externo.

Visualización de los hallazgos y recomendaciones del modo de falla

Una vez finalizada la evaluación, revise los hallazgos y las recomendaciones:

Para ver los hallazgos (consola)

1. Navegue hasta su servicio y elija la pestaña Evaluación.
2. Revise los hallazgos ordenados por gravedad.
3. Elige cualquier resultado para ver el razonamiento detallado y las recomendaciones.

Para enumerar los hallazgos (CLI)

```
aws resiliencehubv2 list-failure-mode-findings \
  --service-arn "arn:aws:resiliencehub:..."
```

Cada hallazgo incluye la siguiente información:

Campo	Description (Descripción)	Ejemplo
Nombre de búsqueda	Breve descripción del modo de fallo	«La base de datos de Single-AZ Amazon Relational Database Service crea un punto único de error crítico»
Description (Descripción)	Explicación detallada del problema	Párrafo que explica por qué esto es un riesgo
Razonamiento	Por qué esto es importante para su arquitectura específica	Architecture-specific contexto del hallazgo
Gravedad	Nivel de impacto	Ninguna, media, baja
Categoría de error	Tipo de fallo	Destino compartido, carga excesiva, latencia excesiva, errores de configuración y errores, puntos únicos de error

Campo	Description (Descripción)	Ejemplo
Componente de política	¿A qué requisitos de política se refiere esto	Multi-AZ recuperación ante desastres
Recomendaciones	Mitigaciones sugeridas	Consulte la tabla de recomendaciones que aparece a continuación

Cada recomendación incluye una recomendación de mitigación, observabilidad y prueba:

- Mitigación: un cambio de infraestructura o configuración para abordar el modo de falla.
- Observabilidad: monitorear o alertar las mejoras para detectar el modo de falla.
- Pruebas: una prueba para validar que la mitigación funciona según lo esperado.

Gestionar los hallazgos

Para cada conclusión, puedes razonar detalladamente sobre el modo de fallo, implementar la solución recomendada, marcar la conclusión como irrelevante si no se aplica a tu caso de uso o usar la gravedad para priorizar lo que debes abordar primero.

Los hallazgos pueden tener los siguientes estados:

- Abierto: requiere atención.
- Resuelto: el problema se ha solucionado. La siguiente evaluación verifica la solución.
- Irrelevante: suprimida por el cliente. El resultado permanece oculto en futuras evaluaciones.

Para marcar un resultado como resuelto (CLI)

```
aws resiliencehubv2 update-failure-mode-finding \
  --service-arn "arn:aws:resiliencehub:..." \
  --finding-id "finding-123" \
  --status "RESOLVED"
```

Para marcar un resultado como irrelevante (CLI)

```
aws resiliencehubv2 update-failure-mode-finding \
  --service-arn "arn:aws:resiliencehub:..." \
```

```
  --finding-id "finding-123" \
  --status "IRRELEVANT"
```

Historial y tendencias de la evaluación

La próxima generación de Resilience Hub conserva el historial de evaluaciones durante 2 años, lo que le permite:

- Haz un seguimiento de cómo tu postura resiliente mejora con el tiempo.
- Vea qué hallazgos se han resuelto y cuáles permanecen abiertos.
- Identifique los problemas recurrentes en las evaluaciones.
- Genere informes de cumplimiento que muestren las tendencias de mejora.

Para ver el historial de evaluaciones (CLI)

```
aws resiliencehubv2 list-failure-mode-assessments \
  --service-arn "arn:aws:resiliencehub:..."
```

Precios

Cada servicio incluye 2 evaluaciones de modos de fallo al mes en la tarifa básica de 15 dólares por servicio y mes para los servicios con un máximo de 150 recursos.

En el caso de los servicios con más de 150 recursos, cada una de las 2 evaluaciones incluidas se cobra a 0,10 USD por recurso por encima del límite de 150 recursos. Las cuotas adicionales que superen las 2 incluidas al mes se cobran a la misma tarifa por recurso, con un mínimo de 50 recursos por evaluación.

Tamaño del servicio	Coste mensual de 2 evaluaciones
100 recursos	15$ (incluidos)
150 recursos	15$ (incluidos)
200 recursos	15$ + (50 x 0,10$ x 2) = 25$
500 recursos	15$ + (350 x 0,10$ x 2) = 85$

Pruebas de resiliencia

En la próxima generación de Resilience Hub, se AWS recomiendan cuatro plantillas de prueba, que se han desarrollado para ayudarlo a validar el funcionamiento de sus servicios y a recuperarse según lo previsto en caso de fallo. Tres pruebas se ajustan a los límites de aislamiento de AWS fallos (zonas de disponibilidad y regiones) y proporcionan una forma coherente de probar la capacidad de recuperación de los servicios ante fallos que se sitúan dentro de esos límites. Hay una prueba adicional que le ayuda a validar que sus servicios pueden recuperarse cuando se producen fallos en sus dependencias. Cada prueba se basa en AWS Fault Injection Service (AWS FIS), que realiza la inyección de errores subyacente. La próxima generación de Resilience Hub amplía la prueba a los recursos de su servicio y evalúa los resultados en función de los criterios de éxito que haya elegido para determinar si se aprueba o no. Las pruebas de resiliencia se realizan a nivel de servicio.

Temas

Cómo funcionan las pruebas de resiliencia

Las pruebas de resiliencia utilizan tres conceptos básicos:

- Plantilla de prueba: una prueba recomendada y preconfigurada que define qué capacidad de resiliencia se debe validar. Una plantilla de prueba especifica las acciones que se deben realizar y declara los parámetros que acepta.
- Prueba: prueba que se crea configurando una plantilla de prueba recomendada para el servicio, que incluye los criterios de éxito, las condiciones de parada y otros ajustes. Cada servicio tiene una prueba por plantilla. Por ejemplo, una zona de disponibilidad: prueba de recuperación configurada para tu servicio de pago con un RTO (objetivo de tiempo de recuperación) de 30 minutos.
- Ejecución de la prueba: ejecución única de una prueba. Cada ejecución de prueba abarca los recursos actuales de su servicio y produce un resultado positivo o negativo, junto con los resultados y un informe. Puede realizar varias ejecuciones de la misma prueba. Por ejemplo,

ejecutar tu zona de disponibilidad: haz una prueba de recuperación mensual para comprobar la recuperación dentro de tu RTO de 30 minutos.

Cuando realizas una prueba de resiliencia, la próxima generación de Resilience Hub realiza lo siguiente:

1. Alcance de la prueba: incluye automáticamente todos los recursos descubiertos en tu servicio que se aplican a la prueba.
2. Configura la prueba: configura la prueba con la configuración que usted proporcione, incluidas las alarmas de éxito, las condiciones de parada y los destinos de los registros.
3. Inyecta errores: ejecuta AWS FIS experimentos para inyectar los errores definidos por la prueba durante el período de tiempo especificado.
4. Evalúa los resultados: determina si el resultado es aprobado o no en función de si el servicio cumplió con los criterios de éxito durante la prueba. Puedes revisar los resultados de las pruebas en la consola o mediante programación. Se genera un informe de prueba para cada ejecución.

Las pruebas de resiliencia se cobran en función de los precios por AWS FIS minuto de acción. Consulte Precios de AWS Fault Injection Service para obtener más información.

Configuración de una prueba

Al crear una prueba a partir de una plantilla, se configuran los siguientes ajustes. Los ajustes se guardan y se reutilizan para futuras ejecuciones; puede editarlos en cualquier momento.

Duración de la prueba

El tiempo durante el que se ejecutan las acciones de prueba. En el caso de las pruebas de recuperación (zona de disponibilidad Multi-Region: recuperación y: recuperación), la duración predeterminada es el RTO más 30 minutos, lo que da tiempo al servicio para recuperarse y confirmar que se mantiene. En el caso de las pruebas sostenidas, el valor predeterminado es de 30 minutos para la validación de dependencias o de 3 horas para el Multi-Region aislamiento. Estos valores predeterminados se aplican en la consola; al usar la API, se indica la duración de forma explícita.

Alcance de la falla

Define dónde se inyectan las fallas: la zona de disponibilidad o las regiones a las que se deben afectar. Cada prueba tiene sus propios parámetros. Para obtener más información, consulte Pruebas disponibles.

Acciones de prueba

Read-only. Definido por la plantilla de prueba. Muestra las acciones de error y sus tipos de recursos objetivo. Si ningún recurso coincide con el tipo de objetivo de una acción, esa acción se omite.

Dependencias a bloquear

Dependencias que se deben bloquear durante la prueba. Seleccione una de las dependencias descubiertas (si la detección de dependencias está habilitada) o introduzca las dependencias manualmente por nombre de dominio DNS. Obligatorio para algunas pruebas, opcional para otras. Para conocer los valores predeterminados y los requisitos, consultePruebas disponibles.

Alarmas de prueba

Alarmas de éxito (obligatorias): CloudWatch alarmas que determinan que los criterios de éxito se aprueben o no. Se necesita una como mínimo. Si seleccionas varias, todas deben pasar para que la prueba pase. Elige alarmas que midan el estado general de tu servicio.

Cómo pasa la prueba:

- Zona de disponibilidad: recuperación: todas las alarmas de éxito deben volver a su OK estado dentro de su Multi-AZ RTO y permanecer allí hasta que finalicen las acciones de prueba.
- Multi-Region: recuperación: todas las alarmas de éxito deben volver a su OK estado actual en su Multi-Region RTO y permanecer allí hasta que finalicen las acciones de prueba.
- Validación de dependencias: todas las alarmas de éxito permanecen en OK estado hasta que finalicen las acciones de prueba.
- Multi-Region: aislamiento: todas las alarmas de éxito permanecen en OK estado hasta que finalicen las acciones de prueba.

Alarmas adicionales (opcionales): solo para la observabilidad. Se muestran en los resultados y en el informe, pero no afectan al resultado aprobado o rechazado.

Plan de cambio de región (Multi-Regionsolo para recuperación, opcional)

Incluir un plan de cambio regional de AWS Application Recovery Controller (ARC) permite a la próxima generación de Resilience Hub incluir el cronograma de conmutación por error en los

resultados y el informe de las pruebas. Opcional; déjelo vacío si utiliza la conmutación por error manual o una automatización personalizada.

Ajustes adicionales (opcional)

Condiciones de parada

CloudWatch alarmas que detienen automáticamente la prueba si superan su umbral. Utilice las condiciones de parada como barreras para proteger sus cargas de trabajo durante las pruebas. Por ejemplo, cree una CloudWatch alarma en una métrica empresarial crítica (como la latencia o la tasa de errores) que detenga la prueba si supera un umbral inaceptable. Las alarmas de estado de parada deben estar en la cuenta en la que se ejecuta la prueba y en la región en la que se inyectan las fallas. Para obtener más información, consulte Condiciones de parada para AWS FIS.

Informes

Se genera automáticamente un informe después de cada ejecución de prueba cuando se configura el destino del informe (el bucket de Amazon S3) en su servicio. Los informes incluyen la configuración de la prueba, el estado de la alarma, el cronograma y los resultados de aprobación o error. Los informes de prueba se incluyen sin costo adicional cuando se utiliza la próxima generación de pruebas de resiliencia de Resilience Hub. Para configurar el destino de un informe, consulta la configuración de informes de tu servicio.

Registros

Envíe registros de prueba detallados a Amazon S3, CloudWatch Logs o ambos. Los registros capturan los eventos con fecha y hora, incluidos el inicio y el final de la acción, la resolución de los objetivos y los errores. Utilice los registros para depurar las pruebas fallidas o para comprender la secuencia en la que se producen los errores. El registro requiere permisos adicionales en su función de ejecución de pruebas. Para obtener más información, consulte Registro de experimentos para AWS FIS.

Permisos de prueba

Se requiere una función de ejecución de IAM. Los permisos varían según el tipo de prueba, las acciones fallidas y las opciones seleccionadas. Para las pruebas con varias cuentas, usa el rol del mismo nombre en cada cuenta. Para obtener más información, consulte Funciones de ejecución de IAM para las pruebas de resiliencia.

Pruebas disponibles

La próxima generación de Resilience Hub proporciona las siguientes plantillas de prueba preconfiguradas:

- Zona de disponibilidad: recuperación: valide que su servicio pueda detectar una alteración de la zona de disponibilidad y recuperarse de ella.
- Validación de dependencias: valide la forma en que su servicio responde cuando sus dependencias dentro de la región se ven afectadas.
- Multi-Region: aislamiento: valida que tu servicio pueda funcionar independientemente de una región cuando la conectividad a otra región no esté disponible.
- Multi-Region: recuperación: valida que tu servicio puede recuperarse y atender a los clientes de otra región dentro de tus objetivos de recuperación cuando una región esté en problemas.

Cada plantilla de prueba declara los parámetros que acepta, incluido si cada parámetro es obligatorio y los valores predeterminados.

Para enumerar las plantillas de prueba (CLI)

```
aws resiliencehubv2 list-test-templates --region region
```

Para ver una plantilla de prueba (CLI)

`get-test-template`Utilícela para ver la definición completa de una plantilla de prueba. La respuesta incluye lo siguiente:

- acciones: las operaciones que realiza la prueba, cada una dirigida a un tipo de recurso específico.
- parámetros: las entradas que proporciona al crear una prueba a partir de la plantilla.

Cada acción incluye lo siguiente:

- actionID: un identificador único para la acción.
- descripción: una descripción de lo que hace la acción.
- ResourceType: el tipo de recurso al que se dirige la acción.

Cada parámetro declara lo siguiente:

- nombre: el nombre del parámetro que proporciona al crear una prueba.
- descripción: una descripción de lo que controla el parámetro.
- tipo: el tipo de valor:`STRING`,`STRING_LIST`, o`INTEGER`.
- obligatorio: si debe proporcionar un valor para el parámetro.
- DefaultValue: el valor que se utiliza cuando no se proporciona ninguno. Se aplica a los parámetros opcionales.
- maxValues: el número máximo de valores que puede proporcionar para el parámetro.

```
aws resiliencehubv2 get-test-template \
  --test-template-arn "arn:aws:resiliencehub:region:aws:test-template/aws-az-
recovery:rtaz001" \
  --region region
```

Proporcione valores para estos parámetros con la `--parameters` opción al crear una prueba. Para ver un ejemplo de cómo crear una prueba, consulteCómo empezar con Resilience Hub de próxima generación.

Temas

- Zona de disponibilidad: recuperación
- Validación de dependencias
- Multi-Region: aislamiento
- Multi-Region: recuperación

Zona de disponibilidad: recuperación

La prueba de recuperación de la zona de disponibilidad inyecta los síntomas de una interrupción del suministro eléctrico en una única zona de disponibilidad, lo que afecta a los recursos informáticos, de redes, de almacenamiento y de bases de datos de esa zona de disponibilidad. Puede ayudarlo a comprobar que su servicio detecta la zona de disponibilidad defectuosa, continúa funcionando en las zonas de disponibilidad en buen estado y vuelve a un estado correcto dentro del RTO definido. Además, esta prueba puede ayudarte a descubrir las dependencias de una sola zona de disponibilidad que quizás desconozcas.

¿Qué hace que esta prueba sea única

- Se dirige a la única zona de disponibilidad que usted elija, centrándose en la resiliencia zonal e interna de la región.
- Se trata de una prueba de recuperación: su servicio debe recuperarse dentro de su RTO.

¿Cómo pasar esta prueba

- Se trata de una prueba de recuperación. La cuenta regresiva del RTO comienza cuando comienzan las acciones de prueba. La prueba pasa si todas las alarmas de éxito vuelven al OK estado de su RTO y permanecen allí hasta que finalicen las acciones de prueba.

Cosas en las que pensar

- Elija alarmas de éxito que midan el estado de los servicios regionales (por ejemplo, la tasa de error regional o la latencia). Evite las alarmas por zona de disponibilidad, ya que se espera que la zona de disponibilidad dañada no esté en buen estado.
- Es más significativo para las arquitecturas multizona de disponibilidad, en las que el tráfico puede cambiar a zonas de disponibilidad en buen estado. También se puede ejecutar en servicios Single-AZ.
- Si tiene activado el cambio automático zonal del AWS Application Recovery Controller (ARC) en sus recursos, los ejercicios de prueba son los que cambian automáticamente. Si el cambio automático no está configurado, se omite la acción.

Parámetros clave de la prueba

- Zona de disponibilidad: elija la zona de disponibilidad que desee modificar. Seleccione una zona de disponibilidad en la que su servicio tenga recursos desplegados.
- Duración: el tiempo durante el que se ejecutan las acciones de prueba. Después, se necesitan unos minutos más para recopilar los resultados finales antes de que finalice la prueba. El RTO se establece de forma predeterminada según su política de servicio, más 30 minutos cuando crea la prueba por primera vez. Configúrala durante más tiempo que tu RTO para validar que la recuperación es sostenida.

Acciones

Esta prueba ejecuta las siguientes AWS FIS acciones para afectar la zona de disponibilidad que seleccione. Si su servicio no tiene recursos que coincidan con el tipo de objetivo de una acción, esa acción se omite. Para obtener más información sobre cada acción, consulta la referencia de AWS FIS acciones.

Action	Description (Descripción)
`aws:ec2:stop-instances`	Detiene las instancias en la zona de disponibilidad alterada mientras dure.
`aws:ec2:api-insufficient-instance-capacity-error`	Bloquea el lanzamiento de nuevas instancias en la zona de disponibilidad dañada.
`aws:ec2:asg-insufficient-instance-capacity-error`	Impide que Auto Scaling aprovisione capacidad en la Arizona.
`aws:network:disrupt-connectivity`	Bloquea el tráfico que entra y sale de la subred y bloquea el acceso a los buzones de directorio One Zone de Amazon S3 Express, si los hay.
`aws:rds:failover-db-cluster`	Conmuta el clúster por error si el escritor se encuentra en la AZ dañada.
`aws:elasticache:replicationgroup-interrupt-az-power`	Termina los nodos de caché en la zona de disponibilidad dañada sin reemplazarlos mientras dure.
`aws:arc:start-zonal-autoshift`	Cambia el tráfico a zonas de disponibilidad en buen estado.

Para ver los parámetros de esta prueba y sus valores predeterminados, utilice`get-test-template`.

Validación de dependencias

La prueba de validación de dependencias bloquea las dependencias dentro de la región para ver cómo se comporta tu servicio cuando no están disponibles. Puede ayudarte a comprobar que

tu servicio se mantiene en buen estado cuando las dependencias blandas están alteradas y las dependencias superficiales que quizás no sabías que eran difíciles. También puedes incluir las dependencias físicas conocidas para entender su impacto.

¿Qué hace que esta prueba sea única

- Se centra en las fallas de dependencia dentro de la región.
- Tú eliges a qué dependencias apuntar.
- Si ha habilitado la detección de dependencias en la próxima generación de Resilience Hub, puede elegir entre las dependencias descubiertas. De lo contrario, puede introducir los puntos finales de DNS manualmente.

¿Cómo pasar esta prueba

- Se trata de una prueba sostenida. La prueba pasa si todas las alarmas de éxito permanecen en OK estado hasta que finalicen las acciones de prueba. Utilícela para comprobar que las dependencias flexibles son realmente débiles; si las alarmas no funcionan correctamente, la dependencia puede resultar difícil.

Cosas en las que pensar

- Empieza con una sola dependencia blanda y aumenta: valida una a la vez antes de bloquear muchas.
- Si incluyes una dependencia física, prepárate para que se produzca una violación de las alarmas y que la prueba falle: las dependencias sólidas tienen un impacto significativo cuando se bloquean. Esto es útil para confirmar que una dependencia es realmente sólida.
- Elija alarmas de éxito que midan el estado general del servicio, no el estado de la dependencia en sí.
- Asegúrese de que sus dependencias se utilizan activamente durante la prueba (el tráfico fluye hacia ellas); esto valida que el bloqueo está surtiendo efecto. Considera agregar alarmas o métricas que rastreen el uso de las dependencias (por ejemplo, el recuento de solicitudes o los errores de conexión) para verificar que la dependencia se esté ejerciendo durante la prueba.
- Las dependencias deben ser puntos finales de DNS que se puedan resolver; si el DNS no se resuelve, la acción fallará.

- El bloqueo de las dependencias que provocan errores en las comprobaciones de estado puede provocar la sustitución del procesamiento (por ejemplo, las tareas de Amazon ECS). La acción de pérdida de paquetes no vuelve a aplicarse a las tareas de reemplazo y puede declararse fallida.

Parámetros clave de la prueba

- Duración: el tiempo durante el que se ejecutan las acciones de prueba. Después, se necesitan unos minutos más para recopilar los resultados finales antes de que finalice la prueba. El valor predeterminado es de 30 minutos cuando se crea la prueba por primera vez.
- Dependencias que se deben bloquear: de forma predeterminada, se preselecciona la dependencia blanda descubierta con el mayor volumen de consultas. Si no se ha clasificado ninguna dependencia como simplificada, no se selecciona ninguna. Puede ajustarlo para que se dirija a dependencias individuales o a grupos específicos, o bien agregar dependencias manualmente por nombre de dominio DNS. Las dependencias adicionales que se agreguen aquí solo se usan para esta prueba y no se guardarán en el momento de la detección de dependencias del servicio. Estos valores predeterminados se aplican en la consola; al usar la API, se proporcionan las dependencias de forma explícita.

Acciones

Esta prueba ejecuta las siguientes AWS FIS acciones para dirigir el tráfico a las dependencias que selecciones. Las acciones conllevan una pérdida de paquetes del 100% en las instancias de Amazon EC2, las tareas de Amazon ECS (Amazon EC2 y Fargate) y los pods de Amazon EKS (Amazon EC2). Si su servicio no tiene recursos que coincidan con el tipo de objetivo de una acción, esa acción se omite.

> **Note**
>
> Las acciones que se utilizan para bloquear las dependencias requieren una configuración adicional: SSM Agent instalado en las instancias de Amazon EC2, un contenedor de SSM Agent en la definición de tareas de Amazon ECS o una cuenta de servicio de Kubernetes para los pods de Amazon EKS.

Action	Description (Descripción)
`aws:ssm:send-command`	Transfiere el tráfico de las instancias de Amazon EC2 a las dependencias seleccionadas.
`aws:ecs:task-network-packet-loss`	Transfiere el tráfico de las tareas de Amazon ECS a las dependencias seleccionadas.
`aws:eks:pod-network-packet-loss`	Transfiere el tráfico de los pods de Amazon EKS a las dependencias seleccionadas.

Para ver los parámetros de esta prueba y sus valores predeterminados, utilice`get-test-template`.

Multi-Region: aislamiento

La Multi-Region prueba de aislamiento bloquea la conectividad entre dos regiones, incluido el tráfico de red, la replicación de datos entre regiones y las dependencias seleccionadas. Puede ayudarlo a comprobar que su servicio funciona de forma independiente cuando no se puede acceder a los recursos de otra región y a descubrir las dependencias interregionales que podrían afectar a la disponibilidad.

