Guía del usuario

# AWS Centro de resiliencia

# AWS Centro de resiliencia: Guía del usuario

# Table of Contents

# ¿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 esos objetivos e implementar recomendaciones de mejora basadas en el Marco AWS Well-Architected. Dentro AWS Resilience Hub, también puedes crear y ejecutar experimentos del Amazon Fault Injection Service, que imitan las interrupciones reales de tu aplicación para ayudarte a entender 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.

Servicios AWS y referencias relacionados con la resiliencia

| AWS servicio de resiliencia | Enlace a la documentación |
| --- | --- |
| AWS Elastic Disaster Recovery | Qué es Elastic Disaster Recovery |
| AWS Backup | ¿Qué es AWS Backup |
| Controlador de recuperación de aplicaciones Amazon Route 53 (Route 53ARC) | Qué es el controlador de recuperación de aplicaciones de Amazon Route 53 |

Temas

- AWS Resilience Hub — Gestión de la resiliencia
- AWS Resilience Hub — Pruebas de resiliencia
- AWS Resilience Hub conceptos
- AWS Resilience Hub personas
- AWS Resilience Hub recursos compatibles

# AWS Resilience Hub — Gestión de la resiliencia

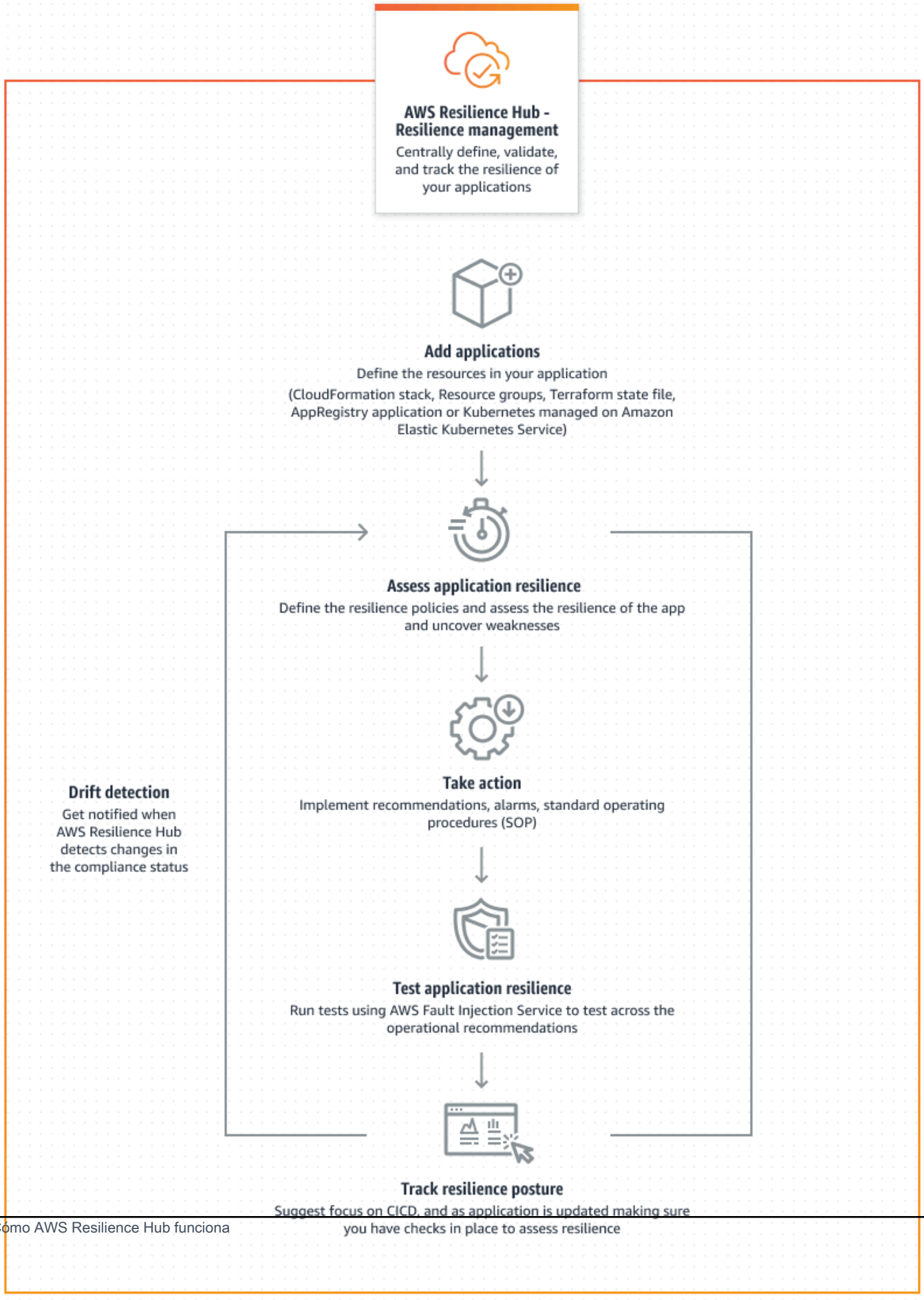
AWS Resilience Hub le ofrece un lugar central para definir, validar y realizar un seguimiento de la resiliencia de su AWS aplicación. AWS Resilience Hub le ayuda a proteger sus aplicaciones de las interrupciones y a reducir los costos de recuperación para optimizar la continuidad del negocio y ayudar 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 (SOPs) 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 los 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.

Después de implementar una aplicación en producción, puede agregarla AWS Resilience Hub a su proceso de CI/CD para validar cada compilación antes de lanzarla a producción.

## ¿Cómo funciona AWS Resilience Hub

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, AppRegistry 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

Describe

Describa su aplicación importando recursos de AWS CloudFormation pilas, AWS Resource Groups archivos de estado de Terraform o clústeres de Amazon Elastic Kubernetes Service, o puede elegir entre aplicaciones que ya estén definidas en. AWS Service Catalog AppRegistry

Definir

Defina las políticas de resiliencia de sus aplicaciones. Estas políticas incluyen las disrupciones en las aplicaciones, la infraestructura, la zona de disponibilidad RTO y la región, así como RPO sus objetivos. 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 Framework para analizar los componentes de una aplicación y descubrir posibles debilidades 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 la recuperación. SOPs A continuación, puede realizar otra evaluación y comparar los resultados con el informe anterior para ver en qué medida mejora la resiliencia. Reitera este proceso hasta que la carga de trabajo estimada RTO y la carga de trabajo estimada RPO cumplan con tus RTO RPO objetivos.

Valide

Realice pruebas para medir la resiliencia de sus AWS recursos y el tiempo que tarda en recuperarse de las aplicaciones, 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 Algunos ejemplos de interrupciones incluyen errores de red no disponibles, conmutaciones por error, procesos detenidos, recuperación de RDS arranque de Amazon y problemas con la zona de disponibilidad.

Visualización y seguimiento

Tras implementar una AWS aplicación en producción, puede utilizarla AWS Resilience Hub para seguir realizando un seguimiento de la capacidad de recuperación 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 le permite realizar pruebas y experimentos de Amazon Fault Injection Service (AWS FIS) en sus AWS cargas de trabajo y mantener una resiliencia óptima. Estas pruebas estresan a 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.

## Resistencia

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 (carga de trabajo estimadaRTO) es el RTO que se estima que cumplirá su aplicación en función de la definición de aplicación importada y, a continuación, ejecutar una evaluación.

## Objetivo de punto de recuperación de carga de trabajo estimado

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

## Aplicación

Una AWS Resilience Hub aplicación es un conjunto de recursos AWS compatibles que se supervisan y evalúan de forma continua 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 cumple sus RPO objetivos RTO y los definidos en la política. Todos sus componentes cumplen con los objetivos políticos definidos. Por ejemplo, ha seleccionado un RPO objetivo RTO de 24 horas para las interrupciones en todas las AWS 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 de copia de seguridad (SOP) 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 RTO los RPO objetivos definidos en la política. Uno o más de ellos AppComponents no satisfacen los objetivos de la política. Por ejemplo, ha seleccionado un RTO RPO objetivo de 24 horas para las interrupciones en todas las AWS regiones, pero la configuración de la 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 error mientras realiza una evaluación de su aplicación para comprobar si los cambios en AppComponent las 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 (SOPs) 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.

## Experimentos de inyección de errores

AWS Resilience Hub recomienda pruebas 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 incidentes en Región de AWS 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.
- Verifique que los procedimientos de recuperación, o los procedimientos operativos estándar (SOPs), funcionen correctamente para recuperar la aplicación tras la interrupción.

Pruebas para SOPs medir la carga de trabajo estimada RTO y la carga de trabajo RPO estimada. Puede probar diferentes configuraciones de aplicaciones y medir si el resultado RTO RPO cumple con los objetivos definidos en su política.

## SOP

Un procedimiento operativo estándar (SOP) es un conjunto prescriptivo de pasos diseñados para recuperar la aplicación de manera eficiente en caso de que se produzca una interrupción o una

alarma. Basado en la evaluación de la aplicación, AWS Resilience Hub recomienda un conjunto de, SOPs y se recomienda prepararlos, probarlos y SOPs medirlos 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 cómo conceder permisos a diferentes personas, consultethe section called “AWS Resilience Hub referencia de personas y IAM permisos”.

Para empezar a crear aplicaciones y ejecutar evaluaciones en ellas AWS Resilience Hub, 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 con
  - 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 sea up-to-date:
    - Arquitectura de aplicaciones
    - Procesos de despliegue
    - Configuraciones de monitoreo
    - Técnicas de optimización del rendimiento
- Acceso de solo lectura: los usuarios con esta persona 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:

- Cálculo
  - Amazon Elastic Compute Cloud (AmazonEC2)

> **Note**
>
> AWS Resilience Hub no admite el antiguo formato Amazon Resource Name (ARN) para acceder a EC2 los recursos de Amazon. El nuevo ARN formato utiliza el identificador de su AWS cuenta y permite etiquetar mejor los recursos del clúster. Además, hace 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 ARN formato, consulta Migración de tu ECS implementación de Amazon al formato nuevo ARN y al de ID de recurso.

  - AWS Lambda
  - Servicio Amazon Elastic Kubernetes (Amazon) EKS
  - Amazon Elastic Container Service (AmazonECS)
  - AWS Step Functions
- Base de datos
  - Amazon Relational Database Service (AmazonRDS)
  - Amazon DynamoDB
  - Amazon DocumentDB
- Redes y entrega de contenido
  - Amazon Route 53
  - Elastic Load Balancing
  - Traducción de direcciones de red () NAT
- Almacenamiento
  - Tienda Amazon Elastic Block (AmazonEBS)
  - Amazon Elastic File System (AmazonEFS)
  - Amazon Simple Storage Service (Amazon S3)
  - Servidor FSx de archivos Amazon para Windows
- Otros
  - Amazon API Gateway
  - Controlador de recuperación de aplicaciones Amazon Route 53 (Amazon Route 53ARC)
  - Amazon Simple Notification Service
  - Amazon Simple Queue Service
  - AWS Auto Scaling
  - AWS Backup

- AWS Recuperación ante desastres elástica

> **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 on AWS Fargate.
> - AWS Resilience Hub apoya 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
>   - RDSServicios de Amazon
>   - Servidor FSx de archivos Amazon para Windows
> - Amazon Route 53 ARC AWS Resilience Hub evalúa únicamente Amazon DynamoDB global, Elastic Load Balancing, RDS Amazon 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 evaluaciones entre regiones para EKS los clústeres de Amazon si el EKS clúster de Amazon está ubicado o si la aplicación se crea en una región habilitada para AWS la suscripción.
> - Actualmente, AWS Resilience Hub evalúa solo los siguientes tipos de recursos de Kubernetes:

- Implementaciones
- ReplicaSets
- Pods

AWS Resilience Hub ignora los siguientes tipos de recursos:

- Recursos que no afectan a la carga de trabajo estimada RTO o a la carga de trabajo estimada RPO: los recursos como`AWS::RDS::DBParameterGroup`, por AWS Resilience Hub ejemplo, que no afectan a la carga de trabajo estimada RTO o a la carga de trabajo estimada`RPO`, se ignoran en.
- Recursos que no son de nivel superior: AWS Resilience Hub solo importa 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 lo importa AWS Resilience Hub.

> **Note**
>
> Recursos no compatibles
>
> - No puede identificar varios recursos mediante los recursos AWS Resource Groups (Amazon Route 53 RecordSets y API -GWHTTP) 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 RDS instancia de Amazon. 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 AppRegistry una aplicación. AWS Resource Groups

# 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

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 (cuentas primarias/secundarias o de recursos) que desee utilizar. AWS Resilience Hub Para obtener más información sobre la creación y administración de AWS cuentas, consulta 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 funciona AWS Resilience Hub con IAM” y para obtener más información sobre cómo añadir una política al rol, consulte the section called “Definir la política de confianza mediante JSON un archivo”.

  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”
- 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.
- Calcular si se pueden cumplir su objetivo de tiempo de recuperación (RTO) y su 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 los recursos de una aplicación o AWS CloudFormation pilas existentes AppRegistry y crea una política de resiliencia adecuada. AWS Resource Groups 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 la carga de trabajo estimada RTO y la carga de trabajo estimada RPO alcancen sus RTO objetivos. RPO

Temas

- Paso 1: Introducción mediante la adición de una aplicación
- Paso 2: ¿Cómo se administra su aplicación?
- Paso 3: Añada recursos a su AWS Resilience Hub aplicación
- RTOPaso 4: Establece y RPO

- Paso 5: Configure las evaluaciones programadas y la notificación de desviaciones
- Paso 6: configurar permisos
- Paso 7: configurar los parámetros de configuración de la aplicación
- Paso 8: Añadir etiquetas
- Paso 9: Revise y publique su aplicación AWS Resilience Hub
- Paso 10: Realice una evaluación de la aplicación AWS Resilience Hub

## Paso 1: Introducción mediante la adición de 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 aplicación 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

Paso 2: ¿Cómo se administra su aplicación?

## Paso 2: ¿Cómo se administra su aplicación?

Además de las AWS CloudFormation pilas AWS Resource Groups, AppRegistry las aplicaciones 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 EKS clústeres de Amazon 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 AWS Resource Groups, AppRegistry aplicaciones y archivos de estado de Terraform.

  Si selecciona esta opción, debe completar uno de los procedimientos de the section called “Agregar colecciones de recursos”.
- EKSsolo: selecciona esta opción si quieres descubrir recursos de los espacios de nombres de los clústeres de AmazonEKS.

  Si selecciona esta opción, debe completar uno de los procedimientos de the section called “Añadir EKS clústeres”
- Colecciones de recursos y EKS: seleccione esta opción si desea descubrir recursos de una de las colecciones de recursos y EKS clústeres de Amazon.

  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 EKS clústeres”.

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

### Next

Paso 3: Añada recursos a su AWS Resilience Hub aplicación

## Paso 3: Añada recursos a su AWS Resilience Hub aplicación

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

- the section called “Agregar colecciones de recursos”
- the section called “Añadir EKS clústeres”

## 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 AWS Resource Groups
- Uso de AppRegistry aplicaciones
- Uso de archivos de estado de Terraform
- Uso de una AWS Resilience Hub aplicación existente

### 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 pilas para descubrir tus recursos basados en pilas.
2. Elige las pilas de la lista desplegable Selecciona 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, introduce el nombre del recurso de Amazon (ARN) de la pila en el cuadro Añadir pila fuera de la AWS región y, a continuación, selecciona Añadir pila ARN. Para obtener más informaciónARNs, consulte Amazon Resource Names (ARNs) en la Referencia AWS general.

### Usando AWS Resource Groups

Elija los AWS Resource Groups 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 AWS Resource Groups que contienen los recursos.
2. Seleccione los recursos de la lista desplegable Seleccionar grupos de recursos.

Para usarlos AWS Resource Groups en una región diferente Cuenta de AWS, diferente o en ambas, introduce el nombre del recurso de Amazon (ARN) de la pila en el ARN cuadro Grupo de recursos y, a continuación, selecciona Añadir grupo de recursos ARN. Para obtener más informaciónARNs, consulte Amazon Resource Names (ARNs) en la Referencia AWS general.

Uso de AppRegistry aplicaciones

Solo puede añadir una AppRegistry aplicación a la vez.

Elija las AppRegistry aplicaciones que contienen los recursos que desea usar en la aplicación que está describiendo.

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

1. Seleccione AppRegistryesta opción de una lista de aplicaciones creadas en AppRegistry.
2. Elija las aplicaciones que se crearon en AppRegistry la lista desplegable Seleccionar aplicación. Solo puede seleccionar una aplicación a la vez.

Uso de archivos de estado de Terraform

Seleccione el archivo de estado de Terraform que contiene los recursos del bucket de S3 que desee usar en la aplicación que está describiendo. 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, seleccione Examinar S3 para navegar hasta la ubicación de su archivo de estado de Terraform.

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

El límite de los archivos de estado de Terraform es de 4 megabytes (MB).

3. Seleccione su bucket S3 en la sección Buckets.
4. En la sección Objetos, seleccione una clave y seleccione Seleccionar.

Uso de una aplicación existente AWS Resilience Hub

Para empezar, utilice una aplicación existente.

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

1. Seleccione Aplicación existente para crear su aplicación a partir de una aplicación existente.
2. Seleccione una aplicación de la lista desplegable Seleccionar aplicación existente.

## Añadir EKS clústeres

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

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

Elige los EKS clústeres y espacios de nombres de Amazon que contienen los recursos que quieres usar en la aplicación que estás describiendo. EKSLos clústeres de Amazon pueden provenir de la Cuenta de AWS que estás utilizando para describir la aplicación o pueden provenir de diferentes cuentas o regiones.

