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 de Amazon Route 53 (Route 53 ARC)	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 recursos apoyados

AWS Resilience Hub — Gestión de la resiliencia

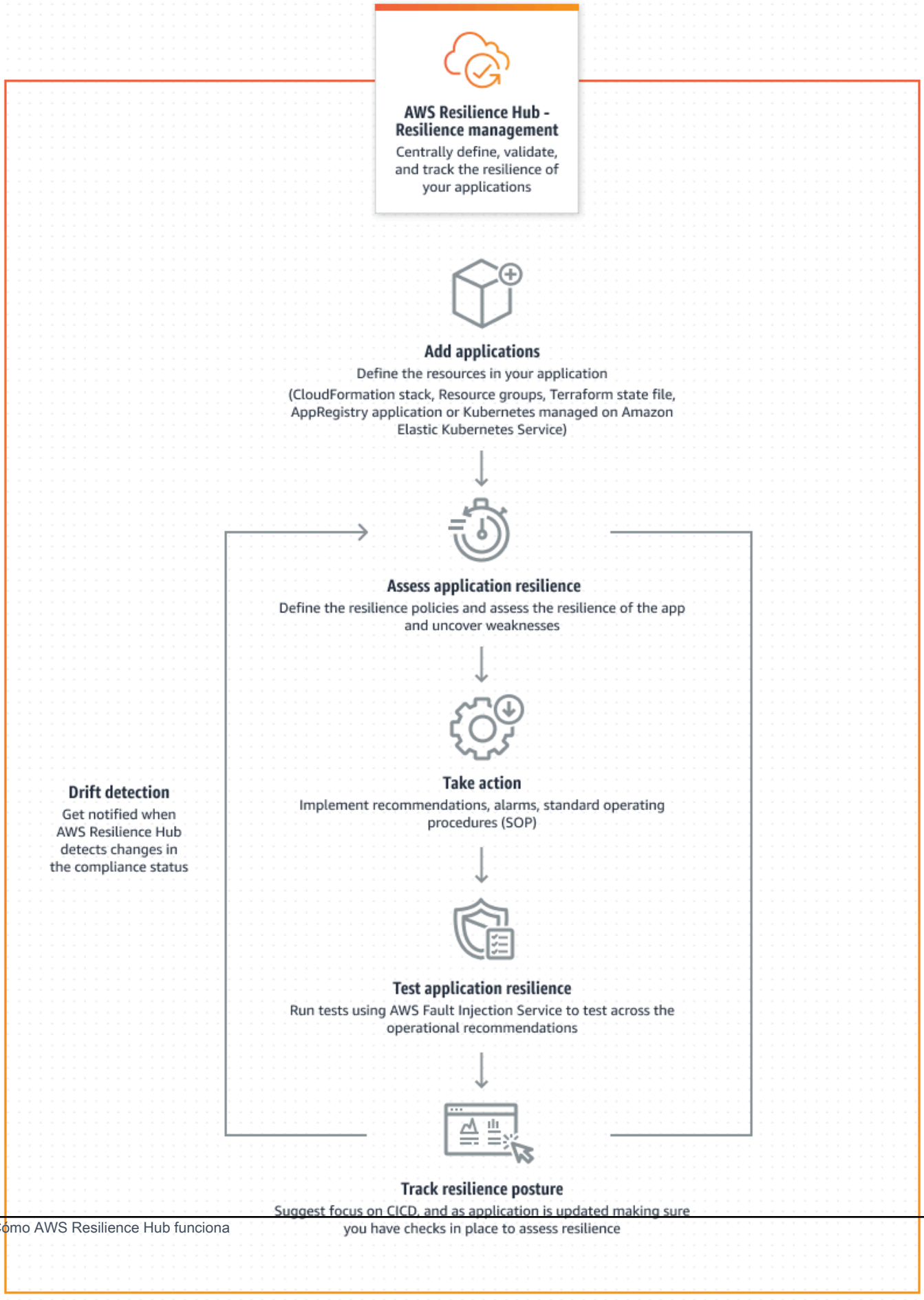
AWS Resilience Hub le ofrece un lugar central para definir, validar y realizar un seguimiento de la resiliencia de su AWS aplicación. AWS Resilience Hub le ayuda a proteger sus aplicaciones de las interrupciones y a reducir los costos de recuperación para optimizar la continuidad del negocio y ayudar 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. Aparte de una guía arquitectónica para mejorar la resiliencia de sus aplicaciones, las recomendaciones proporcionan un código para cumplir con su política de resiliencia e implementar pruebas, alarmas y procedimientos operativos estándar (SOP) que puede implementar y ejecutar con su aplicación en su proceso de integración y entrega (CI/CD).
- Evalúe los objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO) en diferentes condiciones.
- Optimice la continuidad empresarial y, al mismo tiempo, reduzca los costos de recuperación.
- Identifique y resuelva los problemas antes de que se produzcan en la producción.

Después de implementar una aplicación en producción, puede agregarla AWS Resilience Hub a su canalización 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 los objetivos de RTO y RPO para las interrupciones en las aplicaciones, la infraestructura, las zonas de disponibilidad y las regiones. Estos objetivos se usan para estimar si la aplicación cumple con la política de resiliencia.

Evaluar

Una vez que describa su aplicación y le adjunte una política de resiliencia, realice una evaluación de la resiliencia. La AWS Resilience Hub evaluación utiliza las mejores prácticas del AWS Well-Architected 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 los SOP de recuperación. A continuación, puede realizar otra evaluación y comparar los resultados con el informe anterior para ver en qué medida mejora la resiliencia. Repita este proceso hasta que su RTO de carga de trabajo estimada y su RPO de carga de trabajo estimada cumplan sus objetivos de RTO y RPO.

Validar

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

Visualización y seguimiento

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

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

AWS Resilience Hub — Pruebas de resiliencia

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

Objetivo de punto de recuperación de carga de trabajo estimado

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

Aplicación

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

Componente de aplicación

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 al mismo componente de aplicación (AppComponent).

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

Estado de conformidad de la aplicación

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

Se cumple la política

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

Política incumplida

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

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

Sin evaluar

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

Cambios detectados

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

Desviación de resiliencia

AWS Resilience Hub realiza una detección de desviaciones mientras realiza una evaluación de su aplicación para comprobar si cumple con su política de resiliencia. A modo de comparación, AWS Resilience Hub utiliza la política de resiliencia que se definió en la anterior evaluación satisfactoria de la solicitud.

- Desviación: indica que la aplicación ha infringido su política de resiliencia y está en riesgo.
- Sin desviación: indica que el cumplimiento de la aplicación no ha cambiado con respecto a la evaluación anterior.

Evaluación de resiliencia

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

Puntuación de resiliencia

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

Tipo de interrupción

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

Aplicación

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

Infraestructura en la nube

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

Interrupción de la infraestructura en la nube en zonas de disponibilidad

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

Incidente en la región de infraestructura de la nube

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

Experimentos de inyección de errores

AWS Resilience Hub recomienda realizar 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.
- Compruebe que los procedimientos de recuperación, o los procedimientos operativos estándar (SOP), funcionan correctamente para recuperar la aplicación tras la interrupción.

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

SOP

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

AWS Resilience Hub recursos apoyados

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 (Amazon EC2)
  - AWS Lambda
  - Amazon Elastic Kubernetes Service (Amazon EKS)
  - Amazon Elastic Container Service (Amazon ECS)
  - AWS Step Functions
- Base de datos
  - Amazon Relational Database Service (Amazon RDS)
  - Amazon DynamoDB
  - Amazon DocumentDB
- Redes y entrega de contenido
  - Amazon Route 53
  - Elastic Load Balancing
  - Traducción de direcciones de red (NAT)
- Almacenamiento

- Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic File System (Amazon EFS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon FSx para Windows File Server

- Otros
  - Amazon API Gateway
  - Controlador de recuperación de aplicaciones de Amazon Route 53 (Amazon Route 53 ARC)
  - Amazon Simple Notification Service
  - Amazon Simple Queue Service
  - AWS Auto Scaling
  - AWS Backup
  - AWS Recuperación ante desastres de Elastic

> **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 recursos de aplicaciones de AWS Resilience Hub.
> - AWS Resilience Hub es compatible con Amazon EKS y Amazon ECS en AWS Fargate.
> - AWS Resilience Hub admite la evaluación de AWS Backup los recursos como parte de los siguientes servicios:
>   - Amazon EBS
>   - Amazon EFS
>   - Amazon S3
>   - Base de datos global de Amazon Aurora
>   - Amazon DynamoDB
>   - Servicios de Amazon RDS
>   - Amazon FSx para Windows File Server

- Amazon Route 53 ARC in AWS Resilience Hub evalúa únicamente Amazon DynamoDB global, Elastic Load Balancing, Amazon RDS y grupos. AWS Auto Scaling
- AWS Resilience Hub Para evaluar los recursos entre regiones, agrupe los recursos en un único componente de aplicación. Para obtener más información sobre los recursos compatibles con cada uno de los componentes de la aplicación AWS Resilience Hub y los recursos de agrupación, consulte Agrupar recursos en un AppComponent.
- Actualmente, AWS Resilience Hub no admite las evaluaciones entre regiones para los clústeres de Amazon EKS si el clúster de Amazon EKS está ubicado o si la aplicación se crea en una región con la opción de suscripción habilitada AWS .
- Actualmente, AWS Resilience Hub evalúa solo los siguientes tipos de recursos de Kubernetes:
  - Implementaciones
  - ReplicaSets
  - Pods

AWS Resilience Hub ignora los siguientes tipos de recursos:

- Recursos que no afectan al RTO de la carga de trabajo estimada o al RPO de la carga de trabajo estimada: los recursos como `AWS::RDS::DBParameterGroup`, que no afectan al RTO de la carga de trabajo estimada o al RPO de la carga de trabajo estimada no se tienen en cuenta por AWS Resilience Hub.
- 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 es importado por. AWS Resilience Hub

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

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

- Estos recursos pueden afectar a la recuperación de las aplicaciones, pero por AWS Resilience Hub el momento no son totalmente compatibles. AWS Resilience Hub se esfuerza por avisar a los usuarios sobre los recursos no compatibles si la aplicación está respaldada por una AWS CloudFormation pila, un archivo de estado de Terraform o AppRegistry una aplicación. AWS Resource Groups

Introducción

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

Requisitos previos

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

- Cuentas de AWS: crea una o más cuentas de AWS para cada tipo de cuenta (cuentas principales/secundarias o de recursos) que desees usar en AWS Resilience Hub. Para obtener más información sobre la creación y administración de cuentas AWS, consulte lo siguiente:
  - Usuario primerizo de AWS: Primeros pasos: ¿Es la primera vez que utiliza AWS?
  - Administrar una cuenta AWS – https://docs.aws.amazon.com/accounts/latest/reference/managing-accounts.html
- Permisos de AWS Identity and Access Management (IAM): después de crear las cuentas de AWS, debe configurar los roles y permisos de IAM necesarios para cada una de las cuentas que haya creado. Por ejemplo, si ha creado una cuenta de AWS para acceder a los recursos de la aplicación, debe configurar un nuevo rol y configurar los permisos de IAM necesarios para que AWS Resilience Hub pueda acceder 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 un archivo JSON”.