¿Qué hace que esta prueba sea única

- Se centra en el aislamiento de la región (pérdida de conectividad entre regiones) en lugar de en la recuperación a otra región.
- Bloquea el tráfico de red, detiene la replicación entre regiones (Amazon S3, DynamoDB, MemoryDB) y, de forma opcional, bloquea las dependencias entre las dos regiones.
- Valida que la región pueda funcionar por sí sola.

¿Cómo pasar esta prueba

- Se trata de una prueba sostenida. La prueba pasa si todas las alarmas de éxito permanecen en `OK` estado hasta que finalicen las acciones de prueba.

Cosas en las que pensar

- Elija alarmas de éxito que midan el estado de salud de la región aislada y valide que siga atendiendo el tráfico de forma independiente.
- Esta prueba se aplica tanto a las arquitecturas como a active/active las active/passive arquitecturas.
- Un caso de uso clave: valide que su región de recuperación pueda funcionar de forma independiente. Por ejemplo, si la principal es `us-east-1` y la secundaria es`us-west-2`, utilízala para validar que `us-west-2` funciona de forma independiente cuando está aislada de `us-east-1` ella.
- Esta prueba también es un buen paso previo a la recuperación Multi-Region: valida la independencia antes de probar la conmutación por error total. La prueba puede ayudar a descubrir las dependencias entre regiones que son críticas.
- Asegúrate de que tus dependencias se utilizan activamente durante la prueba (el tráfico fluye hacia ellas); esto valida que el bloqueo esté surtiendo efecto. Considera agregar alarmas o métricas que rastreen el uso de las dependencias (por ejemplo, el recuento de solicitudes o los errores de conexión) para verificar que la dependencia se esté ejerciendo durante la prueba.
- Las dependencias deben ser puntos finales de DNS que se puedan resolver.
- El bloqueo de las dependencias que provocan errores en las comprobaciones de estado puede provocar la sustitución del procesamiento (por ejemplo, las tareas de Amazon ECS). La acción de pérdida de paquetes no vuelve a aplicarse a las tareas de reemplazo y puede declararse fallida.

Parámetros clave de la prueba

- Región aislada: la región en la que está probando para un funcionamiento independiente.
- Región de destino: la región que se está bloqueando (se ha interrumpido la conectividad con esta región).
- Duración: el tiempo durante el que se ejecutan las acciones de prueba. Después, se necesitan unos minutos más para recopilar los resultados finales antes de que finalice la prueba. El valor predeterminado es de 3 horas cuando se crea la prueba por primera vez.
- Dependencias que bloquear (opcional): si la detección de dependencias está habilitada, la lista muestra las dependencias desde la región aislada hasta la región de destino. Puede seleccionarlas de esta lista o agregarlas manualmente por nombre de dominio DNS. No se selecciona ninguna dependencia de forma predeterminada. Otras acciones de esta prueba (conectividad de red, pausa de la replicación) se ejecutan de todos modos. Las dependencias

adicionales que se agreguen aquí solo se usan para esta prueba y no se guardarán en el momento de la detección de dependencias del servicio. Estos valores predeterminados se aplican en la consola; al usar la API, se proporcionan las dependencias de forma explícita.

Acciones

Esta prueba ejecuta las siguientes AWS FIS acciones para dirigir el tráfico a las dependencias que selecciones. Las acciones conllevan una pérdida de paquetes del 100% en las instancias de Amazon EC2, las tareas de Amazon ECS (Amazon EC2 y Fargate) y los pods de Amazon EKS (Amazon EC2). Si su servicio no tiene recursos que coincidan con el tipo de objetivo de una acción, esa acción se omite.

> **Note**
>
> Las acciones que se utilizan para bloquear las dependencias requieren una configuración adicional: SSM Agent instalado en las instancias de Amazon EC2, un contenedor de SSM Agent en la definición de tareas de Amazon ECS o una cuenta de servicio de Kubernetes para los pods de Amazon EKS.

Action	Description (Descripción)
`aws:network:transit-gateway-disrupt-cross-region-connectivity`	Bloquea el tráfico entre regiones a través de Transit Gateway y enlaza con la región de destino.
`aws:network:route-table-disrupt-cross-region-connectivity`	Bloquea el tráfico interregional desde las subredes a la región de destino.
`aws:network:disrupt-vpc-endpoint`	Bloquea el tráfico de los puntos de enlace de VPC interregionales a la región de destino.
`aws:s3:bucket-pause-replication`	Detiene la replicación interregional de Amazon S3 en la región de destino.
`aws:dynamodb:global-table-pause-replication`	Detiene la replicación de la tabla global de DynamoDB.

Action	Description (Descripción)
`aws:memorydb:multi-region-cluster-pause-replication`	Detiene la replicación de clústeres multirregionales de MemoryDB.
`aws:ssm:send-command`	Transfiere el tráfico de las instancias de Amazon EC2 a las dependencias seleccionadas.
`aws:ecs:task-network-packet-loss`	Transfiere el tráfico de las tareas de Amazon ECS a las dependencias seleccionadas.
`aws:eks:pod-network-packet-loss`	Transfiere el tráfico de los pods de Amazon EKS a las dependencias seleccionadas.

Para ver los parámetros de esta prueba y sus valores predeterminados, utilice`get-test-template`.

Multi-Region: recuperación

La Multi-Region prueba de recuperación introduce errores en las dependencias de una región para validar que su servicio puede recuperarse y atender a los clientes de una región de recuperación que esté dentro de sus objetivos de recuperación. Esta prueba se aplica a ambas active/active active/passive arquitecturas. Por ejemplo, puede iniciar el procedimiento de recuperación y confirmar que el servicio se recupera dentro del objetivo de tiempo de recuperación (RTO) definido en la región de recuperación.

¿Qué hace que esta prueba sea única

- Valida la recuperación en otra región en función de sus objetivos de recuperación, no solo de la resiliencia dentro de la región.
- Tú eliges qué dependencias quieres reducir en la región principal, de modo que puedas practicar la detección y la recuperación.
- La prueba se integra con el conmutador regional ARC para que pueda hacer un seguimiento de los detalles de ejecución del plan en el informe de prueba.

¿Cómo pasar esta prueba

- Esta es una prueba de recuperación. La cuenta regresiva del RTO comienza cuando comienzan las acciones de prueba. La prueba pasa si todas las alarmas de éxito vuelven al 0K estado de su Multi-Region RTO y permanecen allí hasta que finalicen las acciones de prueba. Su servicio debe tener una política de resiliencia con un Multi-Region RTO definido.

Cosas en las que pensar

- Elija dependencias en la región afectada que sean lo suficientemente importantes como para iniciar el procedimiento de recuperación. Elija las dependencias sólidas o los puntos de enlace de DNS que, si se bloquean, perjudicarían significativamente a esa región.
- La prueba detecta errores en la región afectada: la acción de recuperación la realizas tú mismo (por ejemplo, activando failover/ARC el plan de cambio de región). La prueba comprueba si tu región de recuperación se encuentra en buen estado dentro de tu RTO mediante la evaluación del estado de alarma.
- Elija alarmas de éxito en la región de recuperación que validen su tráfico de servicio, o utilice alarmas global/application de nivel similar que reflejen la experiencia general del cliente.
- Considere establecer una duración superior a la de su RTO para validar que la recuperación se mantiene.
- Asegúrate de que tus dependencias se usen de forma activa durante la prueba (el tráfico fluye hacia ellas); esto valida que el bloqueo esté surtiendo efecto. Considera agregar alarmas o métricas que rastreen el uso de las dependencias (por ejemplo, el recuento de solicitudes o los errores de conexión) para verificar que la dependencia se esté ejerciendo durante la prueba.
- Las dependencias deben ser puntos finales de DNS que se puedan resolver.
- El bloqueo de las dependencias que provocan errores en las comprobaciones de estado puede provocar la sustitución del procesamiento (por ejemplo, las tareas de Amazon ECS). La acción de pérdida de paquetes no vuelve a aplicarse a las tareas de reemplazo y puede declararse fallida.

Parámetros clave de la prueba

- Región deteriorada: la región en la que se inyectan las fallas.
- Región de recuperación: la región en la que espera que se recupere su servicio.
- Duración: el tiempo durante el que se ejecutan las acciones de prueba. Después, se necesitan unos minutos más para recopilar los resultados finales antes de que finalice la prueba. El Multi-

Region RTO se establece de forma predeterminada según su política de servicio, más 30 minutos cuando crea la prueba por primera vez.

- Dependencias que se deben bloquear: elija las dependencias que, de bloquearse, perjudicarían considerablemente su servicio y ayudarían a validar la conmutación por error a otra región. De forma predeterminada, se preselecciona la dependencia física descubierta con el mayor volumen de consultas. Si no se ha clasificado ninguna dependencia como rígida, no se selecciona ninguna. Puede ajustar o agregar manualmente las dependencias por nombre de dominio DNS. Las dependencias adicionales que se agreguen aquí solo se usan para esta prueba y no se guardarán en el momento de la detección de dependencias del servicio. Estos valores predeterminados se aplican en la consola; al usar la API, se proporcionan las dependencias de forma explícita.
- Plan de cambio de región (opcional): adjuntar un plan de cambio de región ARC permite a la próxima generación de Resilience Hub incluir el cronograma real de conmutación por error en los resultados y el informe de las pruebas. Si utilizas la conmutación por error manual o una automatización personalizada, deja este campo vacío.

Acciones

Esta prueba ejecuta las siguientes AWS FIS acciones para dirigir el tráfico a las dependencias que selecciones. Las acciones conllevan una pérdida de paquetes del 100% en las instancias de Amazon EC2, las tareas de Amazon ECS (Amazon EC2 y Fargate) y los pods de Amazon EKS (Amazon EC2). Si su servicio no tiene recursos que coincidan con el tipo de objetivo de una acción, esa acción se omite.

> **Note**
>
> Las acciones que se utilizan para bloquear las dependencias requieren una configuración adicional: SSM Agent instalado en las instancias de Amazon EC2, un contenedor de SSM Agent en la definición de tareas de Amazon ECS o una cuenta de servicio de Kubernetes para los pods de Amazon EKS.

Action	Description (Descripción)
`aws:ssm:send-command`	Transfiere el tráfico de las instancias de Amazon EC2 a las dependencias seleccionadas.

Action	Description (Descripción)
`aws:ecs:task-network-packet-loss`	Transfiere el tráfico de las tareas de Amazon ECS a las dependencias seleccionadas.
`aws:eks:pod-network-packet-loss`	Transfiere el tráfico de los pods de Amazon EKS a las dependencias seleccionadas.

Para ver los parámetros de esta prueba y sus valores predeterminados, utilice`get-test-template`.

Ejecuta la prueba e informa

Ejecuciones de prueba

Cada vez que se inicia una prueba, se crea una ejecución de prueba. Puedes ver las pruebas realizadas en varios lugares:

- Nivel de servicio: vaya a su servicio → pestaña de pruebas → ejecuciones de prueba en la parte inferior. Muestra todas las ejecuciones de ese servicio.
- Página de pruebas (navegación de la izquierda): muestra las ejecuciones de prueba en todos sus servicios. Filtra por servicio, nombre de la prueba o estado.
- Panel de control: el gráfico de resultados de las pruebas muestra pass/fail la distribución en toda la organización.

Cada ejecución de prueba incluye el estado de la prueba, la información sobre el tiempo, los resultados de las alarmas de éxito, un cronograma de acciones y cualquier dependencia bloqueada o de los eventos de registro capturados durante la ejecución. Puedes profundizar en la ejecución de una prueba para ver todos los detalles, como el identificador del AWS FIS experimento y los resultados de las acciones individuales.

Puedes realizar varias ejecuciones de la misma prueba. Por ejemplo, realizar una prueba de recuperación mensual en la zona de disponibilidad para hacer un seguimiento de las mejoras de resiliencia a lo largo del tiempo. También puede enumerar las ejecuciones de prueba y recuperar los detalles de las mismas mediante programación mediante las operaciones de la `GetTestRun` API `ListTestRuns` y. Consulte la Referencia de la API.

Informes de pruebas

Un informe de prueba se genera automáticamente una vez finalizada cada ejecución de prueba, si el destino del informe (el bucket de Amazon S3) está configurado en su servicio. Si no se configura ningún destino, no se genera ningún informe.

Los informes capturan la configuración de la prueba, los resultados de los criterios de éxito, un cronograma visual de la respuesta del servicio y el pass/fail resultado general.

Dónde encontrar los informes:

- Página de informes (barra de navegación de la izquierda): muestra todos los informes (de evaluación y prueba) de sus servicios.
- Detalles de la prueba: descárguelos directamente desde la página de detalles de la ejecución de la prueba.

Los informes de las pruebas de resiliencia de Resilience Hub se incluyen sin coste adicional.

También puede recuperar los resultados de la ejecución de las pruebas e informar los metadatos mediante programación mediante las operaciones de la `ListTestRunSources` API `GetTestRun` y. Consulte la Referencia de la API.

Funciones de ejecución de IAM para las pruebas de resiliencia

Para ejecutar una prueba de resiliencia, debes proporcionar una función de ejecución de IAM que AWS Fault Injection Service (AWS FIS) asume que inyecta errores en tus recursos. Este rol se establece en la prueba y Resilience Hub lo usa cuando se inicia una ejecución de prueba.

Al crear una prueba en la consola, Resilience Hub puede crear este rol automáticamente. Use las políticas de este tema cuando cree o personalice el rol usted mismo, por ejemplo, con la AWS CLI.

Los permisos que necesita un rol dependen de la plantilla de prueba, ya que cada plantilla ejecuta un conjunto diferente de AWS FIS acciones. En este tema se proporciona una política de permisos para cada una de las cuatro plantillas de prueba. Para obtener más información sobre las plantillas, consultePruebas disponibles.

Resilience Hub admite dos modelos de cuentas:

- Single-account— La prueba se centra en los recursos de la misma cuenta en la que se ejecuta el experimento. Creas un rol de ejecución.

- Multi-account— La prueba se dirige a los recursos de otras cuentas. Creas un rol de orquestador en la cuenta en la que se ejecuta el experimento y un rol objetivo en cada cuenta que contenga los recursos específicos.

Le recomendamos que siga la práctica de seguridad estándar para conceder privilegios mínimos. Las siguientes políticas limitan cada permiso al tipo de recurso al que va dirigida la acción. Las pruebas de resiliencia no pueden limitar los permisos a los ID de recursos individuales, porque la próxima generación de Resilience Hub resuelve los recursos objetivo en tiempo de ejecución.

Temas

Single-account rol de ejecución

Para una prueba de una sola cuenta, cree un rol de ejecución con una política de confianza que AWS FIS permita asumirlo y una política de permisos para la plantilla de prueba que utilice.

Política de confianza

El rol de ejecución debe confiar en el AWS FIS servicio. La política de confianza es la misma para todas las plantillas de prueba. `aws:SourceArn`Las condiciones `aws:SourceAccount` y protegen contra el confuso problema del suplente, por lo que solo los experimentos que pertenezcan a tu cuenta pueden asumir esa función.

```
{
  "Version": "2012-10-17"       ,
  "Statement": [
    {
      "Sid": "FISTrustPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "fis.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        },
```

```
        "ArnLike": {
          "aws:SourceArn": "arn:aws:fis:*:account-id:experiment/*"
        }
      }
    }
  ]
}
```

Política de permisos

Adjunta la política de permisos de la plantilla de prueba que usa tu prueba.

Temas

- Zona de disponibilidad: recuperación
- Validación de dependencias
- Multi-Region: aislamiento
- Multi-Region: recuperación
- Crea el rol y adjúntalo a tu prueba

Zona de disponibilidad: recuperación

La plantilla Zona de disponibilidad: recuperación ejecuta AWS FIS acciones contra los siguientes servicios: Amazon EC2, Amazon EC2 Auto Scaling, Amazon, Amazon ElastiCache RDS, las ACL de red y el cambio zonal del controlador de recuperación de AWS aplicaciones. Adjunte la siguiente política de permisos al rol de ejecución.

```
{
  "Version": "2012-10-17"       ,
  "Statement": [
    {
      "Sid": "EC2StopAndStartInstances",
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource": "arn:aws:ec2:*:account-id:instance/*"
    },
```

```
    {
      "Sid": "EC2DescribeInstances",
      "Effect": "Allow",
      "Action": "ec2:DescribeInstances",
      "Resource": "*"
    },
    {
      "Sid": "EC2EncryptedVolumesKmsGrant",
      "Effect": "Allow",
      "Action": "kms:CreateGrant",
      "Resource": "arn:aws:kms:*:account-id:key/*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "ec2.*.amazonaws.com"
        },
        "Bool": {
          "kms:GrantIsForAWSResource": "true"
        },
        "ForAllValues:StringEquals": {
          "kms:GrantOperations": ["Decrypt", "CreateGrant"]
        },
        "Null": {
          "kms:GrantOperations": "false"
        },
        "StringEquals": {
          "kms:GrantConstraintType": "EncryptionContextSubset"
        },
        "ForAnyValue:StringEquals": {
          "kms:EncryptionContextKeys": "aws:ebs:id"
        }
      }
    },
    {
      "Sid": "EC2InjectApiError",
      "Effect": "Allow",
      "Action": "ec2:InjectApiError",
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "ec2:FisActionId": [
            "aws:ec2:api-insufficient-instance-capacity-error",
            "aws:ec2:asg-insufficient-instance-capacity-error"
          ]
        }
```

```
      }
    },
    {
      "Sid": "AutoScalingDescribe",
      "Effect": "Allow",
      "Action": [
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeTags"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ElastiCacheInterruptAzPower",
      "Effect": "Allow",
      "Action": [
        "elasticache:InterruptClusterAzPower",
        "elasticache:DescribeReplicationGroups"
      ],
      "Resource": "arn:aws:elasticache:*:account-id:replicationgroup:*"
    },
    {
      "Sid": "EBSPauseVolumeIO",
      "Effect": "Allow",
      "Action": "ec2:PauseVolumeIO",
      "Resource": "arn:aws:ec2:*:account-id:volume/*"
    },
    {
      "Sid": "EBSDescribeVolumes",
      "Effect": "Allow",
      "Action": "ec2:DescribeVolumes",
      "Resource": "*"
    },
    {
      "Sid": "NetworkTagManagedNacl",
      "Effect": "Allow",
      "Action": "ec2:CreateTags",
      "Resource": "arn:aws:ec2:*:account-id:network-acl/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkAcl",
          "aws:RequestTag/managedByFIS": "true"
        }
      }
    },
```

```
    {
      "Sid": "NetworkCreateManagedNacl",
      "Effect": "Allow",
      "Action": "ec2:CreateNetworkAcl",
      "Resource": "arn:aws:ec2:*:account-id:network-acl/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "NetworkCreateNaclOnVpc",
      "Effect": "Allow",
      "Action": "ec2:CreateNetworkAcl",
      "Resource": "arn:aws:ec2:*:account-id:vpc/*"
    },
    {
      "Sid": "NetworkModifyManagedNacl",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkAclEntry",
        "ec2:DeleteNetworkAcl"
      ],
      "Resource": "arn:aws:ec2:*:account-id:network-acl/*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "NetworkDescribe",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeManagedPrefixLists"
      ],
      "Resource": "*"
    },
    {
      "Sid": "NetworkReplaceNaclAssociation",
```

```
      "Effect": "Allow",
      "Action": "ec2:ReplaceNetworkAclAssociation",
      "Resource": [
        "arn:aws:ec2:*:account-id:subnet/*",
        "arn:aws:ec2:*:account-id:network-acl/*"
      ]
    },
    {
      "Sid": "NetworkPrefixListEntries",
      "Effect": "Allow",
      "Action": "ec2:GetManagedPrefixListEntries",
      "Resource": "arn:aws:ec2:*:account-id:prefix-list/*"
    },
    {
      "Sid": "RDSFailoverCluster",
      "Effect": "Allow",
      "Action": [
        "rds:FailoverDBCluster",
        "rds:DescribeDBClusters"
      ],
      "Resource": "arn:aws:rds:*:account-id:cluster:*"
    },
    {
      "Sid": "RDSDescribeForTargetResolution",
      "Effect": "Allow",
      "Action": "rds:DescribeDBInstances",
      "Resource": "arn:aws:rds:*:account-id:db:*"
    },
    {
      "Sid": "ARCZonalShiftManagedElb",
      "Effect": "Allow",
      "Action": [
        "arc-zonal-shift:StartZonalShift",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:UpdateZonalShift",
        "arc-zonal-shift:CancelZonalShift"
      ],
      "Resource": [
        "arn:aws:elasticloadbalancing:*:account-id:loadbalancer/app/*",
        "arn:aws:elasticloadbalancing:*:account-id:loadbalancer/net/*"
      ]
    },
    {
      "Sid": "ARCZonalShiftManagedAsgEks",
```

```
      "Effect": "Allow",
      "Action": [
        "arc-zonal-shift:StartZonalShift",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:UpdateZonalShift",
        "arc-zonal-shift:CancelZonalShift"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "arc-zonal-shift:ResourceIdentifier": [
            "arn:aws:autoscaling:*:account-id:autoScalingGroup:*",
            "arn:aws:eks:*:account-id:cluster/*"
          ]
        }
      }
    },
    {
      "Sid": "ARCZonalShiftList",
      "Effect": "Allow",
      "Action": "arc-zonal-shift:ListManagedResources",
      "Resource": "*"
    },
    {
      "Sid": "TargetResolutionByTags",
      "Effect": "Allow",
      "Action": "tag:GetResources",
      "Resource": "*"
    },
    {
      "Sid": "FISExperimentLogging",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource": "*"
    },
    {
      "Sid": "FISExperimentLogGroupAccess",
      "Effect": "Allow",
```

```
      "Action": [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy",
        "logs:DescribeLogGroups"
      ],
      "Resource": "*"
    }
  ]
}
```