> **Note**
>
> AWS Resilience Hub Para evaluar tus EKS clústeres de Amazon, debes añadir manualmente los espacios de nombres correspondientes a cada una de las secciones de EKS clústeres en EKSclústeres y espacios de nombres de Amazon. El nombre del espacio de nombres debe coincidir exactamente con el nombre del espacio de nombres de tus clústeres de Amazon. EKS

Para añadir EKS clústeres de Amazon

1. Selecciona los EKS clústeres de Amazon de la lista desplegable Elegir EKS clústeres que estén asociados a tu región Cuenta de AWS y a tu región.
2. Para usar EKS clústeres de Amazon que estén en una región diferente Cuenta de AWS, diferente o en ambas, introduce el nombre del recurso de Amazon (ARN) de la pila en el cuadro Entre cuentas o regiones y, a continuación, selecciona Añadir EKS ARN. Para obtener más informaciónARNs, 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 tu EKS clúster de Amazon”.

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

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

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

   - EKSnombre del clúster: indica el nombre de los EKS clústeres de Amazon 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 EKS clústeres de Amazon seleccionados en su aplicación. Puede identificar el estado mediante las siguientes opciones:

- Espacio de nombres obligatorio: indica que no has incluido ningún espacio de nombres del clúster de Amazon. EKS
- Espacios de nombres añadidos: indica que has 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 EKS clúster de Amazon, 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 de tu 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 EKS clústeres de Amazon, selecciona Aplicar espacios de nombres a todos los clústeres. EKS

     Si eliges esta opción, tu selección de espacio de nombres anterior en los demás EKS clústeres de Amazon se anulará con la selección de espacio de nombres actual.
4. Para incluir los espacios de nombres actualizados en su aplicación, seleccione Actualizar.

Next

RTOPaso 4: Establece y RPO

## RTOPaso 4: Establece y RPO

Puede definir una nueva política de resiliencia con sus propios RPO objetivos RTO o puede elegir una política de resiliencia existente con objetivos o objetivos predefinidosRTO. 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.
3. (Opcional) Escriba una descripción de la política de resiliencia.
4. Defina sus objetivosRTO/RPOen la sección RTO/RPOobjetivos.

> **Note**
>
> - Hemos rellenado una RTO y predeterminada RPO para su aplicación. Puede cambiar el RTO y RPO ahora o después de evaluar la solicitud.
> - AWS Resilience Hub le permite introducir un valor cero en los RPOcampos RTOy 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 RPOlos campos RTOy, la carga de trabajo estimada RTO y RPO los resultados de la carga de trabajo estimada estarán próximos a cero y el estado de conformidad de su solicitud pasará a ser Política infringida.

5. Para definirRTO/RPOpara su infraestructura y la zona de disponibilidad, elija la flecha derecha para expandir la RPO sección Infraestructura RTO y.
6. En RTO/RPOtargets, introduzca un valor numérico en el cuadro y, a continuación, elija la unidad de tiempo que representa el valor para ambos RTORPO.

   Repita estas entradas para la infraestructura y la zona de disponibilidad en la RPO sección Infraestructura RTO y.
7. (Opcional) Si tiene una aplicación multirregional y quiere definir una región RTORPO, active Región: opcional.

   En RTOy RPO, introduce un valor numérico en el cuadro y, a continuación, elige la unidad de tiempo que representa el valor para ambos RTO. RPO

## Next

the section called “Paso 5: Configurar la evaluación programada y la notificación de deriva”

# Paso 5: Configure 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 el IAM rol adecuado.
   - Si la aplicación está configurada con los permisos IAM de usuario actuales, debe crear el `AWSResilienceHubAsssessmentExecutionPolicy`

     mediante el procedimiento adecuado en the section called “Cómo funciona AWS Resilience Hub 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, active Recibir notificaciones cuando la aplicación se desvíe.

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

   > **Note**
   >
   > - AWS Resilience Hub Para permitir la publicación de notificaciones en tus SNS temas de Amazon, tu SNS tema de Amazon 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 tus SNS temas de Amazon”.

- 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 SNS temas de Amazon que estén en una región diferente Cuenta de AWS o diferente, o en ambas, selecciona Introducir SNS tema ARN e introduce el nombre del recurso de Amazon (ARN) del SNS tema de Amazon en el cuadro Proporcionar un SNS tema. Para obtener más informaciónARNs, consulte Amazon Resource Names (ARNs) en la Referencia AWS general.

### Next

Paso 6: configurar permisos

## Paso 6: configurar 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 IAM las funciones y IAM los permisos

1. Para seleccionar un IAM rol existente que se usará para acceder a los recursos de la cuenta actual, seleccione un IAM rol de la lista desplegable Seleccione un IAM rol.

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

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

- AWS IAMconsola: si elige esta opción, debe completar el procedimiento descrito en Para crear su rol de AWS Resilience Hub en la IAM consola.

- AWS CLI— Si elige esta opción, debe completar todos los pasos que se indican 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 IAM funciones desde una cuenta cruzada (opcional).
3. Para seleccionar IAM roles de una cuenta cruzada, introduzca el rol ARNs del IAM rol en el ARN cuadro Introducir un IAM rol. Asegúrese ARNs de que los IAM roles que va a introducir no pertenezcan a la cuenta corriente.
4. Si desea utilizar el IAM usuario actual para descubrir los recursos de la aplicación, seleccione la flecha derecha para expandir la sección Usar los permisos del IAM usuario actual y seleccione Tengo entendido que debo configurar los permisos manualmente para habilitar la funcionalidad requerida en ellos AWS Resilience Hub.

   Si selecciona esta opción, es posible que algunas de las AWS Resilience Hub funciones (como la notificación de errores) no funcionen según lo esperado y se ignorarán las entradas que proporcionó en los pasos 1 y 3.

### Next

Paso 7: configurar los parámetros de configuración de la aplicación

## Paso 7: configurar 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

Paso 8: Añadir etiquetas

## Paso 8: Añadir etiquetas

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

(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

Paso 9: Revise y publique su aplicación AWS Resilience Hub

## Paso 9: Revise y publique su aplicación AWS Resilience Hub

Después de la publicación, aún puede revisar la aplicación y editar sus recursos. Cuando termine, seleccione Publicar para publicar la aplicación.

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

Paso 10: Realice una evaluación de la aplicación AWS Resilience Hub

# Paso 10: Realice una evaluación de la 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.

# Uso 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 que se produzcan interrupciones en las aplicaciones.

Temas:



## 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 eventos de resiliencia (por ejemplo, una base de datos no disponible o una validación de resiliencia fallida), alertas e información de servicios como CloudWatch Amazon 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 (SOP) de recuperación 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 Visualizar los experimentos de inyección de errores.

# 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 AWS 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 resiliencia realizando otra evaluación, comparando los resultados y, a continuación, reiterando el proceso hasta que la carga de trabajo estimada y la carga de trabajo estimada RPO cumplan sus RTO objetivos RTO y objetivos. 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 desfase: indica si su solicitud se ha desviado o no de la anterior evaluación satisfactoria y establece 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 se agregaron o eliminaron los recursos de las fuentes de entrada, que se incluyen en la versión actual de la aplicación.
  - Sin desviaciones: indica que se estima que la aplicación sigue cumpliendo RTO los RPO objetivos definidos en la política. Además, también indica que los recursos de las fuentes de entrada, que se incluyen en la versión actual de la aplicación, no se agregaron ni eliminaron.
- Carga de trabajo estimada RTO: indica la carga RTO de trabajo estimada máxima posible de la aplicación. Este valor es la carga RTO de trabajo máxima estimada de todos los tipos de interrupciones a partir de la última evaluación correcta.
- Carga de trabajo estimada RPO: indica la carga RPO de trabajo estimada máxima posible de la aplicación. Este valor es la carga RTO de trabajo máxima estimada de todos los tipos de interrupciones a partir de la última evaluación correcta.
- 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 del recurso de Amazon (ARN) de su aplicación. Para obtener más informaciónARNs, consulte Amazon Resource Names (ARNs) en la Referencia AWS general.

> **Note**
>
> AWS Resilience Hub puede evaluar completamente la resiliencia de los ECS recursos de Amazon 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 gestionarla.

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

- Resumen de la evaluación
- Resumen
- 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 Al 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 el resultado de unLLM.

## 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 la correcta. SOP

Por ejemplo, supongamos que se AWS Resilience Hub recomienda realizar una prueba con una alarma y otra. SOP Cuando se ejecuta la prueba, la alarma inicia la asociada ySOP, 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 Gestión de los experimentos de Amazon Fault Injection Service.

## 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.

Agregue 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 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. Selecciona Apagar.

Para activar 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 deriva.
   - Selecciona Activar la notificación en la sección de desviaciones de aplicaciones.
4. Complete los pasos indicados yPaso 5: Configure 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 yPaso 5: Configure 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 Paso 6: configurar 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, AWS CloudFormation pilas, AppRegistry aplicaciones AWS Resource Groups, archivos de estado de Terraform de Amazon EKS 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 “Paso 3: agregar recursos a la 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, seleccione el número que aparece debajo de cada criterio 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 o aplicación agregada manualmente. AppRegistry AWS Resource Groups

> **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 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. Las fuentes de entrada incluyen AWS CloudFormation pilas, AppRegistry aplicaciones AWS Resource Groups, 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 fuentes: la AWS CloudFormation pila que contiene el recurso. Esta columna depende del tipo de estructura de aplicación que haya seleccionado.
- 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.
- 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 Paso 3: Añada recursos a su AWS Resilience Hub aplicación 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 Añadir.

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 Añadir.

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::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

Cuando se importa 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, pero es posible que no siempre sea 100% preciso. Además, AWS Resilience Hub realiza las siguientes actividades una vez que la aplicación y sus recursos se hayan importado correctamente:

- Analiza sus 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 los mismos recursos que las recomendaciones y permite aceptarlos, modificarlos (añadirlos o eliminarlos) o rechazarlos. 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 la carga de trabajo estimada RTO y la carga de trabajo estimada RPO para generar recomendaciones.

Los siguientes son ejemplos de agrupaciones correctas:

- Agrupe las bases de datos y réplicas principales en una sola. AppComponent
- Agrupe un bucket de Amazon S3 y su replicación de destino en uno solo AppComponent.
- Agrupe EC2 las instancias de Amazon que ejecutan la misma aplicación en una sola AppComponent.
- Agrupa una SQS cola de Amazon y su cola de letra muerta en una sola. AppComponent
- Agrupe ECS los servicios de Amazon en una región y realice la conmutación por error de ECS los servicios de Amazon en otra región en una sola AppComponent.

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

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

### AWS Resilience Hub recomendaciones de agrupación de recursos

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

> **Note**
>
> Puede conceder los IAM permisos 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 agrupación 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 agrupación 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 mediante lo siguiente:

   - 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 o AWS Resource Groups la AppRegistry aplicación agregada manualmente.
   - ID físico: el identificador asignado real al recurso, como un ID de EC2 instancia de Amazon 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 agrupación 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 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 agrupación de recursos

1. Complete los pasos del Para ver las recomendaciones de agrupación 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 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 Guardar.
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 Ejecución y gestión de las AWS Resilience Hub evaluaciones de resiliencia.

## 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 o AWS Resource Groups la aplicación agregada manualmente. AppRegistry

     > **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 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.
- AppComponent tipo: el tipo de fuente de entrada. Las fuentes de entrada incluyen AWS CloudFormation pilas, AppRegistry aplicaciones AWS Resource Groups, archivos de estado de Terraform y recursos añadidos manualmente.

  > **Note**
  >
  > Para editar tus EKS clústeres de Amazon, sigue los pasos del procedimiento Para editar las fuentes de entrada de tu AWS Resilience Hub solicitud.

- 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.
- 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 diez aplicaciones, debe eliminar una o más aplicaciones antes de poder añadir más.

Eliminación de una aplicación

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 “Paso 1: Introducción mediante la adición de una aplicación” a the section called “Paso 8: Añadir etiquetas a su 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.

# Ejecución y gestión de las AWS Resilience Hub evaluaciones de resiliencia

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 y prueba. SOP 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. SOPlas recomendaciones proporcionan scripts que gestionan los procesos de recuperación comunes, 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.

## Realizar evaluaciones de resiliencia

Puede ejecutar un informe de evaluación de la resiliencia desde varias ubicaciones en AWS Resilience Hub. Para obtener más información acerca de su aplicación, consulte the section called “Administración de aplicaciones ”.

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, seleccione un informe de evaluación de la tabla Evaluaciones de la 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

## Revisión

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 las políticas actuales RTO y RPO las políticas y determina si el componente de aplicación puede alcanzar 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. Seleccione Publicar y evaluar para incluir los recursos actualizados en la aplicación y recibir una evaluación de resiliencia precisa.

Puede identificar las fuentes de entrada desviadas mediante lo siguiente:

- 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 o AWS Resource Groups la AppRegistry aplicación agregada manualmente.
- Cambio: indica si se agregó o eliminó un recurso de entrada.
- Nombre de la fuente: 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 la fuente 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 AWS región 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 una carga de trabajo estimadaRTO.

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 una carga de trabajo estimadaRPO.

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.

- Estimado RTO

  Indica si la configuración de la política se ajusta a los requisitos de la política. Proporcionamos dos valores, nuestro estimado RTO y el objetivo RTO. Por ejemplo, si ve un valor de 2 horas en la carga de trabajo objetivo RTO y 40 millones en la carga de trabajo estimada RTO, indica que tenemos una carga RTO de trabajo estimada de 40 minutos, mientras que la actual RTO de su solicitud es de dos horas. Basamos nuestro RTO cálculo de la carga de trabajo estimada en la configuración, no en la política. Como resultado, una base de datos de zonas de disponibilidad múltiple tendrá la misma carga de trabajo estimada en caso RTO de fallo en una zona de disponibilidad, independientemente de la política que seleccione.

- RTOderiva

  Indica el tiempo durante el cual su solicitud se ha desviado de la carga RTO de trabajo estimada de la anterior evaluación satisfactoria. Proporcionamos dos valores: el estimado RTO y el de RTOdesviación. Por ejemplo, si ve un valor de 2 horas en la estimación RTO y 40 minutos por debajo de la RTOdesviación, esto indica que su solicitud se desvía en 40 minutos de la carga RTO de trabajo estimada de la anterior evaluación satisfactoria.

- Estimación RPO

  Muestra la RPO política de carga de trabajo estimada real que AWS Resilience Hub calcula, en función de la RPO política específica que haya establecido para cada componente de la aplicación. Por ejemplo, es posible que haya fijado en una hora el RPO objetivo de su política de resiliencia para los fallos 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 RTO RPO objetivo que puedes optar por no suministrar es la Región. En el caso de algunas aplicaciones, resulta útil planificar la recuperación cuando existe una dependencia crucial de un AWS servicio, que podría dejar de estar disponible en toda la región.

Si eliges esta opción, por ejemplo, si RTO estableces RPO objetivos para la región, recibirás un tiempo de recuperación estimado y recomendaciones operativas en caso de producirse este tipo de errores.

- RPOderiva

  Indica el tiempo durante el cual su solicitud se ha desviado de la carga RPO de trabajo estimada de la anterior evaluación satisfactoria. Proporcionamos dos valores: el estimado RPO y el de RPOdesviación. Por ejemplo, si ve un valor de 2 horas en la estimación RPO y 40 minutos por debajo de la RPOdesviación, esto indica que su solicitud se desvía en 40 minutos de la carga RPO de trabajo estimada de la anterior evaluación satisfactoria.

## Revisar las recomendaciones de resiliencia

Las recomendaciones de resiliencia evalúan los componentes de la aplicación y recomiendan cómo optimizarlos en función de la carga de trabajo estimada RTO y la carga de trabajo estimadaRPO, los costes y los cambios mínimos.

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

> **Note**
>
> - AWS Resilience Hub ofrece hasta tres opciones AWS Resilience Hub recomendadas.
> - Si establece la región RTO y RPO los objetivos, AWS Resilience Hub muestra Optimize for RegionRTO/RPOen las opciones recomendadas. Si la región RTO y RPO los objetivos no están configurados, se muestra Optimizar para la zona de disponibilidad (AZ)RTO/RPO. Para obtener más información sobre cómo establecer RPO objetivos RTO regionales o objetivos al crear políticas de resiliencia, consulteCrear políticas de resiliencia .
> - La carga de trabajo estimada RTO y RPO los valores de carga de trabajo estimados 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. Debería utilizar sus propias pruebas (como Amazon Fault Injection Service) para comprobar los tiempos de recuperación reales de su aplicación.

Optimice para la zona de disponibilidadRTO/RPO

Los tiempos de recuperación de la carga de trabajo estimados más bajos posibles (RTO/RPO) durante una interrupción en la zona de disponibilidad (AZ). Si la configuración no se puede cambiar lo suficiente como para cumplir los RTO RPO objetivos, 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.

Optimiza para la regiónRTO/RPO

Los tiempos de recuperación de la carga de trabajo estimados (RTO/RPO) más bajos posibles durante una interrupción regional. Si la configuración no se puede cambiar lo suficiente como para cumplir con los RTO RPO objetivos establecidos, 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 para reducir 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).

- Carga de trabajo estimada RTO y RPO

  La carga de trabajo estimada RTO y la carga de trabajo estimada RPO después de los cambios.

AWSResilience Hub evalúa si un componente de la aplicación (AppComponent) puede cumplir con una política de resiliencia. Si no AppComponent cumple con una política de AWS resiliencia y Resilience Hub no puede hacer ninguna recomendación para facilitar su cumplimiento, es posible que se deba a que el tiempo de recuperación del seleccionado AppComponent no se puede cumplir dentro de las limitaciones de la. AppComponent Algunos ejemplos de AppComponent restricciones incluyen 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 de AWS CloudFormation plantilla para descargar y administrar la infraestructura de la aplicación como 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 Amazon Simple Storage Service URI en lugar de utilizarCLI/APIcon 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 ha creado a través de un Amazon Simple Storage Service (Amazon URL 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” 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 recomendadosSOPs, 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 SOP de an en la columna Estado.

    b. En Acciones, elija Excluir los seleccionados para excluir los seleccionados 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.

# 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 la aplicación cambian, debe realizar una evaluación de la resiliencia para asegurarse de que dispone de las alarmas correctas para la aplicación actualizada.

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 AWS 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 Amazon S3URL, descargarla y colocarla en su canalización de código o crear una pila a través de la AWS CloudFormation consola.