  Para empezar rápidamente a añadir permisos de IAM a los usuarios, grupos y roles, puede usar nuestras políticas administradas por AWS (the section called “AWS políticas gestionadas”). Es más fácil utilizar las políticas administradas por AWS para cubrir los casos de uso comunes en su Cuenta de AWS que escribirlas uno mismo. AWS Resilience Hub añade permisos adicionales a una política administrada por AWS para ampliar el soporte a otros servicios de AWS e incluir nuevas características. 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 siguientes temas:
    - the section called “Publicar una nueva versión de la aplicación”
    - the section called “Realizar evaluaciones de resiliencia”

- Si no utiliza las políticas administradas por AWS para asignar los permisos de IAM adecuados a los usuarios, grupos y roles, debe configurar estos permisos de forma manual. Para obtener más información sobre las políticas administradas por AWS, consulte the section called “AWSResilienceHubAsssessmentExecutionPolicy”.

Añadir una aplicación a AWS Resilience Hub

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

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

Esta sección le guía a través de cómo agregar una aplicación. Reúne recursos de una aplicación 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 el RTO de carga de trabajo estimado y el RPO de carga de trabajo estimado alcancen sus objetivos de RTO y RPO.

Temas

- 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 solicitud 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 clústeres de Amazon EKS como recursos opcionales. En esta sección se proporcionan las siguientes opciones, que le ayudan a determinar la ubicación de los recursos de su aplicación.

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

Si selecciona esta opción, debe completar uno de los procedimientos de the section called "Agregar colecciones de recursos".

- Solo EKS: seleccione esta opción si desea detectar recursos de los espacios de nombres de los clústeres de Amazon EKS.

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

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

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

Next

Paso 3: Agregue recursos a su aplicación AWS Resilience Hub

Paso 3: Agregue recursos a su aplicación AWS Resilience Hub

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 clústeres de EKS"

Agregar colecciones de recursos

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

- Uso de AWS CloudFormation pilas
- Usando 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 AWS de la región y, a continuación, selecciona Añadir ARN de pila. Para obtener más información sobre los ARN, consulte Nombres de recursos de Amazon (ARN) en la AWS Referencia 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 de recurso de Amazon (ARN) de la pila en el cuadro ARN del grupo de recursos y, a continuación, selecciona Agregar ARN del grupo de recursos. Para obtener

más información sobre los ARN, consulte Nombres de recursos de Amazon (ARN) en la AWS Referencia general.

AppRegistry Uso de aplicaciones

Solo puede añadir una AppRegistry aplicación a la vez.

Elija las AppRegistry aplicaciones que contengan los recursos que desee utilizar 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 campo URL de S3 y seleccione Agregar URL de S3.

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 clústeres de EKS

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

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

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

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

Para agregar clústeres de Amazon EKS

1. Elija los clústeres de Amazon EKS de la lista desplegable Elegir clústeres de EKS que estén asociados a su región Cuenta de AWS y a su región.
2. Para utilizar clústeres de Amazon EKS que se encuentren en una región diferente Cuenta de AWS, diferente o en ambas, introduzca el nombre del recurso de Amazon (ARN) de la pila en el cuadro Entre cuentas o regiones y, a continuación, seleccione Añadir ARN de EKS. Para obtener más información sobre los ARN, consulte Nombres de recursos de Amazon (ARN) en la AWS Referencia general.

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

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

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

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

   - Nombre del clúster de EKS: indica el nombre de los clústeres de Amazon EKS seleccionados.
   - Número de espacios de nombres: indica el número de espacios de nombres seleccionados en los clústeres de Amazon EKS.
   - Estado: indica si AWS Resilience Hub ha incluido los espacios de nombres de los clústeres de Amazon EKS seleccionados en su aplicación. Puede identificar el estado mediante las siguientes opciones:

- Espacio de nombres obligatorio: indica que no ha incluido ningún espacio de nombres del clúster de Amazon EKS.
- Espacios de nombres agregados: indica que ha incluido uno o más espacios de nombres del clúster de Amazon EKS.

2. Para añadir un espacio de nombres, en el cuadro de diálogo Actualizar espacios de nombres, seleccione Añadir un nuevo espacio de nombres.

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

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

     El nombre del espacio de nombres debe coincidir exactamente con el nombre del espacio de nombres del clúster de Amazon EKS.
   - Para eliminar un espacio de nombres, seleccione Eliminar, situado junto al espacio de nombres.
   - Para aplicar los espacios de nombres seleccionados a todos los clústeres de Amazon EKS, seleccione Aplicar espacios de nombres a todos los clústeres de EKS.

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

Next

Paso 4: establecer RTO y RPO

Paso 4: establecer RTO y RPO

Puede definir una nueva política de resiliencia con sus propios objetivos de RTO/RPO, o puede elegir una política de resiliencia existente con objetivos de RTO/RPO predefinidos. 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 de 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 su RTO/RPO en la sección Objetivos de RTO/RPO.

> **Note**
>
> - Hemos rellenado un RTO y un RPO predeterminados para su aplicación. Puede cambiar el RTO y el RPO ahora o después de evaluar la aplicación.
> - AWS Resilience Hub le permite introducir un valor cero en los campos RTO y RPO de su política de resiliencia. Sin embargo, al evaluar su aplicación, el resultado de evaluación más bajo posible es cercano a cero. Por lo tanto, si introduce un valor cero en los campos RTO y RPO, los resultados estimados de RTO y RPO de carga de trabajo serán próximos a cero y el Estado de conformidad de su aplicación pasará a ser Política infringida.

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

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

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

Next

the section called “Paso 5: Configurar la detección de desviaciones de resiliencia”

Paso 5: Detección de desviaciones

AWS Resilience Hub le permite configurar la detección de desviaciones de resiliencia para evaluar su aplicación a diario y recibir notificaciones si se detecta alguna desviación o si una evaluación ha fallado.

Para configurar la detección de desviaciones de resiliencia

1. Para evaluar su aplicación a diario, active Evaluar automáticamente esta aplicación a diario.

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

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

     mediante el procedimiento adecuado en the section called “Cómo funciona AWS Resilience Hub con IAM”.
2. Para recibir una notificación cuando se AWS Resilience Hub detecte cualquier cambio en el estado de cumplimiento, o si la evaluación diaria de resiliencia no es satisfactoria, activa Recibir notificaciones sobre cualquier incumplimiento de la política de resiliencia.

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

   > **Note**
   >
   > - Para permitir que AWS Resilience Hub publique notificaciones en sus temas de Amazon SNS, su tema de Amazon SNS debe estar configurado con los permisos adecuados. Para obtener más información acerca de la configuración de permisos, consulte the section called “ AWS Resilience Hub Habilitar la publicación en sus temas de Amazon SNS”.

- Las evaluaciones diarias pueden afectar a su cuota de ejecuciones. Para obtener más información sobre cuotas, consulte Puntos de conexión y cuotas de AWS Resilience Hub en la Referencia general de AWS .

Para usar temas de Amazon SNS que estén en una región diferente Cuenta de AWS o diferente, o en ambas, seleccione Introducir el ARN del tema de SNS e introduzca el nombre de recurso de Amazon (ARN) del tema de Amazon SNS en el cuadro Proporcione un tema de SNS. Para obtener más información sobre los ARN, consulte Nombres de recursos de Amazon (ARN) en la AWS Referencia 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 las los permisos y roles de IAM

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

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

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

- AWS Consola de IAM: si elige esta opción, debe completar el procedimiento descrito en Para crear su función de centro de resiliencia de AWS en la consola de IAM.
- AWS CLI: si elige esta opción, debe completar todos los pasos de la AWS CLI.
- CloudFormation plantilla: si elige esta opción, según el tipo de cuenta (cuenta principal o cuenta secundaria), debe crear los roles con la AWS CloudFormation plantilla adecuada.

2. Seleccione la flecha derecha para ampliar la sección Añadir roles de IAM desde una cuenta cruzada (opcional).
3. Para seleccionar los roles de IAM de una cuenta cruzada, introduzca los ARN del rol de IAM en el cuadro Introducir un ARN de rol de IAM. Asegúrese de que los ARN de los roles de IAM que va a introducir no pertenezcan a la cuenta actual.
4. Si desea usar el usuario de IAM actual para descubrir los recursos de su aplicación, seleccione la flecha derecha para ampliar la sección Usar los permisos del usuario de IAM actual y seleccione Entiendo que debo configurar manualmente los permisos para habilitar la funcionalidad requerida en AWS Resilience Hub.