Validación de dependencias

La plantilla de validación de dependencias ejecuta AWS FIS acciones que bloquean el tráfico de dependencias dentro de la región procedente de las cargas de trabajo de Amazon EC2, Amazon ECS y Amazon EKS. Adjunte la siguiente política de permisos al rol de ejecución.

```
{
  "Version": "2012-10-17"       ,
  "Statement": [
    {
      "Sid": "SsmSendCommandOnDocuments",
      "Effect": "Allow",
      "Action": "ssm:SendCommand",
      "Resource": [
        "arn:aws:ssm:*::document/AWSFIS-Run-Network-Packet-Loss-Sources",
        "arn:aws:ssm:*::document/AWSFIS-Run-Network-Packet-Loss-ECS"
      ]
    },
    {
      "Sid": "SsmSendCommandOnInstances",
      "Effect": "Allow",
      "Action": "ssm:SendCommand",
      "Resource": [
        "arn:aws:ec2:*:account-id:instance/*",
        "arn:aws:ssm:*:account-id:managed-instance/*",
        "arn:aws:ecs:*:account-id:task/*/*"
      ]
    },
    {
      "Sid": "SsmListAndCancelCommands",
      "Effect": "Allow",
```

```
      "Action": [
        "ssm:ListCommands",
        "ssm:CancelCommand"
      ],
      "Resource": "*"
    },
    {
      "Sid": "Ec2DescribeForTargetResolution",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EcsDescribeForTargetResolution",
      "Effect": "Allow",
      "Action": [
        "ecs:DescribeTasks",
        "ecs:DescribeContainerInstances",
        "ecs:ListTasks"
      ],
      "Resource": [
        "arn:aws:ecs:*:account-id:task/*/*",
        "arn:aws:ecs:*:account-id:container-instance/*/*",
        "arn:aws:ecs:*:account-id:cluster/*"
      ]
    },
    {
      "Sid": "EksDescribeCluster",
      "Effect": "Allow",
      "Action": "eks:DescribeCluster",
      "Resource": "arn:aws:eks:*:account-id:cluster/*"
    },
    {
      "Sid": "TargetResolutionByTags",
      "Effect": "Allow",
      "Action": "tag:GetResources",
      "Resource": "*"
    },
    {
      "Sid": "FISExperimentLogging",
      "Effect": "Allow",
```

```
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource": "*"
    },
    {
      "Sid": "FISExperimentLogGroupAccess",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy",
        "logs:DescribeLogGroups"
      ],
      "Resource": "*"
    }
  ]
}
```

Multi-Region: aislamiento

La plantilla Multi-Region: isolation ejecuta AWS FIS acciones que interrumpen la conectividad entre regiones (tablas de rutas, pasarelas de tránsito y puntos de enlace de VPC) y detiene la replicación entre regiones en Amazon S3, Amazon DynamoDB y Amazon MemoryDB. Adjunte la siguiente política de permisos al rol de ejecución.

```
{
  "Version": "2012-10-17"       ,
  "Statement": [
    {
      "Sid": "RouteTableDisruptCrossRegion",
      "Effect": "Allow",
      "Action": [
        "ec2:AssociateRouteTable",
        "ec2:DisassociateRouteTable",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:CreateRoute"
      ],
```

```
      "Resource": [
        "arn:aws:ec2:*:account-id:route-table/*",
        "arn:aws:ec2:*:account-id:subnet/*"
      ]
    },
    {
      "Sid": "RouteTableManagedCreate",
      "Effect": "Allow",
      "Action": "ec2:CreateRouteTable",
      "Resource": "arn:aws:ec2:*:account-id:route-table/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "RouteTableManagedCreateOnVpc",
      "Effect": "Allow",
      "Action": "ec2:CreateRouteTable",
      "Resource": "arn:aws:ec2:*:account-id:vpc/*"
    },
    {
      "Sid": "RouteTableManagedDelete",
      "Effect": "Allow",
      "Action": "ec2:DeleteRouteTable",
      "Resource": [
        "arn:aws:ec2:*:account-id:route-table/*",
        "arn:aws:ec2:*:account-id:vpc/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "PrefixListManagedCreate",
      "Effect": "Allow",
      "Action": "ec2:CreateManagedPrefixList",
      "Resource": "arn:aws:ec2:*:account-id:prefix-list/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/managedByFIS": "true"
```

```
        }
      }
    },
    {
      "Sid": "PrefixListManagedModifyDelete",
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteManagedPrefixList",
        "ec2:ModifyManagedPrefixList"
      ],
      "Resource": "arn:aws:ec2:*:account-id:prefix-list/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "NetworkInterfaceManagedCreate",
      "Effect": "Allow",
      "Action": "ec2:CreateNetworkInterface",
      "Resource": "arn:aws:ec2:*:account-id:network-interface/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "NetworkInterfaceManagedCreateOnSubnetAndSg",
      "Effect": "Allow",
      "Action": "ec2:CreateNetworkInterface",
      "Resource": [
        "arn:aws:ec2:*:account-id:subnet/*",
        "arn:aws:ec2:*:account-id:security-group/*"
      ]
    },
    {
      "Sid": "NetworkInterfaceManagedDelete",
      "Effect": "Allow",
      "Action": "ec2:DeleteNetworkInterface",
      "Resource": "arn:aws:ec2:*:account-id:network-interface/*",
      "Condition": {
        "StringEquals": {
```

```
          "aws:ResourceTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "FISCreateTags",
      "Effect": "Allow",
      "Action": "ec2:CreateTags",
      "Resource": [
        "arn:aws:ec2:*:account-id:route-table/*",
        "arn:aws:ec2:*:account-id:prefix-list/*",
        "arn:aws:ec2:*:account-id:network-interface/*",
        "arn:aws:ec2:*:account-id:security-group/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "Ec2NetworkDescribeAndRead",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSecurityGroups",
        "ec2:GetManagedPrefixListEntries",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeInstances"
      ],
      "Resource": "*"
    },
    {
      "Sid": "TgwDisruptCrossRegion",
      "Effect": "Allow",
      "Action": [
```

```
        "ec2:AssociateTransitGatewayRouteTable",
        "ec2:DisassociateTransitGatewayRouteTable"
      ],
      "Resource": [
        "arn:aws:ec2:*:account-id:transit-gateway-route-table/*",
        "arn:aws:ec2:*:account-id:transit-gateway-attachment/*"
      ]
    },
    {
      "Sid": "VpcEndpointDisrupt",
      "Effect": "Allow",
      "Action": "ec2:ModifyVpcEndpoint",
      "Resource": [
        "arn:aws:ec2:*:account-id:vpc-endpoint/*",
        "arn:aws:ec2:*:account-id:security-group/*"
      ]
    },
    {
      "Sid": "VpcEndpointSecurityGroupManaged",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress"
      ],
      "Resource": [
        "arn:aws:ec2:*:account-id:security-group/*",
        "arn:aws:ec2:*:account-id:vpc/*"
      ]
    },
    {
      "Sid": "SsmSendCommandOnDocuments",
      "Effect": "Allow",
      "Action": "ssm:SendCommand",
      "Resource": [
        "arn:aws:ssm:*::document/AWSFIS-Run-Network-Packet-Loss-Sources",
        "arn:aws:ssm:*::document/AWSFIS-Run-Network-Packet-Loss-ECS"
      ]
    },
    {
      "Sid": "SsmSendCommandOnInstances",
      "Effect": "Allow",
      "Action": "ssm:SendCommand",
      "Resource": [
```

```
        "arn:aws:ec2:*:account-id:instance/*",
        "arn:aws:ssm:*:account-id:managed-instance/*",
        "arn:aws:ecs:*:account-id:task/*/*"
      ]
    },
    {
      "Sid": "SsmListAndCancelCommands",
      "Effect": "Allow",
      "Action": [
        "ssm:ListCommands",
        "ssm:CancelCommand"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EcsDescribeForTargetResolution",
      "Effect": "Allow",
      "Action": [
        "ecs:DescribeTasks",
        "ecs:DescribeContainerInstances",
        "ecs:ListTasks"
      ],
      "Resource": [
        "arn:aws:ecs:*:account-id:task/*/*",
        "arn:aws:ecs:*:account-id:container-instance/*/*",
        "arn:aws:ecs:*:account-id:cluster/*"
      ]
    },
    {
      "Sid": "EksDescribeCluster",
      "Effect": "Allow",
      "Action": "eks:DescribeCluster",
      "Resource": "arn:aws:eks:*:account-id:cluster/*"
    },
    {
      "Sid": "DynamoDbGlobalTablePauseReplication",
      "Effect": "Allow",
      "Action": [
        "dynamodb:PutResourcePolicy",
        "dynamodb:GetResourcePolicy",
        "dynamodb:DeleteResourcePolicy",
        "dynamodb:DescribeTable",
        "dynamodb:InjectError"
      ],
```

```
      "Resource": "arn:aws:dynamodb:*:account-id:table/*"
    },
    {
      "Sid": "S3PauseReplicationConfiguration",
      "Effect": "Allow",
      "Action": [
        "s3:PutReplicationConfiguration",
        "s3:GetReplicationConfiguration"
      ],
      "Resource": "arn:aws:s3:::*",
      "Condition": {
        "BoolIfExists": {
          "s3:IsReplicationPauseRequest": "true"
        },
        "StringEquals": {
          "aws:ResourceAccount": "account-id"
        }
      }
    },
    {
      "Sid": "S3PauseReplication",
      "Effect": "Allow",
      "Action": "s3:PauseReplication",
      "Resource": "arn:aws:s3:::*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "account-id"
        }
      }
    },
    {
      "Sid": "S3ListAllBuckets",
      "Effect": "Allow",
      "Action": "s3:ListAllMyBuckets",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "account-id"
        }
      }
    },
    {
      "Sid": "MemoryDbMultiRegionPauseReplication",
      "Effect": "Allow",
```

```
      "Action": [
        "memorydb:PauseMultiRegionClusterReplication",
        "memorydb:DescribeMultiRegionClusters"
      ],
      "Resource": "arn:aws:memorydb::account-id:multiregioncluster/*"
    },
    {
      "Sid": "TargetResolutionByTags",
      "Effect": "Allow",
      "Action": "tag:GetResources",
      "Resource": "*"
    },
    {
      "Sid": "FISExperimentLogging",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource": "*"
    },
    {
      "Sid": "FISExperimentLogGroupAccess",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy",
        "logs:DescribeLogGroups"
      ],
      "Resource": "*"
    }
  ]
}
```

Multi-Region: recuperación

La plantilla de recuperación Multi-Region: ejecuta AWS FIS acciones que bloquean el tráfico de dependencias en la región afectada para lograr la conmutación por error entre regiones. Adjunte la siguiente política de permisos a la función de ejecución.

```
{
  "Version": "2012-10-17"       ,
  "Statement": [
    {
      "Sid": "SsmSendCommandOnDocuments",
      "Effect": "Allow",
      "Action": "ssm:SendCommand",
      "Resource": [
        "arn:aws:ssm:*::document/AWSFIS-Run-Network-Packet-Loss-Sources",
        "arn:aws:ssm:*::document/AWSFIS-Run-Network-Packet-Loss-ECS"
      ]
    },
    {
      "Sid": "SsmSendCommandOnInstances",
      "Effect": "Allow",
      "Action": "ssm:SendCommand",
      "Resource": [
        "arn:aws:ec2:*:account-id:instance/*",
        "arn:aws:ssm:*:account-id:managed-instance/*",
        "arn:aws:ecs:*:account-id:task/*/*"
      ]
    },
    {
      "Sid": "SsmListAndCancelCommands",
      "Effect": "Allow",
      "Action": [
        "ssm:ListCommands",
        "ssm:CancelCommand"
      ],
      "Resource": "*"
    },
    {
      "Sid": "Ec2DescribeForTargetResolution",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EcsDescribeForTargetResolution",
```

```
      "Effect": "Allow",
      "Action": [
        "ecs:DescribeTasks",
        "ecs:DescribeContainerInstances",
        "ecs:ListTasks"
      ],
      "Resource": [
        "arn:aws:ecs:*:account-id:task/*/*",
        "arn:aws:ecs:*:account-id:container-instance/*/*",
        "arn:aws:ecs:*:account-id:cluster/*"
      ]
    },
    {
      "Sid": "EksDescribeCluster",
      "Effect": "Allow",
      "Action": "eks:DescribeCluster",
      "Resource": "arn:aws:eks:*:account-id:cluster/*"
    },
    {
      "Sid": "TargetResolutionByTags",
      "Effect": "Allow",
      "Action": "tag:GetResources",
      "Resource": "*"
    },
    {
      "Sid": "FISExperimentLogging",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource": "*"
    },
    {
      "Sid": "FISExperimentLogGroupAccess",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy",
        "logs:DescribeLogGroups"
      ],
```

```
      "Resource": "*"
    }
  ]
}
```

Crea el rol y adjúntalo a tu prueba

Guarde la política de confianza como `trust-policy.json` y la política de permisos como y`permissions-policy.json`, a continuación, cree el rol con la AWS CLI.

```
aws iam create-role \
  --role-name my-resilience-testing-role \
  --assume-role-policy-document file://trust-policy.json

aws iam put-role-policy \
  --role-name my-resilience-testing-role \
  --policy-name resilience-testing \
  --policy-document file://permissions-policy.json
```

Configure el rol en la prueba para que Resilience Hub lo utilice en las ejecuciones de prueba.

```
aws resiliencehubv2 update-test \
  --test-id test-id \
  --role-name my-resilience-testing-role
```

Multi-account roles de ejecución

Para una prueba con varias cuentas, AWS FIS utiliza una cadena de funciones. AWS FIS asume la función de orquestador en la cuenta en la que se ejecuta el experimento. A continuación, el rol de orquestador asume un rol objetivo en cada cuenta que contenga los recursos específicos. Crea el rol de orquestador una vez y crea un rol objetivo en cada cuenta objetivo.

Función de cuenta de Orchestrator

Crea el rol de orquestador en la cuenta en la que se ejecuta el experimento. Su política de confianza AWS FIS permite asumirlo, con la misma protección de diputado confuso que la política de confianza de una sola cuenta.

Política de confianza

```
{
  "Version": "2012-10-17"       ,
  "Statement": [
    {
      "Sid": "FISTrustPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "fis.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "orchestrator-account-id"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:fis:*:orchestrator-account-id:experiment/*"
        }
      }
    },
    {
      "Sid": "SelfAssume",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::orchestrator-account-id:role/orchestrator-role-name"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Política de permisos

La política de permisos de Orchestrator es la misma para todas las plantillas de prueba. Permite que el rol asuma las funciones de la cuenta objetivo, resuelva los objetivos y gestione el registro y el ciclo de vida de los experimentos. Indica el ARN de cada rol de la cuenta objetivo en la declaración. `AssumeTargetAccountRole`

```
{
  "Version": "2012-10-17"       ,
  "Statement": [
    {
```

```
      "Sid": "AssumeTargetAccountRole",
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": [
        "arn:aws:iam::target-account-id:role/target-role-name"
      ]
    },
    {
      "Sid": "FISExperimentLogging",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource": "*"
    },
    {
      "Sid": "FISExperimentLogGroupAccess",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy",
        "logs:DescribeLogGroups"
      ],
      "Resource": "*"
    },
    {
      "Sid": "FISExperimentLifecycle",
      "Effect": "Allow",
      "Action": [
        "fis:GetExperiment",
        "fis:StopExperiment",
        "fis:ListExperimentResolvedTargets"
      ],
      "Resource": "arn:aws:fis:*:orchestrator-account-id:experiment/*"
    },
    {
      "Sid": "OrchestratorTagGetResources",
      "Effect": "Allow",
      "Action": "tag:GetResources",
      "Resource": "*"
```

```
    },
    {
      "Sid": "OrchestratorDescribeForTargetResolution",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeRouteTables",
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVolumes",
        "rds:DescribeDBClusters",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeCacheClusters",
        "ecs:DescribeTasks",
        "ecs:ListTasks",
        "ecs:DescribeServices",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeClusters",
        "eks:DescribeCluster",
        "eks:ListClusters",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeTable",
        "dynamodb:ListGlobalTables",
        "memorydb:DescribeMultiRegionClusters",
        "memorydb:DescribeClusters",
        "autoscaling:DescribeAutoScalingGroups",
        "elasticloadbalancing:DescribeLoadBalancers",
        "arc-zonal-shift:ListManagedResources",
        "arc-zonal-shift:GetManagedResource",
        "iam:GetRole",
        "iam:ListRoles",
        "s3:GetBucketTagging",
        "s3:ListAllMyBuckets",
        "s3:GetReplicationConfiguration",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource": "*"
```

```
    }
  ]
}
```

Función de la cuenta objetivo

Cree un rol objetivo en cada cuenta que contenga recursos específicos. Su política de confianza permite que el orquestador asuma el rol de orquestador. La `sts:ExternalId` condición restringe la operación de suposición a los AWS FIS experimentos que pertenezcan a la cuenta del orquestador. La `aws:PrincipalArn` condición atribuye la confianza al rol de orquestador.

Política de confianza

```
{
  "Version": "2012-10-17"       ,
  "Statement": [
    {
      "Sid": "OrchestratorRoleAssumeRole",
      "Effect": "Allow",
      "Principal": {
        "AWS": "orchestrator-account-id"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringLike": {
          "sts:ExternalId": "arn:aws:fis:*:orchestrator-account-id:experiment/*"
        },
        "ArnEquals": {
          "aws:PrincipalArn": "arn:aws:iam::orchestrator-account-id:role/orchestrator-
role-name"
        }
      }
    }
  ]
}
```

Política de permisos

Adjunta la política de permisos de la plantilla de prueba que usa tu prueba. Estas políticas otorgan los permisos de inyección de errores para los recursos de destino. Los permisos de registro y ciclo de vida de los experimentos los otorga la función de orquestador, no la función de destino.

Temas

- Zona de disponibilidad: recuperación
- Validación de dependencias
- Multi-Region: aislamiento
- Multi-Region: recuperación

Zona de disponibilidad: recuperación

Adjunte la siguiente política de permisos al rol objetivo de la zona de disponibilidad: plantilla de recuperación.

```
{
  "Version": "2012-10-17"       ,
  "Statement": [
    {
      "Sid": "EC2StopAndStartInstances",
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource": "arn:aws:ec2:*:target-account-id:instance/*"
    },
    {
      "Sid": "EC2DescribeInstances",
      "Effect": "Allow",
      "Action": "ec2:DescribeInstances",
      "Resource": "*"
    },
    {
      "Sid": "EC2EncryptedVolumesKmsGrant",
      "Effect": "Allow",
      "Action": "kms:CreateGrant",
      "Resource": "arn:aws:kms:*:target-account-id:key/*",
```

```
      "Condition": {
        "StringLike": {
          "kms:ViaService": "ec2.*.amazonaws.com"
        },
        "Bool": {
          "kms:GrantIsForAWSResource": "true"
        },
        "ForAllValues:StringEquals": {
          "kms:GrantOperations": ["Decrypt", "CreateGrant"]
        },
        "StringEquals": {
          "kms:GrantConstraintType": "EncryptionContextSubset"
        },
        "ForAnyValue:StringEquals": {
          "kms:EncryptionContextKeys": "aws:ebs:id"
        }
      }
    },
    {
      "Sid": "EC2InjectApiError",
      "Effect": "Allow",
      "Action": "ec2:InjectApiError",
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "ec2:FisActionId": [
            "aws:ec2:api-insufficient-instance-capacity-error",
            "aws:ec2:asg-insufficient-instance-capacity-error"
          ]
        }
      }
    },
    {
      "Sid": "AutoScalingDescribe",
      "Effect": "Allow",
      "Action": [
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeTags"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ElastiCacheInterruptAzPower",
      "Effect": "Allow",
```

```
      "Action": [
        "elasticache:InterruptClusterAzPower",
        "elasticache:DescribeReplicationGroups"
      ],
      "Resource": "arn:aws:elasticache:*:target-account-id:replicationgroup:*"
    },
    {
      "Sid": "EBSPauseVolumeIO",
      "Effect": "Allow",
      "Action": "ec2:PauseVolumeIO",
      "Resource": "arn:aws:ec2:*:target-account-id:volume/*"
    },
    {
      "Sid": "EBSDescribeVolumes",
      "Effect": "Allow",
      "Action": "ec2:DescribeVolumes",
      "Resource": "*"
    },
    {
      "Sid": "NetworkTagManagedNacl",
      "Effect": "Allow",
      "Action": "ec2:CreateTags",
      "Resource": "arn:aws:ec2:*:target-account-id:network-acl/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkAcl",
          "aws:RequestTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "NetworkCreateManagedNacl",
      "Effect": "Allow",
      "Action": "ec2:CreateNetworkAcl",
      "Resource": "arn:aws:ec2:*:target-account-id:network-acl/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "NetworkCreateNaclOnVpc",
      "Effect": "Allow",
```

```
      "Action": "ec2:CreateNetworkAcl",
      "Resource": "arn:aws:ec2:*:target-account-id:vpc/*"
    },
    {
      "Sid": "NetworkModifyManagedNacl",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkAclEntry",
        "ec2:DeleteNetworkAcl"
      ],
      "Resource": "arn:aws:ec2:*:target-account-id:network-acl/*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "NetworkDescribe",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeManagedPrefixLists"
      ],
      "Resource": "*"
    },
    {
      "Sid": "NetworkReplaceNaclAssociation",
      "Effect": "Allow",
      "Action": "ec2:ReplaceNetworkAclAssociation",
      "Resource": [
        "arn:aws:ec2:*:target-account-id:subnet/*",
        "arn:aws:ec2:*:target-account-id:network-acl/*"
      ]
    },
    {
      "Sid": "NetworkPrefixListEntries",
      "Effect": "Allow",
      "Action": "ec2:GetManagedPrefixListEntries",
      "Resource": "arn:aws:ec2:*:target-account-id:prefix-list/*"
    },
    {
```

```
      "Sid": "RDSFailoverCluster",
      "Effect": "Allow",
      "Action": [
        "rds:FailoverDBCluster",
        "rds:DescribeDBClusters"
      ],
      "Resource": "arn:aws:rds:*:target-account-id:cluster:*"
    },
    {
      "Sid": "RDSDescribeForTargetResolution",
      "Effect": "Allow",
      "Action": "rds:DescribeDBInstances",
      "Resource": "arn:aws:rds:*:target-account-id:db:*"
    },
    {
      "Sid": "ARCZonalShiftManagedElb",
      "Effect": "Allow",
      "Action": [
        "arc-zonal-shift:StartZonalShift",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:UpdateZonalShift",
        "arc-zonal-shift:CancelZonalShift"
      ],
      "Resource": [
        "arn:aws:elasticloadbalancing:*:target-account-id:loadbalancer/app/*",
        "arn:aws:elasticloadbalancing:*:target-account-id:loadbalancer/net/*"
      ]
    },
    {
      "Sid": "ARCZonalShiftManagedAsgEks",
      "Effect": "Allow",
      "Action": [
        "arc-zonal-shift:StartZonalShift",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:UpdateZonalShift",
        "arc-zonal-shift:CancelZonalShift"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "arc-zonal-shift:ResourceIdentifier": [
            "arn:aws:autoscaling:*:target-account-id:autoScalingGroup:*",
            "arn:aws:eks:*:target-account-id:cluster/*"
          ]
```

```
        }
      }
    },
    {
      "Sid": "ARCZonalShiftList",
      "Effect": "Allow",
      "Action": "arc-zonal-shift:ListManagedResources",
      "Resource": "*"
    },
    {
      "Sid": "TargetResolutionByTags",
      "Effect": "Allow",
      "Action": "tag:GetResources",
      "Resource": "*"
    }
  ]
}
```

Validación de dependencias

Adjunte la siguiente política de permisos al rol objetivo de la plantilla de validación de dependencias.