Para crear una alarma basada en AWS Resilience Hub las recomendaciones, debe crear una AWS CloudFormation plantilla para las alarmas recomendadas e incluirlas en su 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 del 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” 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 DATA en INSUFFICIENT_ 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 AWS 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 SOP carpeta.
4. Para copiar la ruta de Amazon S3, seleccione la casilla de verificación situada delante del JSON archivo y elija 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 AWS 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 AWS CloudFormation plantilla mediante Amazon S3 URL y descargarla y colocarla en su canalización de código o crear una pila a través de la AWS 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 mediante 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.
- FISen 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 él 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 DATA en INSUFFICIENT_ 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 del 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 del 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 DATA en INSUFFICIENT_ 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. Prepare, pruebe y mida sus SOP con antelación para garantizar una recuperación oportuna en caso de una interrupción operativa.

En función de los componentes de la aplicación, AWS Resilience Hub recomienda los SOP que debe preparar. 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.

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 AWS 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 AWS CloudFormation plantilla a partir de las AWS Resilience Hub recomendaciones es un buen comienzo. Utilice la AWS CloudFormation plantilla para generar una AWS 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 AWS CloudFormation plantilla para los SOP recomendados e incluirlos en su base de código.

Cree una AWS CloudFormation plantilla para las recomendaciones de los 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” 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 los SOP que están implementados en su aplicación mediante 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.

## Pruebas de los SOP

Como se ha mencionado anteriormente, la mejor práctica consiste en añadir AWS FIS experimentos a las canalizaciones de CI/CD para probar los SOP con regularidad; de este modo, se garantiza que estén listos para funcionar en caso de que se produzca una interrupción.

Pruebe los SOP proporcionados y los AWS Resilience Hub personalizados.

# Visualización de los procedimientos operativos estándar

Para ver los SOP implementados 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 Resumen de los procedimientos operativos estándar, la tabla Procedimientos operativos estándar implementados muestra la lista de los SOP que se generan a partir de las recomendaciones del SOP.

   Puede identificar sus SOP de 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 los SOP recomendados 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. Seleccione la pestaña Procedimientos operativos estándar.

   En la tabla Procedimientos operativos estándar puede obtener más información sobre los SOP recomendados 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.

# Gestión de los experimentos de Amazon Fault Injection Service

En esta sección, se describe cómo crear y ejecutar experimentos del Servicio de inyección de errores de Amazon (AWS FIS) en AWS Resilience Hub. Realiza AWS FIS experimentos para medir la resiliencia de sus AWS recursos y el tiempo que tarda en recuperarse de las aplicaciones, la infraestructura, la zona de disponibilidad y Región de AWS los incidentes.

Para medir la resiliencia, estos AWS FIS experimentos simulan las interrupciones en sus recursos. AWS Algunos ejemplos de interrupciones incluyen errores de red no disponibles, conmutaciones por error, procesos detenidos en Amazon EC2 AWS o ASG, recuperación de arranque en Amazon RDS y 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 . La mayoría de los AWS FIS experimentos invocan acciones de automatización de Systems Manager para realizar interrupciones y monitorear las alarmas, y otros AWS FIS experimentos utilizan solo acciones de AWS FIS automatización personalizadas para AWS servicios específicos (como la acción EKS de Amazon). Para obtener más información sobre acciones AWS FIS , consulte la referencia de acciones AWS FIS.

Puede utilizar los AWS FIS experimentos en su estado predeterminado o personalizarlos en función de sus necesidades. AWS FIS Se puede acceder a los experimentos desde AWS Resilience Hub (the section called “Visualizar los experimentos de inyección de errores”) o desde AWS FIS la consola (AWS FIS).

Temas

- Crear AWS FIS experimentos a partir de las recomendaciones operativas
- Realizar un AWS FIS experimento desde AWS Resilience Hub
- Visualizar los experimentos de inyección de errores
- Comprobación de estado/fallos en el experimento del Servicio de inyección de errores de Amazon

## Crear AWS FIS experimentos a partir de las recomendaciones operativas

AWS Resilience Hub recomienda que pruebe la aplicación después de ejecutar un informe de evaluación. Puede acceder a estos experimentos y ejecutarlos desde el informe de evaluación de su aplicación.

AWS Resilience Hub proporciona una lista de AWS FIS experimentos, que son documentos de Systems Manager con parámetros de prueba. Al seleccionar un AWS FIS experimento de la lista, AWS Resilience Hub crea una AWS CloudFormation plantilla con los parámetros que defina en el documento de Systems Manager. Tras crear la AWS CloudFormation pila, podrá ver los AWS FIS experimentos aprovisionados para su aplicación.

La AWS CloudFormation plantilla consta de un rol de IAM para cada documento de Systems Manager, con los permisos mínimos necesarios para ejecutarse.

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

Para crear una AWS CloudFormation plantilla para el AWS FIS experimento

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 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” y, a continuación, vuelva a este paso.
6. En Recomendaciones operativas, seleccione Experimentos de inyección de errores.
7. Seleccione todas las pruebas que desee incluir.
8. Selecciona Crear CloudFormation plantilla. La creación de la AWS CloudFormation plantilla puede tardar unos minutos.
9. Elija Plantillas.

   Puede ver la AWS CloudFormation plantilla recién creada en la tabla de plantillas.

   Complete el siguiente procedimiento para incluir las recomendaciones 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, elige el nombre de la plantilla de AWS FIS experimento que acabas de crear.

Puede identificar las pruebas que se implementan en su aplicación con la siguiente información:

- Nombre de la prueba: nombre de la prueba que ha creado para la aplicación.
- Descripción: describe el objetivo de la prueba.
- Estado: indica el estado de implementación actual de la prueba.

  Esta columna muestra uno de los siguientes valores:

  - Implementada: indica que la prueba está implementada en la aplicación.
  - No implementada: indica que la prueba no está implementada ni incluida en la aplicación.
  - Excluida: indica que la prueba está excluida de la aplicación.
  - Inactiva: indica que la prueba se ha implementado en los últimos 30 días AWS FIS, pero no se ha ejecutado en los últimos 30 días.
- 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 experimento.

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 de prueba.
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 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.

## Realizar un AWS FIS experimento desde AWS Resilience Hub

En su aplicación, primero debe crear una plantilla de AWS FIS experimento a partir de las recomendaciones operativas antes de AWS Resilience Hub poder ejecutar el AWS FIS experimento.

Para iniciar un AWS FIS experimento

1. En el menú de navegación a la izquierda, elija Aplicaciones.
2. En la tabla Aplicaciones, abra una aplicación.
3. Seleccione la pestaña Experimentos de inyección de errores.
4. Seleccione el botón de opción antes de la plantilla de experimentos utilizada para crear el experimento que desea ejecutar en la tabla Plantillas de experimentos y, a continuación, seleccione Iniciar experimento.

Para detener un AWS FIS experimento

1. En el menú de navegación a la izquierda, elija Aplicaciones.
2. En la tabla Aplicaciones, abra una aplicación.
3. Seleccione la pestaña Experimentos de inyección de errores.
4. Seleccione el botón de opción antes del experimento en la tabla Experimento y, a continuación, elija Detener el experimento.

## Visualizar los experimentos de inyección de errores

En AWS Resilience Hub, consulte los AWS FIS experimentos que configuró para medir la resiliencia de sus AWS recursos y el tiempo que tarda en recuperarse de las aplicaciones, la infraestructura, la zona de disponibilidad y Región de AWS los incidentes.

Para ver AWS FIS los experimentos desde el panel de control, selecciona Panel de control en el menú de navegación de la izquierda. En la tabla de experimentos, puede identificar los AWS FIS experimentos implementados utilizando la siguiente información:

- ID del experimento: identificador del experimento de AWS FIS .
- ID de plantilla de experimento: identificador de la plantilla de AWS FIS experimento que se utilizó para crear el AWS FIS experimento.
- Plantilla de origen: proporciona el nombre de recurso de Amazon (ARN) de la AWS CloudFormation pila que contiene los detalles del AWS FIS experimento.
- Estado: indica si el AWS FIS experimento se ha completado correctamente o no.

Para ver los AWS FIS experimentos implementados desde las aplicaciones

1. En el menú de navegación a la izquierda, elija Aplicaciones.
2. En la tabla Aplicaciones, abra una aplicación.
3. Seleccione Experimentos de inyección de errores.
4. Seleccione la pestaña Experimento.

   En la pestaña Experimento, puede ver una lista de los AWS FIS experimentos activos en la tabla de experimentos.

   En la tabla Experimentos, puede identificar el experimento de AWS FIS implementado con la siguiente información:

   - Nombre de la prueba: nombre de la prueba recomendada por AWS Resilience Hub que se utilizó para crear el AWS FIS experimento.
   - ID del experimento: identificador del experimento de AWS FIS .
   - Descripción: describe el objetivo del AWS FIS experimento.
   - Hora de creación: fecha y hora en que se creó el experimento de AWS FIS .
   - Hora de la última actualización: fecha y hora en que se actualizó el experimento de AWS FIS por última vez.
   - Plantilla de origen: proporciona el nombre de recurso de Amazon (ARN) de la AWS CloudFormation pila que contiene los detalles del AWS FIS experimento.

Para ver los experimentos recomendados 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. Seleccione la pestaña Experimentos de inyección de errores.

   En la tabla Plantillas de experimentación de inyección de errores, puede obtener más información sobre las pruebas recomendadas utilizando la siguiente información:

   - Nombre: nombre de la prueba recomendada.
   - Descripción: describe el objetivo de la prueba.
   - Estado: indica el estado de implementación actual de la prueba.

     Esta columna muestra uno de los siguientes valores:

     - Implementada: indica que la prueba está implementada en la aplicación.
     - No implementada: indica que la prueba no está implementada ni incluida en la aplicación.
     - Excluida: indica que la prueba está excluida de la aplicación.
     - Inactivo: indica que la prueba se ha implementado en AWS FIS, pero no se ha ejecutado en los últimos 30 días.
   - Configuración: indica si hay alguna dependencia de configuración pendiente que deba abordarse.
   - Tipo: indica el tipo de prueba.
   - AppComponent— Indica los componentes de la aplicación (AppComponents) que están asociados a esta prueba. Para obtener más información sobre los recursos compatibles AppComponents, consulte Agrupación de recursos en un AppComponent.

- Riesgo: indica el nivel de riesgo de que falle la prueba. Los niveles de riesgo se indican utilizando los valores Alto, Medio y Bajo para indicar los niveles de riesgo alto, moderado y bajo, respectivamente.
- 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.

## Comprobación de estado/fallos en el experimento del Servicio de inyección de errores de Amazon

AWS Resilience Hub le permite realizar un seguimiento del estado del experimento que ha iniciado. Para obtener más información, consulte el procedimiento Para ver los experimentos recomendados a partir de las evaluaciones enthe section called “Visualizar los experimentos de inyección de errores”.

Temas

- Análisis de la ejecución de AWS FIS experimentos con AWS Systems Manager
- AWS FIS experimente errores al probar los pods de Kubernetes que se ejecutan en sus clústeres de Amazon Elastic Kubernetes Service

### Análisis de la ejecución de AWS FIS experimentos con AWS Systems Manager

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

1. Vaya a CloudTrail> Historial de eventos.
2. Filtre los eventos por Nombre de usuario mediante el ID del experimento.
3. Vea 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

del detalle 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 alarmas no se implementó antes de que se ejecutara el experimento de prueba/SOP. 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 la sección 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 AWS CloudFormation pila de pruebas) al usuario de Kubernetes.
- No se pudo iniciar el AWS FIS Pod: se alcanzó el número máximo de contenedores de sidecar defectuosos. 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 realizar una prueba con una alarma y otraSOP. La prueba se ejecuta, activa la alarma e inicia la asociadaSOP. 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 recomendaciones de alarmas y pruebas, consultethe section called “Incluir o excluir recomendaciones operativas”. SOP

## 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) que deben corregirse para resolver las infracciones de la política de resiliencia de la aplicación. Elija el valor para ver los RPO detalles deRTO/en el informe de evaluación de su solicitud.
     - 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 su 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:

- RTO/RPOconformidad: 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 definidos en la política de resiliencia de la aplicación. Elija el valor para ver las RPO estimacionesRTO/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.
- SOPsimplementada: 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.
- FISexperimentos 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. Elija el valor situado junto a RTO/RPOpara ver los detalles en la pestaña de recomendaciones de resiliencia del informe de evaluación de su solicitud.
  - 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 el número 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 solicitud.

## 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 la puntuación solo se pueden obtener mediante el. `ScoringComponentResiliencyScore` API Para obtener más información al respectoAPI, 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 AppComponents y los tipos de interrupciones

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 | Descripción | Fórmula | 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.<br><br>**Note**<br>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)`<br><br>Algunas partes de la fórmula son las siguientes:<br><br>• 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.<br>• Número total de pruebas recomendadas: indica las pruebas recomendadas en AWS Resilience Hub función de los recursos de la aplicación.<br>• 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:<br><br>`T = (10 + 5) / 20`<br><br>Es decir, `T = .75 or 75 points` |

| Componente de puntuación | Descripción | Fórmula | 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.<br><br>**Note**<br>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)`<br><br>Algunas partes de la fórmula son las siguientes:<br><br>• 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.<br>• Número total de alarmas recomendadas: indica las CloudWatch alarmas de Amazon recomendadas en AWS Resilience Hub función de los recursos de la aplicación.<br>• 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:<br><br>`A = (10 + 5) / 20`<br><br>Es decir, `A = .75 or 75 points` |

| Componente de puntuación | Descripción | Fórmula | Ejemplo |
| --- | --- | --- | --- |
| | | excluido de la aplicación. | |

| Componente de puntuación | Descripción | Fórmula | Ejemplo |
| --- | --- | --- | --- |
| SOPcobertura (S) | Una puntuación normalizada (0 a 100 puntos) basada en el número de los SOPs que se han implementado y excluido satisfactoriamente, del número total de AWS Resilience Hub recomendados. SOPs | `S = ((Total number of SOPs implemented) + (Total number of SOPs excluded)) / (Total number of SOPs recommended)`<br><br>Algunas partes de la fórmula son las siguientes:<br><br>• 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.<br>• Número total de SOPs recomendados: indica el número SOPs recomendado en AWS Resilience Hub función de los recursos de la aplicación.<br>• 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 las 20 AWS Resilience Hub recomendadasSOPs, la SOP cobertura se calcula de la siguiente manera:<br><br>`S = (10 + 5) / 20`<br><br>Es decir, `S = .75 or 75 points` |

| Componente de puntuación | Descripción | Fórmula | Ejemplo |
| --- | --- | --- | --- |
| RTO/RPOconformidad (P) | Una puntuación normalizada (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 resiliencia (P) se calcula de la siguiente manera:<br>• Si ha establecido objetivos regionales RTO y RPO objetivos , P se calcula de la siguiente manera:<br>`P = (20 + 30)/ 100`<br>Es decir, `P = .5 or 50 points`<br>• Si no ha establecido RPO objetivos ni RTO regionales, P se calcula de la siguiente manera: |

| Componente de puntuación | Descripción | Fórmula | Ejemplo |
| --- | --- | --- | --- |
| | | | `P = (22.22 + 33.33)/ 99.9`<br><br>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 | Descripción | Fórmula | 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:<br>`RS = (T * Weight(T) +`<br><br>`A * Weight(A) +`<br><br>`S * Weight(S) +`<br><br>`P * Weight(P)) /`<br><br>`(Weight(T) + Weight(A) + Weight(S) + Weight(P))` | Las fórmulas para calcular la cobertura de cada tabla de tipos de recomendación son las siguientes:<br><br>• `Test coverage (T) = .75`<br>• `Alarms (A) = .75`<br>• `SOPs (S) = .75`<br>• `Meeting resiliency policy (P) = .5` |

| Componente de puntuación | Descripción | Fórmula | Ejemplo |
| --- | --- | --- | --- |
| | | | La puntuación de resiliencia por aplicación se calcula de la siguiente forma:<br><br>`RS = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) /(.2 + .2 + .2 + .4)`<br><br>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 AWS Resilience Hub: APIs

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

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

| Componente de puntuación | Descripción | Fórmula | 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 | Descripción | Fórmula | 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.<br><br>Es decir: RSao = Weighted Average (T, A, S, P)<br><br>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:<br><br>RSao = (T * Weight(T) +<br><br>A * Weight(A) +<br><br>S * Weight(S) +<br><br>P * Weight(P)) /<br><br>(Weight(T) + Weight(A) + Weight(S) + Weight(P)) | recomendaciones son las siguientes:<br><br>• Test coverage (T) = .75<br>• Alarms (A) = .75<br>• SOPs (S) = .75<br>• Meeting resiliency policy (P) = .5<br><br>La puntuación de resiliencia por tipo de interrupción AppComponent y por tipo de interrupción se calcula de la siguiente manera:<br><br>RSao = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4)<br><br>Es decir, RSao = .65 or 65 points |

| Componente de puntuación | Descripción | Fórmula | Ejemplo |
| --- | --- | --- | --- |
| | con la política de resilienc ia del tipo AppCompon ent de interrupción. SOPs | | |

| Componente de puntuación | Descripción | Fórmula | 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)<br><br>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:<br><br>RSa = (T * Weight(T) +<br><br>A * Weight(A) +<br><br>S * Weight(S) +<br><br>P * Weight(P)) /<br><br>(Weight(T) + Weight(A) + Weight(S) + Weight(P)) | Las suposiciones RSa para todos los tipos de recomendaciones son las siguientes:<br><br>• Test coverage (T) = .75<br>• Alarms (A) = .75<br>• SOPs (S) = .75<br>• Meeting resiliency policy (P) = .5<br><br>La puntuación de resiliencia por AppComponent se calcula de la siguiente manera:<br><br>RSa = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4)<br><br>Es decir, RSa = .65 or 65 points |

| Componente de puntuación | Descripción | Fórmula | Ejemplo |
| --- | --- | --- | --- |
| | AppComponent | | |

| Componente de puntuación | Descripción | Fórmula | 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)`<br><br>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:<br><br>`RSo = (T * Weight(T) + A * Weight(A) +`<br><br>`S * Weight(S) + P * Weight(P)) /`<br><br>`(Weight(T) + Weight(A) + Weight(S) + Weight(P))` | Las suposiciones `RSo` para todos los tipos de recomendaciones son las siguientes:<br><br>• `Test coverage (T) = .75`<br>• `Alarms (A) = .75`<br>• `SOPs (S) = .75`<br>• `Meeting resiliency policy (P) = .5`<br><br>La puntuación de resiliencia por tipo de interrupción se calcula de la siguiente forma:<br><br>`RSo = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 *.4)) /`<br><br>`(.2 + .2 + .2 + .4)`<br><br>Es decir, `RSo = .65 or 65 points` |

| Componente de puntuación | Descripción | Fórmula | 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 pruebasSOPs, 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 RTO ni RPO los objetivos de 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 alarmasSOPs, 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 |
| Región | 10 puntos | N/A |

# Integrar las recomendaciones operativas en su aplicación con AWS CloudFormation

Tras seleccionar Crear CloudFormation plantilla en la página de recomendaciones operativas, AWS Resilience Hub crea una AWS CloudFormation plantilla que describe la alarma, el procedimiento operativo estándar (SOP) o el AWS FIS experimento específicos para su aplicación. La AWS 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 AWS CloudFormation plantilla JSON con formato en la que se describe una recomendación de alarma realizada 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 AWS CloudFormation plantilla

La forma más sencilla de integrar una alarma 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. SOP El archivo JSON con formato que se proporciona a continuación proporciona un esquema básico de cómo se describe una tabla de DynamoDB en una plantilla. AWS 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 AWS CloudFormation plantillas SOPs y AWS FIS realizar experimentos, adoptará el mismo enfoque: sustituirá las referencias codificadas por referencias IDs dinámicas que seguirán funcionando incluso después de cambios de hardware.