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

Next

Paso 8: Añadir etiquetas

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 de AWS Resilience Hub

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

Para usar AWS Resilience Hub, usted:

- Describa sus aplicaciones de AWS en AWS Resilience Hub.
- Administre sus recursos de AWS en AWS Resilience Hub.
- Cree políticas de resiliencia eficaces.
- Administre las evaluaciones que indiquen la resiliencia de sus aplicaciones.
- Administre las alarmas, los procedimientos operativos estándar (SOP) y las pruebas de sus aplicaciones.

Descripción y administración de aplicaciones de AWS Resilience Hub

Una aplicación de AWS Resilience Hub es una colección de recursos de AWS estructurados para prevenir y recuperar interrupciones de las aplicaciones de AWS.

Para describir una aplicación de AWS Resilience Hub, debe proporcionar un nombre de aplicación, recursos de una o más pilas de AWS CloudFormation (hasta un máximo de cinco) 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 aplicación de AWS Resilience Hub, debe publicarla para poder poner en marcha una evaluación de resiliencia en ella. A continuación, puede utilizar las recomendaciones de la evaluación para mejorar la capacidad de recuperación mediante la ejecución de otra evaluación, la comparación de los resultados y la repetición del proceso hasta que su RPO de carga de trabajo estimada y su RPO de carga de trabajo estimada cumplan sus objetivos de RPO y RPO.

Para ayudar a realizar un seguimiento de los cambios en la aplicación, AWS Resilience Hub muestra las versiones anteriores de la aplicación desde el momento en que se creó en AWS Resilience Hub. Esta visibilidad le ayuda a revisar las configuraciones anteriores de la aplicación y a tomar decisiones sobre la configuración actual de la aplicación. AWS Resilience Hub utiliza los siguientes estados para identificar las versiones de la aplicación:

- Borrador: indica que la versión de la aplicación se está modificando y aún no se ha publicado.
- Versión actual: indica que la versión de esta aplicación es la versión publicada más recientemente. AWS Resilience Hub utiliza esta versión de la aplicación para ejecutar evaluaciones de resiliencia.
- Ver todas las versiones: seleccione el signo más (+) para ver todas las versiones anteriores en un formato de solo lectura.

Puede identificar sus aplicaciones en la página 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 aplicación como Evaluada, No evaluada, Política infringida o Cambios detectados.
  - Evaluada: AWS Resilience Hub ha evaluado su aplicación.
  - No evaluada: AWS Resilience Hub no ha evaluado su aplicación.
  - Política infringida: AWS Resilience Hub ha determinado que su aplicación 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 proporcionadas por AWS Resilience Hub antes de volver a evaluar la resiliencia de su aplicación. 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 aplicación. Debe volver a evaluar su aplicación para que AWS Resilience Hub pueda 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.
  - Desactivada: esto indica que su aplicación no se evalúa automáticamente a diario por AWS Resilience Hub y que debe evaluarla manualmente.
- Estado de desviación de la resiliencia: indica si su aplicación se ha desviado o no de la última evaluación satisfactoria.
  - 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.

  - Sin desviar: indica que se estima que la aplicación sigue cumpliendo los objetivos de RTO y RPO definidos en la política.
- RTO de carga de trabajo estimada: indica el RTO máximo de carga de trabajo estimado posible de la aplicación. Este valor es el RTO máximo estimado de la carga de trabajo de todos los tipos de interrupciones de la última evaluación exitosa.
- RPO de carga de trabajo estimado: indica el RPO de carga de trabajo estimado máximo posible de su aplicación. Este valor es el RTO máximo estimado de la carga de trabajo de todos los tipos de interrupciones de la última evaluación exitosa.
- Hora de la última evaluación: indica la fecha y la hora en que su aplicación se evaluó correctamente por última vez.
- Hora de creación: fecha y hora en que se creó la aplicación.
- ARN: el nombre de recurso de Amazon (ARN) de su aplicación. Para obtener más información sobre los ARN, consulte Nombres de recursos de Amazon (ARN) en la AWS Referencia general.

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

En los temas siguientes se muestran los diferentes enfoques para describir una aplicación AWS Resilience Hub y cómo administrarlas.

Temas

Visualización de un resumen de la aplicación AWS Resilience Hub

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

Para ver un resumen de la aplicación

1. En el panel de navegación, elija Aplicaciones.
2. En la página Aplicaciones, elija el nombre de la aplicación.

La página de resumen de aplicaciones contiene las siguientes secciones.

Temas

Detalles

La sección Detalles del resumen de aplicaciones muestra un resumen de las selecciones de la aplicación.

- Estado de la aplicación: indica si la aplicación está activa o no.
- Descripción: la descripción de su aplicación.
- Estado de conformidad: indica el estado de conformidad de su aplicación.
- Fecha de la última evaluación: indica la fecha y la hora en que se evaluó su aplicación por última vez.
- Política de resiliencia: muestra el nombre de la política de resiliencia adjunta a su aplicación. Para obtener más información sobre las políticas de resiliencia, consulte Administrar las políticas de resiliencia.
- Evaluación programada: indica si la evaluación diaria está activa o inactiva.
- Estado de desviación de la resiliencia: indica si su aplicación se ha desviado o no de la última evaluación satisfactoria.
- Fecha de la última desviación: indica la fecha y la hora en que se comprobó la existencia de desviaciones en su aplicación.

Para actualizar la evaluación programada

1. Para actualizar la evaluación programada en su aplicación, en Acciones, seleccione Actualizar la detección de desviaciones de resiliencia.
2. Para actualizar la detección de la desviación de resiliencia, complete los pasos que se indican en Paso 5: Detección de desviaciones y, a continuación, vuelva a este procedimiento.
3. Elija Actualizar.

> **Note**
>
> Para activar la detección de la desviación de resiliencia en las aplicaciones existentes, debe realizar una evaluación manualmente después de activar la función de detección de la desviación de resiliencia por primera vez. Para obtener más información sobre cómo ejecutar evaluaciones, consulte Realizar evaluaciones de resiliencia.

Resiliencia de la aplicación

Las métricas que se muestran en la sección Resiliencia de la aplicación 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 recomendaciones de AWS Resilience Hub para cumplir con la política de resiliencia, las alarmas, los procedimientos operativos estándar (SOP) y las pruebas de la aplicación.

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

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

Puntuación de resiliencia a lo largo del tiempo

Con la puntuación de resiliencia a lo largo del tiempo, puede ver un gráfico de la resiliencia de su aplicación durante los últimos 30 días. Si bien en el menú desplegable se pueden enumerar 10 de sus aplicaciones, AWS Resilience Hub solo muestra un gráfico de hasta cuatro aplicaciones a la vez. Para obtener más información sobre las evaluaciones programadas, consulte Paso 5: Detección de desviaciones .

> **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 utiliza Amazon CloudWatch para generar estos gráficos. Seleccione Ver métricas en CloudWatch para crear y ver información más detallada sobre la resiliencia de la aplicación en el panel de CloudWatch. Para obtener más información sobre CloudWatch, consulte Uso de los paneles en la Guía del usuario de Amazon CloudWatch.

Alarmas implementadas

En la sección Alarmas implementadas del resumen de la aplicación se enumeran las alarmas que configuró en Amazon CloudWatch para supervisar 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 Experimentos del Servicio de inyección de errores de Amazon.

Edición de recursos de aplicaciones de AWS Resilience Hub

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

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

> **Note**
>
> Al editar los recursos, solo se modifica la referencia AWS Resilience Hub 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 editar los AppComponents para que reflejen mejor la estructura de la aplicación.

Añada o actualice los recursos de la aplicación editando una versión preliminar de la aplicación y publicando los cambios en una nueva versión (de lanzamiento). 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 del informe de evaluación de su aplicación.

Para actualizar la detección de desviaciones de resiliencia de su aplicación

1. En el panel de navegación, elija Aplicaciones.
2. En la página Aplicaciones, seleccione la aplicación para la que desea activar o desactivar la detección de desviación de resiliencia.
3. En Acciones, seleccione Actualizar la detección de desviaciones de resiliencia.
4. Para actualizar la detección de la desviación de resiliencia, complete los pasos que se indican en Paso 5: Detección de desviaciones y, a continuación, vuelva a este procedimiento.
5. Elija Actualizar.

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 los orígenes de entrada, los recursos y los componentes 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 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 los orígenes de entrada, los recursos y los componentes de la aplicación, complete los pasos que se indican a continuación.

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 del origen que se importa de una pila de AWS CloudFormation, se le redirigirá a la página de detalles de la pila en la consola AWS CloudFormation.
   - 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. Los orígenes de entrada incluyen clústeres de Amazon EKS, pilas de AWS CloudFormation, aplicaciones de AppRegistry, AWS Resource Groups, archivos de estado de Terraform y recursos añadidos manualmente.

- Recursos asociados: el número de recursos que están asociados al origen de entrada. Seleccione un número para ver todos los recursos asociados a un origen de entrada en la pestaña Recursos.

2. Para añadir orígenes de entrada a la aplicación, en la sección Orígenes de entrada, seleccione Añadir orígenes de entrada. Para obtener más información sobre cómo agregar fuentes de entrada, consulte the section called “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 tipos de AppComponent, los recursos No compatibles 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 pila de AWS CloudFormation, el archivo de estado de Terraform, la aplicación agregada manualmente, la aplicación AppRegistry o 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 acerca de la agrupación de recursos de AppComponent, consulte Agrupar recursos en un AppComponent.
- 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 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.
- Tipo de origen: el tipo de origen de entrada. Los orígenes de entrada incluyen pilas de AWS CloudFormation, aplicaciones de AppRegistry, AWS Resource Groups, archivos de estado de Terraform y recursos agregados manualmente.

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

- Pila de origen: la pila de AWS CloudFormation 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 componente AWS Resilience Hub que se asignó a este recurso cuando se descubrió la estructura de su aplicación.
- Nombre: el nombre del recurso de la aplicación.
- Cuenta: la cuenta de AWS que posee el 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: Agregue recursos a su aplicación AWS Resilience Hub 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 un AppComponent de la lista desplegable de AppComponent.
   c. Introduzca el ID lógico del recurso en el cuadro Nombre del recurso.
   d. Introduzca el ID del recurso físico, el nombre del recurso o el ARN del recurso en el cuadro Identificador del recurso.
   e. Elija Agregar.