```
{
  "Version": "2012-10-17"       ,
  "Statement": [
    {
      "Sid": "SsmSendCommandOnDocuments",
      "Effect": "Allow",
      "Action": "ssm:SendCommand",
      "Resource": [
        "arn:aws:ssm:*::document/AWSFIS-Run-Network-Packet-Loss-Sources",
        "arn:aws:ssm:*::document/AWSFIS-Run-Network-Packet-Loss-ECS"
      ]
    },
    {
      "Sid": "SsmSendCommandOnInstances",
      "Effect": "Allow",
      "Action": "ssm:SendCommand",
      "Resource": [
        "arn:aws:ec2:*:target-account-id:instance/*",
        "arn:aws:ssm:*:target-account-id:managed-instance/*",
        "arn:aws:ecs:*:target-account-id:task/*/*"
```

```
      ]
    },
    {
      "Sid": "SsmListAndCancelCommands",
      "Effect": "Allow",
      "Action": [
        "ssm:ListCommands",
        "ssm:CancelCommand"
      ],
      "Resource": "*"
    },
    {
      "Sid": "Ec2DescribeForTargetResolution",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EcsDescribeForTargetResolution",
      "Effect": "Allow",
      "Action": [
        "ecs:DescribeTasks",
        "ecs:DescribeContainerInstances",
        "ecs:ListTasks"
      ],
      "Resource": [
        "arn:aws:ecs:*:target-account-id:task/*/*",
        "arn:aws:ecs:*:target-account-id:container-instance/*/*",
        "arn:aws:ecs:*:target-account-id:cluster/*"
      ]
    },
    {
      "Sid": "EksDescribeCluster",
      "Effect": "Allow",
      "Action": "eks:DescribeCluster",
      "Resource": "arn:aws:eks:*:target-account-id:cluster/*"
    },
    {
      "Sid": "TargetResolutionByTags",
      "Effect": "Allow",
      "Action": "tag:GetResources",
```

```
      "Resource": "*"
    }
  ]
}
```

Multi-Region: aislamiento

Adjunte la siguiente política de permisos al rol objetivo de la plantilla Multi-Region: aislamiento.

```
{
  "Version": "2012-10-17"       ,
  "Statement": [
    {
      "Sid": "RouteTableDisruptCrossRegion",
      "Effect": "Allow",
      "Action": [
        "ec2:AssociateRouteTable",
        "ec2:DisassociateRouteTable",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:CreateRoute"
      ],
      "Resource": [
        "arn:aws:ec2:*:target-account-id:route-table/*",
        "arn:aws:ec2:*:target-account-id:subnet/*"
      ]
    },
    {
      "Sid": "RouteTableManagedCreate",
      "Effect": "Allow",
      "Action": "ec2:CreateRouteTable",
      "Resource": "arn:aws:ec2:*:target-account-id:route-table/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "RouteTableManagedCreateOnVpc",
      "Effect": "Allow",
      "Action": "ec2:CreateRouteTable",
      "Resource": "arn:aws:ec2:*:target-account-id:vpc/*"
```

```
    },
    {
      "Sid": "RouteTableManagedDelete",
      "Effect": "Allow",
      "Action": "ec2:DeleteRouteTable",
      "Resource": [
        "arn:aws:ec2:*:target-account-id:route-table/*",
        "arn:aws:ec2:*:target-account-id:vpc/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "PrefixListManagedCreate",
      "Effect": "Allow",
      "Action": "ec2:CreateManagedPrefixList",
      "Resource": "arn:aws:ec2:*:target-account-id:prefix-list/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "PrefixListManagedModifyDelete",
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteManagedPrefixList",
        "ec2:ModifyManagedPrefixList"
      ],
      "Resource": "arn:aws:ec2:*:target-account-id:prefix-list/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "NetworkInterfaceManagedCreate",
      "Effect": "Allow",
      "Action": "ec2:CreateNetworkInterface",
```

```
      "Resource": "arn:aws:ec2:*:target-account-id:network-interface/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "NetworkInterfaceManagedCreateOnSubnetAndSg",
      "Effect": "Allow",
      "Action": "ec2:CreateNetworkInterface",
      "Resource": [
        "arn:aws:ec2:*:target-account-id:subnet/*",
        "arn:aws:ec2:*:target-account-id:security-group/*"
      ]
    },
    {
      "Sid": "NetworkInterfaceManagedDelete",
      "Effect": "Allow",
      "Action": "ec2:DeleteNetworkInterface",
      "Resource": "arn:aws:ec2:*:target-account-id:network-interface/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "FISCreateTags",
      "Effect": "Allow",
      "Action": "ec2:CreateTags",
      "Resource": [
        "arn:aws:ec2:*:target-account-id:route-table/*",
        "arn:aws:ec2:*:target-account-id:prefix-list/*",
        "arn:aws:ec2:*:target-account-id:network-interface/*",
        "arn:aws:ec2:*:target-account-id:security-group/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/managedByFIS": "true"
        }
      }
    },
    {
```

```
      "Sid": "Ec2NetworkDescribeAndRead",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSecurityGroups",
        "ec2:GetManagedPrefixListEntries",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeInstances"
      ],
      "Resource": "*"
    },
    {
      "Sid": "TgwDisruptCrossRegion",
      "Effect": "Allow",
      "Action": [
        "ec2:AssociateTransitGatewayRouteTable",
        "ec2:DisassociateTransitGatewayRouteTable"
      ],
      "Resource": [
        "arn:aws:ec2:*:target-account-id:transit-gateway-route-table/*",
        "arn:aws:ec2:*:target-account-id:transit-gateway-attachment/*"
      ]
    },
    {
      "Sid": "VpcEndpointDisrupt",
      "Effect": "Allow",
      "Action": "ec2:ModifyVpcEndpoint",
      "Resource": [
        "arn:aws:ec2:*:target-account-id:vpc-endpoint/*",
        "arn:aws:ec2:*:target-account-id:security-group/*"
      ]
    },
    {
      "Sid": "VpcEndpointSecurityGroupManaged",
      "Effect": "Allow",
      "Action": [
```

```
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress"
      ],
      "Resource": [
        "arn:aws:ec2:*:target-account-id:security-group/*",
        "arn:aws:ec2:*:target-account-id:vpc/*"
      ]
    },
    {
      "Sid": "SsmSendCommandOnDocuments",
      "Effect": "Allow",
      "Action": "ssm:SendCommand",
      "Resource": [
        "arn:aws:ssm:*::document/AWSFIS-Run-Network-Packet-Loss-Sources",
        "arn:aws:ssm:*::document/AWSFIS-Run-Network-Packet-Loss-ECS"
      ]
    },
    {
      "Sid": "SsmSendCommandOnInstances",
      "Effect": "Allow",
      "Action": "ssm:SendCommand",
      "Resource": [
        "arn:aws:ec2:*:target-account-id:instance/*",
        "arn:aws:ssm:*:target-account-id:managed-instance/*",
        "arn:aws:ecs:*:target-account-id:task/*/*"
      ]
    },
    {
      "Sid": "SsmListAndCancelCommands",
      "Effect": "Allow",
      "Action": [
        "ssm:ListCommands",
        "ssm:CancelCommand"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EcsDescribeForTargetResolution",
      "Effect": "Allow",
      "Action": [
        "ecs:DescribeTasks",
        "ecs:DescribeContainerInstances",
        "ecs:ListTasks"
```

```
      ],
      "Resource": [
        "arn:aws:ecs:*:target-account-id:task/*/*",
        "arn:aws:ecs:*:target-account-id:container-instance/*/*",
        "arn:aws:ecs:*:target-account-id:cluster/*"
      ]
    },
    {
      "Sid": "EksDescribeCluster",
      "Effect": "Allow",
      "Action": "eks:DescribeCluster",
      "Resource": "arn:aws:eks:*:target-account-id:cluster/*"
    },
    {
      "Sid": "DynamoDbGlobalTablePauseReplication",
      "Effect": "Allow",
      "Action": [
        "dynamodb:PutResourcePolicy",
        "dynamodb:GetResourcePolicy",
        "dynamodb:DeleteResourcePolicy",
        "dynamodb:DescribeTable",
        "dynamodb:InjectError"
      ],
      "Resource": "arn:aws:dynamodb:*:target-account-id:table/*"
    },
    {
      "Sid": "S3PauseReplicationConfiguration",
      "Effect": "Allow",
      "Action": [
        "s3:PutReplicationConfiguration",
        "s3:GetReplicationConfiguration"
      ],
      "Resource": "arn:aws:s3:::*",
      "Condition": {
        "BoolIfExists": {
          "s3:IsReplicationPauseRequest": "true"
        }
      }
    },
    {
      "Sid": "S3PauseReplication",
      "Effect": "Allow",
      "Action": "s3:PauseReplication",
      "Resource": "arn:aws:s3:::*"
```

```
    },
    {
      "Sid": "S3ListAllBuckets",
      "Effect": "Allow",
      "Action": "s3:ListAllMyBuckets",
      "Resource": "*"
    },
    {
      "Sid": "MemoryDbMultiRegionPauseReplication",
      "Effect": "Allow",
      "Action": [
        "memorydb:PauseMultiRegionClusterReplication",
        "memorydb:DescribeMultiRegionClusters"
      ],
      "Resource": "arn:aws:memorydb::target-account-id:multiregioncluster/*"
    },
    {
      "Sid": "TargetResolutionByTags",
      "Effect": "Allow",
      "Action": "tag:GetResources",
      "Resource": "*"
    }
  ]
}
```

Multi-Region: recuperación

Adjunte la siguiente política de permisos al rol objetivo de la plantilla de recuperación Multi-Region:.

```
{
  "Version": "2012-10-17"       ,
  "Statement": [
    {
      "Sid": "SsmSendCommandOnDocuments",
      "Effect": "Allow",
      "Action": "ssm:SendCommand",
      "Resource": [
        "arn:aws:ssm:*::document/AWSFIS-Run-Network-Packet-Loss-Sources",
        "arn:aws:ssm:*::document/AWSFIS-Run-Network-Packet-Loss-ECS"
      ]
    },
    {
```

```
      "Sid": "SsmSendCommandOnInstances",
      "Effect": "Allow",
      "Action": "ssm:SendCommand",
      "Resource": [
        "arn:aws:ec2:*:target-account-id:instance/*",
        "arn:aws:ssm:*:target-account-id:managed-instance/*",
        "arn:aws:ecs:*:target-account-id:task/*/*"
      ]
    },
    {
      "Sid": "SsmListAndCancelCommands",
      "Effect": "Allow",
      "Action": [
        "ssm:ListCommands",
        "ssm:CancelCommand"
      ],
      "Resource": "*"
    },
    {
      "Sid": "Ec2DescribeForTargetResolution",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EcsDescribeForTargetResolution",
      "Effect": "Allow",
      "Action": [
        "ecs:DescribeTasks",
        "ecs:DescribeContainerInstances",
        "ecs:ListTasks"
      ],
      "Resource": [
        "arn:aws:ecs:*:target-account-id:task/*/*",
        "arn:aws:ecs:*:target-account-id:container-instance/*/*",
        "arn:aws:ecs:*:target-account-id:cluster/*"
      ]
    },
    {
      "Sid": "EksDescribeCluster",
      "Effect": "Allow",
```

```
      "Action": "eks:DescribeCluster",
      "Resource": "arn:aws:eks:*:target-account-id:cluster/*"
    },
    {
      "Sid": "TargetResolutionByTags",
      "Effect": "Allow",
      "Action": "tag:GetResources",
      "Resource": "*"
    }
  ]
}
```

Cree los roles y adjúntelos a su prueba

En la cuenta de orquestador, crea el rol de orquestador.

```
aws iam create-role \
  --role-name my-orchestrator-role \
  --assume-role-policy-document file://orchestrator-trust-policy.json

aws iam put-role-policy \
  --role-name my-orchestrator-role \
  --policy-name resilience-testing-orchestrator \
  --policy-document file://orchestrator-permissions-policy.json
```

En cada cuenta de destino, crea el rol de destino con la política de permisos de tu plantilla de prueba.

```
aws iam create-role \
  --role-name my-target-role \
  --assume-role-policy-document file://target-trust-policy.json

aws iam put-role-policy \
  --role-name my-target-role \
  --policy-name resilience-testing-target \
  --policy-document file://target-permissions-policy.json
```

Configura el rol de orquestador como el rol de ejecución en tu prueba.

```
aws resiliencehubv2 update-test \
  --test-id test-id \
  --role-name my-orchestrator-role
```

Panel de control e informes

El panel de control de última generación de Resilience Hub ofrece una vista centralizada de la postura de resiliencia de su organización, lo que permite a los SRE supervisar el cumplimiento, hacer un seguimiento de las tendencias y generar informes en todos los servicios.

Temas

Descripción general del panel central del SRE

El panel es su punto de partida para comprender la resiliencia en todos sus servicios. Proporciona:

- Resumen de la postura de resiliencia: estado general de cumplimiento en todos los servicios
- Actividad de evaluación: evaluaciones recientes y futuras
- Descripción general de los hallazgos: hallazgos del modo de falla abierto por gravedad
- Dependencias: dependencias descubiertas recientemente o no clasificadas
- Resultados de las pruebas: Pass/fail estado de las pruebas de resiliencia en todos sus servicios

Service-level ver

Profundice en cualquier servicio para ver información detallada sobre su estado actual. Las siguientes secciones están disponibles en la vista de niveles de servicio.

Sección	Qué muestra
Configuración	Fuentes de entrada, modelo de permisos, sistema asociado y recorridos de usuario
Topología	Mapa visual de recursos y conexiones
Modos de fallo	Hallazgos del modo de falla a partir de la evaluación más reciente, con indicación de la gravedad y el estado

Sección	Qué muestra
Dependencias	Dependencias descubiertas con estado crítico y permitido
Historial	Historial de evaluaciones y tendencia en la puntuación de resiliencia

Filtrado por política, cuenta, región y sistema

Puede filtrar las vistas del panel con los siguientes filtros.

Filtro	Description (Descripción)
Política	Mostrar solo los servicios que utilizan una política de resiliencia específica
Cuenta	Céntrese en los servicios de una AWS cuenta específica
Region	Filtrar por Región de AWS
System (Sistema)	Mostrar servicios dentro de un sistema específico
Gravedad	Filtre los hallazgos del modo de falla por nivel de gravedad
Compliance status (Estado de conformidad)	Cumple, no cumple con los requisitos o no se ha evaluado

Para AWS los usuarios de Organizations, están disponibles los siguientes filtros adicionales:

- Unidad organizativa: filtrar por unidad organizativa
- Cuenta de miembro: concéntrese en una cuenta de miembro específica

Generar informes sobre las posturas de cumplimiento y resiliencia

Requisitos previos

Antes de que puedas generar un informe, tu servicio debe tener:

- Una configuración de salida de informes que especifique el bucket de Amazon S3 en el que se entregan los informes.
- Un rol de invocador que confía en la próxima generación del servicio Resilience Hub y tiene permiso para escribir en el bucket de Amazon S3 configurado.
- Al menos una evaluación completada con un estado de. SUCCESS

Puede configurar los resultados de los informes al crear o actualizar un servicio:

```
aws resiliencehubv2 update-service \
  --service-arn "arn:aws:resiliencehub:us-east-1:123456789012:service/my-
service:abc123" \
  --report-configuration '{"reportOutputs": [{"s3": {"bucketPath": "my-report-bucket",
 "bucketOwner": "123456789012"}}]}'
```

El rol de invocador debe tener una política de permisos que se conceda `s3:PutObject` en el bucket de destino. El siguiente ejemplo muestra la política mínima requerida.