Al utilizar una referencia a la tabla de DynamoDB, AWS 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 AWS CloudFormation necesario reemplazar el recurso.

> **Note**
>
> Puede elegir métodos más avanzados para administrar los recursos de su aplicación AWS CloudFormation , como anidar pilas o consultar las salidas de recursos en una pila independiente AWS 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).

# Uso AWS Resilience Hub APIs para describir y administrar la aplicación

Como alternativa para describir y administrar la aplicación mediante AWS Resilience Hub la consola, AWS Resilience Hub permite describir y administrar las aplicaciones mediante AWS Resilience Hub APIs. En este capítulo se explica cómo crear una aplicación utilizando AWS Resilience Hub APIs. También define la secuencia en la que debe ejecutarse APIs y los valores de los parámetros que debe proporcionar con los ejemplos correspondientes. 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”

## Paso 1: 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 acerca de los AWS Resilience Hub APIs que se utilizan para preparar una solicitud, consulte los temas siguientes:

- the section called “Crear una aplicación”
- 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

Para crear una nueva aplicación en AWS Resilience Hub, debe llamar al `CreateApp` API y proporcionar un nombre de aplicación único. Para obtener más información al respectoAPI, consultehttps://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 uso `CreateApp`API.

### 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

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

El siguiente ejemplo muestra cómo crear `newPolicy` para su aplicación en AWS Resilience Hub uso `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 lo siguiente APIs para importar recursos a la aplicación:

- `ImportResourcesToDraftAppVersion`— Esto API le permite importar recursos a la versión preliminar de su aplicación desde diferentes fuentes de entrada. Para obtener más información al respectoAPI, consultehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_ImportResourcesToDraftAppVersion.html.
- `PublishAppVersion`— API Publica una nueva versión de la aplicación junto con la versión actualizada AppComponents. Para obtener más información al respectoAPI, consultehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_PublishAppVersion.html.
- `DescribeDraftAppVersionResourcesImportStatus`— Esto API le permite supervisar el estado de importación de sus recursos a una versión de la aplicación. Para obtener más

información al respectoAPI, consultehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeDraftAppVersionResourcesImportStatus.html.

El siguiente ejemplo muestra cómo importar recursos a la aplicación durante su AWS Resilience Hub uso `ImportResourcesToDraftAppVersion`API.

### 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>
        }
    ]
}
```

El siguiente ejemplo muestra cómo añadir recursos manualmente a la aplicación durante su AWS Resilience Hub uso `CreateAppVersionResource`API.

### 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"
            }
        ]
    }
}
```

El siguiente ejemplo muestra cómo supervisar el estado de importación de los recursos que se AWS Resilience Hub utilizan `DescribeDraftAppVersionResourcesImportStatus`API.

## 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 solicitud, utilice `PublishAppVersion`API. Para obtener más información al respectoAPI, consultehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_PublishAppVersion.html.

   El siguiente ejemplo muestra cómo publicar la versión preliminar de la aplicación en AWS Resilience Hub uso `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 utilizando `UpdateApp`API. Para obtener más información al respectoAPI, consultehttps://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 en AWS Resilience Hub uso `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"
    }
}
```

# Paso 2: Ejecutar y administrar evaluaciones de resiliencia AWS Resilience Hub

Tras 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 la carga de trabajo estimada RTO y estimada RPO que se define en la política de resiliencia. La evaluación compara la configuración de cada componente de la aplicación con la política y formula recomendaciones de alarma y prueba. SOP

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 de las evaluaciones de resiliencia AWS Resilience Hub

Para realizar evaluaciones de resiliencia AWS Resilience Hub y monitorear su estado, debe usar lo siguiente: APIs

- `StartAppAssessment`— Esto API crea una nueva evaluación para una aplicación. Para obtener más información al respectoAPI, consultehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_StartAppAssessment.html.
- `DescribeAppAssessment`— Esto API describe una evaluación de la solicitud y proporciona el estado de finalización de la evaluación. Para obtener más información al respectoAPI, consultehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeAppAssessment.html.

El siguiente ejemplo muestra cómo empezar a ejecutar una nueva evaluación en el AWS Resilience Hub uso `StartAppAssessment`API.

## 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": {}
    }
}
```

El siguiente ejemplo muestra cómo supervisar el estado de la evaluación al AWS Resilience Hub utilizarla `DescribeAppAssessment`API. 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 utilizando lo siguienteAPIs.

- `DescribeAppAssessment`— Esto API le permite hacer un seguimiento del estado actual de su solicitud 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 al respectoAPI, consultehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeAppAssessment.html.
- `ListAlarmRecommendations`— Esto API le permite obtener las recomendaciones de alarma utilizando el nombre del recurso de Amazon (ARN) de la evaluación. Para obtener más información al respectoAPI, consultehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_ListAlarmRecommendations.html.

> **Note**
>
> Para obtener las recomendaciones SOP y FIS probarlas, utilice `ListSopRecommendations` y `ListTestRecommendations`APIs.

El siguiente ejemplo muestra cómo obtener las recomendaciones de alarma utilizando el nombre del recurso de Amazon (ARN) de la evaluación que utiliza `ListAlarmRecommendations`API.

> **Note**
>
> Para obtener las recomendaciones SOP y FIS probarlas, sustitúyalas por una `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) utilizando `ListAppComponentRecommendations`API.

## 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"
                }
```

```
            ]
        }
    ]
}
```

# Paso 3: Modificación de su 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, AWS Resilience Hub le permite agregar manualmente el recurso a su aplicación mediante `CreateAppVersionResource`API. Para obtener más información al respectoAPI, consultehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateAppVersionResource.html.

Para ello, debe proporcionar los siguientes parámetrosAPI:

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

El siguiente ejemplo muestra cómo añadir recursos manualmente a la aplicación durante su AWS Resilience Hub uso `CreateAppVersionResource`API.

### 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 la siguiente administración de recursosAPIs.

- `UpdateAppVersionResource`— Esto API actualiza los detalles de los recursos de una aplicación. Para obtener más información al respectoAPI, consulte UpdateAppVersionResource.
- `DeleteAppVersionAppComponent`— Esto API los elimina AppComponent de la aplicación. Para obtener más información al respectoAPI, consulte DeleteAppVersionAppComponent.

En el siguiente ejemplo se muestra cómo actualizar los detalles de los recursos de la aplicación en AWS Resilience Hub uso `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 de AWS Resilience Hub uso `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 `UpdateAppVersionResource`API. Estos recursos no se tendrán en cuenta al calcular la resiliencia de la aplicación. Para obtener más información al respectoAPI, consultehttps://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 la aplicación durante su AWS Resilience Hub uso `UpdateAppVersionResource`API.

### 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 modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de cumplimiento aplicables AWS 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. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

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 AWS compartida modelo 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. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las

tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte la sección Privacidad de datos FAQ. Para obtener información sobre la protección de datos en Europa, consulte el modelo de responsabilidad AWS compartida y la entrada del GDPR blog sobre AWS seguridad.

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

- Utilice la autenticación multifactorial (MFA) con cada cuenta.
- UseSSL/TLSpara comunicarse con AWS los recursos. Necesitamos TLS 1.2 y recomendamos TLS 1.3.
- Configure API y registre la actividad del usuario con AWS CloudTrail.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita entre FIPS 140 y 3 módulos criptográficos validados para acceder a AWS través de una interfaz de línea de comandos o unaAPI, utilice un FIPS terminal. Para obtener más información sobre los FIPS puntos finales disponibles, consulte la Norma federal de procesamiento de información () FIPS 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con Resilience Hub u otro dispositivo Servicios de AWS mediante la consola, API AWS CLI, o. AWS SDKs Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, le recomendamos encarecidamente que no incluya información sobre las credenciales URL para validar su solicitud a ese servidor.

## Cifrado en reposo

AWS Resilience Hub cifra los 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 AWS los servicios y respalda las acciones para los recursos objetivo.

# Identity and Access Management for AWS Resilience Hub

AWS Identity and Access Management (IAM) es una Servicio de AWS que ayuda a un administrador a controlar de forma segura el acceso a AWS los recursos. IAMlos administradores controlan quién puede autenticarse (iniciar sesión) y quién está autorizado (tiene permisos) para usar los recursos de AWS Resilience Hub. IAMes una Servicio de AWS que puede utilizar sin coste adicional.

Temas

## Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realices en AWS Resilience Hub.

Usuario del servicio: si utiliza el servicio AWS Resilience Hub para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que utilice más funciones de AWS Resilience Hub para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una función de AWS Resilience Hub, consulteSolución de problemas de identidad y acceso a AWS Resilience Hub.

Administrador de servicios: si está a cargo de los recursos de AWS Resilience Hub en su empresa, probablemente tenga acceso completo a AWS Resilience Hub. Es su trabajo determinar a qué funciones y recursos de AWS Resilience Hub deben acceder los usuarios del servicio. A continuación, debe enviar solicitudes a su IAM administrador para cambiar los permisos de los usuarios del servicio. Revise la información de esta página para comprender los conceptos básicos deIAM. Para obtener más información sobre cómo su empresa puede utilizar IAM AWS Resilience Hub, consulteCómo funciona AWS Resilience Hub con IAM.

IAMadministrador: si es IAM administrador, tal vez quiera obtener más información sobre cómo puede redactar políticas para administrar el acceso a AWS Resilience Hub. Para ver ejemplos de políticas basadas en la identidad de AWS Resilience Hub que puede utilizarIAM, consulte. Ejemplos de políticas basadas en la identidad para AWS Resilience Hub

## Autenticación con identidades

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

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (IAMIdentity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, el administrador configuró previamente la federación de identidades mediante roles. IAM Cuando accede AWS mediante la federación, asume indirectamente un rol.

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

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

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

## Cuenta de AWS usuario root

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

## Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, 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 de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en IAM Identity Center, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus aplicaciones Cuentas de AWS . Para obtener información sobre IAM Identity Center, consulte ¿Qué es IAM Identity Center? en la Guía AWS IAM Identity Center del usuario.

## Usuarios y grupos de IAM

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

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

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

## IAMroles

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

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

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información sobre los roles para la federación, consulte Creación de un rol para un proveedor de identidad externo en la Guía del IAM usuario. Si usa IAM Identity Center, configura un conjunto de permisos. Para controlar a qué pueden acceder sus identidades después de autenticarse, IAM Identity Center correlaciona el conjunto de permisos con un rol en. IAM Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos IAM de usuario temporales: un IAM usuario o rol puede asumir un IAM rol para asumir temporalmente diferentes permisos para una tarea específica.
- Acceso multicuenta: puedes usar un IAM rol para permitir que alguien (un responsable de confianza) de una cuenta diferente acceda a los recursos de tu cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunos Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para conocer la diferencia entre las funciones y las políticas basadas en recursos para el acceso multicuenta, consulta el tema sobre el acceso a los recursos entre cuentas IAM en la Guía del IAM usuario.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros. Servicios de AWS Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un IAM usuario o un rol para realizar acciones en AWS ellas, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FASutiliza los permisos del principal que llama a an Servicio de AWS, junto con los que solicitan, Servicio de AWS para realizar solicitudes a los servicios descendentes. FASlas solicitudes solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información detallada sobre la política a la hora de realizar FAS solicitudes, consulte Reenviar las sesiones de acceso.
  - Función de servicio: una función de servicio es una IAMfunción que un servicio asume para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentroIAM. Para obtener más información, consulte Crear un rol para delegar permisos Servicio de AWS en un rol en el IAMManual del usuario.

  - Función vinculada a un servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un IAM administrador puede ver los permisos de los roles vinculados al servicio, pero no editarlos.
- Aplicaciones que se ejecutan en Amazon EC2: puedes usar un IAM rol para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y que realizan AWS CLI o AWS API solicitan. Esto es preferible a almacenar las claves de acceso dentro de la EC2 instancia. Para asignar un AWS rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte Uso de un IAM rol para conceder permisos a aplicaciones que se ejecutan en EC2 instancias de Amazon en la Guía del IAM usuario.

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

## Administración de acceso mediante políticas

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

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

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

IAMlas políticas definen los permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la

acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de AWS Management Console AWS CLI, el o el AWS API.

## Políticas basadas en identidad

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

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

## Políticas basadas en recursos

Las políticas basadas en recursos son documentos de JSON política que se adjuntan a un recurso. Algunos ejemplos de políticas basadas en recursos son las políticas de confianza de IAM roles y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

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

## Listas de control de acceso () ACLs

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

Amazon S3 AWS WAF y Amazon VPC son ejemplos de servicios compatiblesACLs. Para obtener más informaciónACLs, consulte la descripción general de la lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

## Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

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

## Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud

cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del IAM usuario.

## Cómo funciona AWS Resilience Hub con IAM

Antes de administrar el acceso IAM a AWS Resilience Hub, conozca qué IAM funciones están disponibles para usar con AWS Resilience Hub.

IAMfunciones que puede usar con AWS Resilience Hub

| IAMcaracterística | AWS Soporte para Resilience Hub |
|---|---|
| Políticas basadas en identidades | Sí |
| Políticas basadas en recursos | No |
| Acciones de políticas | Sí |
| Recursos de políticas | Sí |
| Claves de condición de política (específicas del servicio) | Sí |
| ACLs | No |
| ABAC(etiquetas en las 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 IAM las funciones, consulte AWS los servicios con los que funcionan IAM en la Guía del IAM usuario.

### Políticas basadas en la identidad para AWS Resilience Hub

Compatibilidad con las políticas basadas en identidad: sí

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

Con las políticas IAM basadas en la identidad, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para obtener más información sobre todos los elementos que puede utilizar en una JSON política, consulte la referencia sobre los elementos de la IAM JSON política en la Guía del IAMusuario.

Ejemplos de políticas basadas en la identidad para AWS Resilience Hub

Para ver ejemplos de políticas basadas en la identidad de AWS Resilience Hub, consulte. Ejemplos de políticas basadas en la identidad para AWS Resilience Hub

## Políticas basadas en recursos dentro de Resilience Hub AWS

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de JSON política que se adjuntan a un recurso. Algunos ejemplos de políticas basadas en recursos son las políticas de confianza de IAM roles y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar una cuenta completa o IAM entidades de otra cuenta como principales en una política basada en recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el IAM administrador de la cuenta de confianza también debe conceder permiso a la entidad principal (usuario o rol) para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de

la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte el tema Acceso a recursos entre cuentas IAM en la Guía del IAM usuario.

## Acciones políticas para AWS Resilience Hub

Compatibilidad con las acciones de política: sí

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

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

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

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. Ejemplos de políticas basadas en la identidad para AWS Resilience Hub

## Recursos de políticas para Resilience Hub AWS

Compatibilidad con los recursos de políticas: sí

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

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

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Para ver una lista de los tipos de recursos de AWS Resilience Hub y sus ARNs correspondientes, consulte los recursos definidos por AWS Resilience Hub en la Referencia de autorización de servicios. Para saber con qué acciones puede especificar cada recurso, consulte Acciones definidas por AWS Resilience Hub. ARN

Para ver ejemplos de políticas basadas en la identidad de AWS Resilience Hub, consulte. Ejemplos de políticas basadas en la identidad para AWS Resilience Hub

## Condiciones políticas: claves para Resilience Hub AWS

Compatibilidad con claves de condición de políticas específicas del servicio: sí

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

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

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación

lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

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

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del IAMusuario.

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. Ejemplos de políticas basadas en la identidad para AWS Resilience Hub

## ACLsen AWS Resilience Hub

SoportesACLs: No

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

## ABACcon AWS Resilience Hub

Soportes ABAC (etiquetas en las políticas): parciales

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define los permisos en función de los atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a IAM entidades (usuarios o roles) y a muchos AWS recursos. Etiquetar entidades y recursos es el primer paso deABAC. Luego, diseñe ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso al que está intentando acceder.

ABACes útil en entornos de rápido crecimiento y ayuda en situaciones en las que la administración de políticas se vuelve engorrosa.

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 al respectoABAC, consulte ¿Qué es? ABAC en la Guía IAM del usuario. Para ver un tutorial con los pasos de configuraciónABAC, consulte Usar el control de acceso basado en atributos (ABAC) en la Guía del IAMusuario.

## Uso de credenciales temporales con Resilience Hub AWS

Compatibilidad con credenciales temporales: sí

Algunas Servicios de AWS no funcionan cuando se inicia sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre cuáles Servicios de AWS funcionan con credenciales temporales, consulta la sección Servicios de AWS Cómo trabajar con credenciales temporales IAM en la Guía del IAM usuario.

Está utilizando credenciales temporales si inicia sesión AWS Management Console con cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de rol, consulte Cambiar a un rol (consola) en la Guía del IAMusuario.

Puede crear credenciales temporales manualmente con la tecla AWS CLI o AWS API. A continuación, puede utilizar esas credenciales temporales para acceder AWS. 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.

## Sesiones de acceso directo para AWS Resilience Hub

Admite sesiones de acceso directo (FAS): Sí

Cuando utilizas un IAM usuario o un rol para realizar acciones en AWSél, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FASutiliza los permisos del principal que llama a una Servicio de AWS y los

solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. FASlas solicitudes solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información detallada sobre la política a la hora de realizar FAS solicitudes, consulte Reenviar las sesiones de acceso.

### Funciones de servicio de AWS Resilience Hub

Compatibilidad con roles de servicio: sí

Una función de servicio es una IAMfunción que asume un servicio para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentroIAM. Para obtener más información, consulte Crear un rol para delegar permisos Servicio de AWS en un rol en el IAMManual del usuario.

> **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.

## Ejemplos de políticas basadas en la identidad para AWS Resilience Hub

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos de AWS Resilience Hub. Tampoco pueden realizar tareas con AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS API. Para conceder a los usuarios permiso para realizar acciones en los recursos que necesitan, un IAM administrador puede crear IAM políticas. A continuación, el administrador puede añadir las IAM políticas a las funciones y los usuarios pueden asumir las funciones.

Para obtener información sobre cómo crear una política IAM basada en la identidad mediante estos documentos de JSON política de ejemplo, consulte Creación de IAM políticas en la Guía del IAMusuario.

Para obtener más información sobre las acciones y los tipos de recursos definidos por AWS Resilience Hub, incluido el formato 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. ARNs

Temas



## Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad 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. Para obtener más información, consulte las políticas AWS gestionadas o las políticas AWS gestionadas para las funciones laborales en la Guía del IAM usuario.
- Aplique permisos con privilegios mínimos: cuando establezca permisos con IAM políticas, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Para obtener más información sobre cómo IAM aplicar permisos, consulte Políticas y permisos IAM en la IAM Guía del usuario.
- Utilice las condiciones en IAM las políticas para restringir aún más el acceso: puede añadir una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de política para especificar que todas las solicitudes deben enviarse medianteSSL. También puedes usar condiciones para conceder el acceso a las acciones del

servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte los elementos IAM JSON de la política: Condición en la Guía del IAM usuario.

- Utilice IAM Access Analyzer para validar sus IAM políticas y garantizar permisos seguros y funcionales: IAM Access Analyzer valida las políticas nuevas y existentes para que se ajusten al lenguaje de las políticas (JSON) y IAM a las IAM mejores prácticas. IAMAccess Analyzer proporciona más de 100 comprobaciones de políticas y recomendaciones prácticas para ayudarle a crear políticas seguras y funcionales. Para obtener más información, consulte la validación de políticas de IAM Access Analyzer en la Guía del IAM usuario.
- Requerir autenticación multifactorial (MFA): si se encuentra en una situación en la que se requieren IAM usuarios o un usuario raíz Cuenta de AWS, actívela MFA para aumentar la seguridad. Para solicitarlo MFA cuando se convoque a API las operaciones, añada MFA condiciones a sus políticas. Para obtener más información, consulte Configuración del API acceso MFA protegido en la Guía del IAM usuario.

Para obtener más información sobre las prácticas recomendadasIAM, consulte las prácticas recomendadas de seguridad IAM en la Guía del IAM usuario.

Uso de la consola AWS 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 realicen llamadas al AWS CLI o al AWS API. En su lugar, permita el acceso únicamente a las acciones que coincidan con la API operación que están intentando 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 Añadir permisos a un usuario en la Guía del IAM usuario.

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 o eliminarlos.

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam: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": "*"
        }
    ]
}
```