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

   a. Introduzca el ID lógico del recurso en el cuadro Nombre del recurso.
   b. Seleccione Guardar.

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

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

   b. Seleccione Guardar.

9. Para cambiar el componente de aplicación, seleccione un recurso, seleccione Cambiar componente de aplicación en Acciones y complete los siguientes pasos:

   a. Seleccione un AppComponent de la lista desplegable de AppComponent.

   b. Elija Agregar.

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

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

Para editar los AppComponents de su aplicación

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

   > **Note**
   >
   > Para obtener más información acerca de la agrupación de recursos de AppComponent, consulte Agrupar recursos en un AppComponent.

   En la sección AppComponents se enumeran todos los componentes lógicos en los que están agrupados los recursos. Puede identificar los AppComponents de la siguiente manera:

   - Nombre de AppComponent: el nombre del componente AWS Resilience Hub que se asignó a este recurso cuando se descubrió la estructura de su aplicación.
   - Tipo de AppComponent: el tipo de componente AWS Resilience Hub.
   - 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 un nuevo AppComponent y complete los siguientes pasos:

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

   b. Seleccione el tipo de AppComponent en la lista desplegable Tipo de AppComponent.

   c. Seleccione Guardar.

3. Para editar un AppComponent, seleccione un AppComponent y, a continuación, seleccione Editar AppComponent en Acciones.

4. Para eliminar un AppComponent, seleccione un AppComponent y, a continuación, seleccione Eliminar AppComponent de 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 Publicación de una nueva versión de la aplicación AWS Resilience Hub.

Agrupar recursos en un AppComponent

Un 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 al mismo componente de aplicación (AppComponent). AWS Resilience Hub tiene reglas que rigen 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`.

Cuando la aplicación se importa a AWS Resilience Hub una AWS CloudFormation pila, un archivo de estado de Terraform AWS Resource Groups, un clúster de Amazon Elastic Kubernetes Service AppRegistry o una AWS Resilience Hub aplicación, hace todo lo posible por agrupar los recursos relacionados en una misma unidad, pero es posible que no siempre tenga una AppComponent precisión del 100 por ciento. Usted es quien mejor conoce la arquitectura de su aplicación, por lo que puede reagrupar los recursos que ya se han agrupado en una diferente. AWS Resilience Hub

AppComponent Por ejemplo, si tiene tres instancias de EC2 en una AWS CloudFormation pila, AWS Resilience Hub crea una única AppComponent por cada instancia de EC2, pero es posible que las tres instancias de EC2 ejecuten el mismo software de aplicación. En este caso, la opción correcta es reagrupar las tres instancias de EC2 en un solo `ComputeAppComponent`. Al reagrupar los recursos, solo debe reagrupar el recurso en uno solo. AppComponent También puede ampliar su lista de recursos y combinar los recursos desagrupados en un. AppComponent

Son AWS Resilience Hub AppComponents compatibles con 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 for Windows File Server.
  - `AWS::S3::Bucket`

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 en uno solo AppComponent.
- Agrupe las instancias de Amazon EC2 que ejecutan la misma aplicación en una sola. AppComponent
- Agrupe una cola de Amazon SQS y su cola de letra muerta en una sola. AppComponent
- Agrupe los servicios de Amazon ECS en una región y realice la conmutación por error de los servicios de Amazon ECS en otra región en una sola AppComponent.

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

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 el recurso que desea reagrupar.
7. En Acciones, elija Cambiar AppComponent.

   Aparece el AppComponent cuadro de diálogo Cambiar.
8. Para eliminar la imagen actual AppComponent de la AppComponentsección, elija una X en la esquina superior derecha de la etiqueta que muestra su 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.

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. Elija los recursos que desea agrupar.

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

7. Elija Acciones y luego elija Recursos de grupo.

   Aparece la AppComponent ventana Combinar.
8. Elija 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.

Publicación de una nueva versión de la aplicación AWS Resilience Hub

Tras realizar los cambios en los recursos de su aplicación AWS Resilience Hub tal y como se describe en Edición de recursos de aplicaciones de AWS Resilience Hub, 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, procedimientos operativos estándar y pruebas recomendadas a la aplicación.

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 por defecto 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 la aplicación AWS Resilience Hub

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 en 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, seleccione 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, orígenes 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 recursos de la aplicación AWS Resilience Hub

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 pila de AWS CloudFormation, el archivo de estado de Terraform, la aplicación agregada manualmente, la aplicación AppRegistry o 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”.

   - Estado: indica si AWS Resilience Hub evaluará la resiliencia del recurso.

- Tipo de recurso: el tipo de recurso identifica el recurso componente de la aplicación. Por ejemplo, `AWS::EC2::Instance` declara una instancia de Amazon EC2. Para obtener más información acerca de la agrupación de recursos de AppComponent, consulte Agrupar recursos en un AppComponent.
- 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 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.
- Tipo de origen: el tipo de origen de entrada.
- Tipo de AppComponent: tipo de origen de entrada. Los orígenes de entrada incluyen pilas de AWS CloudFormation, aplicaciones de AppRegistry, AWS Resource Groups, archivos de estado de Terraform y recursos agregados manualmente.

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

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

4. Elija Guardar y actualizar.

Eliminación de una aplicación AWS Resilience Hub

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

Para eliminar 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 que AWS Resilience Hub solicitó la información.
- Parámetro: indica la información específica del área de aplicación, que AWS Resilience Hub utilizará 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 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 la aplicación se recuperará de un tipo de interrupción, como el software, el hardware, la Zona de disponibilidad o la Región de AWS. 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 aplicación 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 la Región de AWS. 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 determina si se estima que la aplicación cumpla o no 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 cómo se compara su aplicación 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 coste 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, SOP y pruebas. Estas recomendaciones de configuración pueden mejorar la velocidad de los procedimientos de recuperación.

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

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 sus políticas de RTO y RPO actuales y determina si el componente de aplicación puede satisfacer los objetivos de la política.

Información general

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

RTO

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

RPO

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

Detalles

Proporciona descripciones detalladas de cada tipo de interrupción mediante las pestañas Todos los resultados y Desviaciones de cumplimiento de la aplicación. La pestaña Todos los resultados

muestra todas las interrupciones, incluidas las desviaciones de cumplimiento, mientras que la pestaña Desviaciones de cumplimiento de la aplicación muestra solo las desviaciones de cumplimiento. El tipo de interrupción incluye la Aplicación, la infraestructura de nube (Infraestructura y Zona de disponibilidad) y la Región, y proporciona la siguiente información al respecto:

- AppComponent

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

- RTO estimado

  Indica si la configuración de la política se ajusta a los requisitos de la política. Proporcionamos dos valores: nuestro RTO estimado y su RTO objetivo. Por ejemplo, si ve un valor de 2 h en el RTO fijado como objetivo y 40 min en el RTO estimado de la carga de trabajo, significa que proporcionamos un RTO estimado de la carga de trabajo de 40 minutos, mientras que el RTO actual de su aplicación es de dos horas. Para calcular el RTO estimado de la carga de trabajo, nos basamos en la configuración, no en la política. Como resultado, una base de datos de zonas de disponibilidad múltiple tendrá el mismo RTO estimado de carga de trabajo en caso de fallo en una zona de disponibilidad, independientemente de la política que seleccione.

- Desviación del RTO

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

- RPO estimado

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

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

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

- Desviación del RPO

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

Revisar las recomendaciones de resiliencia

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

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

> **Note**
>
> - AWS Resilience Hub ofrece hasta tres opciones AWS Resilience Hub recomendadas.
> - Si establece objetivos de RTO y RPO regionales, AWS Resilience Hub mostrará Optimizar para el RTO/RPO regional en las opciones recomendadas. Si no se han establecido los objetivos de RTO y RPO regionales, aparecerá Optimizar para RTO/RPO de zona de disponibilidad (AZ). Para obtener más información sobre cómo establecer objetivos regionales de RTO/RPO y, al mismo tiempo, crear políticas de resiliencia, consulte Crear políticas de resiliencia .
> - Los valores de RTO de carga de trabajo estimados y RPO de carga de trabajo estimados para las aplicaciones y sus configuraciones se determinan teniendo en cuenta la cantidad de datos y la cantidad de datos individuales. 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 el RTO/RPO para la zona de disponibilidad

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

Optimizar para el RTO/RPO de la región

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

Optimice en función de los costes

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

Optimizar para cambios mínimos

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

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

- Descripción

  Describe las configuraciones sugeridas por AWS Resilience Hub.
- Cambios

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

- Costo básico

  El costo estimado asociado a los cambios recomendados.

  > **Note**
  >
  > El costo base puede variar en función del uso y no incluye descuentos ni ofertas del Programa de descuentos empresariales (EDP).

- RTO y RPO estimados de la carga de trabajo

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

AWS Resilience Hub evalúa si un componente de la aplicación (AppComponent) puede cumplir con una política de resiliencia. Si no AppComponent cumple con una política de resiliencia y AWS Resilience Hub no puede hacer ninguna recomendación para facilitar el cumplimiento, es posible que el tiempo de recuperación de lo seleccionado AppComponent no pueda cumplirse dentro de las limitaciones del AppComponent. Algunos ejemplos de AppComponent restricciones son el tipo de recurso, el tamaño del almacenamiento o la configuración de los recursos.

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

Revisar las recomendaciones operativas

Las recomendaciones operativas contienen recomendaciones para configurar alarmas, procedimientos operativos estándar y AWS FIS experimentos mediante AWS CloudFormation plantillas.

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 URI de Amazon Simple Storage Service en lugar de utilizar una CLI/API con un archivo local como entrada.