```
{
  "Version": "2012-10-17"       ,
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::my-report-bucket/*"
    }
  ]
}
```

> **Note**
>
> Si su bucket usa un prefijo en `bucketPath` (por ejemplo,`my-report-bucket/reports`), defina el recurso según corresponda (por ejemplo,`arn:aws:s3:::my-report-bucket/reports/*`).

> **Note**
>
> Si su bucket de Amazon S3 está configurado con SSE-KMS cifrado, la función de invocador también necesita `kms:GenerateDataKey` `kms:Encrypt` permisos en la clave KMS del bucket.

Generar un informe de evaluación del modo de error

Para generar un informe después de realizar una evaluación:

1. Navegue hasta su servicio.
2. Seleccione la pestaña Evaluación.
3. Elija Generar informe.

Informes de ejecución de pruebas

Los informes de prueba se generan automáticamente una vez finalizada cada ejecución de prueba si se ha configurado un destino para el informe. No hace falta realizar ningún otro paso. Para obtener más información sobre lo que se incluye, consulteEjecuta la prueba e informa.

Visualización de informes

En el menú de navegación de la izquierda, selecciona Informes. La página de informes muestra todos los informes generados (evaluaciones en modo de fallo y ejecuciones de prueba) a los que tiene acceso.

AWS Integración de organizaciones

Resilience Hub de última generación se integra con AWS Organizations para permitir la gestión de la resiliencia en toda la organización desde una única cuenta de administrador delegado (DA). Esto elimina la necesidad de iniciar sesión en cuentas individuales para evaluar la resiliencia en toda la empresa. Puede ver en toda la organización la postura de resiliencia y los cuadros de mando agregados sin necesidad de iniciar sesión en cuentas individuales.

Métrica	Valor
Cuentas por organización	Más de 50 000

Métrica	Valor
Servicios en toda la organización	10 000
Latencia de consultas en el panel	Independiente del tamaño de la organización
Latencia de agregación de datos	Menos de 5 minutos

Temas

Descripción general de la gobernanza de múltiples cuentas en la próxima generación de Resilience Hub

Resilience Hub de última generación permite una gobernanza centralizada de la resiliencia en toda su AWS organización. Con la integración de Organizations, puede:

- Consulta la postura de resiliencia de todas las cuentas desde un único panel.
- Cree y publique políticas de resiliencia para toda la organización.
- Supervise el cumplimiento en cientos de cuentas y servicios.
- Filtre por cuenta Región de AWS, unidad organizativa (OU) y política.

Los siguientes conceptos básicos se aplican al modelo de integración de Organizations:

Concepto	Description (Descripción)
Administrador delegado	Una cuenta de miembro designada para administrar la próxima generación de Resilience Hub en toda la organización
Org-level políticas	Políticas de resiliencia creadas por el DA, visibles y asignables en todas las cuentas de los miembros
Service-Linked Funciones	Se crean automáticamente en las cuentas de los miembros para un acceso multicuenta de solo lectura

En AWS Organizations, el administrador delegado:

- Tiene visibilidad de todos los sistemas y servicios en todas las cuentas de los miembros.
- Crea y publica políticas de resiliencia para toda la organización asociándolas a los viajes de los usuarios en sistemas compartidos.
- Visualiza los paneles de control agregados sobre las posturas de resiliencia.

Service-Linked Los roles (SLR) se crean automáticamente en todas las cuentas de los miembros cuando se habilita el acceso confiable, lo que proporciona al DA una visibilidad multicuenta de solo lectura sin necesidad de configurar la IAM manual.

Configuración de la integración de Organizations

Para utilizar la próxima generación de Resilience Hub with AWS Organizations, debe designar una cuenta de administrador delegado que gestione las políticas y la visibilidad de toda la organización.

Requisitos previos

- AWS Las organizaciones deben configurarse con todas las funciones habilitadas.
- Debe tener acceso a la cuenta de administración para permitir un acceso confiable.
- Identifique qué cuenta de miembro servirá como administrador delegado.
- La cuenta de administración debe crear el Service-Linked rol (SLR) para que funcione la integración de Organizations. Sin la SLR, el administrador delegado no puede acceder a los datos de las cuentas de los miembros.

> **Important**
>
> La cuenta de administración debe crear el Service-Linked rol (SLR) durante la configuración. La integración de Organizations no funciona sin la SLR y el administrador delegado no puede acceder a los datos de las cuentas de los miembros hasta que se cree la SLR.

Pasos de configuración rápidos

1. Desde la cuenta de administración, abra la consola de última generación de Resilience Hub y elija la configuración de AWS Organizations.
2. Seleccione las casillas de verificación para habilitar el acceso confiable y cree el Service-Linked rol (SLR).
3. Seleccione Crear integración.
4. (Opcional) Registre un administrador delegado seleccionando Registrar en la misma página.
5. Desde la cuenta de administrador delegado, seleccione la región de origen en la consola Resilience Hub de próxima generación.
6. Los propietarios de los servicios individuales de las cuentas de los miembros crean sus propias funciones de invocador para sus servicios. Para obtener información sobre la configuración del rol de invocador, consulte. Configuración de Resilience Hub de próxima generación

Una vez completada la configuración, Resilience Hub de próxima generación realiza las siguientes acciones:

1. Service-Linked Los roles se crean en todas las cuentas de los miembros. Esto puede llevar más tiempo en el caso de las grandes organizaciones debido a la limitación de las API.
2. La próxima generación de Resilience Hub recupera la estructura organizativa inicial.
3. La cuenta DA gana visibilidad entre cuentas a través de las SLR.
4. Comienza la sincronización de la estructura de la organización (basada en eventos y un trabajo de conciliación de 12 horas).

Service-Linked Funciones

Service-Linked Los roles (`AWSServiceRoleForResilienceHub`) son roles de IAM que se crean automáticamente en cada cuenta de miembro al habilitar el acceso confiable

`resiliencehub.amazonaws.com` desde la cuenta de administración. Estas funciones proporcionan al administrador delegado una visibilidad multicuenta de solo lectura de los recursos de las cuentas de los miembros sin necesidad de configurar manualmente la IAM.

Las SLR se crean automáticamente cuando se incorpora una nueva cuenta a la organización.

Los propietarios de los servicios individuales de las cuentas de los miembros siguen creando sus propias funciones de invocador para ejecutar las evaluaciones de sus servicios. La SLR proporciona visibilidad entre cuentas al DA; no reemplaza la función de invocador utilizada para el descubrimiento y la evaluación. Para obtener información sobre la configuración del rol de invocador, consulte. Configuración de Resilience Hub de próxima generación

Aplicar políticas de resiliencia en todas las cuentas

Una cuenta de administración o un administrador delegado pueden aplicar políticas de resiliencia en todas las cuentas de los miembros asociando una política a un sistema y luego asociando los servicios de las cuentas de los miembros a ese sistema. La política a nivel de sistema se aplica a todos los servicios asociados.

1. Cree una política de resiliencia en la cuenta de administración o la cuenta DA.
2. Cree un sistema y asocie la política a él.
3. Asocie los servicios de las cuentas de los miembros al sistema.

La política a nivel de sistema se aplica a todos los servicios asociados a ese sistema, independientemente de la cuenta de miembro propietaria del servicio.

Visualización de la postura de resiliencia de toda la organización

El administrador delegado ve las vistas agregadas de toda la organización. El panel de la organización muestra:

- Servicios totales en todas las cuentas con su estado de cumplimiento.
- Los resultados se resumen por gravedad en toda la organización.
- Actividad y tendencias de la evaluación.
- Servicios sin políticas ni evaluaciones recientes.

Administrar la incorporación de cuentas de miembros

La incorporación de las cuentas de los miembros se gestiona automáticamente a través de las SLR:

- Cuentas nuevas: cuando una nueva cuenta se une a la organización, se crea automáticamente una SLR en la nueva cuenta, la cuenta aparece en la vista de organización del DA y el DA puede ver los servicios creados en la nueva cuenta.
- Cuentas eliminadas: cuando una cuenta abandona la organización, el DA deja de ver los datos de esa cuenta y los servicios de la cuenta eliminada siguen funcionando de forma independiente.

Permisos de IAM necesarios para la configuración de administrador delegado

Se requieren los siguientes permisos de IAM para cada función de la integración de Organizations:

Cuenta de administración

La cuenta de administración necesita permisos para:

- `organizations:EnableAWSServiceAccess`
- `organizations:RegisterDelegatedAdministrator`
- `iam:CreateServiceLinkedRole`(para la propia SLR de la cuenta de administración)

Cuenta de administrador delegado

La cuenta DA utiliza los permisos estándar de la API de Resilience Hub de próxima generación. Cross-account el acceso se gestiona mediante cámaras réflex; no se necesita ninguna configuración de IAM adicional para ver los datos de las cuentas de los miembros.

Cuentas de miembros

Propietarios de los servicios en las cuentas de los miembros:

- Cree sus propias funciones de invocador mediante el mismo proceso que en la configuración de una sola cuenta. Para obtener más información, consulte Configuración de Resilience Hub de próxima generación.
- Puede ver y aplicar las políticas a nivel de organización publicadas por el DA.

- La SLR gestiona la visibilidad entre cuentas de DA de forma automática; no es necesario realizar cambios adicionales en el IAM de las cuentas de los miembros.

En la siguiente tabla se resume lo que el DA puede y no puede hacer:

Action	compatible
Vea los servicios, las conclusiones y las dependencias de las cuentas de los miembros	Sí
Cree sistemas a nivel de organización que hagan referencia a los servicios para los miembros	Sí
Asocie los servicios para los miembros a los sistemas a nivel de la organización	Sí
Cree políticas a nivel de organización	Sí
Eliminar los servicios de las cuentas de los miembros	No
Inicie las evaluaciones de los servicios para miembros	Sí
Modifique los recursos de la cuenta de miembro	No

El acceso multicuenta de DA no permite realizar operaciones destructivas en los recursos de los miembros. El DA administra los sistemas y políticas a nivel de la organización y consulta los datos de los miembros.

Migrar desde AWS Resilience Hub

Si ya es cliente AWS Resilience Hub (versión 1), esta guía lo ayudará a comprender los cambios con la próxima generación de Resilience Hub y cómo migrar sus aplicaciones. La siguiente tabla resume los cambios clave entre las dos versiones.

Área	AWS Resilience Hub v1	Resilience Hub de próxima generación
Primitiva básica	Aplicación	Sistema + Servicios
Motor de evaluación	Controles estáticos basados en reglas	GenAI-powered análisis del modo de falla
Visibilidad de dependencias	Ninguno	Detección de dependencias
Multi-account	Limitado	Integración total de AWS las organizaciones
Políticas	RTO/RPO Política única por aplicación	Políticas modulares y componibles (recuperación de datos, disponibilidad y recuperación de datos)
Pruebas	AWS FIS plantillas de experimentos (configuración manual)	Pruebas de resiliencia recomendadas (preconfiguradas, segmentadas automáticamente) pass/fail
Versión de la API	/v1	/v2

Temas

- ¿Qué cambia con el Resilience Hub de próxima generación
- Mapeo conceptual: AWS Resilience Hub de la versión 1 al Resilience Hub de próxima generación
- Step-by-step guía de migración
- Transición de precios
- Limitaciones conocidas durante la migración

¿Qué cambia con el Resilience Hub de próxima generación

La próxima generación de Resilience Hub presenta una nueva jerarquía de modelado de aplicaciones, GenAI-powered evaluaciones y detección automática de dependencias. En esta sección se resumen los cambios clave.

- Nueva jerarquía: la versión 1 del concepto de «aplicación» se asigna a un «servicio» como la principal unidad de evaluación. Los servicios se agrupan en sistemas y los recorridos de los usuarios describen las rutas a través de ellos.
- GenAI-powered Evaluaciones de los modos de fallo: las comprobaciones estáticas basadas en reglas se sustituyen por un análisis generativo de IA que produce hallazgos detallados sobre los modos de fallo con un razonamiento específico para su arquitectura.
- Descubrimiento de dependencias: la próxima generación de Resilience Hub descubre automáticamente las dependencias entre los servicios y los recursos externos, una capacidad que no estaba disponible en la versión 1.
- Políticas de resiliencia modulares: las políticas ahora son componibles. Puede combinar la recuperación ante desastres (DR), el SLO de disponibilidad y las condiciones de recuperación de datos en una sola política, en lugar de en un solo par. RTO/RPO
- Integración total con AWS las organizaciones: Organization-wide la gestión desde una única cuenta de administrador delegado reemplaza el limitado soporte multicuenta de la versión 1.

Mapeo conceptual: AWS Resilience Hub de la versión 1 al Resilience Hub de próxima generación

La siguiente tabla asigna los conceptos de la AWS Resilience Hub versión 1 a sus equivalentes en la próxima generación de Resilience Hub.

AWS Resilience Hub Concepto v1	Concepto Resilience Hub de próxima generación	Notas
Aplicación	Servicio	Su «aplicación» de la versión 1 se convierte en un «servicio» de próxima generación de Resilience Hub: la unidad principal de evaluación

AWS Resilience Hub Concepto v1	Concepto Resilience Hub de próxima generación	Notas
Controles de resiliencia	Conclusiones de la evaluación del modo de falla	Las comprobaciones estáticas se sustituyeron por GenAI-powered hallazgos con razonamiento
Evaluación de la aplicació n	Evaluación del modo de falla del servicio	El mismo concepto, ahora a nivel de servicio con un rendimiento más rico
Política de evaluación (RTO/RPO)	Política de resiliencia (modular)	Las políticas ahora son componibles: recuperación ante desastres, disponibi lidad, SLO, recuperación de datos
Aplicación (como agrupación)	Sistema + Trayectorias de usuario	El aspecto de «agrupamiento» de las aplicaciones se relaciona con los sistemas y los recorridos de los usuarios
— (no disponible)	Detección de dependenc ias	Nueva capacidad en la próxima generación de Resilience Hub
— (no disponible)	Funciones de servicio	Flujos de trabajo técnicos dentro de un servicio; nuevos en la próxima generación de Resilience Hub

Step-by-step guía de migración

Siga estos pasos para migrar sus aplicaciones de la AWS Resilience Hub versión 1 existentes a la próxima generación de Resilience Hub.

Identifique la aplicación que desea migrar

Usa la API AWS Resilience Hub de la versión 1 para encontrar el ARN de la aplicación que deseas migrar.

```
# List your v1 applications
aws resiliencehub list-apps
```

Anote el ARN de la aplicación que desea migrar. Utilizará este ARN en el siguiente paso.

Usa la API de migración

La próxima generación de Resilience Hub proporciona API de migración que gestionan la transición por usted. La `import-app` API crea el servicio automáticamente; no es necesario crear primero un sistema o servicio de forma manual.

```
# Import a v1 application to a next generation Resilience Hub service
aws resiliencehubv2 import-app \
  --v1-app-arn "arn:aws:resiliencehub:us-east-1:123456789012:app/my-app:..."

# Import a v1 policy to a next generation Resilience Hub policy
aws resiliencehubv2 import-policy \
  --v1-policy-arn "arn:aws:resiliencehub:us-east-1:123456789012:resiliency-policy/..."
```

La API de migración realiza las siguientes acciones:

- Crea un servicio a partir de tu aplicación v1 (dentro de un sistema nuevo o existente)
- Conserva las fuentes de entrada y la configuración de los recursos
- Convierte su política v1 en una política de resiliencia con condiciones modulares
- Mantiene el historial de evaluaciones para garantizar la continuidad

Ejecute su primera evaluación en modo de fallo

Tras la migración, ejecute una evaluación del modo de fallo para ver los resultados mejorados.

```
aws resiliencehubv2 start-failure-mode-assessment \
  --service-arn "arn:aws:resiliencehub:..."
```

Los resultados del modo de fallo incluyen un razonamiento detallado específico para su arquitectura, recomendaciones con orientación sobre costos y complejidad, y un mapeo de políticas que muestra qué requisitos están en riesgo.

Habilite nuevas capacidades

Aproveche las funciones que no están disponibles en la versión 1.

1. Habilite la detección de dependencias: descubra las dependencias ocultas entre los servicios y los recursos externos.

2. Configure las organizaciones: habilite la gobernanza multicuenta en toda su organización.
3. Agregue condiciones de rendimiento: defina qué significa «disponible» más allá del tiempo de actividad mediante las condiciones de SLO de disponibilidad.

Transición de precios

En la siguiente tabla se muestra cómo se asignan los componentes de precios de AWS Resilience Hub la versión 1 a la próxima generación de Resilience Hub.

Componente	AWS Resilience Hub v1	Resilience Hub de próxima generación
Tarifa base	$ 15/application /mes	$ /mes 15/service
Evaluaciones incluidas	Sin límite	2 por mes
Exceso de recursos	Ninguno	0 dólares. 10/resource más de 150 por evaluación
Detección de dependencias	No disponible	$ 10/service /mes (opcional)

Se conserva el precio de entrada de 15 dólares. La mayoría de los clientes (servicios con 150 recursos o menos que utilizan 2 o menos evaluaciones al mes) pagan la misma cantidad.

Limitaciones conocidas durante la migración

Las siguientes limitaciones se aplican durante el período de migración de la AWS Resilience Hub versión 1 a la próxima generación de Resilience Hub.

Limitación	Description (Descripción)	Solución
Historial de evaluaciones	Los resultados de las evaluacio nes de la versión 1 no se migran automáticamente a la próxima generación del formato Resilience Hub	Los resultados de la versión 1 permanecen accesibles a través de las API de la versión 1 durante el período de transición

Limitación	Description (Descripción)	Solución
Comprobaciones de resiliencia personalizadas	Las comprobaciones personalizadas de la versión 1 no se migran	Revise los hallazgos del modo de falla: las evaluaciones de GenAI generalmente cubren los mismos problemas
AppRegistry fuente de entrada	AppRegistry no se admite como fuente de entrada en la próxima generación de Resilience Hub	Usa fuentes de entrada alternativas, como CloudFormation pilas o etiquetas de recursos

Seguridad en Resilience Hub de próxima generación

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

La seguridad es una responsabilidad compartida entre AWS usted y usted. El modelo de responsabilidad compartida describe esto como seguridad de la nube y seguridad en la nube.

En este tema se describen las funciones de seguridad y las prácticas recomendadas de la próxima generación de Resilience Hub, incluidos los permisos de IAM, el cifrado de datos, la seguridad de la red y los registros de auditoría.

Temas

- Referencia de roles y permisos de IAM
- Cifrado de datos
- Puntos de conexión de VPC
- CloudTrail integración
- Consideraciones de conformidad

Referencia de roles y permisos de IAM

El papel del IAM en la evaluación y las pruebas de resiliencia

Para realizar una evaluación o una prueba de resiliencia, la próxima generación de Resilience Hub debe poder asumir una función de IAM. Las evaluaciones requieren permisos de solo lectura para

descubrir y comprender la configuración de sus recursos. AWS Las pruebas de resiliencia también requieren permisos para iniciar y gestionar AWS Fault Injection Service (AWS FIS) experimentos en tu nombre.

Puede crear un rol de IAM en la consola de AWS IAM. Elija una política de confianza personalizada y utilice una política de confianza como la siguiente:

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

Para los permisos, adjunte la política `AWSResilienceHubV2AssessmentExecutionPolicy` gestionada. Esta política otorga acceso de solo lectura a AWS los servicios para el descubrimiento, la evaluación y la administración de la resiliencia.

> **Note**
>
> `AWSResilienceHubV2AssessmentExecutionPolicy`Sustituye al anterior `AWSResilienceHubAsssessmentExecutionPolicy` para su uso por el de la próxima generación de Resilience Hub. Para obtener más detalles acerca de los permisos incluidos en esta política, consulte AWSResilienceHubV2AssessmentExecutionPolicy.

Si utilizas pruebas de resiliencia, adjunta también la política `AWSResilienceHubResilienceTestingPolicy` gestionada. Esta política otorga a Resilience Hub los AWS FIS permisos necesarios para iniciar y gestionar experimentos en tu nombre.

> **Note**
>
> Si la política gestionada no está disponible en tu cuenta, crea una política integrada con los mismos permisos. Para ver el contenido de la política, consulteAWSResilienceHubResilienceTestingPolicy.

Función de IAM Service-Linked

La próxima generación de Resilience Hub crea automáticamente un Service-Linked rol con la política `AWSResilienceHubServiceRolePolicy` administrada.

Permisos de acceso a los archivos estatales de Terraform

Si va a incluir los archivos de estado de Terraform en su servicio Resilience Hub de próxima generación, conceda permisos para leer los archivos de Terraform desde su bucket de Amazon S3 con una política como la siguiente:

```
{
  "Version": "2012-10-17"       ,
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::s3-bucket-name/path-to-state-file"
    },
    {
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::s3-bucket-name"
    }
  ]
}
```

Función de ejecución de IAM para las pruebas de resiliencia

Las pruebas de resiliencia se ejecutan bajo una función de IAM que AWS Fault Injection Service supone inyectar errores en sus recursos. Los permisos necesarios dependen de la plantilla de prueba, y las pruebas de una sola cuenta y de varias cuentas utilizan estructuras de roles diferentes.

Para ver las políticas de confianza y permisos de cada prueba, consulte. Funciones de ejecución de IAM para las pruebas de resiliencia

Permisos de Amazon EKS

Si va a incluir clústeres de Amazon EKS en su servicio de Resilience Hub de próxima generación, siga el siguiente proceso de 3 pasos para conceder permisos a Resilience Hub de próxima generación para leer los datos de configuración de sus clústeres de Amazon EKS mediante el control de acceso basado en roles (RBAC) de Kubernetes.

Paso 1: aplique lo siguiente a su clúster de Amazon EKS

Esto otorga a Resilience Hub de última generación acceso de solo lectura a los recursos de Kubernetes que necesita en todos los espacios de nombres:

```
cat << EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: resilience-hub-eks-access-cluster-role
rules:
- apiGroups:
    - ""
  resources:
    - pods
    - replicationcontrollers
    - nodes
    - services
  verbs:
    - get
    - list
- apiGroups:
    - apps
  resources:
    - deployments
    - replicasets
  verbs:
    - get
    - list
- apiGroups:
    - policy
  resources:
```

```
    - poddisruptionbudgets
  verbs:
    - get
    - list
- apiGroups:
    - autoscaling.k8s.io
  resources:
    - verticalpodautoscalers
  verbs:
    - get
    - list
- apiGroups:
    - autoscaling
  resources:
    - horizontalpodautoscalers
  verbs:
    - get
    - list
- apiGroups:
    - karpenter.sh
  resources:
    - provisioners
    - nodepools
  verbs:
    - get
    - list
- apiGroups:
    - karpenter.k8s.aws
  resources:
    - awsnodetemplates
    - ec2nodeclasses
  verbs:
    - get
    - list
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: resilience-hub-eks-access-cluster-role-binding
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
```

```
  kind: ClusterRole
  name: resilience-hub-eks-access-cluster-role
  apiGroup: rbac.authorization.k8s.io
---
EOF
```

Paso 2: Asigne la función de IAM al grupo de Kubernetes

Asigne el rol de IAM que creó al grupo de Kubernetes. `resilience-hub-eks-access-group` Puede utilizar las entradas de acceso de Amazon EKS (recomendado) o las. `aws-auth` ConfigMap

Opción A: usar las entradas de acceso de EKS (recomendado)

Las entradas de acceso EKS son el método preferido para administrar la autenticación de clústeres. El clúster debe utilizar el modo de `API_AND_CONFIG_MAP` autenticación `API` o.

```
aws eks create-access-entry \
  --cluster-name cluster-name \
  --principal-arn arn:aws:iam::ACCOUNT-ID:role/ResilienceHubRole \
  --type STANDARD \
  --kubernetes-groups '["resilience-hub-eks-access-group"]'
```

Opción B: usar aws-auth ConfigMap

Si su clúster usa el modo de `API_AND_CONFIG_MAP` autenticación `CONFIG_MAP` o, puede editar el aws-auth en su lugar: ConfigMap

Con eksctl:

```
eksctl create iamidentitymapping \
  --cluster cluster-name \
  --region region \
  --arn arn:aws:iam::ACCOUNT-ID:role/ResilienceHubRole \
  --group resilience-hub-eks-access-group \
  --username AwsResilienceHubAssessmentEKSAccessRole
```

O edite manualmente: ConfigMap

```
kubectl edit -n kube-system configmap/aws-auth
```

Añada esto `mapRoles` en la sección de datos:

```
- groups:
    - resilience-hub-eks-access-group
  rolearn: arn:aws:iam::ACCOUNT-ID:role/ResilienceHubRole
  username: AwsResilienceHubAssessmentEKSAccessRole
```

Paso 3: Verificar

Confirme que los recursos de RBAC existen y que la asignación de funciones está establecida:

```
kubectl get clusterrole resilience-hub-eks-access-cluster-role
kubectl describe clusterrolebinding resilience-hub-eks-access-cluster-role-binding
```

Si utiliza entradas de acceso (opción A):

```
aws eks describe-access-entry \
  --cluster-name cluster-name \
  --principal-arn arn:aws:iam::ACCOUNT-ID:role/ResilienceHubRole
```

Si usa aws-auth ConfigMap (opción B):