Lista de las aplicaciones disponibles AWS Resilience Hub

La siguiente política concede a los usuarios el permiso para enumerar las aplicaciones de AWS Resilience Hub disponibles.

```
{
  "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.

```
{
  "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.

```
{
  "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.

```
{
  "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.

```
{
  "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.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
```

```
      "Effect": "Allow",
      "Action": [
          "resiliencehub:UpdateApp"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ],
      "Condition": {
        "StringLike" : { "resiliencehub:policyArn" : "arn:aws:resiliencehub:us-
west-2:111122223333:resiliency-policy/*" }
      }
    }
  ]
}
```

## Configure IAM roles y permisos

AWS Resilience Hub le permite configurar los IAM roles que le gustaría usar 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:

  - Permiso de solo lectura para leer sus recursos (se AWS Resilience Hub recomienda utilizar la política `AWSResilienceHubAsssessmentExecutionPolicy` gestionada).
  - Confíe en la política para asumir esta función, lo 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 “Paso 6: configurar 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 la función ARNs para otras cuentas, que se utilizará en lugar del nombre de la función de invocación.

- Acceso IAM de usuario actual: AWS Resilience Hub utilizará el IAM usuario actual para acceder a los recursos de la aplicación. Cuando sus recursos estén en una cuenta diferente, AWS Resilience Hub asumirá las siguientes IAM funciones 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.

## Solución de problemas de identidad y acceso a AWS Resilience Hub

Utilice la siguiente información para ayudarle a diagnosticar y solucionar problemas comunes que pueden surgir al trabajar con AWS Resilience Hub yIAM.

Temas



### No estoy autorizado a realizar ninguna acción en AWS Resilience Hub

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

El siguiente ejemplo de error se produce cuando el `mateojackson` IAM usuario intenta usar la consola para ver detalles sobre un *`my-example-widget`* recurso ficticio pero no tiene los `resiliencehub:`*`GetWidget`* permisos ficticios.

```
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 AWS el 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 el rol al servicio.

El siguiente ejemplo de error se produce cuando un IAM usuario denominado `marymajor` intenta usar 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 el rol al servicio.

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

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

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

## Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a los recursos de mi Centro de AWS Resiliencia

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

Para más información, consulte lo siguiente:

- Para saber si AWS Resilience Hub admite estas funciones, consulte. Cómo funciona AWS Resilience Hub con IAM

- Para obtener información sobre cómo proporcionar acceso a los recursos de su propiedad, consulte Proporcionar acceso a un IAM usuario en otro Cuenta de AWS de su propiedad en la Guía del IAM usuario. Cuentas de AWS
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo permitir el acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del IAM usuario.
- Para obtener información sobre cómo proporcionar acceso mediante la federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (federación de identidades) en la Guía del IAM usuario.
- Para saber la diferencia entre el uso de roles y políticas basadas en recursos para el acceso entre cuentas, consulte el acceso a recursos entre cuentas IAM en la Guía del usuario. IAM

## 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 IAM políticas que se apliquen a los usuarios, grupos o roles.

Cada AWS Resilience Hub aplicación se puede configurar para usar the section called “Rol de invocador” (un IAM rol) o usar los permisos de IAM usuario actuales (junto con un conjunto de roles predefinidos 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 (cuentas secundarias o de recursos), debe configurar un nuevo rol en cada cuenta que contenga los recursos de la aplicación.

Temas

- the section called “Uso del IAM rol”
- the section called “Uso de los permisos IAM de usuario actuales”

## Uso IAM del rol

AWS Resilience Hub utilizará un IAM rol existente predefinido para acceder a tus recursos en la cuenta principal o en la cuenta secundaria o de recursos. Esta es la opción de permiso recomendada para acceder a sus recursos.

Temas

- the section called “Rol de invocador”
- the section called “Funciones en AWS cuentas diferentes 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 AWS a los servicios y recursos. Por ejemplo, puedes crear un rol de invocador que tenga permiso para acceder a tu CFN plantilla 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 tu función de invocador, la política de confianza de la función debe especificar al director del AWS Resilience Hub servicio (resiliencehub.amazonaws.com) como 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 de invocador en la consola IAM”
- the section called “Administrar funciones con el IAM API”
- the section called “Definir la política de confianza mediante JSON un archivo”

Crear un rol de invocador en la consola IAM

Para permitir el acceso AWS Resilience Hub a AWS los servicios y recursos, debe crear un rol de invocador en la cuenta principal mediante la IAM consola. Para obtener más información sobre la creación de roles mediante la IAM consola, consulte Crear un rol para un AWS servicio (consola).

Para crear un rol de invocador en la cuenta principal mediante IAM la consola

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.

```
{
  "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 rol o usuario actual para el rol de invocador al crear o actualizar la aplicación. Sin embargo, no necesita este permiso para ejecutar una evaluación.

Administrar los roles con el IAM API

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 evitar las comillas (`' '`) en la JSON cadena puede variar según la versión de shell.

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 JSON un archivo

Puede definir la política de confianza para el rol mediante un JSON archivo independiente y, a continuación, ejecutar el `create-role` comando. 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, utilice el attach-policy-to-rolecomando y podrá empezar por añadir la política `AWSResilienceHubAsssessmentExecutionPolicy` gestionada. Para obtener más información sobre esta política administrada, consulte the section called “AWSResilienceHubAsssessmentExecutionPolicy”.

Ejemplo de **`trust-policy.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

```
{
```

```
    "Role": {
        "Path": "/",
        "RoleName": "AWSResilienceHubAssessmentRole",
        "RoleId": "AROAQFOXMPL6TZ6ITKWND",
        "Arn": "arn:aws:iam::123456789012:role/AWSResilienceHubAssessmentRole",
        "CreateDate": "2020-01-17T23:19:12Z",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [{
                "Effect": "Allow",
                "Principal": {
                    "Service": "resiliencehub.amazonaws.com"
                },
                "Action": "sts:AssumeRole"
            }]
        }
    }
}
```

Ejemplo de **`attach-policy-to-role`**

```
aws iam attach-role-policy --role-name AWSResilienceHubAssessmentRole --
policy-arn arn:aws:iam::aws:policy/
AWSResilienceHubAsssessmentExecutionPolicy
```

Funciones en AWS cuentas diferentes para el acceso entre cuentas (opcional)

Si sus recursos se encuentran en cuentas secundarias o de recursos, 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 IAM consola para las cuentas secundarias o de recursos”
- the section called “Administrar funciones con el IAM API”

- the section called “Definir la política de confianza mediante JSON un archivo”

Crear un rol en la IAM consola para las cuentas secundarias o de recursos

Para permitir el acceso 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 IAM consola para las cuentas secundarias o de recursos mediante la consola 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.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::primary_account_id:role/InvokerRoleName"
        ]
      },
      "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.
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"
      ]
}
```

Administrar los roles con la IAM API

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 evitar las comillas (`' '`) en la JSON cadena puede variar según la versión de shell.

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 del rol mediante un JSON archivo independiente. En el siguiente ejemplo, `trust-policy.json` es un archivo que se encuentra en el directorio actual.

Definir la política de confianza mediante JSON un archivo

Puede definir la política de confianza para el rol mediante un JSON archivo independiente y, a continuación, ejecutar el `create-role` comando. 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, utilice el attach-policy-to-rolecomando y podrá empezar por añadir la política `AWSResilienceHubAsssessmentExecutionPolicy` gestionada. Para obtener más información sobre esta política administrada, consulte the section called “AWSResilienceHubAsssessmentExecutionPolicy”.

Ejemplo de **`trust-policy.json`**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::primary_account_id:role/InvokerRoleName"
        ]
      },
```

```
      "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

```
{
    "Role": {
        "Path": "/",
        "RoleName": "AWSResilienceHubAssessmentRole2",
        "RoleId": "AROAT2GICMEDJML6EVQRG",
        "Arn": "arn:aws:iam::262412591366:role/AWSResilienceHubAssessmentRole2",
        "CreateDate": "2023-08-02T07:49:23+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": [
                            "arn:aws:iam::262412591366:role/
AWSResilienceHubAssessmentRole"
                        ]
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }
    }
}
```

### Ejemplo de **attach-policy-to-role**

```
aws iam attach-role-policy --role-name AWSResilienceHubAssessmentRole --
policy-arn arn:aws:iam::aws:policy/
AWSResilienceHubAsssessmentExecutionPolicy.
```

## Uso de los permisos IAM de usuario actuales

Utilice este método si desea utilizar sus permisos de IAM usuario actuales para crear y ejecutar una evaluación. Puede adjuntar la política `AWSResilienceHubAsssessmentExecutionPolicy` gestionada a su IAM usuario o a 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 IAM usuario.

### 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 AWS Resilience Hub permitir la realización de tareas programadas relacionadas con la evaluación

1. Asocie la política administrada por `AWSResilienceHubAsssessmentExecutionPolicy` al rol.
2. Agregue 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.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Action": [
        "iam:GetRole",
        "sts:AssumeRole"
      ],
      "Resource": "arn:aws:iam::primary_account_id:role/
AwsResilienceHubAdminAccountRole"
    },
    {
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": [
        "arn:aws:iam::primary_account_id:role/
AwsResilienceHubAssessmentEKSAccessRole"
      ]
    }
  ]
}
```

Política de confianza para el rol de evaluación programada (**`AwsResilienceHubPeriodicAssessmentRole`**)

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

Configuración entre cuentas

Las siguientes políticas de IAM permisos 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.
- Cuentas secundarias o de recursos: 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 tu EKS clúster de Amazon”.

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 usuario o rol actual debe tener el `iam:assumeRole` permiso para asumir este rol.
> - 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 cuenta: AWS

```
{
  {
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Resource": [
        "arn:aws:iam::secondary_account_id_1:role/AwsResilienceHubExecutorAccountRole",
        "arn:aws:iam::secondary_account_id_2:role/AwsResilienceHubExecutorAccountRole",
        ...
      ],
      "Action": [
        "sts:AssumeRole"
      ]
    }
  ]
}
```

La política de confianza del rol de administrador (`AwsResilienceHubAdminAccountRole`) es la siguiente:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::primary_account_id:role/caller_IAM_role"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::primary_account_id:role/
AwsResilienceHubPeriodicAssessmentRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Configuración de cuentas secundarias o de recursos

En cada una de sus cuentas secundarias, debe crear un nuevo `AwsResilienceHubExecutorAccountRole` y habilitar el rol de administrador creado