En AWS Resilience Hub, puede realizar las siguientes acciones:

- Puede aprovisionar las alarmas, los SOP y los AWS FIS experimentos seleccionados. Para aprovisionar alarmas, procedimientos operativos estándar y AWS FIS experimentos, seleccione la recomendación adecuada e introduzca un nombre único. AWS Resilience Hub crea una plantilla basada en las recomendaciones seleccionadas. En Plantillas, puede acceder a las plantillas que haya creado a través de una URL de Amazon Simple Storage Service (Amazon S3).
- Puede incluir o excluir las alarmas, los SOP y AWS FIS los experimentos seleccionados que se recomendaron para su aplicación en cualquier momento. 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, los SOP y AWS FIS los experimentos (pruebas) recomendados para mejorar la puntuación de resiliencia de su aplicación en cualquier momento. 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 (SOP) recomendados de su aplicación

1. Complete los siguientes pasos para excluir los SOP recomendados:

   a. En la pestaña Procedimientos operativos estándar, en la tabla SOP, seleccione todos los SOP (con el estado Implementado o No implementado) que desee excluir. Puede identificar el estado de implementación actual de un SOP en la columna Estado.
   b. En Acciones, seleccione Excluir seleccionados para excluir los SOP seleccionados de la aplicación.
   c. En el cuadro de diálogo Excluir recomendaciones, seleccione uno de los siguientes motivos (opcional) y elija Excluir seleccionados para excluir los SOP seleccionados de la aplicación.

      - Ya implementados: seleccione esta opción si ya ha implementado estos SOP en un servicio de AWS o en cualquier otro proveedor de servicios externo.
      - No pertinente: seleccione esta opción si los SOP no se ajustan a los requisitos de su empresa.
      - Demasiado complicado de implementar: seleccione esta opción si cree que estos SOP son demasiado complicados de implementar.
      - Ninguno: seleccione esta opción si no desea especificar el motivo.

2. Para incluir SOP, complete los siguientes pasos:

   a. En la pestaña Procedimientos operativos estándar, en la tabla SOP, 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 seleccionados para incluir todos los SOP seleccionados 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 (como 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 una URL de Amazon S3, descargarla y colocarla en su canal de código o crear una pila a través de la consola de AWS CloudFormation .

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

Para crear alarmas en las recomendaciones operativas

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

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

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

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

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

     Esta columna muestra uno de los siguientes valores:

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

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

7. En la pestaña Alarmas, para filtrar las recomendaciones de la tabla Alarmas en función de un estado específico, seleccione un número inferior al mismo.
8. Seleccione las alarmas recomendadas que desee configurar para su aplicación y elija Crear CloudFormation plantilla.
9. En el cuadro de diálogo Crear CloudFormation plantilla, puede utilizar el nombre generado automáticamente o puede introducir un nombre para la 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 de Amazon S3, en la tabla Objetos, seleccione el enlace a la carpeta SOP.
4. Para copiar la ruta de Amazon S3, seleccione la casilla situada delante del archivo JSON y seleccione Copiar URL.
5. Crea 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 la URL de Amazon S3 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 Alarmas, puede identificar las alarmas implementadas utilizando la siguiente información:

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

Para ver las alarmas implementadas desde las aplicaciones

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

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

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

     Esta columna muestra uno de los siguientes valores:

     - Implementado: indica que las alarmas recomendadas por AWS Resilience Hub están implementadas en su aplicación. Seleccione el número siguiente para ver todas las alarmas recomendadas e implementadas en la pestaña Recomendaciones operativas.
     - No implementadas: indica que las alarmas recomendadas por la aplicación AWS Resilience Hub están incluidas, pero no están implementadas, en la aplicación. Seleccione el número siguiente para ver todas las alarmas recomendadas y no implementadas en la pestaña Recomendaciones operativas.
     - Excluidas: indica que las alarmas recomendadas por AWS Resilience Hub están excluidas de la aplicación. Seleccione el número siguiente para ver todas las alarmas recomendadas y excluidas en la pestaña Recomendaciones operativas. Para obtener más

información sobre cómo incluir y excluir las alarmas recomendadas, consulte Incluir o excluir recomendaciones operativas.

- Inactivo: indica que las alarmas están desplegadas en Amazon CloudWatch, pero el estado está establecido en INSUFFICIENT_DATA en Amazon. CloudWatch Seleccione el número siguiente para ver todas las alarmas implementadas e inactivas en la pestaña Recomendaciones operativas.

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

Para ver las alarmas recomendadas a partir de las evaluaciones

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

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

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

   - Nombre: nombre de la evaluación que proporcionó en el momento de la creación.
   - Estado: indica el estado de ejecución de la evaluación.
   - Estado de conformidad: indica si la evaluación cumple con la política de resiliencia.
   - Estado de desviación de la resiliencia: indica si su aplicación se ha desviado o no de la última evaluación satisfactoria.
   - Versión de la aplicación: versión de su aplicación.
   - Invocador: indica el rol que invocó la evaluación.
   - Hora de inicio: indica la hora de inicio de la evaluación.

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

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

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

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

     Esta columna muestra uno de los siguientes valores:

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

   - Configuración: indica si hay alguna dependencia de configuración pendiente que deba abordarse.
   - Tipo: indica el tipo de alarma.
   - AppComponent— Indica los componentes de la aplicación (AppComponents) que están asociados a esta alarma.

- ID de referencia: indica el identificador lógico del evento de AWS CloudFormation pila en AWS CloudFormation.
- ID de recomendación: indica el identificador lógico del recurso de AWS CloudFormation pila en AWS CloudFormation.

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 el disco basándose en un documento de automatización de SSM existente. Para ejecutar este documento SSM, necesita un rol de IAM específico con los permisos correspondientes. AWS Resilience Hub crea metadatos en la aplicación que indican qué documento de automatización de SSM se debe ejecutar en caso de escasez de espacio en el disco y qué rol 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 experimento de AWS FIS denominado documento de automatización de 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 plantilla AWS CloudFormation 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 experimento de AWS FIS 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 su aplicación y generar una plantilla de AWS CloudFormation a partir de las recomendaciones AWS Resilience Hub es un buen comienzo. Utilice la plantilla de AWS CloudFormation para generar una pila de AWS CloudFormation y, a continuación, utilice los parámetros de 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 implemente su aplicación, también implementará el SOP más actualizado.

Temas

Creación de un SOP basado en recomendaciones AWS Resilience Hub

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

Para crear un SOP basado en recomendaciones AWS Resilience Hub debe crear una plantilla de AWS CloudFormation para los SOP recomendados e incluirlos en su base de código.

Cree una plantilla de AWS CloudFormation para las recomendaciones del SOP

1. Abra la consola de AWS Resilience Hub.
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. seleccione Crear plantilla de CloudFormation. La creación de la plantilla de AWS CloudFormation puede tardar unos minutos.

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

Para incluir las recomendaciones de AWS Resilience Hub 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 pila de AWS CloudFormation 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 pila de AWS CloudFormation en la consola AWS CloudFormation. 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 pila de AWS CloudFormation debe proporcionar la ruta de Amazon S3 que copió en el 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 sugerido por AWS Resilience Hub 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. Añadir un experimento de AWS FIS para probar su 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 en AWS Resilience Hub y personalizarlos según sea necesario. Por ejemplo, añada o elimine los permisos

necesarios para el rol de IAM, cambie la configuración del experimento de AWS FIS 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 mencionó anteriormente, la mejor práctica consiste en añadir experimentos de AWS FIS 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 tanto los SOP proporcionados por AWS Resilience Hub como los 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 sobre los AppComponents compatibles, consulte Agrupar recursos en un AppComponent.

- ID de referencia: indica el identificador lógico del evento de la pila de AWS CloudFormation en AWS CloudFormation.
- ID de recomendación: indica el identificador lógico del recurso de la pila de AWS CloudFormation enAWS CloudFormation.

Experimentos del Servicio de inyección de errores de Amazon

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 la aplicación, 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 (SOP) y las pruebas de la aplicación. Según el tipo de recursos que utilice la aplicación, AWS Resilience Hub recomienda alarmas, procedimientos operativos estándar y un conjunto de pruebas para cada tipo de interrupción.

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

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

Acceder a la puntuación de resiliencia de sus aplicaciones

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

Acceder a la puntuación de resiliencia desde el panel

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

Acceder a la puntuación de resiliencia desde las aplicaciones

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

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

   - Para ver los elementos de acción que deben completarse para mejorar y lograr la máxima puntuación de resiliencia posible, seleccione la pestaña Elementos de acción. Cuando se selecciona, AWS Resilience Hub muestra lo siguiente:
     - RTO/RPO: indica la cantidad de tiempos de recuperación (RTO/RPO) que deben corregirse para resolver las infracciones de la política de resiliencia de la aplicación. Elija el valor para ver los datos del RTO/RPO en el informe de evaluación de su aplicación.
     - Alarmas: indica el número de CloudWatch alarmas de Amazon recomendadas que deben implementarse en tu aplicación. Elija el valor para ver las CloudWatch alarmas de Amazon que deben corregirse en el informe de evaluación de su aplicación.
     - SOP: indica el número de SOP recomendados que deben implementarse en la aplicación. Elija el valor para ver los SOP que deben corregirse en el informe de evaluación de su aplicación.
     - FIS: indica el número de pruebas recomendadas que deben implementarse en la aplicación. Seleccione el valor para ver las pruebas que deben corregirse en el informe de evaluación de su aplicación.