```
kubectl get configmap aws-auth -n kube-system -o yaml | grep -A 3 "ResilienceHubRole"
```

Cifrado de datos

La próxima generación de Resilience Hub cifra sus datos para ayudar a protegerlos del acceso no autorizado.

Cifrado en reposo

Todos los datos de Resilience Hub de próxima generación se cifran en reposo.

Almacén de datos	Cifrado
Tablas de DynamoDB	AWS-claves administradas (predeterminadas) o claves administradas por el cliente AWS KMS
Objetos S3 (topología, resultados de la evaluación)	SSE-S3 (predeterminado) o SSE-KMS con claves administradas por el cliente

Cifrado en reposo con claves gestionadas por el cliente

Resilience Hub de última generación proporciona cifrado de forma predeterminada para proteger los datos confidenciales de los clientes que están en reposo. Claves propiedad de AWS

- La próxima generación de Resilience Hub utiliza estas claves de forma predeterminada para cifrar automáticamente los datos confidenciales. No puede ver, administrar Claves propiedad de AWS, usar ni auditar su uso. Sin embargo, no tiene que realizar ninguna acción ni cambiar ningún programa para proteger las claves que cifran sus datos. Para obtener más información, consulte https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#aws-owned-cmk en la Guía para desarrolladores de AWS Key Management Service .

Si bien no puede deshabilitar esta capa de cifrado ni seleccionar un tipo de cifrado alternativo, puede agregar una segunda capa de cifrado especificando una clave administrada por el cliente al crear un recurso de servicio:

- Claves administradas por el cliente La próxima generación de Resilience Hub admite el uso de una clave de cifrado simétrico administrada por el cliente que usted crea, posee y administra. Como usted tiene el control total de este cifrado, puede realizar dichas tareas como:
  - Establecer y mantener políticas de claves
  - Establecer y mantener concesiones y políticas de IAM
  - Habilitar y deshabilitar políticas de claves
  - Rotar el material criptográfico
  - Adición de etiquetas de

- Crear alias de clave
- Programar la eliminación de claves

Para obtener más información, consulte las claves administradas por el cliente en la Guía para desarrolladores de AWS Key Management Service .

La siguiente tabla resume cómo Resilience Hub de próxima generación cifra los datos confidenciales.

Cifrado de tipos de datos en Resilience Hub de próxima generación

Tipo de datos:	AWS cifrado de clave propia	Cifrado de claves gestionado por el cliente (opcional)
`description` Descripciones de los servicios, los sistemas y las políticas de resiliencia.	Habilitado	Habilitado
`finding` La evaluación busca nombres, descripciones, razonamientos y comentarios.	Habilitado	Habilitado
`recommendation` Descripciones de las recomendaciones y cambios sugeridos relacionados con los hallazgos.	Habilitado	Habilitado
`serviceFunction` Nombres y descripciones de las funciones de servicio.	Habilitado	Habilitado
`assumption` Texto de suposición asociado a las funciones de servicio.	Habilitado	Habilitado

Tipo de datos:	AWS cifrado de clave propia	Cifrado de claves gestionado por el cliente (opcional)
`userJourney` Descripciones de los viajes del usuario.	Habilitado	Habilitado
`event` Descripciones del registro de eventos de servicio.	Habilitado	Habilitado
`assessmentData` Datos intermedios generados por los flujos de trabajo de evaluación de los agentes, incluida la topología, la configuración de los recursos y los datos de trabajo almacenados en Amazon S3.	Habilitado	Habilitado
Identificadores de recursos Nombres de recursos, ARN, tipos de recursos y regiones. Los nombres de los recursos se utilizan en el contexto de los identificadores y el cifrado y no deben contener datos confidenciales.	Habilitado	No compatible

> **Note**
>
> La nueva generación de Resilience Hub permite automáticamente el cifrado en Claves propiedad de AWS reposo sin coste alguno. Sin embargo, se aplican AWS KMS cargos por el uso de una clave administrada por el cliente. Para obtener más información acerca de los precios, consulte Precios de AWS Key Management Service.

> **Important**
>
> La próxima generación de Resilience Hub solo admite claves KMS de cifrado simétrico. No puede usar ningún otro tipo de clave KMS para cifrar los recursos de Resilience Hub de próxima generación. Para obtener ayuda para determinar si una clave KMS es una clave de cifrado simétrica, consulte Identificación de claves KMS simétricas y asimétricas en la Guía para desarrolladores.AWS Key Management Service

Cómo utiliza Resilience Hub de próxima generación las subvenciones en AWS KMS

La próxima generación de Resilience Hub requiere una subvención para utilizar su clave gestionada por el cliente durante los flujos de trabajo de evaluación asincrónica.

Cuando crea un servicio con una clave gestionada por el cliente, Resilience Hub de próxima generación crea una subvención en su nombre enviando una CreateGrantsolicitud a. AWS KMS La concesión se limita al contexto de cifrado de su servicio y solo permite las siguientes operaciones:

- `Encrypt`— Cifre los campos confidenciales, como las conclusiones, las recomendaciones y las suposiciones generadas durante los flujos de trabajo de evaluación.
- `Decrypt`— Descifre los datos previamente cifrados durante el procesamiento de la evaluación.
- `GenerateDataKey`— Genere claves de datos para cifrar los datos de evaluación intermedia almacenados en Amazon S3.

La subvención se retira cuando se elimina el servicio. También puedes revocar el acceso a la concesión o eliminar el acceso del servicio a la clave gestionada por el cliente en cualquier momento. Si lo hace, Resilience Hub de próxima generación no podrá acceder a ninguno de los datos cifrados por la clave gestionada por el cliente, lo que afectará a las operaciones de la API y a los flujos de trabajo de evaluación que dependen de esos datos.

Para las operaciones de API sincrónicas (como crear o actualizar un servicio), Resilience Hub de última generación utiliza directamente los permisos de la persona que llama en la clave KMS, sin necesidad de concederlos.

Creación de una clave administrada por el cliente

Puede crear una clave de cifrado simétrico gestionada por el cliente mediante las API Consola de administración de AWS o las API. AWS KMS

Para crear una clave de cifrado simétrico gestionada por el cliente

Siga los pasos de Creación de claves de KMS de cifrado simétricas en la Guía para desarrolladores de AWS Key Management Service .

Especificar una clave gestionada por el cliente para Resilience Hub de próxima generación

Puede especificar una clave gestionada por el cliente al crear un servicio, un sistema o una política de resiliencia. Cuando proporciona un identificador de clave de KMS, Resilience Hub de próxima generación utiliza esa clave para cifrar todos los datos confidenciales asociados al recurso.

Puede especificar la clave mediante cualquiera de los siguientes identificadores clave:

- ID de clave (por ejemplo,`1234abcd-12ab-34cd-56ef-1234567890ab`)
- ARN clave (por ejemplo,) `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`
- Nombre de alias (por ejemplo,`alias/my-key`)
- Alias ARN (por ejemplo,) `arn:aws:kms:us-west-2:111122223333:alias/my-key`

Para especificar una clave gestionada por el cliente, utilice el `kmsKeyId` parámetro al llamar a las operaciones `CreateServiceCreateSystem`, o de la `CreatePolicy` API.

Política de claves

Las políticas de clave controlan el acceso a la clave administrada por el cliente. Cada clave administrada por el cliente debe tener exactamente una política de clave, que contiene instrucciones que determinan quién puede usar la clave y cómo puede utilizarla. Cuando crea la clave administrada por el cliente, puede especificar una política de clave. Para obtener más información, consulte Administración del acceso a las claves en la Guía para desarrolladores de AWS Key Management Service .

La siguiente política clave permite que Resilience Hub de próxima generación utilice su clave. Limita cada permiso únicamente a las operaciones que requiere la próxima generación de Resilience Hub, y utiliza condiciones de contexto de cifrado para garantizar que su clave solo se pueda utilizar para sus recursos específicos. Reemplace *CUSTOMER-ACCOUNT-ID* *CUSTOMER-ROLE* y *REGION* con sus valores.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "AllowResilienceHubDescribeKey",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::CUSTOMER-ACCOUNT-ID:role/CUSTOMER-ROLE"
            },
            "Action": "kms:DescribeKey",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "resiliencehub.REGION.amazonaws.com"
                }
            }
        },
        {
            "Sid": "AllowResilienceHubEncryptDecryptForServices",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::CUSTOMER-ACCOUNT-ID:role/CUSTOMER-ROLE"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "resiliencehub.REGION.amazonaws.com"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:resiliencehub:service-arn":
"arn:aws:resiliencehub:*:CUSTOMER-ACCOUNT-ID:service/*"
                }
            }
        },
        {
            "Sid": "AllowResilienceHubEncryptDecryptForSystems",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::CUSTOMER-ACCOUNT-ID:role/CUSTOMER-ROLE"
            },
            "Action": [
                "kms:Encrypt",
```

```
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "resiliencehub.REGION.amazonaws.com"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:resiliencehub:system-arn":
"arn:aws:resiliencehub:*:CUSTOMER-ACCOUNT-ID:system/*"
                }
            }
        },
        {
            "Sid": "AllowResilienceHubEncryptDecryptForPolicies",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::CUSTOMER-ACCOUNT-ID:role/CUSTOMER-ROLE"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "resiliencehub.REGION.amazonaws.com"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:resiliencehub:policy-arn":
"arn:aws:resiliencehub:*:CUSTOMER-ACCOUNT-ID:policy/*"
                }
            }
        },
        {
            "Sid": "AllowResilienceHubCreateGrantForAsyncWorkflows",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::CUSTOMER-ACCOUNT-ID:role/CUSTOMER-ROLE"
            },
            "Action": "kms:CreateGrant",
            "Resource": "*",
```

```
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "resiliencehub.REGION.amazonaws.com",
                    "kms:GrantConstraintType": "EncryptionContextSubset"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:resiliencehub:service-arn":
 "arn:aws:resiliencehub:*:CUSTOMER-ACCOUNT-ID:service/*"
                },
                "ForAllValues:StringEquals": {
                    "kms:GrantOperations": [
                        "Encrypt",
                        "Decrypt",
                        "GenerateDataKey"
                    ]
                }
            }
        }
    ]
}
```

Las declaraciones de política proporcionan los siguientes permisos:

- AllowResilienceHubDescribeKey— Permite que Resilience Hub, de última generación, valide que su clave existe y que es una clave de cifrado simétrica cuando la especifica durante la creación del servicio.
- AllowResilienceHubEncryptDecryptForServices— Permite a Resilience Hub de última generación cifrar y descifrar datos de nivel de servicio (hallazgos, recomendaciones, suposiciones, funciones del servicio, eventos y datos de evaluación) durante las llamadas sincrónicas a la API. Se ajusta a sus recursos de servicio por contexto de cifrado.
- AllowResilienceHubEncryptDecryptForSystems— Permite que Resilience Hub, de última generación, cifre y descifre los datos a nivel del sistema (descripciones del sistema y descripciones del recorrido del usuario) durante las llamadas sincrónicas a la API. Se basa en los recursos del sistema por contexto de cifrado.
- AllowResilienceHubEncryptDecryptForPolicies— Permite a Resilience Hub, de última generación, cifrar y descifrar datos a nivel de políticas (descripciones de las políticas de resiliencia) durante las llamadas sincrónicas a la API. Se basa en los recursos de su política por contexto de cifrado.
- AllowResilienceHubCreateGrantForAsyncWorkflows— Permite que Resilience Hub, de próxima generación, cree una subvención para flujos de trabajo de evaluación asíncronos. La concesión se

limita únicamente a las operaciones necesarias (cifrar, descifrar GenerateDataKey) y debe incluir una restricción de subconjunto de contexto de cifrado vinculada al ARN de su servicio.

Para obtener más información sobre cómo especificar permisos en una política, consulte la Guía para desarrolladores de AWS Key Management Service .

Para obtener información sobre la solución de problemas de acceso a las claves, consulte la Guía para desarrolladores de AWS Key Management Service .

Contexto de cifrado de Resilience Hub de última generación

Un contexto de cifrado es un conjunto opcional de pares clave-valor que pueden contener información contextual adicional sobre los datos.

AWS KMS utiliza el contexto de cifrado como datos autenticados adicionales para respaldar el cifrado autenticado. Al incluir un contexto de cifrado en una solicitud de cifrado de datos, AWS KMS vincula el contexto de cifrado a los datos cifrados. Para descifrar los datos, debe incluir el mismo contexto de cifrado en la solicitud.

Contexto de cifrado Resilience Hub de última generación

La próxima generación de Resilience Hub utiliza las siguientes claves de contexto de cifrado según el tipo de recurso:

Claves de contexto de cifrado

Clave de contexto de cifrado	Alcance	Utilizado para
`aws:resiliencehub:service-arn`	Servicio	Hallazgos, recomendaciones, suposiciones, funciones de servicio, dependencias, eventos y datos de evaluación
`aws:resiliencehub:system-arn`	Sistema	Descripciones del sistema y descripciones del recorrido del usuario
`aws:resiliencehub:policy-arn`	Política	Descripciones de las políticas de resiliencia

Ejemplo de contexto de cifrado para una operación de nivel de servicio:

```
"encryptionContext": {
    "aws:resiliencehub:service-arn": "arn:aws:resiliencehub:us-
west-2:111122223333:service/my-service:abc123"
}
```

Uso del contexto de cifrado para la supervisión

Si utiliza una clave de cifrado simétrico gestionada por el cliente para cifrar sus datos, puede utilizar el contexto de cifrado en los registros y registros de auditoría para identificar cómo se utiliza la clave gestionada por el cliente. El contexto de cifrado aparece en los registros generados por. AWS CloudTrail

Uso del contexto de cifrado para controlar el acceso

Puede utilizar el contexto de cifrado en las políticas clave y en las políticas de IAM `conditions` para controlar el acceso a su clave de cifrado simétrico gestionada por el cliente. Puede usar también una restricción de contexto de cifrado en una concesión.

La próxima generación de Resilience Hub utiliza una restricción de subconjunto del contexto de cifrado en las subvenciones para garantizar que los flujos de trabajo asíncronos solo puedan cifrar y descifrar los datos que pertenezcan al servicio específico para el que se creó la subvención.

Supervisión de sus claves de cifrado para Resilience Hub de última generación

Cuando utiliza una clave gestionada por el cliente con sus recursos de Resilience Hub de próxima generación, puede utilizarla AWS CloudTrailpara realizar un seguimiento de las solicitudes que envía Resilience Hub de próxima generación AWS KMS.

CreateGrant

Cuando crea un servicio con una clave gestionada por el cliente, Resilience Hub de próxima generación envía una `CreateGrant` solicitud en su nombre para permitir que los flujos de trabajo de evaluación asincrónica utilicen su clave. La concesión es específica del servicio y está limitada por el contexto de cifrado. Resilience Hub, de última generación, se utiliza `RetireGrant` para eliminar la subvención cuando se elimina el servicio.

El siguiente evento de ejemplo registra la operación `CreateGrant`:

```
{
    "eventVersion": "1.11",
    "userIdentity": {
```

```
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLE:session-name",
        "arn": "arn:aws:sts::111122223333:assumed-role/YourRole/session-name",
        "accountId": "111122223333",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/YourRole",
                "accountId": "111122223333",
                "userName": "YourRole"
            }
        },
        "invokedBy": "resiliencehub.amazonaws.com"
    },
    "eventTime": "2026-01-15T10:07:22Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "resiliencehub.amazonaws.com",
    "userAgent": "resiliencehub.amazonaws.com",
    "requestParameters": {
        "granteePrincipal": "resiliencehub.amazonaws.com",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "retiringPrincipal": "resiliencehub.amazonaws.com",
        "operations": [
            "Decrypt",
            "GenerateDataKey",
            "Encrypt"
        ],
        "constraints": {
            "encryptionContextSubset": {
                "aws:resiliencehub:service-arn": "arn:aws:resiliencehub:us-
west-2:111122223333:service/my-service:abc123"
            }
        }
    },
    "responseElements": {
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
```

```
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "56d4e434-abb6-4dd7-8558-ad38560d03b1",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

GenerateDataKey

Cuando Resilience Hub de última generación cifra los datos con la clave gestionada por el cliente, envía una `GenerateDataKey` solicitud para generar una clave de datos. Esto ocurre tanto durante las llamadas a la API sincrónicas (por ejemplo, al crear un servicio con una descripción) como en los flujos de trabajo de evaluación asíncronos.

El siguiente evento de ejemplo registra la operación `GenerateDataKey`:

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "resiliencehub.amazonaws.com"
    },
    "eventTime": "2026-01-15T11:18:36Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "resiliencehub.amazonaws.com",
    "userAgent": "resiliencehub.amazonaws.com",
    "requestParameters": {
        "numberOfBytes": 32,
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "encryptionContext": {
```

```
            "aws:resiliencehub:service-arn": "arn:aws:resiliencehub:us-
west-2:111122223333:service/my-service:abc123",
            "aws-crypto-public-key": "AwAnnorjRE
+DFQYIuDKjGEvlXwro5Rdiegk8flmq7m0N..."
        }
    },
    "responseElements": null,
    "requestID": "c5bedc9b-e6d6-45f8-b121-c9851a3d718a",
    "eventID": "e839a7ed-e4a9-32a3-b92a-2c7237a40c82",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Decrypt

Cuando recupera recursos mediante operaciones de API o cuando los flujos de trabajo de evaluación procesan datos previamente almacenados, Resilience Hub de próxima generación envía `Decrypt` solicitudes para descifrar los datos.

El siguiente evento de ejemplo registra la operación `Decrypt`:

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLE:session-name",
        "arn": "arn:aws:sts::111122223333:assumed-role/YourRole/session-name",
        "accountId": "111122223333",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLE",
```

```
                "arn": "arn:aws:iam::111122223333:role/YourRole",
                "accountId": "111122223333",
                "userName": "YourRole"
            }
        },
        "invokedBy": "resiliencehub.amazonaws.com"
    },
    "eventTime": "2026-01-15T11:27:49Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "resiliencehub.amazonaws.com",
    "userAgent": "resiliencehub.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "encryptionContext": {
            "aws:resiliencehub:service-arn": "arn:aws:resiliencehub:us-
west-2:111122223333:service/my-service:abc123",
            "aws-crypto-public-key": "A/9P3BC05WjeQONZR1fBiEqWKEse/
Yk1lMxd2VIh2ED5..."
        }
    },
    "responseElements": null,
    "requestID": "30f8e9bc-4e0a-4359-8bc3-8278ef42c206",
    "eventID": "195ef070-c952-4c28-9883-29bca297a08c",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

DescribeKey

La próxima generación de Resilience Hub envía `DescribeKey` solicitudes para comprobar que la clave gestionada por el cliente asociada a su servicio existe en la cuenta y la región y es una clave de cifrado simétrica válida.

El siguiente evento de ejemplo registra la operación `DescribeKey`:


```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLE:session-name",
        "arn": "arn:aws:sts::111122223333:assumed-role/YourRole/session-name",
        "accountId": "111122223333",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/YourRole",
                "accountId": "111122223333",
                "userName": "YourRole"
            }
        },
        "invokedBy": "resiliencehub.amazonaws.com"
    },
    "eventTime": "2026-01-15T10:07:13Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "resiliencehub.amazonaws.com",
    "userAgent": "resiliencehub.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": null,
    "requestID": "e427932c-448b-49aa-88e1-b311c27ba753",
    "eventID": "48c596a5-83c7-4603-b0cf-be0ff2548623",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
```

```
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Más información

Los siguientes recursos proporcionan más información sobre cifrado de datos en reposo.

- Para obtener más información acerca de los conceptos básicos de AWS Key Management Service, consulte la Guía para desarrolladores de AWS Key Management Service .
- Para obtener más información sobre las prácticas recomendadas de seguridad AWS Key Management Service, consulte la Guía para AWS Key Management Service desarrolladores.

Cifrado en tránsito

Todos los datos en tránsito se cifran mediante TLS 1.2 o una versión posterior, lo que incluye:

- Llamadas a la API a los puntos finales de Resilience Hub de próxima generación
- Cross-service comunicación (del Resilience Hub de última generación al servicio de topología, del Resilience Hub de próxima generación a Amazon Bedrock)
- Cross-account transferencia de credenciales (cifrada antes de la transmisión) AWS KMS

Puntos de conexión de VPC

Puedes crear un punto de enlace de VPC para Resilience Hub de próxima generación a fin de mantener el tráfico entre tu VPC y el servicio dentro de la AWS red, sin necesidad de atravesar la Internet pública. Esto se utiliza AWS PrivateLink para la conectividad privada.

Puede usar los puntos de enlace de la VPC para conectar de forma privada su VPC a la próxima generación de Resilience Hub sin necesidad de que el tráfico atraviese la Internet pública.

CloudTrail integración

Resilience Hub de próxima generación se integra con AWS CloudTrail (CloudTrail) para registrar todas las llamadas a la API realizadas al servicio, incluidas las llamadas desde la consola de Resilience Hub de próxima generación y las llamadas programáticas a la API de Resilience Hub de próxima generación.

Consideraciones de conformidad

Para obtener información sobre los programas de cumplimiento que se aplican a la próxima generación de Resilience Hub, consulte el ámbito de AWS los servicios según el programa de cumplimiento.

Retención de datos

La siguiente tabla muestra los períodos de retención de los datos almacenados en Resilience Hub de próxima generación.

Tipo de datos:	Retención
Resultados de la evaluación y hallazgos del modo de falla	2 años
Registros de eventos del sistema y del servicio	2 años
Recursos detectados	1 año de TTL
Instantáneas de topología	2 años
Datos de dependencia	Duración de la habilitación más 30 días retrospectiva

Manejo de datos de IA generativa

Las evaluaciones del modo de fallo utilizan Amazon Bedrock para la inferencia de inteligencia artificial. Se aplican las siguientes prácticas de manejo de datos:

- Los datos de los clientes se procesan de la Región de AWS misma manera que el servicio
- Los datos no se utilizan para entrenar o mejorar los modelos básicos

- Las entradas y los resultados de la evaluación se almacenan en cubos Resilience Hub-owned S3 de próxima generación, cifrados en reposo
- Los clientes pueden optar por excluirse por completo de las funciones de IA generativa

Recomendaciones de privilegios mínimos

Siga estas recomendaciones para aplicar los principios de privilegios mínimos a su configuración de Resilience Hub de próxima generación:

1. ExternalId Utilízalo para funciones multicuenta: `ExternalId` esta condición incluida en las políticas de confianza entre cuentas evita que los diputados puedan cometer ataques confusos.
2. Usa Service-Linked los roles organizacionales: evita la configuración manual de los roles entre cuentas siempre que sea posible. Service-Linked Los roles proporcionan un acceso auditable y con alcance automático.

Monitorización del Resilience Hub de próxima generación

Puede supervisar la próxima generación de Resilience Hub con Amazon CloudWatch y Amazon EventBridge para realizar un seguimiento de la actividad de evaluación, detectar problemas y automatizar las respuestas. AWS CloudTrail

Temas

- CloudWatch referencia de métricas
- CloudTrail registro de eventos
- EventBridge notificaciones
- Configuración de CloudWatch alarmas para el Resilience Hub de próxima generación

CloudWatch referencia de métricas

Cuando una evaluación del modo de fallo se completa correctamente, Next Generation Resilience Hub publica las métricas de cumplimiento de las políticas en el Amazon CloudWatch (CloudWatch) de tu cuenta, en el espacio de `ResilienceHub` nombres. Las métricas se emiten solo una vez finalizada la evaluación. Si no se ha realizado ninguna evaluación o si la evaluación no arrojó resultados alcanzables, no se informa de ninguna métrica.

El modelo de permisos de tu servicio debe incluir una función de invocador que permita a Next Generation Resilience Hub emitir métricas a tu cuenta. `cloudwatch:PutMetricData`

Métricas de evaluación

Las siguientes métricas se emiten después de cada evaluación exitosa del modo de falla. Se publica un punto de datos por cada componente de política que contiene los resultados de la evaluación.

Métrica	Dimensiones	Description (Descripción)	Valores
`PolicyAchievable`	`Service`, `PolicyComponent=AvailabilitySlo`	Si su objetivo de SLO de disponibilidad es alcanzable.	1.0 o 0.0
`PolicyAchievable`	`Service`, `PolicyComponent=MultiAzRtoRpo`	Si sus objetivos de RTO y RPO Multi-AZ son alcanzables.	1.0 o 0.0
`PolicyAchievable`	`Service`, `PolicyComponent=MultiRegionRtoRpo`	Si sus objetivos de RTO y RPO multirregionales son alcanzables.	1.0 o 0.0

En la siguiente tabla se describen las dimensiones métricas.

Dimensión	Description (Descripción)
`Service`	El nombre del servicio que se está evaluando.
`PolicyComponent`	El componente de la política de resiliencia que se está evaluando. Valores posibles: `AvailabilitySlo` , `MultiAzRtoRpo` , `MultiRegionRtoRpo` .

> **Note**
>
> Solo se emiten los componentes políticos para los que la evaluación arroja un resultado de viabilidad.

Utilice la `Minimum` estadística al crear alarmas en esta métrica. Un valor `Minimum` de 0.0 indica que al menos una evaluación determinó que la política no se podía cumplir durante el período de evaluación.

CloudTrail registro de eventos

La próxima generación de Resilience Hub está integrada con AWS CloudTrail (CloudTrail). Todas las llamadas a la API se registran como eventos CloudTrail, incluidas las llamadas desde la consola de próxima generación de Resilience Hub y las llamadas programáticas a la API de Resilience Hub de próxima generación.

Eventos compatibles con el Resilience Hub de próxima generación

Se ha iniciado sesión en todas las acciones de la API de Resilience Hub de próxima generación CloudTrail, incluidas las siguientes.

Categoría	Eventos de ejemplo
Sistemas	`CreateSystem` , `DeleteSystem` , `GetSystem` , `ListSystems`
Services	`CreateService` , `UpdateService` , `DeleteService` , `ListServices`
Políticas	`CreateResiliencePolicy` , `UpdateResiliencePolicy` , `DeleteResiliencePolicy`
Evaluaciones	`StartFailureModeAssessment` , `GetFailureModeAssessment` , `ListFailureModeFindings`
Discovery	`StartServiceTopologyDiscovery` , `ListDependencies` , `ClassifyDependency`

Categoría	Eventos de ejemplo
Pruebas de resiliencia	`CreateTest` , `GetTest`, `ListTests` , `UpdateTest` , `DeleteTest` , `StartTestRun` , `StopTestRun` , `GetTestRun` , `ListTestRuns` , `ListTestTemplates` , `GetTestTemplate` , `PutTestSources` , `DeleteTestSources` , `ListTestSources` , `ListTestRunSources` , `ListTestRunEvents` , `ListResolvedTestRunTargetResources`

Ejemplo de CloudTrail evento

El siguiente es un ejemplo de CloudTrail evento para una llamada a la `StartFailureModeAssessment` API.

```
{
  "eventVersion": "1.08",
  "eventSource": "resiliencehub.amazonaws.com",
  "eventName": "StartFailureModeAssessment",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.1",
  "userAgent": "aws-cli/2.x",
  "requestParameters": {
    "serviceArn": "arn:aws:resiliencehub:us-east-1:123456789012:service/
checkout:abc123"
  },
  "responseElements": {
    "assessmentId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "status": "PENDING"
  }
}
```

EventBridge notificaciones

Con Amazon EventBridge, puede supervisar los recursos de la próxima generación de Resilience Hub mediante reglas basadas en eventos. Estas reglas pueden desencadenar acciones en otros AWS servicios. Por ejemplo, puede crear una regla que señale un tema de Amazon SNS cada vez que finalice una evaluación del modo de fallo o se descubra una nueva dependencia.