anteriormente para asumir este rol. Como esta función la 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:

```
{
  {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::primary_account_id:role/AwsResilienceHubAdminAccountRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

## 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 haya nuevas API operaciones disponibles para los servicios existentes.

Para obtener más información, consulte las políticas AWS administradas en la Guía del IAM usuario.

## AWSResilienceHubAsssessmentExecutionPolicy

Puede adjuntarlas `AWSResilienceHubAsssessmentExecutionPolicy` a sus IAM identidades. 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 SOP plantillas 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 deseas publicar en otro bucket de Amazon S3, puedes hacerlo mientras llamas `CreateRecommendationTemplate`API. 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 que están 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 Elastic Compute Cloud (AmazonEC2): muestra los EC2 recursos de Amazon asociados a tu AWS cuenta y proporciona `Describe` permisos para ellos.

- Amazon Elastic Container Registry (AmazonECR): proporciona `Describe` permisos para ECR los recursos de Amazon asociados a su AWS cuenta.
- Amazon Elastic Container Service (AmazonECS): proporciona `Describe` permisos para ECS los recursos de Amazon asociados a su AWS cuenta.
- Amazon Elastic File System (AmazonEFS): proporciona `Describe` permisos para EFS los recursos de Amazon asociados a su AWS cuenta.
- Amazon Elastic Kubernetes Service (EKSAmazon): muestra los recursos de Amazon asociados a su `Describe` cuenta y proporciona permisos para EKS ellos. AWS
- Amazon EC2 Auto Scaling: muestra y proporciona `Describe` permisos para los recursos de Amazon EC2 Auto Scaling que están asociados a su AWS cuenta.
- Amazon EC2 Systems Manager (SSM): proporciona `Describe` permisos para SSM los recursos asociados a su AWS cuenta.
- Amazon Fault Injection Service (AWS FIS): muestra los experimentos y las plantillas de AWS FIS experimentos asociados a tu AWS cuenta y proporciona `Describe` permisos para ellos.
- Amazon FSx for Windows File Server (AmazonFSx): muestra los FSx recursos de Amazon asociados a tu AWS cuenta y proporciona `Describe` permisos para ellos.
- AmazonRDS: muestra los RDS recursos de Amazon asociados a tu 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 — Muestra los Amazon Route 53 Resolver recursos asociados a tu AWS cuenta y proporciona `Describe` permisos para ellos.
- Amazon Simple Notification Service (AmazonSNS): muestra los SNS recursos de Amazon asociados a tu AWS cuenta y proporciona `Describe` permisos para ellos.
- Amazon Simple Queue Service (AmazonSQS): muestra los SQS recursos de Amazon asociados a tu AWS cuenta y proporciona `Describe` permisos para ellos.
- 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 los recursos de Amazon EC2 Auto Scaling asociados a su AWS cuenta y obtiene `Describe` permisos para ellos.
- 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.
- AWS Directory Service — Enumera los AWS Directory Service recursos 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
- AWS Resource Groups (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 las SOPs que están configuradas para su aplicación.

La siguiente IAM política es necesaria para que una AWS cuenta añada permisos para los usuarios, grupos de usuarios y funciones que proporcionen los permisos necesarios para que tu equipo pueda acceder a los AWS servicios mientras realiza las evaluaciones.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "AWSResilienceHubFullResourceStatement",
            "Effect": "Allow",
            "Action": [
                "application-autoscaling:DescribeScalableTargets",
                "autoscaling:DescribeAutoScalingGroups",
                "backup:DescribeBackupVault",
                "backup:GetBackupPlan",
                "backup:GetBackupSelection",
                "backup:ListBackupPlans",
                "backup:ListBackupSelections",
                "cloudformation:DescribeStacks",
                "cloudformation:ListStackResources",
                "cloudformation:ValidateTemplate",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:GetMetricData",
                "cloudwatch:GetMetricStatistics",
                "datasync:DescribeTask",
                "datasync:ListLocations",
                "datasync:ListTasks",
                "devops-guru:ListMonitoredResources",
                "dlm:GetLifecyclePolicies",
                "dlm:GetLifecyclePolicy",
                "docdb-elastic:GetCluster",
                "docdb-elastic:GetClusterSnapshot",
                "docdb-elastic:ListClusterSnapshots",
                "docdb-elastic:ListTagsForResource",
                "drs:DescribeJobs",
                "drs:DescribeSourceServers",
                "drs:GetReplicationConfiguration",
                "ds:DescribeDirectories",
                "dynamodb:DescribeContinuousBackups",
                "dynamodb:DescribeGlobalTable",
                "dynamodb:DescribeLimits",
                "dynamodb:DescribeTable",
                "dynamodb:ListGlobalTables",
                "dynamodb:ListTagsOfResource",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeFastSnapshotRestores",
                "ec2:DescribeFleets",
                "ec2:DescribeHosts",
                "ec2:DescribeInstances",
                "ec2:DescribeNatGateways",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeRegions",
```

```
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcEndpoints",
                "ecr:DescribeRegistry",
                "ecs:DescribeCapacityProviders",
                "ecs:DescribeClusters",
                "ecs:DescribeContainerInstances",
                "ecs:DescribeServices",
                "ecs:DescribeTaskDefinition",
                "ecs:ListContainerInstances",
                "ecs:ListServices",
                "eks:DescribeCluster",
                "eks:DescribeFargateProfile",
                "eks:DescribeNodegroup",
                "eks:ListFargateProfiles",
                "eks:ListNodegroups",
                "elasticache:DescribeCacheClusters",
                "elasticache:DescribeGlobalReplicationGroups",
                "elasticache:DescribeReplicationGroups",
                "elasticache:DescribeSnapshots",
                "elasticfilesystem:DescribeFileSystems",
                "elasticfilesystem:DescribeLifecycleConfiguration",
                "elasticfilesystem:DescribeMountTargets",
                "elasticfilesystem:DescribeReplicationConfigurations",
                "elasticloadbalancing:DescribeListeners",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "fis:GetExperimentTemplate",
                "fis:ListExperimentTemplates",
                "fis:ListExperiments",
                "fsx:DescribeFileSystems",
                "lambda:GetFunctionConcurrency",
                "lambda:GetFunctionConfiguration",
                "lambda:ListAliases",
                "lambda:ListEventSourceMappings",
                "lambda:ListFunctionEventInvokeConfigs",
                "lambda:ListVersionsByFunction",
                "rds:DescribeDBClusterSnapshots",
                "rds:DescribeDBClusters",
                "rds:DescribeDBInstanceAutomatedBackups",
                "rds:DescribeDBInstances",
```

```
                "rds:DescribeDBProxies",
                "rds:DescribeDBProxyTargets",
                "rds:DescribeDBSnapshots",
                "rds:DescribeGlobalClusters",
                "rds:ListTagsForResource",
                "resource-groups:GetGroup",
                "resource-groups:ListGroupResources",
                "route53-recovery-control-config:ListClusters",
                "route53-recovery-control-config:ListControlPanels",
                "route53-recovery-control-config:ListRoutingControls",
                "route53-recovery-readiness:GetReadinessCheckStatus",
                "route53-recovery-readiness:GetResourceSet",
                "route53-recovery-readiness:ListReadinessChecks",
                "route53:GetHealthCheck",
                "route53:ListHealthChecks",
                "route53:ListHostedZones",
                "route53:ListResourceRecordSets",
                "route53resolver:ListResolverEndpoints",
                "route53resolver:ListResolverEndpointIpAddresses",
                "s3:ListBucket",
                "servicecatalog:GetApplication",
                "servicecatalog:ListAssociatedResources",
                "sns:GetSubscriptionAttributes",
                "sns:GetTopicAttributes",
                "sns:ListSubscriptionsByTopic",
                "sqs:GetQueueAttributes",
                "sqs:GetQueueUrl",
                "ssm:DescribeAutomationExecutions",
                "states:DescribeStateMachine",
                "states:ListStateMachineVersions",
                "states:ListStateMachineAliases",
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AWSResilienceHubApiGatewayStatement",
            "Effect": "Allow",
            "Action": [
                "apigateway:GET"
            ],
            "Resource": [
                "arn:aws:apigateway:*::/apis/*",
                "arn:aws:apigateway:*::/restapis/*",
```

```
                "arn:aws:apigateway:*::/usageplans"
            ]
        },
        {
            "Sid": "AWSResilienceHubS3ArtifactStatement",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:PutObject",
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::aws-resilience-hub-artifacts-*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "AWSResilienceHubS3AccessStatement",
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketTagging",
                "s3:GetBucketVersioning",
                "s3:GetMultiRegionAccessPointRoutes",
                "s3:GetReplicationConfiguration",
                "s3:ListAllMyBuckets",
                "s3:ListMultiRegionAccessPoints"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "AWSResilienceHubCloudWatchStatement",
            "Effect": "Allow",
            "Action": [
```

```
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "ResilienceHub"
                }
            }
        },
        {
            "Sid": "AWSResilienceHubSSMStatement",
            "Effect": "Allow",
            "Action": [
                "ssm:GetParametersByPath"
            ],
            "Resource": "arn:aws:ssm:*:*:parameter/ResilienceHub/*"
        }
    ]
}
```

## AWS Resilience Hub actualizaciones de las políticas AWS gestionadas

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas AWS Resilience Hub desde que este servicio comenzó a realizar el seguimiento de estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase al RSS feed de la página del historial del AWS Resilience Hub documento.

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| AWSResilienceHubAssessmentExecutionPolicy— Cambiar | AWS Resilience Hub actualizado `AWSResilienceHubAssessmentExecutionPolicy` para conceder `Describe` permisos que le permitan acceder a los recursos y las configuraciones en Amazon DocumentDB, Elastic Load Balancing y AWS | 1 de agosto de 2024 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| | Lambda durante la ejecución de las evaluaciones. | |
| AWSResilienceHubAssessmentExecutionPolicy— Cambio | AWS Resilience Hub actualizado `AWSResilienceHubAssessmentExecutionPolicy` para conceder `Describe` permisos que le permitan leer la configuración del servidor de archivos de Amazon FSx para Windows mientras se ejecutan las evaluaciones. | 26 de marzo de 2024 |
| AWSResilienceHubAssessmentExecutionPolicy— Cambiar | AWS Resilience Hub actualizado `AWSResilienceHubAssessmentExecutionPolicy` para conceder `Describe` permisos que le permitan leer la AWS Step Functions configuración mientras se ejecutan las evaluaciones. | 30 de octubre de 2023 |
| AWSResilienceHubAssessmentExecutionPolicy— Cambiar | AWS Resilience Hub actualizado `AWSResilienceHubAssessmentExecutionPolicy` para conceder `Describe` permisos que te permitan acceder a los recursos de Amazon RDS mientras ejecutas las evaluaciones. | 5 de octubre de 2023 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| AWSResilienceHubAssessmentExecutionPolicy—Nuevo | Esta AWS Resilience Hub política proporciona acceso a otros AWS servicios para realizar evaluaciones. | 26 de junio de 2023 |
| 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 IAM permisos

Puedes conceder IAM los permisos 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:

- IAMpermisos para el personaje de administrador de aplicaciones de infraestructura
- IAMpermisos para el personaje de administrador de continuidad empresarial
- IAMpermisos para el personaje propietario de la aplicación
- IAMpermisos para conceder acceso de solo lectura

### IAMpermisos 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.

```
{
  "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": "*"
    }
  ]
}
```

## IAMpermisos para el personaje de administrador de continuidad empresarial

La siguiente política otorga los permisos necesarios para el personaje de gerente de continuidad empresarial.

```
{
  "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": "*"
    }
  ]
}
```

## IAMpermisos para el personaje propietario de la aplicación

La siguiente política otorga los permisos necesarios para la persona propietaria de la aplicación.

```
{
  "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": "*"
    }
  ]
}
```

### IAMpermisos para conceder acceso de solo lectura

La siguiente política concede los permisos necesarios para el acceso de solo lectura.

```
{
  "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 por 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 IAM políticas, 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 y IAM políticas de bucket de Amazon S3 para permitir el acceso de AWS Resilience Hub 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.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<s3-bucket-name>/<path-to-state-file>"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<s3-bucket-name>"
    }
  ]
}
```

- Política de identidad: la política de identidad asociada al rol de invocador definido para esta aplicación o al IAM rol AWS actual de AWS Resilience Hub la cuenta principal AWS . Para obtener más información, consulte el siguiente ejemplo.

```
{
  "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 conKMS, debe añadir el siguiente `kms:Decrypt` permiso.

```
{
      "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.

```
 {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>/<path-
to-state-file>"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>"
    }
  ]
}
```

- Política de identidad: la política de identidad asociada al rol de AWS cuenta, que se ejecuta AWS Resilience Hub en la AWS cuenta principal. Para obtener más información, consulte el siguiente ejemplo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
```

```
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>/<path-
to-state-file>"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>"
    }
  ]
}
```

**Note**

Si utiliza la política administrada por `AWSResilienceHubAsssessmentExecutionPolicy`, no se requiere permiso de `ListBucket`.

**Note**

Si sus archivos de estado de Terraform están cifrados conKMS, debe añadir el siguiente `kms:Decrypt` permiso.

```
{
      "Effect": "Allow",
      "Action": [
              "kms:Decrypt",
      ],
      "Resource": "<arn_of_kms_key>"
}
```

# Habilitar el 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 EKS (Amazon) mediante el análisis de la infraestructura del 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 (K8s), que se implementan como parte del clúster de Amazon. EKS AWS Resilience Hub Para consultar tu EKS clúster de Amazon para analizar y evaluar la carga de trabajo, debes completar lo siguiente:

- Crea o usa un rol AWS Identity and Access Management (IAM) existente en la misma cuenta que el EKS clúster de Amazon.
- Habilita IAM el acceso de usuarios y roles a tu EKS clúster de Amazon y otorga permisos adicionales de solo lectura a los recursos de K8 dentro del clúster de Amazon. EKS Para obtener más información sobre cómo habilitar el acceso de IAM usuarios y roles a su EKS clúster de Amazon, consulte Habilitar el acceso de IAM usuarios y roles a su clúster: Amazon EKS.

El AWS IAMAuthenticator for Kubernetes, que se ejecuta en el plano de control de Amazon, habilita el acceso a tu EKS clúster de Amazon mediante IAM entidades. EKS El autenticador obtiene la información de la configuración de `aws-auth ConfigMap`.

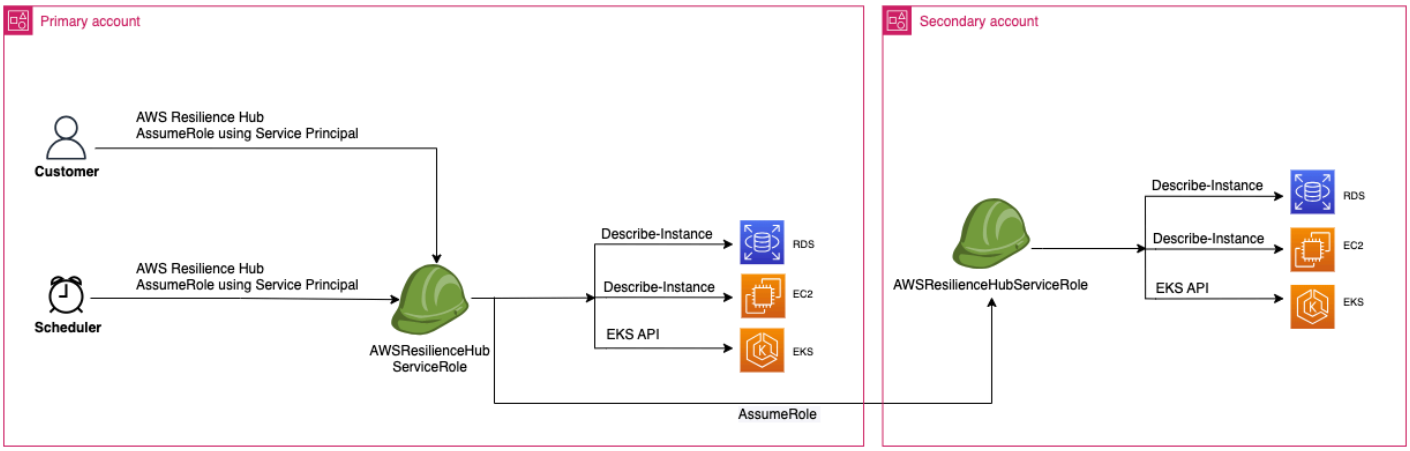
> **Note**
>
> - Para obtener más información sobre todos los `aws-auth ConfigMap` ajustes, consulte Formato de configuración completo en. GitHub
> - Para obtener más información sobre IAM las distintas identidades, consulte Identidades (usuarios, grupos y roles) en la Guía del IAM usuario.
> - Para obtener más información sobre la configuración del control de acceso basado en roles (RBAC) de Kubernetes, consulte Uso de la autorización. RBAC

AWS Resilience Hub consulta los recursos de tu EKS clúster de Amazon mediante un IAM rol de tu cuenta. Para AWS Resilience Hub poder acceder a los recursos de su EKS clúster de Amazon, el IAM rol utilizado 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 tu EKS clúster de Amazon mediante una de las siguientes opciones de IAM rol:

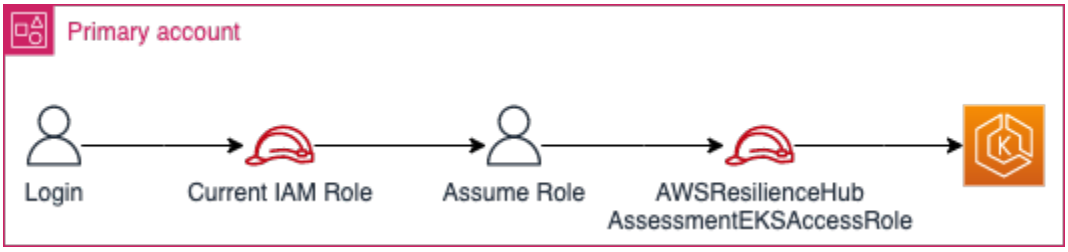
- Si su aplicación está configurada para usar el acceso basado en roles para acceder a los recursos, el rol de invocador o el rol de cuenta secundaria transferido AWS Resilience Hub al crear una aplicación se usará para acceder a su EKS clúster de Amazon durante la evaluación.

  El siguiente diagrama conceptual muestra cómo se AWS Resilience Hub accede a los EKS clústeres de Amazon cuando la aplicación está configurada como una aplicación basada en roles.

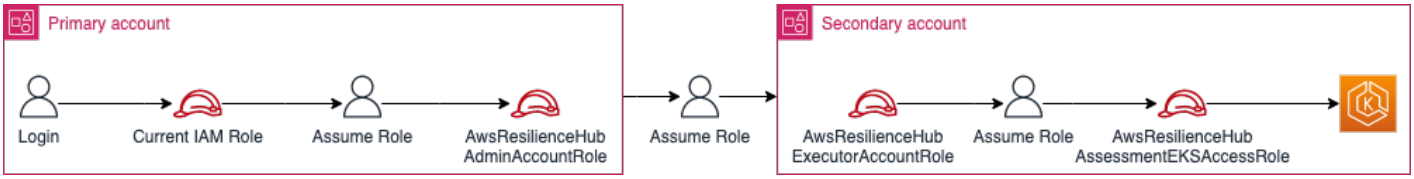



- Si tu aplicación está configurada para usar el IAM usuario actual para acceder al recurso, debes crear un nuevo IAM rol con el nombre `AwsResilienceHubAssessmentEKSAccessRole` en la misma cuenta que el del EKS clúster de Amazon. Esta IAM función se utilizará entonces para acceder a tu EKS clúster de Amazon.

  El siguiente diagrama conceptual muestra cómo AWS Resilience Hub accede a EKS los clústeres de Amazon desplegados en su cuenta principal cuando la aplicación está configurada para usar los permisos de IAM usuario actuales.




  El siguiente diagrama conceptual muestra cómo se AWS Resilience Hub accede a EKS los clústeres de Amazon desplegados en una cuenta secundaria cuando la aplicación está configurada para usar los permisos de IAM usuario actuales.




## Otorgar AWS Resilience Hub acceso a los recursos de tu EKS clúster de Amazon

AWS Resilience Hub le permite acceder a los recursos ubicados en los EKS clústeres de Amazon siempre que haya configurado los permisos necesarios.

Otorgar los permisos necesarios AWS Resilience Hub para descubrir y evaluar los recursos dentro del EKS clúster de Amazon

1. Configura un IAM rol para acceder al EKS clúster de Amazon.

   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 sobre cómo AWS Resilience Hub utiliza IAM los roles, consultethe section called "Cómo funciona AWS Resilience Hub con IAM".

   Si has configurado tu aplicación con los permisos de IAM usuario actuales, debes crear un `AwsResilienceHubAssessmentEKSAccessRole` IAM rol en la misma cuenta que la del EKS clúster de Amazon. Esta IAM función se utilizará después al acceder a tu EKS clúster de Amazon.

   Al importar y evaluar tu aplicación, AWS Resilience Hub usa un IAM rol para acceder a los recursos de tu EKS clúster de Amazon. Este rol debe crearse en la misma cuenta que tu EKS clúster de Amazon y se asignará a un grupo de Kubernetes que incluya los permisos necesarios AWS Resilience Hub para evaluar tu clúster de Amazon. EKS

   Si tu EKS clúster de Amazon está en la misma cuenta que la cuenta AWS Resilience Hub llamante, el rol debe crearse con la siguiente política de IAM confianza. En esta política de IAM confianza, `caller_IAM_role` se utiliza en la cuenta corriente APIs para solicitar información AWS Resilience Hub.

   > **Note**
   >
   > `caller_IAM_role`Es el rol que está asociado a su cuenta AWS de usuario.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::eks_cluster_account_id:role/caller_IAM_role"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Si tu EKS clúster de Amazon está en una cuenta cruzada (una cuenta diferente AWS Resilience Hub a la cuenta de llamada), debes crear el `AwsResilienceHubAssessmentEKSAccessRole` IAM rol mediante la siguiente política de IAM confianza:

> **Note**
>
> Como requisito previo, para acceder a un EKS clúster de Amazon que esté desplegado en una cuenta diferente a la cuenta del AWS Resilience Hub usuario, debe configurar el acceso multicuenta. Para obtener más información, consulte

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::eks_cluster_account_id:role/
AwsResilienceHubExecutorRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. Cree `ClusterRole` `ClusterRoleBinding` (oRoleBinding) 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 tu 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 EKS clúster de Amazon, debe crear los siguientes y. `ClusterRole` `ClusterRoleBinding`

      - `resilience-hub-eks-access-cluster-role`(`ClusterRole`) — Define los permisos necesarios AWS Resilience Hub para evaluar tu EKS clúster de Amazon.
      - `resilience-hub-eks-access-cluster-role-binding`(`ClusterRoleBinding`): define un grupo con un nombre `resilience-hub-eks-access-group` en tu EKS clúster de Amazon que otorga a sus usuarios los permisos necesarios para ejecutar evaluaciones de resiliencia. 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. Otorgar AWS Resilience Hub 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 EKS clúster de Amazon y evaluar su resiliencia, debe crear los siguientes roles. `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 tu EKS clúster de Amazon a fin de evaluar la resiliencia de tu 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, concederás AWS Resilience Hub los permisos necesarios para evaluar los recursos dentro del espacio de `kube-system` nombres mientras evalúas tu clúster de AmazonEKS.

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 el `aws-auth ConfigMap` para mapearlo `resilience-hub-eks-access-group` con el IAM rol que se usa para acceder al EKS clúster de Amazon.

   Este paso crea un mapeo entre el IAM rol utilizado en el paso 1 y el grupo de Kubernetes creado en el paso 2. Este mapeo otorga permisos a los IAM roles para acceder a los recursos dentro del EKS clúster de Amazon.

   > **Note**
   >
   > - `ROLE-NAME`Se refiere a la IAM función que se utiliza para acceder al EKS clúster de Amazon.
   >   - Si su 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 AWS Resilience Hub al crear la aplicación.
   >   - Si la aplicación está configurada para usar el IAM usuario actual para acceder a los recursos, debe ser el. `AwsResilienceHubAssessmentEKSAccessRole`
   > - `ACCOUNT-ID`debe ser el ID de AWS cuenta del EKS clúster de Amazon.

   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
```