- Para ver la puntuación de cada componente que afecta a su puntuación de resiliencia, seleccione Desglose de puntuaciones. Cuando se selecciona esta opción, AWS Resilience Hub muestra lo siguiente:
  - Conformidad con la RTO/RPO: indica el grado de conformidad de los componentes de la aplicación (AppComponents) con los tiempos estimados de recuperación de la carga de trabajo y con los tiempos de recuperación objetivo definidos en la política de resiliencia de la aplicación. Seleccione el valor para ver las estimaciones de RTO/RPO 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.
  - SOP implementados: indica la contribución real de los SOP implementados en comparación con su contribución máxima posible a la puntuación de resiliencia de su aplicación. Seleccione el valor para ver los SOP implementados en el informe de evaluación de su aplicación.
  - Experimentos del FIS implementados: indica la contribución real de las pruebas implementadas en comparación con su contribución máxima posible a la puntuación de resiliencia de su aplicación. Seleccione el valor para ver las pruebas implementadas en el informe de evaluación de su aplicación.
- Para ver las infracciones de la política de resiliencia y las recomendaciones operativas, seleccione la flecha derecha para ampliar la sección Desglose de las recomendaciones operativas y de incumplimiento de la política. Cuando está expandido, AWS Resilience Hub muestra lo siguiente:
  - Incumplimientos de la política de resiliencia: indica la cantidad de componentes de la aplicación que infringen la política de resiliencia de la aplicación. Seleccione el valor situado junto a RTO/RPO para ver los datos relativos en la pestaña Recomendaciones de resiliencia del informe de evaluación de su aplicación.
  - Recomendaciones operativas: indica las recomendaciones operativas que no se han implementado o ejecutado para mejorar la resiliencia de su aplicación mediante las pestañas Pendientes y Excluidas. Las recomendaciones operativas incluyen todas las recomendaciones que están inactivas y las que no se han implementado.

    Para ver las recomendaciones operativas que deben implementarse, seleccione la pestaña Pendientes. Cuando se selecciona, AWS Resilience Hub muestra lo siguiente:

- Alarmas: indica el número de CloudWatch alarmas de Amazon recomendadas que deben implementarse.
- SOP: indica el número de SOP recomendados que deben implementarse.
- FIS: indica la cantidad de pruebas recomendadas que deben implementarse.

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

- Alarmas: indica el número de CloudWatch alarmas de Amazon recomendadas que están excluidas de tu aplicación.
- SOP: indica el número de SOP recomendados que están excluidos de la aplicación.
- FIS: indica el número de pruebas recomendadas que están excluidas de la aplicación.

Calcular las puntuaciones de resiliencia

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

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

Tablas

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

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

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

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

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

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

Componente de puntuación	Descripción	Fórmula	Ejemplo
Conformidad con RTO/RPO (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: • Si ha establecido objetivos de RTO y RPO regionales, P se calcula de la siguiente manera: `P = (20 + 30)/ 100` Es decir, `P = .5 or 50 points` • Si no ha establecido objetivos de RTO y RPO regionales, P se calcula de la siguiente manera:

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

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

Fórmula para calcular la puntuación de resiliencia

Componente de puntuación	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:
		`RS = (T * Weight(T) +`
		`A * Weight(A) +`
		`S * Weight(S) +`
		`P * Weight(P)) /`
		`(Weight(T) + Weight(A) + Weight(S) + Weight(P))`
			Las fórmulas para calcular la cobertura de cada tabla de tipos de recomendación son las siguientes:
			• `Test coverage (T) = .75`
			• `Alarms (A) = .75`
			• `SOPs (S) = .75`
			• `Meeting resiliency policy (P) = .5`

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

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

- 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. Es decir: RSao = Weighted Average (T, A, S, P) Los valores T, A, S, P se calculan para todas las pruebas recomendadas, las alarmas y los procedimi	ent y por tipo se calcula mediante la siguiente fórmula: RSao = (T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))	recomendaciones son las siguientes: • Test coverage (T) = .75 • Alarms (A) = .75 • SOPs (S) = .75 • Meeting resiliency policy (P) = .5 La puntuación de resiliencia por tipo de interrupción AppComponent y por tipo de interrupción se calcula de la siguiente manera: RSao = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4) Es decir, RSao = .65 or 65 points

Componente de puntuación	Descripción	Fórmula	Ejemplo
	entos operativos estándar y para cumplir con la política de resilienc ia del tipo de AppCompon ent interrupc ión.		

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)`
	
	Los valores para `T, A, S, P` se calculan para todas las pruebas, alarmas y procedimientos operativos estándar recomendados y para
		La puntuación de resiliencia per AppComponent se calcula mediante la siguiente fórmula:
		
		`RSa = (T * Weight(T) +`
		
		`A * Weight(A) +`
		
		`S * Weight(S) +`
		
		`P * Weight(P)) /`
		
		`(Weight(T) + Weight(A) + Weight(S) + Weight(P))`
			Las suposiciones `RSa` para todos los tipos de recomendaciones son las siguientes:
			
			• `Test coverage (T) = .75`
			• `Alarms (A) = .75`
			• `SOPs (S) = .75`
			• `Meeting resiliency policy (P) = .5`
			
			La puntuación de resiliencia por AppComponent se calcula de la siguiente manera:
			
			`RSa = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4)`
			
			Es decir, `RSa = .65 or 65 points`

Componente de puntuación	Descripción	Fórmula	Ejemplo
	cumplir con la política de resiliencia del. AppComponent		

Componente de puntuación	Descripción	Fórmula	Ejemplo

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

Componente de puntuación	Descripción	Fórmula	Ejemplo
	relacionadas con el tipo de interrupción.		

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, los procedimientos operativos estándar (SOP), las pruebas, la política de resiliencia de las reuniones y los tipos de interrupciones. Los tipos de interrupciones incluyen Aplicación, Infraestructura, Zona de disponibilidad y Región.

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

Ponderación de las alarmas, procedimientos operativos estándar, pruebas y objetivo de la política

Tipo de recomendación	Peso
Alarmas	20 puntos
SOP	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 elegir Crear plantilla CloudFormation en la página Recomendaciones operativas, AWS Resilience Hub crea una plantilla de AWS CloudFormation que describe la alarma, el procedimiento operativo estándar (SOP) o el experimento específico de AWS FIS para su aplicación. La plantilla de AWS CloudFormation 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 Recomendaciones operativas.

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

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

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",
  "Parameters" : {
    "SNSTopicARN" : {
      "Type" : "String",
      "Description" : "The ARN of the 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."
      }
    }
  }
}
```

Modificación de la plantilla AWS CloudFormation

La forma más sencilla de integrar una alarma, un SOP o un recurso de AWS FIS en la aplicación principal consiste simplemente en añadirlos como otro recurso a la plantilla que describe la plantilla de la aplicación. El archivo con formato JSON que se proporciona a continuación proporciona un esquema básico de cómo se describe una tabla de DynamoDB en una plantilla de 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 necesita reemplazar los recursos codificados por una referencia dinámica en las pilas de aplicaciones.

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 las plantillas de AWS CloudFormation para los SOP y los experimentos de AWS FIS, adoptará el mismo enfoque: sustituirá los identificadores de referencia codificados por referencias dinámicas que seguirán funcionando incluso después de los cambios de hardware.

Al usar una referencia a la tabla de DynamoDB, usted permite a AWS CloudFormation 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 AWS CloudFormation necesita reemplazar el recurso.

> **Note**
>
> Puede elegir métodos más avanzados para administrar los recursos de su aplicación con AWS CloudFormation, como anidar pilas o consultar las salidas de recursos en una pila de AWS CloudFormation independiente. (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 usar herramientas de terceros, como Terraform de HashiCorp, para aprovisionar Infraestructura como código (IaC).

Uso de las API AWS Resilience Hub para describir y administrar la aplicación

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

- 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 sobre las API AWS Resilience Hub que se utilizan para preparar una aplicación, consulte los siguientes temas:

- the section called “Cree 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 a la API `CreateApp` y proporcionar un nombre de aplicación único. Para obtener más información acerca esta API, consulte https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateApp.html.

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

Solicitud

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

Respuesta

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

Creación de una política de resiliencia

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

En el siguiente ejemplo, se muestra cómo crear un `newPolicy` para su aplicación en AWS Resilience Hub mediante una API `CreateResiliencyPolicy`.

Solicitud

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

Respuesta

```
{
```

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

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

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

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

información acerca esta API, consulte https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeDraftAppVersionResourcesImportStatus.html.

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

Solicitud

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

Respuesta

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

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

Solicitud

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

Respuesta

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

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

Solicitud

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

Respuesta

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

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

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

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

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

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

   Solicitud

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

   Respuesta

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

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

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

   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

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

Para obtener más información, consulte los siguientes temas:

- 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 en AWS Resilience Hub y supervisar su estado, debe usar las siguientes API:

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

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

Solicitud

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

Respuesta

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

```
            "policy": {
                "AZ": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                },
                "Hardware": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                },
                "Software": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                }
            }
        },
        "tags": {}
    }
}
```

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

Solicitud

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

Respuesta

```
{
    "assessment": {
        "appArn": "<App_ARN>",
        "appVersion": "release",
        "cost": {
            "amount": 0.0,
            "currency": "USD",
            "frequency": "Monthly"
        },
        "resiliencyScore": {
            "score": 0.27,
            "disruptionScore": {
```

```
                "AZ": 0.42,
                "Hardware": 0.0,
                "Region": 0.0,
                "Software": 0.38
            }
        },
        "compliance": {
            "AZ": {
                "achievableRtoInSecs": 0,
                "currentRtoInSecs": 4500,
                "currentRpoInSecs": 86400,
                "complianceStatus": "PolicyMet",
                "achievableRpoInSecs": 0
            },
            "Hardware": {
                "achievableRtoInSecs": 0,
                "currentRtoInSecs": 2595601,
                "currentRpoInSecs": 2592001,
                "complianceStatus": "PolicyBreached",
                "achievableRpoInSecs": 0
            },
            "Software": {
                "achievableRtoInSecs": 0,
                "currentRtoInSecs": 4500,
                "currentRpoInSecs": 86400,
                "complianceStatus": "PolicyMet",
                "achievableRpoInSecs": 0
            }
        },
        "complianceStatus": "PolicyBreached",
        "assessmentStatus": "Success",
        "startTime": "2022-10-27T08:15:10.452000+03:00",
        "endTime": "2022-10-27T08:15:31.883000+03:00",
        "assessmentName": "first-assessment",
        "assessmentArn": "<Assessment_ARN>",
        "policy": {
            "policyArn": "<Policy_ARN>",
            "policyName": "newPolicy",
            "dataLocationConstraint": "AnyLocation",
            "policy": {
                "AZ": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                },
```