Puede crear reglas EventBridge para actuar en relación con los siguientes eventos de la próxima generación de Resilience Hub:

- Evaluación del modo de falla completada: se emite cuando una evaluación del modo de falla se completa correctamente.
- Falló la evaluación del modo de falla: se emite cuando falla un flujo de trabajo de evaluación del modo de falla.
- Evaluación en modo de fallo en cola: se emite cuando una evaluación está en cola para su procesamiento retrasado. La evaluación se vuelve a intentar en un plazo de 24 horas.
- Búsqueda del modo de falla resuelta: se emite cuando la búsqueda de un modo de falla se marca como resuelta o irrelevante.
- Se descubrió una nueva dependencia: se emite cuando el descubrimiento de una dependencia identifica una nueva dependencia para su servicio.

Para capturar los eventos específicos de la próxima generación de Resilience Hub que te interesen, define patrones específicos para cada evento que EventBridge puedas usar para detectarlos. Los patrones de eventos de tienen la misma estructura que los eventos con los que coinciden. El patrón cita los campos para los que se desea encontrar coincidencias y proporciona los valores que está buscando.

La próxima generación de Resilience Hub emite los eventos en la medida de lo posible y los envía prácticamente EventBridge en tiempo real cuando el servicio funciona con normalidad. Sin embargo, algunas situaciones pueden retrasar o impedir la entrega de los eventos.

Para obtener más información sobre EventBridge las reglas y los patrones de eventos, consulte Eventos y patrones de eventos en EventBridge.

Crear una EventBridge regla para los eventos de la próxima generación de Resilience Hub

Con EventBridge ella, puedes crear reglas que definan las acciones que debes tomar cuando la próxima generación de Resilience Hub emita eventos para tus servicios.

La próxima generación de Resilience Hub emite todos los eventos con la fuente. `aws.resiliencehub` Tu patrón de eventos debe incluir esta fuente para que coincida con los eventos de la próxima generación de Resilience Hub. Puedes filtrar aún más `detail-type` para que coincidan con tipos de eventos específicos.

Para introducir o pegar un patrón de eventos en la EventBridge consola, elige la opción Introducir mi propio patrón. Para ayudarte a determinar los patrones de eventos que pueden resultar útiles, este tema incluyeEjemplos de patrones de eventos y eventos.

Para crear una regla para un evento de la próxima generación de Resilience Hub

1. Abre la EventBridge consola en https://console.aws.amazon.com/events/.
2. Para ello Región de AWS, elija la región en la que se implementará su servicio en la próxima generación de Resilience Hub.
3. Seleccione Creación de regla.
4. Ingrese un Name (Nombre) para la regla y opcionalmente, una descripción.
5. Para Bus de eventos, deje el valor predeterminado, predeterminado.
6. Elija Siguiente.
7. Para la fuente del evento, deje el valor predeterminado, AWS events.
8. En Patrón de eventos, elija Introducir lo mío.
9. Ingresa o pega un patrón de eventos que incluya `"source": ["aws.resiliencehub"]` y el que `detail-type` quieras combinar. Para ver ejemplos, consulte Ejemplos de patrones de eventos y eventos.
10. Seleccione Siguiente y configure su objetivo (por ejemplo, un tema de Amazon SNS, una función de Lambda o un grupo de CloudWatch registros).
11. Complete el flujo de trabajo de creación de reglas seleccionando Crear regla.

Ejemplos de patrones de eventos y eventos

Los patrones de eventos de tienen la misma estructura que los eventos con los que coinciden. El patrón cita los campos para los que se desea encontrar coincidencias y proporciona los valores que está buscando.

Puedes copiar y pegar los patrones de eventos de esta sección EventBridge para crear reglas que supervisen los eventos de la próxima generación de Resilience Hub.

Seleccione todos los eventos de finalización de la evaluación en modo de falla

El siguiente patrón coincide con todas las evaluaciones finalizadas.

```
{
```

```
  "source": ["aws.resiliencehub"],
  "detail-type": ["Failure Mode Assessment Completed"]
}
```

Seleccione todos los eventos de error en la evaluación del modo de falla

El siguiente patrón coincide con todas las evaluaciones fallidas.

```
{
  "source": ["aws.resiliencehub"],
  "detail-type": ["Failure Mode Assessment Failed"]
}
```

Seleccione todos los eventos de dependencia nuevos descubiertos

El siguiente patrón coincide con todos los eventos de dependencia nuevos.

```
{
  "source": ["aws.resiliencehub"],
  "detail-type": ["New Dependency Discovered"]
}
```

Seleccione todos los eventos de la próxima generación de Resilience Hub

El siguiente patrón coincide con todos los eventos independientemente del tipo.

```
{
  "source": ["aws.resiliencehub"]
}
```

Seleccione los eventos de evaluación con resultados de alta gravedad

El siguiente patrón coincide con las evaluaciones que identificaron al menos un hallazgo de alta gravedad.

```
{
  "source": ["aws.resiliencehub"],
  "detail-type": ["Failure Mode Assessment Completed"],
  "detail": {
    "highSeverityCount": [{"numeric": [">", 0]}]
```

```
  }
}
```

En las siguientes secciones se proporcionan ejemplos de eventos para cada tipo de evento.

Evento completado de la evaluación del modo de fallo

El siguiente es un ejemplo de evento emitido cuando una evaluación del modo de fallo finaliza correctamente.

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Failure Mode Assessment Completed",
  "source": "aws.resiliencehub",
  "account": "111122223333",
  "time": "2026-01-15T10:30:00Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:resiliencehub:us-east-1:111122223333:service/my-service:abc123"
  ],
  "detail": {
    "assessmentId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "status": "SUCCESS",
    "findingsCount": 5,
    "highSeverityCount": 2
  }
}
```

El objeto `detail` contiene los siguientes campos:

Campo	Description (Descripción)
`assessmentId`	El identificador único de la evaluación completada.
`status`	El estado de la evaluación. Valor:`SUCCESS`.
`findingsCount`	El número total de hallazgos de modos de falla identific ados.
`highSeverityCount`	El número de hallazgos de alta gravedad identificados.

Evento fallido en la evaluación del modo de falla

El siguiente es un ejemplo de evento emitido cuando falla una evaluación del modo de falla.

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Failure Mode Assessment Failed",
  "source": "aws.resiliencehub",
  "account": "111122223333",
  "time": "2026-01-15T10:30:00Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:resiliencehub:us-east-1:111122223333:service/my-service:abc123"
  ],
  "detail": {
    "assessmentId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "status": "FAILED",
    "failureReason": "Unable to assume the invoker role specified in the service
 configuration."
  }
}
```

El objeto `detail` contiene los siguientes campos:

Campo	Description (Descripción)
`assessmentId`	El identificador único de la evaluación fallida.
`status`	El estado de la evaluación. Valor:`FAILED`.
`failureReason`	Una descripción de por qué falló la evaluación.

Evento en cola de evaluación en modo de error

El siguiente es un ejemplo de evento emitido cuando una evaluación está en cola para su procesamiento retrasado. La evaluación se vuelve a intentar y finaliza en 24 horas.

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
```

```
  "detail-type": "Failure Mode Assessment Queued",
  "source": "aws.resiliencehub",
  "account": "111122223333",
  "time": "2026-01-15T10:30:00Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:resiliencehub:us-east-1:111122223333:service/my-service:abc123"
  ],
  "detail": {
    "assessmentId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222"
  }
}
```

El objeto `detail` contiene los siguientes campos:

Campo	Description (Descripción)
`assessmentId`	El identificador único de la evaluación en cola.

Cuando se completa la evaluación en cola, se emite un `Failure Mode Assessment Failed` evento `Failure Mode Assessment Completed` o independiente.

Modo de error al buscar un evento resuelto

El siguiente es un ejemplo de evento emitido cuando la detección de un modo de fallo se marca como Resuelta o Irrelevante.

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Failure Mode Finding Resolved",
  "source": "aws.resiliencehub",
  "account": "111122223333",
  "time": "2026-01-15T10:30:00Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:resiliencehub:us-east-1:111122223333:service/my-service:abc123"
  ],
  "detail": {
    "findingId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "status": "RESOLVED",
```

```
    "severity": "HIGH",
    "category": "SINGLE_POINT_OF_FAILURE"
  }
}
```

El objeto `detail` contiene los siguientes campos:

Campo	Description (Descripción)
`findingId`	El identificador único del hallazgo resuelto.
`status`	El estado de la resolución. Valores:`RESOLVED`,`IRRELEVANT` .
`severity`	La gravedad del hallazgo. Valores:`HIGH`,`MEDIUM`,`LOW`.
`category`	La categoría del modo de fallo (por ejemplo,`SINGLE_POINT_OF_FAILURE` ,`SHARED_FATE`).

Se descubrió un nuevo evento de dependencia

El siguiente es un ejemplo de evento emitido cuando el descubrimiento de dependencias identifica una nueva dependencia para tu servicio. Este evento se emite después de un período de estabilización para reducir el ruido durante la detección inicial.

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "New Dependency Discovered",
  "source": "aws.resiliencehub",
  "account": "111122223333",
  "time": "2026-01-15T10:30:00Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:resiliencehub:us-east-1:111122223333:service/my-service:abc123"
  ],
  "detail": {
    "dependencyId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "dependencyName": "S3",
    "dnsName": "s3.us-east-1.amazonaws.com.",
    "location": "us-east-1",
```

```
    "provider": "AWS",
    "sourceRegions": [
      "us-east-1",
      "us-west-2"
    ]
  }
}
```

El objeto `detail` contiene los siguientes campos:

Campo	Description (Descripción)
`dependencyId`	El identificador único de la dependencia descubierta.
`dependencyName`	El nombre de la dependencia (por ejemplo, el nombre del AWS servicio).
`dnsName`	El nombre DNS que usa el servicio para comunicarse con la dependencia.
`location`	La ubicación Región de AWS o donde está alojada la dependencia.
`provider`	El proveedor de la dependencia. Los valores incluyen `AWSThirdParty` ,`Internal`.
`sourceRegions`	Las regiones desde las que su servicio se comunica con esta dependencia.

Configuración de CloudWatch alarmas para el Resilience Hub de próxima generación

Puede crear CloudWatch alarmas basadas en las métricas de última generación de Resilience Hub para recibir notificaciones cuando una política de resiliencia deje de ser viable.

Alarma: la política no es realizable

El siguiente ejemplo crea una alarma que se activa cuando la política de SLO de disponibilidad no se puede cumplir para un servicio denominado. `my-service`

```
aws cloudwatch put-metric-alarm \
  --alarm-name "ResilienceHub-PolicyNotAchievable-AvailabilitySlo" \
  --metric-name "PolicyAchievable" \
  --namespace "ResilienceHub" \
  --dimensions Name=Service,Value=my-service Name=PolicyComponent,Value=AvailabilitySlo
 \
  --statistic Minimum \
  --period 86400 \
  --threshold 1 \
  --comparison-operator LessThanThreshold \
  --evaluation-periods 1 \
  --treat-missing-data notBreaching \
  --alarm-actions "arn:aws:sns:us-east-1:123456789012:resilience-hub-alerts"
```

Esta alarma entra en `ALARM` estado cuando cualquier evaluación del período de evaluación indica que la política no se puede cumplir (valor métrico 0.0). La `--treat-missing-data notBreaching` configuración garantiza que la alarma no se active entre evaluaciones cuando no haya puntos de datos.

Cuotas y límites

Tu AWS cuenta tiene cuotas predeterminadas, antes denominadas límites, para cada AWS servicio. A menos que se indique lo contrario, cada cuota es Región de AWS específica. Puede solicitar aumentos para algunas cuotas, mientras que otras no se pueden aumentar.

Cuotas de servicio

En la siguiente tabla se enumeran las cuotas del Resilience Hub de próxima generación.

#	Recurso	Cuota predeterminada	Ajustable
1	Sistemas por cuenta, por Región de AWS	500	Sí
2	Servicios por cuenta por Región de AWS	100	Sí
3	Viajes de usuario por sistema	20	No
4	Recursos evaluables por servicio	500	Sí

#	Recurso	Cuota predeterminada	Ajustable
5	Recursos totales por servicio	2,000	No
6	Fuentes de entrada por servicio	20	Sí
7	Funciones de servicio por servicio	20	No
8	Políticas de resiliencia por cuenta y por Región de AWS	100	No
9	Se incluyen evaluaciones de los modos de fallo por servicio y mes	2	No
10	Se hace un seguimiento de las dependencias por servicio	10 000	No
11	Cross-account ARN de rol por servicio	5	No
12	Métricas de servicio por servicio	10	No
13	Ejecuciones de pruebas activas por servicio	1	No
14	Fuentes de prueba por prueba	5	No
15	Pruebas por plantilla de prueba	1	No

Las pruebas de resiliencia se ejecutan continuamente AWS Fault Injection Service, por lo que las cuotas de AWS FIS servicio también se aplican a las ejecuciones de las pruebas. Estas incluyen las cuotas para el número máximo de experimentos activos y la duración máxima de la acción. Para obtener más información, consulta Cuotas y limitaciones para AWS Fault Injection Service.

Límites estrictos

No se pueden aumentar las cuotas siguientes.

#	Recurso	Límite invariable
1	Sistemas por cuenta por Región de AWS (máximo)	1 000
2	Servicios por cuenta por Región de AWS (máximo)	500
3	Fuentes de entrada por servicio (máximo)	100
4	Recursos por servicio (máximo)	1 000
5	Viajes de usuario por sistema (máximo)	100
6	Cross-account ARN de rol por servicio	5
7	Se incluyen evaluaciones de modos de fallo por servicio y mes	2

Solicitud de aumentos de cuota

Puedes solicitar un aumento para las cuotas ajustables en la consola de cuotas de servicio o poniéndote en contacto con el equipo de AWS soporte.

Para solicitar un aumento de cuota mediante las cuotas de servicio:

1. Abra la consola de Service Quotas.
2. En el panel de navegación, elija Servicios de AWS .
3. Elija AWS Resilience Hub.
4. Elige la cuota que quieres aumentar.
5. Elija Solicitar aumento de cuota.
6. Ingrese el nuevo valor de cuota y seleccione Solicitar.

Para solicitar un aumento de cuota a través de AWS Support:

1. Abre el Centro AWS de soporte.
2. Seleccione Crear caso.
3. Seleccione Aumento del límite de servicio.

4. Seleccione Resilience Hub como servicio.
5. Complete la información requerida y envíe su solicitud.

Por lo general, las solicitudes de aumento de cuota se procesan en unos pocos días hábiles.

Solución de problemas de Resilience Hub de próxima generación

Esta sección proporciona soluciones para los problemas comunes que pueden surgir al usar la próxima generación de Resilience Hub.

Temas

Problemas de detección de dependencias

Los siguientes son problemas comunes relacionados con el descubrimiento de dependencias.

El descubrimiento no devuelve las dependencias esperadas

Síntoma: has activado la detección de dependencias, pero no ves las dependencias que sabes que existen.

En la siguiente tabla se enumeran las posibles causas y soluciones.

Causa	Solución
La dependencia usa IP directa (no DNS)	La detección de dependencias se basa en las consultas de DNS. No se descubren las conexiones

Causa	Solución
	realizadas por la dirección IP. Realice un seguimiento manual de IP-based las dependencias.
Recursos informáticos que no están en una VPC	Non-VPC Las funciones de Lambda no generan consultas de resolución de Route 53. Conecte Lambda a una VPC o realice un seguimiento manual de las dependencias.
No se invocó la dependencia en un período de 35 días	Las dependencias se deben haber llamado dentro del período retrospectivo de 35 días. Es posible que no aparezcan las llamadas muy poco frecuentes.
Resolución de DNS mediante un solucionador que no sea de Route 53	Los solucionadores de DNS personalizados omiten el registro de consultas de Route 53. Asegúrese de que su VPC utilice el solucionador predeterminado de Route 53.

Brechas de atribución de Kubernetes

Síntoma: se descubren dependencias, pero se atribuyen a un servicio incorrecto en un clúster de EKS compartido.

Causa: cuando varios servicios comparten un clúster de EKS, las consultas de DNS se atribuyen a nivel de nodo, no a nivel de pod.

Solución: La atribución mejorada a nivel de pod está prevista para una versión futura. Actualmente, revisa manualmente las dependencias de los clústeres compartidos.

Non-VPC Lambda no aparece

Síntoma: no se descubren las dependencias de las funciones de Lambda.

Causa: las funciones de Lambda que no están conectadas a una VPC no realizan consultas de DNS a través de los solucionadores de Route 53.

Solución: conecte la función Lambda a una VPC o realice un seguimiento manual de sus dependencias fuera de Resilience Hub.

Problemas de evaluación del modo de error

Los siguientes son problemas comunes relacionados con las evaluaciones del modo de falla.

La evaluación no se ha completado

Síntoma: la evaluación permanece en `IN_PROGRESS` estado durante más de 30 minutos.

En la tabla siguiente se enumeran las posibles causas y soluciones.

Causa	Solución
Amplio servicio (muchos recursos)	Las evaluaciones de los servicios con 1000 o más recursos pueden llevar más tiempo. Espere hasta 60 minutos.
Problema con los permisos del rol de invocador	Verifique que el rol de invocador tenga `ReadOnlyAccess` y `AWSResilienceHubV2AssessmentExecutionPolicy` esté adjunto.
La topología no está completa	Asegúrese de que `StartServiceTopologyDiscovery` se haya completado correctamente antes de iniciar una evaluación.
Error de servicio	Si la evaluación falla, compruebe el mensaje de error de la `GetFailureModeAssessment` respuesta.

La evaluación falla porque no se encontró la topología

Síntoma: `StartFailureModeAssessment` devuelve un error acerca de la falta de topología.

Solución: ejecútelo `StartServiceTopologyDiscovery` primero y espere a que se complete correctamente. Las evaluaciones requieren una topología completa.

Los hallazgos del modo de falla no coinciden con la política esperada

Síntoma: los resultados del modo de falla de la evaluación no parecen estar relacionados con la política aplicada.

Causas posibles:

- La política se aplicó después de que se ejecutara la evaluación. Vuelva a ejecutar la evaluación.
- Se aplican varias políticas (según el recorrido del usuario y el nivel de servicio); compruebe todas las políticas aplicadas.
- La detección del modo de fallo se refiere a una Well-Architected mejor práctica, no a un requisito de política específico.

La evaluación no arroja ningún resultado sobre el modo de falla

Síntoma: la evaluación finaliza correctamente, pero no arroja ningún resultado en el modo de fallo.

Causas posibles:

- El servicio tiene muy pocos recursos (la evaluación necesita una arquitectura suficiente para poder analizarla).
- No se aplica ninguna política (las evaluaciones sin políticas producen menos resultados).
- La arquitectura ya cumple con todos los requisitos.

Errores de IAM y permisos

Los siguientes son errores comunes de IAM y permisos.

Códigos de error de permisos comunes y resolución

En la siguiente tabla se enumeran los códigos de error de permisos más comunes y su resolución recomendada.

Error	Causa	Resolución
`AccessDeniedException: Unable to assume role`	La política de confianza de los roles de invocador no incluye `resilienchub.amazonaws.com`	Actualiza la política de confianza del rol.
`AccessDeniedException: Cross-account role`	Cross-account la política de confianza del rol no	Verifique la política de confianza y. `ExternalId`

Error	Causa	Resolución
	permite asumir el rol de invocador	
`AccessDeniedException: sts:AssumeRole`	El rol de invocador no tiene `sts:AssumeRole` permiso para los roles multicuenta	Añade `sts:AssumeRole` permisos a la función de invocador.
`InvalidParameterException: Role does not exist`	El nombre del rol en `permissionModel` no coincide con un rol de IAM existente	Compruebe el nombre del rol y la cuenta.

Verificación de la configuración del rol

Compruebe que su función de invocador esté configurada correctamente mediante los siguientes AWS comandos de la CLI.

Para comprobar que el rol existe:

```
aws iam get-role --role-name AWSResilienceHubAssessmentRole
```

Para verificar la política de confianza:

```
aws iam get-role --role-name AWSResilienceHubAssessmentRole \
  --query 'Role.AssumeRolePolicyDocument'
```

Para simular si un director puede realizar las acciones necesarias:

```
aws iam simulate-principal-policy \
  --policy-source-arn arn:aws:iam::123456789012:role/AWSResilienceHubAssessmentRole \
  --action-names resiliencehub:GetService resiliencehub:StartFailureModeAssessment
```

AWS Problemas de configuración de la organización

Los siguientes son problemas comunes de configuración de AWS las organizaciones.

Errores de configuración del administrador delegado

Error	Causa	Resolución
`AWSOrganizationsNotInUseException`	Organizaciones no habilitadas	Habilite AWS las organizaciones con todas las funciones.
`AccountNotRegisteredException`	La cuenta no es miembro de la organización	Verifica la pertenencia a la cuenta.
`ConstraintViolationException`	La confianza en el servicio no está habilitada	Ejecute `enable-aws-service-access` primero.

Brechas de visibilidad de las cuentas de miembros

Síntoma: el administrador delegado no puede ver los servicios de una cuenta de miembro.

En la tabla siguiente se enumeran las posibles causas y soluciones.

Causa	Solución
Service-linked rol aún no creado	En el caso de las grandes organizaciones, la creación de funciones vinculadas a los servicios puede llevar tiempo. Espere y vuelva a comprobarlo.
La cuenta se suspendió durante la configuración	Anula la suspensión de la cuenta. El trabajo de conciliación de 12 horas creará el rol vinculado al servicio.
La cuenta se unió recientemente a la organización	Las cuentas nuevas reciben automáticamente las funciones vinculadas a los servicios, pero es posible que se produzca un breve retraso.
La confianza de servicio está deshabilitada	Re-enable acceso confiable desde la cuenta de administración.

Verificar que la función vinculada al servicio exista en una cuenta de miembro

Desde la cuenta de miembro, ejecute el siguiente comando para comprobar que existe el rol vinculado al servicio:

```
aws iam get-role --role-name AWSServiceRoleForResilienceHub
```

Si el rol no existe, comprueba que el acceso de confianza esté habilitado y espera a que comience el trabajo de conciliación, que se ejecuta cada 12 horas.

Problemas de detección de recursos

Los siguientes son problemas comunes de detección de recursos.

CloudFormation no se encontró la pila

Síntoma: se produce un error en la detección de recursos y se indica que «no se ha encontrado la pila».

Soluciones:

- Verifique que el ARN de la pila sea correcto y que la pila exista.
- Verifique que el rol de invocador tenga `cloudformation:DescribeStackResources` permiso.
- En el caso de las pilas multicuenta, compruebe que el rol multicuenta tenga acceso.

No se puede acceder al archivo de estado de Terraform

Síntoma: la detección de recursos no puede leer el archivo de estado de Terraform.

Soluciones:

- Compruebe que el bucket de Amazon S3 y la ruta clave son correctos.
- Compruebe que el rol de invocador tenga `s3:GetObject` permiso en el archivo de estado.
- Compruebe que el archivo de estado esté en un formato compatible.

Se descubrieron recursos pero se produjo un error en la generación de la topología

Síntoma: los recursos aparecen en la lista, pero la topología no muestra conexiones.

Soluciones:

- Compruebe que la función de invocador la tiene `ReadOnlyAccess` (necesaria para las consultas de topología).
- Compruebe que los recursos estén en una VPC (conexiones de mapas de generación de topología). VPC-based
- Para los recursos de EKS, verifique que el RBAC de Kubernetes esté configurado.

Tipos de recursos excluidos y no compatibles

La próxima generación de Resilience Hub excluye ciertos tipos de recursos del descubrimiento porque no tienen un valor de resiliencia independiente. Si espera que un recurso aparezca en los recursos descubiertos pero no aparece, es posible que sea de un tipo excluido.

Tipos de recursos nunca descubiertos

La próxima generación de Resilience Hub nunca almacena los siguientes tipos de recursos durante el descubrimiento. Estos tipos de recursos incluyen infraestructuras auxiliares, copias de seguridad puntuales y herramientas operativas que no influyen en el análisis de resiliencia.

Tipo de recurso
`AWS::EC2::EIP`
`AWS::EC2::Volume`
`AWS::EC2::Snapshot`
`AWS::FSx::Snapshot`
`AWS::Lightsail::DiskSnapshot`
`AWS::RDS::DBSnapshot`
`AWS::RDS::DBClusterSnapshot`
`AWS::EC2::FlowLog`
`AWS::CloudWatch::Dashboard`
`AWS::Logs::LogGroup`

Tipo de recurso
AWS::Logs::MetricFilter
AWS::SSM::ResourceDataSync
AWS::RDS::DBParameterGroup
AWS::RDS::DBClusterParameterGroup
AWS::ElastiCache::ParameterGroup
AWS::RDS::DBSubnetGroup
AWS::ElastiCache::SubnetGroup
AWS::EC2::SubnetNetworkAclAssociation
AWS::EC2::VPCGatewayAttachment
AWS::CloudFormation::Stack
AWS::CloudFormation::WaitConditionHandle
AWS::CodeDeploy::DeploymentGroup
AWS::KMS::Alias
AWS::SecretsManager::SecretTargetAttachment
AWS::CloudFormation::CustomResource

Tipos de recursos almacenados pero no facturados

La próxima generación de Resilience Hub descubre y almacena los siguientes tipos de recursos para darles contexto, pero no los tiene en cuenta para su cuota de recursos facturables. No aparecen en el análisis de resiliencia.

Tipo de recurso
AWS::IAM::Role
AWS::IAM::Policy
AWS::IAM::ManagedPolicy
AWS::IAM::InstanceProfile
AWS::Lambda::LayerVersion
AWS::Lambda::Permission
AWS::EC2::LaunchTemplate
AWS::EC2::SecurityGroup
AWS::EC2::SubnetRouteTableAssociation
AWS::CloudFront::OriginRequestPolicy
AWS::CloudFront::CloudFrontOriginAccessIdentity
AWS::SecretsManager::Secret
AWS::CloudWatch::Alarm
AWS::CDK::Metadata

Diferencia entre los recursos descubiertos y los recursos de topología

Es posible que vea más recursos en la respuesta de la `ListResources` API de los que aparecen en el diagrama de topología. No todos los recursos descubiertos aparecen en la vista de topología. La topología es un gráfico de conectividad que muestra cómo interactúan los recursos. La próxima generación de Resilience Hub elimina de la vista de topología los recursos que no tienen conexiones con otros recursos.

Las instancias EC2 o las tareas de ECS no aparecen como recursos facturables

Cuando un recurso principal (como un grupo de Auto Scaling, un servicio de ECS o una implementación de EKS) administra una instancia EC2, una tarea de ECS, un pod de EKS o una interfaz de red, el Resilience Hub de próxima generación clasifica ese recurso como efímero. Los recursos efímeros son transitorios. El recurso principal los reemplaza automáticamente mediante eventos del ciclo de vida. El Resilience Hub de próxima generación los evalúa a través de sus padres, no de forma independiente.

Los siguientes tipos de recursos son efímeros cuando los administra una empresa principal:

Tipo de recurso	Ejemplo: padre
`AWS::EC2::Instance`	Grupo de Auto Scaling o grupo de nodos EKS
`AWS::ECS::Task`	Servicio de ECS
`AWS::EKS::Pod`	Conjunto de implementación o réplicas de EKS
`AWS::EC2::NetworkInterface`	Instancia EC2 gestionada por Auto Scaling

Las instancias independientes de este tipo (no administradas por una empresa principal) siguen siendo facturables.

Problemas con las pruebas de resiliencia

Los siguientes son problemas comunes relacionados con las pruebas de resiliencia.

La ejecución de la prueba no se inicia

Síntoma: al iniciar una ejecución de prueba, se devuelve un`ConflictException`.

Causa: Resilience Hub de próxima generación ejecuta una sola prueba a la vez para un objetivo. La ejecución anterior del servicio aún está en curso.

Solución: espere a que finalice la ejecución actual o deténgala y`StopTestRun`, a continuación, inicie la nueva ejecución.

La ejecución de la prueba falla y se produce un error de acceso denegado

Síntoma: se produce un error en la ejecución de una prueba debido a un `AccessDenied` error de uno de los servicios seleccionados AWS FIS o de uno de ellos.

En la tabla siguiente se enumeran las posibles causas y soluciones.

Causa	Solución
La política de confianza del rol de ejecución no lo permite AWS FIS	Comprueba que el rol confía `fis.amazonaws.com` y que las `aws:SourceAccount` `aws:SourceArn` condiciones coinciden con las de tu cuenta. Para ver la política de confianza, consulteFunciones de ejecución de IAM para las pruebas de resiliencia.
Al rol de ejecución le faltan permisos para la plantilla de prueba	Cada plantilla de prueba ejecuta un conjunto diferente de AWS FIS acciones. Adjunta la política de permisos de la plantilla que estás ejecutando. Para ver las políticas, consulteFunciones de ejecución de IAM para las pruebas de resiliencia.
Multi-account cadena de funciones no configurada	En el caso de una prueba con varias cuentas, verifique que el rol de orquestador pueda asumir el rol objetivo en cada cuenta que contenga los recursos específicos.

La ejecución de la prueba se detiene antes de completarse

Síntoma: la ejecución de una prueba se detiene por sí sola antes de terminar.

Causa: una CloudWatch alarma que configuraste como condición de parada superó su umbral y las pruebas de resiliencia detuvieron la ejecución para limitar el impacto.

Solución: revisa la alarma que activó la condición de parada para determinar el impacto en tu servicio. Después de solucionar el problema subyacente, inicie una nueva prueba.

La ejecución de la prueba finaliza y se omiten todas las acciones

Síntoma: se completa una prueba, pero no se ha detectado ningún error. Se muestran todas las acciones`skipped`.

Causa: ningún recurso coincide con el tipo de recurso objetivo de ninguna acción en la zona de disponibilidad o región seleccionada.

Solución: compruebe que se ha completado la detección de recursos y que ha seleccionado la zona de disponibilidad o región correcta.

La acción por error de dependencia falla y se produce un error de configuración

Síntoma: una acción por error de dependencia falla porque el agente o el sidecar requerido no están configurados.

Causa: las acciones de pérdida de paquetes requieren un agente SSM en Amazon EC2, un contenedor SSM en las definiciones de tareas de Amazon ECS o una cuenta de servicio de Kubernetes para los pods de Amazon EKS.

Solución: siga los pasos de configuración para su tipo de cálculo en la referencia de acciones. AWS FIS

No todas las dependencias están visibles en la prueba

Síntoma: no todas las dependencias descubiertas se muestran en el menú desplegable.

Causa: las dependencias se filtran por prueba para mostrar solo las que son relevantes para el alcance de la prueba.

Solución: cada prueba muestra un subconjunto diferente. Consulte las páginas de prueba individuales en las que se muestran las dependencias.

Problemas conocidos y soluciones

En esta sección se enumeran los problemas conocidos de la próxima generación de Resilience Hub y sus soluciones alternativas recomendadas. Para obtener la información más actualizada, consulte las notas de la versión de la próxima generación de Resilience Hub.

Referencia de la API

En esta sección se ofrece una descripción general de la próxima generación de operaciones de la API de Resilience Hub, organizadas por área de funciones. Para ver las especificaciones completas de la API, incluidos los esquemas de solicitud y respuesta, consulte la referencia de API de Resilience Hub de próxima generación.

Temas

Realización de solicitudes de API y autenticación

Punto de conexión

```
https://resiliencehub.{region}.amazonaws.com
```

Versión de la API

Las API de Resilience Hub de próxima generación utilizan el prefijo de `/v3` ruta. Todas las solicitudes deben estar firmadas con la versión 4 de AWS Signature (SIGv4).

Autenticación

Todas las llamadas a la API requieren AWS credenciales válidas. La próxima generación de Resilience Hub usa AWS IAM para la autorización. Asegúrese de que su política de IAM otorgue las acciones necesarias`resiliencehub:*`.

Acciones

la próxima generación de la API de Resilience Hub ofrece las siguientes categorías de acciones.

Políticas de resiliencia

Action	Método	Description (Descripción)
`CreatePolicy`	POST	Cree una política de resiliencia con el SLO de disponibilidad, RTO/RPO los objetivos y el enfoque de recuperación ante desastres.
`UpdatePolicy`	POST	Actualice los objetivos y la configuración de las políticas.

Action	Método	Description (Descripción)
`GetPolicy`	GET	Recupere los detalles de la política.
`ListPolicies`	GET	Enumere las políticas con el recuento de servicios asociado.
`DeletePolicy`	POST	Eliminar una política.

Sistemas

Action	Método	Description (Descripción)
`CreateSystem`	POST	Cree un sistema con la habilitación opcional de detección de dependencias.
`UpdateSystem`	POST	Actualice la descripción del sistema, el descubrim iento de dependencias y la clave de KMS.
`GetSystem`	GET	Recupera los detalles del sistema.
`ListSystems`	GET	Enumere los sistemas, filtrables por `organizat ionId ouId`, y. `accountId`
`DeleteSystem`	POST	Eliminar un sistema (no debe tener ningún servicio asociado).

Viajes de usuario

Action	Método	Description (Descripción)
`CreateUserJourney`	POST	Cree un recorrido de usuario en un sistema.
`UpdateUserJourney`	POST	Actualice los servicios y la política de viaje del usuario.
`GetUserJourney`	GET	Recupera los detalles del recorrido del usuario.

Action	Método	Description (Descripción)
`ListUserJourneys`	GET	Enumera los recorridos de los usuarios por un sistema.
`DeleteUserJourney`	POST	Eliminar el recorrido de un usuario.

Services

Action	Método	Description (Descripción)
`CreateService`	POST	Cree un servicio con las regiones, el modelo de permisos, la configuración de los informes y la configuración de detección de dependencias.
`UpdateService`	POST	Actualice la configuración del servicio, incluidos el modelo de permisos y el descubrimiento de dependencias.
`GetService`	GET	Obtenga todos los detalles del servicio, incluidos los valores de las políticas vigentes y la puntuación de resiliencia.
`ListServices`	GET	Enumere los servicios, filtrables por `systemId`, `userJourneyId`, `organizationId`, `ouId`, `accountId`, `assessmentStatus` y `policyArn`.
`DeleteService`	POST	Eliminar un servicio.

Orígenes de entrada

Action	Método	Description (Descripción)
`CreateInputSource`	POST	Configure una fuente de descubrimiento de recursos (etiquetas de recursos, CloudFormation pila, archivo de estado de Terraform, clúster de EKS o archivo de

Action	Método	Description (Descripción)
		diseño). En el caso de una única fuente de entrada basada en etiquetas con varias etiquetas, el servicio solo descubre los recursos que coinciden con todas las etiquetas especificadas. En el caso de varias fuentes de entrada basadas en etiquetas, el servicio descubre los recursos que coinciden con alguna de ellas.
`ListInputSources`	GET	Enumera las fuentes de entrada de un servicio.
`DeleteInputSource`	POST	Eliminar una fuente de entrada.

Recursos

Action	Método	Description (Descripción)
`ListResources`	GET	Enumera los recursos descubiertos para un servicio, filtrables por `serviceFunctionId` y. `awsRegion`

Evaluaciones del modo de error

Action	Método	Description (Descripción)
`StartFailureModeAssessment`	POST	Impulse una AI-powered evaluación asincrónica que determine la topología, las funciones de servicio y los modos de fallo.
`ListFailureModeAssessments`	GET	Enumere las evaluaciones con el estado, la puntuación de resiliencia y la información del informe.

Pruebas de resiliencia

Action	Método	Description (Descripción)
`ListTestTemplates`	GET	Enumera las plantillas de prueba disponibles.
`GetTestTemplate`	GET	Recupera una plantilla de prueba, incluidas sus acciones y parámetros.
`CreateTest`	POST	Cree una prueba para un servicio a partir de una plantilla de prueba.
`GetTest`	GET	Recupere una configuración de prueba que incluya los parámetros, las condiciones de parada y el rol.
`UpdateTest`	POST	Actualice una configuración de prueba que incluya los parámetros, las condiciones de parada y el rol.
`ListTests`	GET	Enumera las pruebas de un servicio.
`DeleteTest`	POST	Eliminar una prueba.
`StartTestRun`	POST	Inicie una prueba de funcionamiento de un servicio.
`StopTestRun`	POST	Detenga la ejecución de una prueba.
`ListTestRuns`	GET	Enumera las ejecuciones de prueba de un servicio.
`GetTestRun`	GET	Recupera una ejecución de prueba que incluye el estado, los parámetros y la marca de tiempo.
`ListTestRunEvents`	GET	Enumera los eventos en el cronograma de una ejecución de prueba.
`PutTestSources`	POST	Agregue o actualice las alarmas de criterios de éxito o las alarmas de observabilidad para una prueba.
`DeleteTestSources`	POST	Elimine las alarmas de criterios de éxito o las alarmas de observabilidad de una prueba.

Action	Método	Description (Descripción)
`ListTestSources`	GET	Enumere las alarmas de criterios de éxito o las alarmas de observabilidad para una prueba.
`ListTestRunSources`	GET	Enumere las alarmas de criterios de éxito o las alarmas de observabilidad para una ejecución de prueba.
`ListResolvedTestRunTargetResources`	GET	Enumera los recursos que se resolvieron como objetivos para una ejecución de prueba.

Topología

Action	Método	Description (Descripción)
`ListServiceTopologyEdges`	GET	Enumera los bordes de dependencia de los recursos de un servicio.

Funciones de servicio

Action	Método	Description (Descripción)
`CreateServiceFunction`	POST	Cree una función de servicio con un nivel de criticidad (`PRIMARY/SUPPLEMENTAL`).
`UpdateServiceFunction`	POST	Actualice las propiedades de la función de servicio.
`ListServiceFunctions`	GET	Enumera las funciones de servicio de un servicio.
`DeleteServiceFunction`	POST	Eliminar una función de servicio.
`AddServiceFunctionResources`	POST	Asocie los recursos a una función de servicio (hasta 10 por llamada).

Action	Método	Description (Descripción)
`DeleteServiceFunctionResources`	POST	Elimine las asociaciones de recursos (hasta 10 por llamada).

Hallazgos del modo de error

Action	Método	Description (Descripción)
`GetFailureModeFinding`	GET	Recupere los detalles de búsqueda del modo de falla, incluidas AI-generated las recomendaciones.
`UpdateFailureModeFinding`	POST	Actualice el estado de búsqueda del modo de fallo (resuelto, irrelevante) y añada comentarios.
`ListFailureModeFindings`	GET	Enumere los hallazgos del modo de falla, filtrables por `severityfailureCategory` , y. `status`

Aserciones

Action	Método	Description (Descripción)
`CreateAssertion`	POST	Cree una afirmación de resiliencia con categoría y texto.
`UpdateAssertion`	POST	Actualice el texto o la categoría de la afirmación.
`ListAssertions`	GET	Enumera las afirmaciones, que se pueden filtrar por categoría y fuente (o). `USER` `SYSTEM`
`DeleteAssertion`	POST	Eliminar una afirmación.

Dependencias

Action	Método	Description (Descripción)
`UpdateDependency`	POST	Actualice los metadatos de dependencia (comentario, clasificación de criticidad).
`ListDependencies`	GET	Enumera las dependencias descubiertas para un servicio.

Informes

Action	Método	Description (Descripción)
`CreateReport`	POST	Genere un informe en PDF (`FAILURE_MODE` o `TESTING` escriba); escriba en el bucket de Amazon S3 del cliente. `DEPENDENCY`
`ListReports`	GET	Enumere los informes generados con el estado y la ubicación de salida de Amazon S3.

Events (Eventos)

Action	Método	Description (Descripción)
`ListServiceEvents`	GET	Enumera los eventos de auditoría de un servicio (incluye el actor:`USER`/`SYSTEM`y los cambios de puntuación).
`ListSystemEvents`	GET	Enumera los eventos de auditoría de un sistema.

Migración

Action	Método	Description (Descripción)
`ImportApp`	POST	Importe una aplicación de Resilience Hub de la versión 1 a un servicio de la versión 2.
`ImportPolicy`	POST	Importe una política de la versión 1 al formato de la versión 2.

Tipos de datos

En la siguiente tabla se enumeran los tipos de datos clave que utiliza la próxima generación de la API de Resilience Hub.

Tipo	Description (Descripción)
`SystemEntity`	Sistema con ARN, nombre, descripción y hora de creación.
`UserJourneyEntity`	Recorrido del usuario con nombre, descripción, lista de servicios y política.
`ServiceEntity`	Servicio con ARN, nombre, asociación de sistemas, modelo de permisos y fuentes de entrada.
`ResiliencePolicyEntity`	Política con nombre y componentes (DR, disponibilidad, rendimiento).
`AssessmentEntity`	La evaluación con el identificador, el estado, las marcas de tiempo y el modo de falla cuenta.
`FindingEntity`	Detección del modo de fallo con el identificador, el nombre, la descripción, la gravedad y las recomendaciones.
`RecommendationEntity`	Recomendación con nombre, descripción, costo y complejidad.

Tipo	Description (Descripción)
`DependencyDiscoveryConfig`	Configuración de detección de dependencias con estado, recuento de recursos aptos, mensaje y fecha de la última actualización. Devuelto por y. `GetService ListServices`
`DependencyEntity`	Dependencia con nombre, ubicación, criticidad y estado permitido.
`TopologyEntity`	Topología con ID, marca de tiempo, recuento de recursos y bordes.

DependencyDiscoveryConfig estructura

```
{
  "status": "INITIALIZING | ENABLED | DISABLED",
  "updatedAt": "timestamp",
  "eligibleResourceCount": integer,
  "message": "string"
}
```

En la tabla siguiente se describen los campos de la `DependencyDiscoveryConfig` estructura.

Campo	Obligatorio	Descripción
`status`	Sí	El estado actual del descubrimiento de dependencias. Valores válidos: `INITIALIZING` (la detección está en ejecución), `ENABLED` (la detección está completa y activa) o `DISABLED` (la detección está desactivada).
`updatedAt`	No	La marca de tiempo en la que se actualizó por última vez el estado de detección de dependencias.
`eligibleResourceCount`	No	La cantidad de recursos informáticos aptos para el descubrimiento de dependencias.

Campo	Obligatorio	Descripción
		Devuelve `null` hasta que el proceso de detección de recursos complete su primera ejecución.
`message`	No	Un mensaje que describe el estado actual de la detección. Se devuelve `null` cuando se ha completado el descubrimiento y las dependenc ias están disponibles.

Estructura del modelo de permisos

```
{
  "invokerRoleName": "string",
  "crossAccountRoles": [
    {
      "crossAccountRoleArn": "string",
      "externalId": "string"
    }
  ]
}
```

Estructura de los componentes de la política

```
{
  "multiRegionDr": {
    "required": "boolean",
    "rtoMinutes": "integer",
    "rpoMinutes": "integer"
  },
  "availabilitySlo": {
    "targetPercentage": "number",
    "performanceConditions": {
      "expression": "string",
      "conditions": [
        {
          "type": "FAULT_RATE | LATENCY | VOLUME",
          "operator": "LESS_THAN | GREATER_THAN",
          "value": "number",
```

```
          "percentile": "string"
        }
      ]
    }
  },
  "dataProtection": {
    "rpoMinutes": "integer"
  }
}
```

Códigos de error

En la siguiente tabla se enumeran los códigos de error devueltos por la próxima generación de la API de Resilience Hub.

Código de error	Estado HTTP	Description (Descripción)
`ValidationException`	400	Los parámetros de solicitud no son válidos.
`ResourceNotFoundException`	404	El recurso especificado no existe.
`ConflictException`	409	La operación entra en conflicto con el estado actual (por ejemplo, ya se está ejecutando una evaluación).
`AccessDeniedException`	403	La persona que llama carece de los permisos necesarios.
`ThrottlingException`	429	Se superó la tasa de solicitudes.
`InternalServerException`	500	Error de servicio interno.
`ServiceQuotaExceededException`	402	Se ha superado una cuota de servicio.

Escenarios de error comunes

Escenario	Error	Resolución
Iniciar la evaluación sin topología	`ConflictException`	Ejecute `StartServiceTopologyDiscovery` primero.
Iniciar la evaluación mientras se está ejecutando	`ConflictException`	Espere a que se complete la evaluación actual.
Eliminando el sistema con servicios	`ConflictException`	Elimine primero todas las asociaciones de servicios.
Cross-account acceso sin rol	`AccessDeniedException`	Configure los roles multicuenta o habilite las organizaciones.
Superar 5 funciones multicuenta	`ServiceQuotaExceededException`	Usa AWS Organizations para despliegues más grandes.

Historial de documentos de la Guía del usuario de Resilience Hub de próxima generación

En la siguiente tabla se describen las versiones de la documentación para la próxima generación de Resilience Hub.

AWS Glosario

Para obtener la AWS terminología más reciente, consulte el AWS glosario de la Glosario de AWS Referencia.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.