- Puedes editarlo manualmente `aws-auth ConfigMap` añadiendo los detalles del IAM rol a la `mapRoles ConfigMap` sección de datos secundarios. 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 del recurso de Amazon (ARN) del IAM rol que se va a añadir.
    - ARNSintaxis —`arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>`.
  - `username`— El nombre de usuario de Kubernetes que se va a asignar al IAM rol (). `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.

  Usa la siguiente plantilla para añadir los detalles del IAM rol a la `mapRoles` sección de los siguientes datos. `ConfigMap`

  ```
  - groups:
    - resilience-hub-eks-access-group
    rolearn: arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>
    username: AwsResilienceHubAssessmentEKSAccessRole
  ```

# AWS Resilience Hub Habilitar la publicación 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 de Amazon Simple Notification Service (AmazonSNS). Para enviar notificaciones a un SNS tema de Amazon, asegúrate de tener lo siguiente:

- Una AWS Resilience Hub aplicación activa.
- Un SNS tema de Amazon existente al que se AWS Resilience Hub deben enviar notificaciones. Para obtener más información sobre cómo crear un SNS tema de Amazon, consulta Crear un SNS tema de Amazon.

AWS Resilience Hub Para habilitar la publicación de notificaciones en tu SNS tema de Amazon, debes actualizar la política de acceso del SNS tema de Amazon con lo siguiente:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowResilienceHubPublish",
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:topic-name"
    }
  ]
}
```

> **Note**
>
> Cuando publicas mensajes AWS Resilience Hub de regiones en las que se ha optado por participar en temas ubicados en regiones que están habilitadas de forma predeterminada, debes modificar la política de recursos creada para el SNS tema de Amazon. Cambie el valor de la entidad principal de `resiliencehub.amazonaws.com` a `resiliencehub.<opt-in-region>.amazonaws.com`.

Si utilizas un SNS tema de Amazon Server Side Encrypted (SSE), debes asegurarte de que AWS Resilience Hub tiene el acceso `Decrypt GenerateDataKey` y* a la clave de SNS cifrado de Amazon.

Para proporcionar `Decrypt GenerateDataKey*` acceso a AWS Resilience Hub, debes incluir la siguiente política de permisos de AWS Key Management Service acceso.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowResilienceHubDecrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:region:account-id:key/key-id"
    }
  ]
}
```

## 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 IAM confianza. En esta política de IAM confianza, `caller_IAM_role` (asociada a su cuenta de AWS usuario) se utiliza en la cuenta corriente APIs para solicitar la solicitud AWS Resilience Hub.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "resiliencehub:BatchUpdateRecommendationStatus",
```