```
                "Hardware": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                },
                "Software": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                }
            }
        },
        "tags": {}
    }
}
```

Examen de los resultados de la evaluación

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

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

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

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

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

Solicitud

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

Respuesta


```
{
    "alarmRecommendations": [
        {
            "recommendationId": "78ece7f8-c776-499e-baa8-b35f5e8b8ba2",
            "referenceId": "app_common:alarm:synthetic_canary:2021-04-01",
            "name": "AWSResilienceHub-SyntheticCanaryInRegionAlarm_2021-04-01",
            "description": "A monitor for the entire application, configured to
 constantly verify that the application API/endpoints are available",
            "type": "Metric",
            "appComponentName": "appcommon",
            "items": [
                {
                    "resourceId": "us-west-2",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ],
            "prerequisite": "Make sure 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": "Alarm by AWS ResilienceHub that reports when 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": "Alarm by AWS ResilienceHub 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": "Alarm by AWS ResilienceHub 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": "Alarm by AWS ResilienceHub 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": "Alarm by AWS ResilienceHub 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": "Alarm by AWS Resilience Hub for Amazon ECS that triggers if
 the count of tasks isn't equal Service Desired Count",
            "type": "Metric",
            "appComponentName": "computeappcomponent-nrz",
            "items": [
                {
                    "resourceId": "aws_ecs_service_terraform-us-east-1-demo",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ],
            "prerequisite": "Make sure the Container Insights on Amazon ECS is enabled:
 (see the <a href=\"https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/
deploy-container-insights-ECS-cluster.html\" target=\"_blank\">docs</a>)."
        }
```

```
    ]
}
```

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

Solicitud

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

Respuesta

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

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

```
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        }
                    },
                    "optimizationType": "LeastChange",
                    "description": "Current Configuration",
                    "suggestedChanges": [],
                    "haArchitecture": "BackupAndRestore",
                    "referenceId": "original"
                },
                {
                    "cost": {
                        "amount": 14.74,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "computeappcomponent-nrz",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 0,
                            "expectedRtoDescription": "No expected downtime. You're
launching using EC2, with DesiredCount > 1 in multiple AZs and CapacityProviders with
MinSize > 1",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "ECS Service state is saved on
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
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 ECS service with launch type EC2 and EFS
storage, deployed in multiple AZs. AWS Backup is used to backup EFS and copy snapshots
in-region.",
                    "suggestedChanges": [
                        "Add Auto Scaling Groups and Capacity Providers in multiple
AZs",
                        "Change desired count of the setup",
                        "Remove 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 EFS from backup.
(Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Recovery Point Objective for EFS
from backups, derived from backup frequency"
                        }
                    },
                    "optimizationType": "BestAZRecovery",
                    "description": "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 EFS from backup.
(Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Recovery Point Objective for EFS
from backups, derived from backup frequency"
                        }
                    },
                    "optimizationType": "BestAttainable",
                    "description": "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 al editar una versión preliminar de la aplicación y al publicar 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 siguientes temas:

- 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 un origen de entrada, AWS Resilience Hub le permite añadir el recurso manualmente a su aplicación mediante la API `CreateAppVersionResource`. Para obtener más información acerca esta API, consulte https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateAppVersionResource.html.

Debe proporcionar los siguientes parámetros a esta API:

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

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

Solicitud

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

Respuesta

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

Agrupar los recursos en un único componente de aplicación

Un componente de aplicación (AppComponent) es un grupo de recursos de AWS 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 recursos de AWS pueden pertenecer a qué tipo de AppComponent. AWS Resilience Hub permite

agrupar los recursos en un único AppComponent mediante las siguientes API de administración de recursos.

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

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

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"
    }
}
```

En el siguiente ejemplo, se muestra cómo eliminar el AppComponent vacío que se creó en los ejemplos anteriores en AWS Resilience Hub mediante la API `UpdateAppVersionResource`.

Solicitud

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

Respuesta

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

Excluir un recurso de un AppComponent

AWS Resilience Hub permite excluir los recursos de las evaluaciones mediante la API `UpdateAppVersionResource`. Estos recursos no se tendrán en cuenta al calcular la resiliencia de la aplicación. Para obtener más información acerca esta API, consulte https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_UpdateAppVersionResource.html.

> **Note**
>
> Solo puede excluir los recursos que se importaron de un origen de entrada.

El siguiente ejemplo muestra cómo excluir un recurso de su aplicación en AWS Resilience Hub mediante la API `UpdateAppVersionResource`.

Solicitud

```
aws resiliencehub update-app-version-resource \
--app-arn <App_ARN> \
--resource-name "ec2instance-nvz" \
--excluded
```

Respuesta

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

```
        "resourceName": "ec2instance-nvz",
        "logicalResourceId": {
            "identifier": "ec2",
            "terraformSourceName": "test.state.file"
        },
        "physicalResourceId": {
            "identifier": "i-0b58265a694e5ffc1",
            "type": "Native",
            "awsRegion": "us-west-2",
            "awsAccountId": "123456789101"
        },
        "resourceType": "AWS::EC2::Instance",
        "appComponents": [
            {
                "name": "computeappcomponent-nrz",
                "type": "AWS::ResilienceHub::ComputeAppComponent"
            }
        ]
    }
}
```

Seguridad en AWS Resilience Hub

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

La seguridad es una responsabilidad compartida entre AWS usted y usted. El 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.

Contenidos

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 las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

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

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios 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 módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con Resilience Hub u otro dispositivo Servicios de AWS mediante la consola, la API o los SDK. AWS CLI AWS Cualquier dato que 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, recomendamos encarecidamente que no incluya la información de las credenciales en la URL para validar la solicitud para ese servidor.

Cifrado en reposo

AWS Resilience Hub cifra sus datos en reposo. Los datos en reposo AWS Resilience Hub se cifran mediante un cifrado transparente del lado del servidor. Esto ayuda a reducir la carga y la complejidad operativas que conlleva la protección de información confidencial. Con el cifrado en reposo, puede crear aplicaciones sensibles a la seguridad que cumplen los requisitos de cifrado y normativos.

Cifrado en tránsito

AWS Resilience Hub cifra los datos en tránsito entre el servicio y otros servicios integrados. AWS Todos los datos que pasan entre los servicios integrados AWS Resilience Hub y los servicios integrados se cifran mediante Transport Layer Security (TLS). AWS Resilience Hub proporciona acciones preconfiguradas para tipos específicos de objetivos en todos los AWS servicios y respalda las acciones para los recursos objetivo.

Identity and Access Management for AWS Resilience Hub

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

Temas

- AWS Resilience Hub Habilitar la publicación en tus temas de Amazon Simple Notification Service
- Limitar los permisos para incluir o excluir AWS Resilience Hub recomendaciones

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realice 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. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar la IAM con AWS Resilience Hub, consulteCómo funciona AWS Resilience Hub con IAM.

Administrador de IAM: si es administrador de IAM, puede que le interese obtener más información sobre cómo 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 usar en IAM, 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 usuario de IAM o asumiendo una función de IAM. 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 (Centro de identidades de IAM), 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, su

administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

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 proporciona 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 las solicitudes de la AWS API en la Guía del usuario de IAM.

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 multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Uso de la autenticación multifactor (MFA) en AWSen la Guía del usuario de IAM.

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 las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, 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 Single Sign-On. Puede crear usuarios y grupos en el Centro de identidades de IAM, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. 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 de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

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 permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

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

Los roles de IAM 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 acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS Single Sign-On.
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común 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 usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS 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 sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio

desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

- Función vinculada al 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 administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar una AWS función a una instancia EC2 y ponerla a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

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 documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

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

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

Las políticas de IAM definen 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 la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de 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 roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política 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 puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso (ACL)

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

Amazon S3 y Amazon VPC son ejemplos de servicios que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte Información general de 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 característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). 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 Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. El SCP limita 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 acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations.
- 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 más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

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

Cómo funciona AWS Resilience Hub con IAM

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

Funciones de IAM que puede utilizar con Resilience Hub AWS

Característica de IAM	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
ACL	No
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí
Sesiones de acceso directo (FAS)	Sí
Roles de servicio	Sí

Para obtener una visión general de cómo funcionan AWS Resilience Hub y otros AWS servicios con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en la identidad para Resilience Hub AWS

Compatibilidad con las políticas basadas en identidades	Sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, 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 más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. 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 más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en la identidad para Resilience Hub AWS

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

Compatibilidad con las políticas basadas en recursos	No

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

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. 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 administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso 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 más información, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Acciones políticas para AWS Resilience Hub

Admite acciones de política	Sí

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

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. 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 en AWS Resilience Hub usan 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

Admite recursos de políticas	Sí

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

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el 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 ARN, consulte los recursos definidos por AWS Resilience Hub en la Referencia de autorización de servicios. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte Acciones definidas por AWS Resilience Hub.

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

Condiciones políticas: claves de las condiciones de Resilience AWS Hub

Admite claves de condición de políticas específicas del servicio	Sí

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

El elemento `Condition` (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 un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

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

Para ver una lista de las claves de condición de AWS Resilience Hub, consulte las claves de condición de AWS Resilience Hub en la Referencia de autorización de servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Acciones definidas por AWS Resilience Hub.

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

ACL en Resilience Hub AWS

Admite las ACL	No

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

ABAC con Resilience Hub AWS

Admite ABAC (etiquetas en las políticas)	Parcial

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

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta 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 sobre ABAC, consulte ¿Qué es ABAC? en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con AWS Resilience Hub

Compatible con el uso de 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 Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante 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 más información sobre el cambio de roles, consulte Cambio a un rol (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS 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 más información, consulte Credenciales de seguridad temporales en IAM.

Sesiones de acceso directo para AWS Resilience Hub

Admite Forward access sessions (FAS)	Sí

Cuando utiliza un usuario o un rol de IAM para realizar acciones en AWSél, se le considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS 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 sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Funciones de servicio para AWS Resilience Hub

Compatible con roles de servicio	Sí

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de AWS Resilience Hub. Edite las funciones de servicio solo cuando AWS Resilience Hub le dé instrucciones para hacerlo.

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 mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o la AWS API. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede agregar las políticas de IAM a los roles, y los usuarios pueden asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por AWS Resilience Hub, incluido el formato de los ARN de cada uno de los tipos de recursos, consulte las acciones, los recursos y las claves de condición de AWS Resilience Hub en la Referencia de autorización de servicios.

Temas

- Prácticas recomendadas sobre las políticas
- Uso de la consola Resilience Hub AWS

- Cómo permitir a los usuarios consultar sus propios permisos
- Lista de las aplicaciones disponibles AWS Resilience Hub
- Inicio de una evaluación de la solicitud
- Eliminar la evaluación de una aplicación
- Crear una plantilla de recomendación para una aplicación específica
- Eliminar una plantilla de recomendaciones para una aplicación específica
- Actualizar una aplicación con una política de resiliencia específica

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. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.

- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Política de validación de Analizador de acceso de IAM en la Guía de usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Configuración del acceso a una API protegido por MFA en la Guía de usuario de IAM.

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

Uso de la consola Resilience Hub AWS

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 en su cuenta Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

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

Para garantizar que los usuarios y los roles puedan seguir utilizando la consola de AWS Resilience Hub, adjunte también el AWS Resilience Hub *ConsoleAccess* o la política *ReadOnly* AWS gestionada a las entidades. Para más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

La siguiente política otorga a los usuarios el permiso para enumerar y ver todos los recursos de la AWS Resilience Hub consola, pero no para crearlos, actualizarlos ni eliminarlos.

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