```
      "Resource": "arn:aws:resiliencehub:us-west-2:12345678900:app/0e6237b7-23ba-4103-
adb2-91811326b703"
    }
  ]
}
```

# 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 API llamadas 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 una versión posterior. Recomendamos la versión TLS 1.3 o una versión posterior. Los clientes también deben admitir conjuntos de cifrado con total confidencialidad (PFS), como Ephemeral Diffie-Hellman () o Elliptic Curve Ephemeral Diffie-Hellman (DHE). ECDHE La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben firmarse con un identificador de clave de acceso y una clave de acceso secreta que esté asociada a un director. IAM También puede 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 la postura de resiliencia de las aplicaciones no se vea afectada. 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 ejecutar estas comprobaciones, debe proporcionar IAM los permisos pertinentes AWS Resilience Hub para que pueda acceder a sus recursos. Para obtener más información sobre los IAM permisos necesarios para acceder AWS Resilience Hub a sus recursos y realizar las comprobaciones de resiliencia de este capítulo, consulteAWS 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
- NATGateway
- Amazon Route 53
- Controlador de recuperación de aplicaciones de Amazon Route 53

- Servidor FSx de archivos Amazon para Windows
- AWS Step Functions

# 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 resiliencia 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 EFS archivos de Amazon.

## 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` respaldo está habilitada, lo que garantiza la cobertura de las interrupciones a nivel regional si así lo exige la política del cliente.

## Replicación de datos

AWS Resilience Hub comprueba si se ha definido una replicación de EFS datos de Amazon dentro o entre regiones para el sistema de archivos desplegado. La replicación de EFS datos de Amazon ayuda a mejorar las estimaciones RTO y estimaciones RPO 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.

## Implementación de una sola zona de disponibilidad

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 deployment (Implementación Multi-AZ)

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 la política del cliente
- Instantáneas manuales para sistemas de respaldo de terceros

## Conmutación por error entre regiones

AWS Resilience Hub controles RTO y RPO objetivos que se definen 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 controles RTO y RPO objetivos 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 en la región
- Una réplica de lectura en una zona de disponibilidad diferente
- Un cúmulo de Aurora con una réplica de lectura en otra AZ
- Una instancia Multi-AZ de Amazon Relational Database Service (Amazon) RDS
- Un clúster Amazon RDS Multi-AZ
- Una única 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 interrupciones a nivel regional.

### Recuperación de IP oint-in-time

## Replicación de datos

AWS Resilience Hub si se ha 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 la carga de trabajo estimada RTO y la carga de trabajo estimada RPO 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 RTO objetivos definidos en su política de resiliencia, AWS Resilience Hub comprueba si Amazon S3 Replication Time Control (S3RTC) 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 la política del cliente
- 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 interrupciones a nivel regional.

### Recuperación de IP oint-in-time

AWS Resilience Hub comprueba si se requiere point-in-time recovery (PITR) de acuerdo con el objetivo de su política de RPO resiliencia. Sin embargo, no se admite la copia de seguridad entre

regiones. PITR 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

## 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 EC2 instancia de Amazon como instancia con estado si se cumple uno de los siguientes criterios:

- Si el `DeleteOnTermination` atributo se establece en false para al menos un volumen de Amazon Elastic Block Store (AmazonEBS) adjunto a esta instancia.
- Si Amazon Data Lifecycle Manager o un AWS Backup plan están adjuntos a la EC2 instancia de Amazon o al menos a un EBS volumen de Amazon.
- AWS Elastic Disaster Recovery Se utiliza para replicar los volúmenes de almacenamiento de sus EC2 instancias de Amazon.

> **Note**
>
> Si una EC2 instancia de Amazon no cumple ninguno de los criterios anteriores, la AWS Resilience Hub considerará una EC2 instancia de Amazon sin estado.

### Grupos de escalado automático

AWS Resilience Hub comprueba si hay un grupo de EC2 instancias de Amazon apátridas. Si se descubre, se recomienda organizar lo mismo mediante grupos de Auto Scaling (ASG) con configuración Multi-AZ.

Si ASG se identifica una existente, ARH verificará si está configurada en varias zonas de disponibilidad. Si también ASG se define utilizando únicamente EC2 instancias puntuales de Amazon, se recomienda aumentar su capacidad con EC2 instancias de Amazon bajo demanda para mejorar la resiliencia.

cuando las EC2 instancias puntuales de Amazon no estén disponibles.

### EC2Flota Amazon

AWS Resilience Hub identifica Amazon EC2 Fleet y verifica si está definida como una implementación Multi-AZ y también si solo usa EC2 instancias puntuales de Amazon.

Definir una EC2 flota de Amazon como un despliegue en zonas de disponibilidad múltiples mejorará su resiliencia en caso de que se produzca una interrupción en las zonas de disponibilidad.

Aumentar la EC2 flota de Amazon 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 AmazonEBS.

Para obtener más información sobre AmazonEBS, consulta la EBSdocumentación de Amazon.

### Copia de seguridad programada

AWS Resilience Hub comprueba si uno o ambos de los siguientes elementos están definidos para tus EBS volúmenes de Amazon.

- Una regla de respaldo para un EBS volumen de Amazon específico adjunto a tu EC2 instancia de Amazon.
- Una regla de respaldo para crear copias de seguridad EBS de AMI Amazon en tu EC2 instancia de Amazon.
- Instantáneas manuales para sistemas de respaldo de terceros.

Además, si tu póliza requiere cobertura por interrupciones a nivel regional, AWS Resilience Hub comprueba si tu regla de respaldo tiene habilitada la opción de respaldo entre regiones.

### Respaldo y replicación de datos

AWS Resilience Hub identifica que un EBS volumen de Amazon se considera un volumen con estado si se cumple uno de los siguientes criterios:

- Si el `DeleteOnTermination` atributo está establecido en false para este EBS volumen de Amazon.
- Si Amazon Data Lifecycle Manager o un AWS Backup plan están asociados a este EBS volumen de Amazon o a la EC2 instancia de Amazon a la que está conectado.
- AWS Elastic Disaster Recovery Se utiliza para replicar los volúmenes de almacenamiento de sus EC2 instancias de Amazon.

## 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.

### Amazon VPC Access para clientes

AWS Resilience Hub identifica una AWS Lambda función relacionada con el clienteVPC. La conexión AWS Lambda a subredes AZs de diferentes ubicaciones de Amazon VPC permite la resiliencia de las funciones en caso de una interrupción en la zona de disponibilidad.

### Cola de mensajes fallidos

AWS Resilience Hub comprueba si una AWS Lambda función tiene una cola de letras muertas (DLQ) adjunta para almacenar las solicitudes fallidas. Adjuntar una AWS Lambda función DLQ to 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 AmazonEKS, consulta la EKSdocumentación de Amazon.

## Multi-AZ deployment (Implementación Multi-AZ)

AWS Resilience Hub identifica si el despliegue del pod se ejecuta en varios nodos de trabajo de variosAZs.

Se requiere un EKS clúster de Amazon adicional en otra región si tu política de resiliencia requiere cobertura en caso de una interrupción regional. Este EKS clúster de Amazon adicional también se verifica para las implementaciones de pods que se distribuyen entre varios nodos de trabajo en variosAZs.

## 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:

- El uso de Pod Disruption Budget (PDB): el uso 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 EKS gestionados por Amazon: esta sustitución simplifica las actualizaciones de las imágenes de los nodos de trabajo durante el mantenimiento.
- Admite solicitudes dinámicas CPU y de 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 de Amazon EKS Cluster crezca y satisfaga las demandas de carga de trabajo.

- Configuración del escalador automático de pods horizontales: esta configuración ayuda a 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 (AmazonSNS).

Para obtener más información sobre AmazonSNS, consulta la SNSdocumentación de Amazon.

## Suscripciones temáticas

AWS Resilience Hub comprueba si el SNS tema de Amazon 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 (AmazonSQS).

Para obtener más información sobre AmazonSQS, consulta la SQSdocumentación de Amazon.

## Cola de mensajes fallidos

AWS Resilience Hub comprueba si la SQS cola de Amazon tiene DLQ asociada una 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 (AmazonECS).

Para obtener más información sobre AmazonECS, consulta la ECSdocumentación de Amazon.

## Multi-AZ deployment (Implementación Multi-AZ)

AWS Resilience Hub comprueba si ECS las tareas o los servicios de Amazon se ejecutan en varios tipos AZs según Amazon EC2 o el tipo de AWS Fargate lanzamiento. Se requiere un ECS clúster

de Amazon adicional en otra región si tu póliza necesita cobertura en caso de interrupción regional. También se verifica que el clúster adicional ejecute varias tareas o serviciosAZs.

# 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 deployment (Implementación Multi-AZ)

AWS Resilience Hub comprueba si Elastic Load Balancing se está ejecutando en variosAZs.

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 variasAZs.

# 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.

## Despliegue entre regiones

Si su política debe tener en cuenta la disrupción regional, AWS Resilience Hub comprobará si hay un despliegue adicional del API recurso de Amazon API Gateway en otra región.

## Despliegue API multizona de disponibilidad privado

AWS Resilience Hub comprueba si tu cuenta API está definida como privada en Amazon API Gateway. APIsEl sector privado debe recibir el tráfico a través del punto de conexión de la VPC interfaz de Amazon que esté desplegado en variosAZs.

# 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 deployment (Implementación Multi-AZ)

AWS Resilience Hub comprueba si el clúster de Amazon DocumentDB se ha implementado en varios. AZs 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 varios. AZs

## Implementación de clústeres elásticos y zonas de disponibilidad múltiples

AWS Resilience Hub comprueba si los fragmentos de clústeres elásticos de Amazon DocumentDB utilizan réplicas de lectura que se implementan en diferentes ubicaciones. AZs

## 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.

# NATGateway

En esta sección se enumeran todas las comprobaciones y recomendaciones específicas de NAT Gateway. Para obtener más información sobre NAT las puertas de enlace, consulte NATPuertas de enlace.

## Multi-AZ deployment (Implementación Multi-AZ)

AWS Resilience Hub comprueba si NAT Gateway está desplegado en varios. AZs

Si tu póliza requiere una cobertura en caso de interrupción regional, es necesario implementar una NAT puerta de enlace adicional en otra región. La NAT puerta de enlace adicional, ubicada en una región diferente, también está verificada para su despliegue en variasAZs.

# 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 deployment (Implementación Multi-AZ)

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 variosAZs. 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 variosAZs.

# Controlador de recuperación de aplicaciones de Amazon Route 53

En esta sección se enumeran todas las comprobaciones y recomendaciones específicas de Amazon Route 53 Application Recovery Controller (Route 53ARC).

Para obtener más información sobre Route 53ARC, consulte la ARCdocumentación de Route 53.

## Multi-AZ deployment (Implementación Multi-AZ)

AWS Resilience Hub comprueba si se han desplegado recursos similares en varias regiones y recomienda, como práctica recomendada, definir las comprobaciones de ARC preparación de la Route 53 para aumentar su disponibilidad y preparación en caso de que se produzca una interrupción regional. Se le notificará que se le cobrarán cargos por hora adicionales.

# Servidor FSx de archivos Amazon para Windows

En esta sección se enumeran todas las comprobaciones y recomendaciones específicas de Amazon FSx for Windows File Server. Para obtener más información sobre 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 por interrupciones a nivel regional.

### Replicación de 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 la carga de trabajo estimada RTO y la carga de trabajo estimada RPO a nivel de infraestructura, zona de disponibilidad y región. Además, podría combinarse con una instalación regional 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.

### Despliegue entre regiones

AWS Resilience Hub comprueba si un AWS Step Functions flujo de trabajo del mismo tipo de flujo de trabajo se implementa en una región diferente para recuperarlo en caso de una interrupción regional.

# Trabajar con otros servicios de

En esta sección se describen AWS los servicios con los que se interactúa AWS Resilience Hub.

Temas



# AWS CloudFormation

AWS Resilience Hub está integrado con AWS CloudFormation, un servicio que le ayuda a modelar y configurar sus recursos de AWS para que pueda dedicar menos tiempo a crear y administrar sus recursos e infraestructura. Puede crear una plantilla que describa todos los recursos de AWS que desee (como AWS: :ResilienceHub: ::ResiliencyPolicy y AWS: :ResilienceHub: ::App) y AWS CloudFormation aprovisiona y configura estos recursos para usted.

Cuando utiliza AWS CloudFormation, puede volver a utilizar la plantilla para configurar sus recursos de AWS Resilience Hub de forma coherente y repetida. Solo tiene que describir los recursos una vez y luego aprovisionar los mismos recursos una y otra vez en varias cuentas y regiones de AWS.

## Plantillas de AWS Resilience Hub y AWS CloudFormation

Para aprovisionar y configurar los recursos de AWS Resilience Hub y sus servicios relacionados, debe entender las plantillas de AWS CloudFormation. Las plantillas son archivos de texto con formato de tipo JSON o YAML. Estas plantillas describen los recursos que desea aprovisionar en sus pilas de AWS CloudFormation. Si no está familiarizado con JSON o YAML, puede utilizar Designer de AWS CloudFormation para comenzar a utilizar las plantillas de AWS CloudFormation. Para obtener más información, consulte ¿Qué es Designer de AWS CloudFormation? en la Guía del usuario de AWS CloudFormation.

AWS Resilience Hub admite la creación de AWS: :ResilienceHub: :ResiliencyPolicy y AWS: :ResilienceHub: ::App en AWS CloudFormation. Para obtener más información, incluidos ejemplos de plantillas JSON y YAML para AWS::ResilienceHub:::ResiliencyPolicy y AWS::ResilienceHub:::App, consulte la referencia del tipo de recurso AWS Resilience Hub en la Guía del usuario de AWS CloudFormation.

Puede usar pilas de AWS CloudFormation para definir aplicaciones de AWS Resilience Hub. 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.

### Obtener más información sobre AWS CloudFormation

Para obtener más información sobre AWS CloudFormation, consulte los siguientes recursos:

- AWS CloudFormation
- Guía del usuario de AWS CloudFormation
- Referencia de la API de AWS CloudFormation
- 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 AWS 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 AWS 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 cómo ejecutar, revisar e implementar las evaluaciones, revisar e incluir/excluir las recomendaciones operativas e implementarlas, consulte los siguientes temas:

- the section called “Realizar evaluaciones de resiliencia”
- 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”
- 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 de la Guía AWS Resilience Hub del usuario

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

- APIversión: última
- Última actualización de la documentación: 1 de agosto de 2024

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| AWS Resilience Hub presenta recomendaciones de agrupamiento | AWS Resilience Hub presenta una nueva opción de agrupación inteligente para agrupar los recursos en componentes de la aplicación (AppComponents) mientras se incorporan las aplicaciones. Al realizar evaluaciones de resiliencia AWS Resilience Hub, es importante que los recursos se agrupen con precisión en los adecuados AppComponents para recibir recomendaciones optimizadas 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 incorporación de aplicaciones existente que está disponible en la actualidad. | 1 de agosto de 2024 |

| | | |
|---|---|---|
| | Para obtener más información, consulte los temas siguientes:<br>• the section called “Gestión de los componentes de la aplicación”<br>• the section called “AWS Resilience Hub recomendaciones de agrupación de recursos” | |
| AWS Resilience Hub presenta un nuevo widget de resumen de la evaluación | AWS Resilience Hub presenta un nuevo widget de resumen de la evaluación que utiliza las capacidades de IA generativa de Amazon Bedrock para transformar datos de resiliencia complejos en información altamente procesable. Estos resúmenes de las evaluaciones extraen las conclusiones fundamentales, priorizan los riesgos y recomiendan medidas para mejorar la resiliencia. Al centrarse en los elementos más impactantes, podrá comprender las evaluaciones con mucha más facilidad, lo que le ayudará a obtener información de alto impacto que se centra en los elementos más críticos de su postura de resiliencia.<br>Para obtener más información, 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 las configuraciones en Amazon DocumentDB, Elastic Load Balancing y AWS Lambda mientras ejecuta las evaluaciones.<br><br>Para obtener más información sobre la política AWS administrada, consultethe section called “AWSResilienceHubAsssessmentExecutionPolicy”. | 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 mediante la introducción de un nuevo tipo de detección de desviaciones: la desviación de los recursos de aplicación. Esta mejora detecta cambios, como la adición o eliminación de recursos en las fuentes de entrada de la aplicación. Puede activar los servicios de evaluación AWS Resilience Hub programada y notificación de desviaciones y recibir notificaciones cada vez que se produzca una desviación. La última evaluación de resiliencia identifica las desviaciones y presenta medidas correctivas para que la aplicación vuelva a cumplir con su política de resiliencia.<br><br>Para obtener más información, consulte los temas siguientes:<br><br>• the section called “Detección de desviaciones”<br>• the section called “Paso 5: Configurar la evaluación programada y la notificación de deriva” | 8 de mayo de 2024 |

| | | |
|---|---|---|
| AWS Trusted Advisor mejoras | AWS Resilience Hub ha ampliado la compatibilidad con la adición AWS Trusted Advisor de una comprobación para identificar los component es de la aplicación irrecuper ables (). AppComponents<br><br>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 recomendadas desde AWS Resilience Hub dentro AWS (por ejemplo, Amazon CloudWatch) o desde fuera AWS.<br><br>Para obtener más informaci ón, consulte the section called “Administración de alarmas”. | 26 de marzo de 2024 |

| | | |
|---|---|---|
| AWS Resilience Hub amplía el soporte de Amazon FSx para Windows File Server | AWS Resilience Hub amplía el soporte de evaluación de los recursos de Amazon FSx para Windows File Server y, al mismo tiempo, evalúa la resiliencia de su aplicación. Para las aplicaciones que utilizan Amazon FSx for Windows File Server, AWS Resilience Hub proporciona un nuevo conjunto de recomendaciones de resiliencia, que abarca las implementaciones en zonas de disponibilidad (AZ) y Multi-AZ y los planes de respaldo, así como la replicación de datos. AWS Resilience Hub es compatible con Amazon FSx for Windows File Server, incluida la dependencia del sistema de archivos de Microsoft Active Directory, tanto para implementaciones regionales como entre regiones.<br><br>Para obtener más información, consulte los temas siguientes:<br><br>• the section called “ AWS Resilience Hub Recursos compatibles”<br>• the section called “AWSResilienceHubAssessmentExecutionPolicy” | 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 ayudarle a entender y entender fácilmente las acciones necesarias para mejorar la resiliencia de sus aplicaciones.<br><br>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 EKS recursos de Amazon para incluir nuevas recomendaciones operativas. Mientras realizamos una evaluación que incluye recursos de los EKS clústeres de Amazon, ahora recomendaremos que se ejecuten pruebas y alarmas para ayudar a mejorar la resiliencia de las aplicaciones.<br><br>Para obtener más información, consulte the section called “Gestión de los experimentos de Amazon Fault Injection Service”. | 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 la carga de trabajo estimada RTO y la carga de trabajo estimadaRPO. Esta información adicional indica la carga de trabajo estimada máxima posible RTO y la carga RPO de trabajo estimada de su aplicación a partir de la última evaluación satisfactoria. Este valor es la carga de trabajo máxima estimada RTO y la carga RPO de trabajo estimada de todos los tipos de interrupciones.<br><br>Para obtener más información, consulte the section called “Administración de aplicaciones ”. | 30 de octubre de 2023 |

| | | |
|---|---|---|
| AWS Resilience Hub amplía el apoyo a la evaluación de AWS Step Functions los recursos | 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 de la carga de trabajo estimados (RTO) y los objetivos de punto de recuperación de la carga de trabajo estimados (RPO). Para evaluar las aplicaciones, incluidos AWS Step Functions los recursos, debe configura r los permisos necesario s, ya sea mediante una política AWS administrada o añadiendo manualmente el permiso específico para AWS Resilience Hub poder leer la AWS Step Functions configur ación.<br><br>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 le permite excluir las recomendaciones operativas, incluidas las alarmas, los procedimientos operativos estándar (SOPs) y las pruebas del Amazon Fault Injection Service (AWS FIS). Al realizar la evaluación AWS Resilience Hub, recibirá una estimación de los tiempos de recuperación 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 recomendadas y AWS FIS las pruebas que no sean relevantes para ellas. SOPs 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.<br><br>Para obtener más información, consulte los temas siguientes:<br><br>• the section called “Incluir o excluir recomendaciones operativas”<br>• the section called “Limitar los permisos para incluir o | 9 de agosto de 2023 |

| | | |
|---|---|---|
| | excluir recomendaciones de AWS Resilience Hub ” | |
| Mejorar el diseño de los permisos para AWS Resilience Hub | AWS Resilience Hub presenta un nuevo diseño de permisos para brindar flexibilidad a la hora de configurar AWS Identity and Access Management (IAM) las funciones para AWS Resilience 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.<br><br>Para obtener más información sobre la política AWS administrada, consultethe section called “AWSResilienceHubAsssessmentExecutionPolicy”. | 2 de agosto de 2023 |

| | | |
|---|---|---|
| Detección de desviaciones de resiliencia de 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 (AmazonSNS) reciba notificaciones cuando el objetivo de tiempo estimado de recuperación de la carga de trabajo (RTO) o el objetivo del punto de recuperación de la carga de trabajo estimado (RPO) pasen 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 de forma proactiva a través de SNS los temas de Amazon le permitirá anticipar las posibles interrupciones con antelación y le proporcionará una confianza adicional en que se lograrán los objetivos de recuperación.<br><br>Para obtener más información, consulte los temas siguientes:<br><br>• the section called “Paso 5: Configurar la evaluación | 2 de agosto de 2023 |

programada y la notificación de deriva”

- the section called “Edición de recursos de aplicaciones”

| | | |
|---|---|---|
| AWS Resilience Hub mejora la compatibilidad con 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 AmazonRDS, ahora distinguiremos entre diferente s motores de bases de datos para proporcionar objetivos de tiempo de recuperación de la carga de trabajo estimados más precisos (RTOs). AWS Resilience Hub también proporcionaremos acciones adicionales para implement ar las mejores prácticas de resiliencia en su AWS entorno. Las mejores prácticas pueden incluir información sobre el rendimiento con DevOps Guru for AmazonRDS, una supervisi ón mejorada y una automatiz ación de la implementación azul/ecológica en los motores de bases de datos compatibl es.<br><br>Para obtener más información sobre los permisos necesario s AWS Resilience Hub para incluir recursos de todos los servicios compatibles en su evaluación, consulte. the | 2 de agosto de 2023 |

| | | |
|---|---|---|
| | 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 para Amazon Elastic Block Store (AmazonEBS) para reconocer las EBS instantáneas de Amazon que se toman en la misma EBS región de Amazon mediante DirectAPIs. El soporte ampliado se suma al soporte actual para los clientes que utilizan Amazon Data Lifecycle Manager (Amazon Data Lifecycle Manager) o AWS Backup.<br><br>Para obtener más información, consulte Amazon Elastic Block Store (AmazonEBS). | 2 de agosto de 2023 |

| | | |
|---|---|---|
| Mejoras de Amazon Elastic Compute Cloud | AWS Resilience Hub ha ampliado el soporte para Amazon Elastic Compute Cloud (AmazonEC2). Para aplicaciones de diferente s tamaños, AWS permite EC2 a sus clientes que utilizan Amazon seleccionar la configuración adecuada para su caso de uso. AWS Resilience Hub admite la evaluación en las siguiente s EC2 configuraciones de Amazon:<br>• Instancias bajo demanda.<br>• Copia de seguridad de las instancias AWS Backup de forma AWS Elastic Disaster Recovery automática.<br>• Soporte para grupos que se autoescalan con el controlad or de recuperación de aplicaciones Amazon Route 53 (Route 53) ARC<br><br>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.<br><br>Para obtener más informaci ón, consulte the section called “AWS Resilience Hub | 27 de junio de 2023 |

| | | |
|---|---|---|
| | referencia de permisos de acceso”. | |
| AWS actualizaciones de políticas gestionadas | Se agregó una nueva política que proporciona acceso a otros AWS servicios para ejecutar las evaluaciones.<br><br>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 alertan sobre los riesgos de resiliencia de los modos de capacidad aprovisio nada 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.<br><br>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 AWS Trusted Advisor y las aplicaciones que utilizan Amazon DynamoDB. Si lo utiliza 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.<br><br>Para obtener más información sobre la verificación de la antigüedad de la evaluación 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), la replicación entre regiones (Amazon S3) o la replicación en la misma región de Amazon CRR S3 SRR (), el control de versiones y la AWS copia de seguridad, AWS Resilience Hub ahora evaluará Amazon S3 para la configuración de puntos de acceso multirregionales, control del tiempo de replicación de Amazon S3 (Amazon RTC S3) y recuperación de copias de seguridad (). AWS point-in-time PITR<br><br>Para obtener más información, consulte los temas siguientes:<br><br>• the section called “AWS Resilience Hub referencia de permisos de acceso”<br>• Gestionar el almacenamiento de Amazon S3 | 21 de marzo de 2023 |

| | | |
|---|---|---|
| Soporte adicional para Amazon Elastic Kubernetes Service | AWS Resilience Hub ha añadido el EKS clúster de Amazon como recurso compatible para definir, validar y realizar un seguimiento de la resiliencia de las aplicaciones. Los clientes pueden añadir EKS clústeres de Amazon a aplicaciones nuevas o existentes y recibir evaluaciones y recomendaciones para mejorar la resiliencia. Los clientes pueden agregar recursos de aplicaciones mediante AWS CloudFormation Terraform y AWS Resource Groups. AppRegistry Además, los clientes pueden añadir uno o más EKS clústeres de Amazon directamente en una o más regiones con uno o más espacios de nombres en cada clúster. Esto permite AWS Resilience Hub proporcionar evaluaciones y recomendaciones únicas e interregionales. Además de examinar las implementaciones, las réplicas y los pods ReplicationControllers, AWS Resilience Hub analizarán la resiliencia general del clúster. AWS Resilience Hub admite cargas de trabajo de EKS clústeres de Amazon sin estado. Las | 21 de marzo de 2023 |

| | | |
|---|---|---|
| | nuevas capacidades están disponibles en todas las AWS regiones en las que AWS Resilience Hub se admiten.<br><br>Para obtener más información, consulte los temas siguientes:<br><br>• the section called “Paso 2: Administrar los recursos de la aplicación”<br>• the section called “Añadir EKS clústeres”<br>• the section called “AWS Resilience Hub referencia de permisos de acceso”<br>• AWS Servicios regionales | |
| Soporte adicional para Amazon Elastic File System | Además del soporte actual para las copias de seguridad de Amazon Elastic File System (AmazonEFS), ahora AWS Resilience Hub evaluará Amazon EFS para la EFS replicación de Amazon y la configuración AZ.<br><br>Para obtener más información, consulte los temas siguientes:<br><br>• the section called “ AWS Resilience Hub Recursos compatibles”<br>• ¿Qué es Amazon Elastic File System? | 21 de marzo de 2023 |

| | | |
|---|---|---|
| Soporte para orígenes de entrada de aplicaciones | AWS Resilience Hub ahora proporciona 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.<br><br>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.<br><br>Para obtener más información, consulte los temas siguientes:<br><br>• the section called “Parámetros de configuración de la aplicación”<br>• the section called “Paso 7: configurar los parámetros de configuración de la aplicación”<br>• 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 para los volúmenes de Amazon Elastic Block Store (AmazonEBS), ahora AWS Resilience Hub evaluará las EBS instantáneas de Amazon mediante Amazon Data Lifecycle Manager y Amazon EBS Fast Snapshot Restore ()FSR.<br><br>Para obtener más información, consulte los temas siguientes:<br><br>• the section called “AWS Resilience Hub referencia de permisos de acceso”<br>• Tienda Amazon Elastic Block (AmazonEBS) | 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 prevista (RTOyRPO) 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 continuam ente sus AWS cuentas y proporciona recomendaciones para ayudarle a seguir las AWS mejores prácticas y las directrices de AWS Well-Arch itected.<br><br>Para obtener más informaci ón, consulte the section called “AWS Trusted Advisor”. | 18 de noviembre de 2022 |

| | | |
|---|---|---|
| Soporte para Amazon Simple Notification Service (AmazonSNS) | AWS Resilience Hub ahora evalúa las aplicaciones que utilizan Amazon SNS analizando la SNS configuración de Amazon, incluidos los suscriptores, y ofrece recomendaciones para cumplir los objetivos de recuperación de la carga de trabajo estimados de la organización (carga de trabajo estimada RTO y carga de trabajo estimadaRPO) para las aplicaciones. Amazon SNS es un servicio gestionado que envía mensajes de los editores (productores) a los suscriptores (consumidores).<br><br>Para obtener más información, consulte los temas siguientes:<br><br>• the section called “ AWS Resilience Hub Recursos compatibles”<br>• the section called “Identity and Access Management”<br>• the section called “Agrupación de recursos en un componente de aplicación” | 16 de noviembre de 2022 |

| | | |
|---|---|---|
| Soporte adicional para el controlador de recuperación de aplicaciones Amazon Route 53 (Amazon Route 53ARC) | AWS Resilience Hub ahora evalúa Amazon Route 53 ARC para Elastic Load Balancing y Amazon Relational Database Service (RDSAmazon), que incluye información sobre cuándo Amazon Route ARC 53 sería beneficioso. Ampliando AWS Resilienc e Hub el soporte de ARC evaluación de Amazon Route 53 más allá de AWS Auto Scaling Group (AWS ASG) y Amazon DynamoDB. Amazon Route 53 ARC proporciona una alta disponibilidad para su aplicación, lo que le permite realizar rápidamente una conmutación por error de toda la aplicación a una región de conmutación por error.<br><br>Para obtener más información, consulte los temas siguientes:<br><br>• the section called “ AWS Resilience Hub Recursos compatibles”<br>• the section called “Identity and Access Management” | 16 de noviembre de 2022 |

| | | |
|---|---|---|
| Soporte adicional para AWS Backup | AWS Resilience Hub ahora evalúa Amazon Route 53 ARC para Elastic Load Balancing y Amazon Relational Database Service (RDSAmazon), que incluye información sobre cuándo Amazon Route ARC 53 sería beneficioso. Ampliando AWS Resilienc e Hub el soporte de ARC evaluación de Amazon Route 53 más allá de AWS Auto Scaling Group (AWS ASG) y Amazon DynamoDB. Amazon Route 53 ARC proporciona una alta disponibilidad para su aplicación, lo que le permite realizar rápidamente una conmutación por error de toda la aplicación a una región de conmutación por error.<br><br>Para obtener más información, consulte los temas siguientes:<br><br>• the section called “ AWS Resilience Hub Recursos compatibles”<br>• the section called “Identity and Access Management” | 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 AppComponent agrupamie nto. | 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 |

# Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el Glosario de AWS en la Referencia de Glosario de AWS.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.