```
        {
            "Effect": "Allow",
            "Action": [
                "resiliencehub:List*",
                "resiliencehub:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

Cómo permitir a los usuarios consultar sus propios permisos

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

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

```
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

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/*" }
      }
    }
  ]
}
```

Configuración de roles y permisos de IAM

AWS Resilience Hub le permite configurar las funciones de IAM que le gustaría utilizar al ejecutar las evaluaciones de su aplicación. Hay varias formas de configurar AWS Resilience Hub para obtener acceso de solo lectura a los recursos de la aplicación. Sin embargo, AWS Resilience Hub recomienda lo siguiente:

- Acceso basado en roles: este rol se define y usa en la cuenta corriente. AWS Resilience Hub asumirá este rol para acceder a los recursos de su aplicación.

  Para proporcionar un acceso basado en roles, el rol debe incluir lo siguiente:

  - Permiso de solo lectura para leer sus recursos (se AWS Resilience Hub recomienda utilizar la política `AwsResilienceHubAssessmentPolicy` 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 una función de este tipo 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 los ARN del rol para otras cuentas, que se utilizarán en lugar del nombre del rol del invocador.

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

- `AwsResilienceHubAdminAccountRole` en la cuenta actual
- `AwsResilienceHubExecutorAccountRole` en otras cuentas

Además, cuando configure una evaluación programada, AWS Resilience Hub asumirá esa `AwsResilienceHubPeriodicAssessmentRole` función. Sin embargo, no se recomienda utilizar `AwsResilienceHubPeriodicAssessmentRole` porque hay que configurar manualmente los roles y permisos, y es posible que algunas funcionalidades (como la Detección de desviaciones de resiliencia) 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 los problemas habituales que pueden surgir al trabajar con AWS Resilience Hub e IAM.

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.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `resiliencehub:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 resiliencehub:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `resiliencehub:`*`GetWidget`*.

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

No estoy autorizado a realizar tareas como: PassRole

Si recibe un mensaje de error que indica que no está autorizado a realizar la `iam:PassRole` acción, sus políticas deben actualizarse para que pueda transferir una función a AWS Resilience Hub.

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

El siguiente ejemplo de error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en AWS Resilience Hub. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir 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 admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para saber si AWS Resilience Hub admite estas funciones, consulteCómo funciona AWS Resilience Hub con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en la Guía del usuario de IAM.

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

AWS Resilience Hub referencia de permisos de acceso

Puede usar AWS Identity and Access Management (IAM) para administrar el acceso a los recursos de la aplicación y crear políticas de IAM que se apliquen a los usuarios, grupos o roles.

Todas las AWS Resilience Hub aplicaciones se pueden configurar para que utilicen the section called “Rol de invocador” (una función de IAM) o los permisos de usuario de IAM actuales (junto con un conjunto de funciones predefinidas para la evaluación multicuenta y programada). En esta función, puede adjuntar una política que defina los permisos necesarios AWS Resilience Hub para acceder a otros AWS recursos o recursos de la aplicación. La función de invocador debe tener una política de confianza que se añada a AWS Resilience Hub Service Principal.

Para administrar los permisos de su aplicación, le recomendamos que utilice the section called “AWS políticas gestionadas”. Puede usar estas políticas administradas sin ninguna modificación, o puede usarlas como punto de partida para escribir sus propias políticas restrictivas. Las políticas pueden restringir los permisos de los usuarios a nivel de recursos para diferentes acciones mediante el uso de condiciones opcionales adicionales.

Si los recursos de la aplicación están en cuentas diferentes (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 un rol de IAM”
- the section called “Usar permisos de usuario de IAM actuales”

Uso un rol de IAM

AWS Resilience Hub utilizará una función de IAM predefinida y existente para acceder a los recursos de la cuenta principal o de 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 a los servicios y recursos. AWS Por ejemplo, puede crear un rol de invocador que tenga permiso para acceder a su plantilla CFN y al recurso que crea. Esta página proporciona información sobre cómo crear, ver y administrar un rol de invocador de aplicaciones.

Al crear una aplicación, se proporciona un rol de invocador. AWS Resilience Hub asume este rol para acceder a sus recursos cuando importe recursos o inicie una evaluación. AWS Resilience Hub Para asumir correctamente la función de invocador, la política de confianza de la función debe especificar que el principal del AWS Resilience Hub servicio (resiliencehub.amazonaws.com) es un servicio de confianza.

Para ver el rol de invocador de la aplicación, seleccione Aplicaciones en el panel de navegación y, a continuación, seleccione Actualizar permisos en el menú Acciones de la página Aplicación.

Puede añadir o eliminar permisos de un rol de invocador de aplicación en cualquier momento, o configurar la aplicación para que utilice un rol diferente para acceder a los recursos de la aplicación.

Temas

- the section called “Crear un rol invocador en la consola de IAM”
- the section called “Administración de roles con la API de IAM”
- the section called “Definir la política de confianza mediante un archivo JSON”

Crear un rol invocador en la consola de IAM

Para poder acceder AWS Resilience Hub a los AWS servicios y recursos, debe crear un rol de invocador en la cuenta principal mediante la consola de IAM. Para obtener más información sobre la creación de funciones mediante la consola de IAM, consulte Creación de una función para un AWS servicio (consola).

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

1. Abra la consola de IAM en `https://console.aws.amazon.com/iam/`.
2. En el panel de navegación, seleccione Roles y, a continuación, seleccione Crear rol.
3. Seleccione Política de confianza personalizada, copie la siguiente política en la ventana Política de confianza personalizada y, a continuación, seleccione Siguiente.

> **Note**
>
> Si sus recursos están en cuentas diferentes, debe crear un rol en cada una de esas cuentas y usar la política de confianza de la cuenta secundaria para las demás cuentas.

```
{
  "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 permiso de `iam:passRole` en su rol/usuario de IAM actual al rol invocador cuando cree o actualice la aplicación. Sin embargo, no necesita este permiso para ejecutar una evaluación.

Administración de roles con la API de IAM

La política de confianza de un rol otorga a la entidad principal especificada permiso para asumir el rol. Para crear los roles mediante AWS Command Line Interface (AWS CLI), utilice el `create-role` comando. Al usar este comando, puede especificar las políticas de confianza en línea. El siguiente ejemplo muestra cómo conceder al AWS Resilience Hub servicio el permiso principal para que asuma su función.

> **Note**
>
> El requisito de estar por fuera de las comillas (`' '`) en la cadena JSON puede variar en función de la versión de intérprete de comandos.

Ejemplo de **`create-role`**

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-role-policy-
document '{
  "Version": "2012-10-17","Statement":
  [
```

```
    {
      "Effect": "Allow",
      "Principal": {"Service": "resiliencehub.amazonaws.com"},
      "Action": "sts:AssumeRole"
    }
  ]
}'
```

Definir la política de confianza mediante un archivo JSON

Puede definir la política de confianza para el rol utilizando un archivo JSON independiente y luego ejecutar el comando `create-role`. En el siguiente ejemplo, se muestra un archivo **`trust-policy.json`** que contiene la política de confianza en el directorio actual. Esta política se asocia a un rol mediante la ejecución del comando **`create-role`**. El resultado del comando **`create-role`** se muestra en el Ejemplo de salida. Para añadir permisos a la función, 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 consola de IAM para cuentas secundarias o de recursos”
- the section called “Administración de roles con la API de IAM”

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

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

Para poder acceder AWS Resilience Hub a AWS los servicios y recursos de otras AWS cuentas, debe crear funciones en cada una de estas cuentas.

Para crear un rol en la consola de IAM para las cuentas secundarias o de recursos mediante la consola de IAM

1. Abra la consola de IAM en `https://console.aws.amazon.com/iam/`.
2. En el panel de navegación, seleccione Roles y, a continuación, seleccione Crear rol.
3. Seleccione Política de confianza personalizada, copie la siguiente política en la ventana Política de confianza personalizada y, a continuación, seleccione Siguiente.

> **Note**
>
> Si sus recursos están en cuentas diferentes, debe crear un rol en cada una de esas cuentas y usar la política de confianza de la cuenta secundaria para las demás cuentas.

```
{
  "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"
      ]
}
```

Administración de roles con la API de IAM

La política de confianza de un rol otorga a la entidad principal especificada permiso para asumir el rol. Para crear los roles mediante AWS Command Line Interface (AWS CLI), utilice el `create-role` comando. Al usar este comando, puede especificar las políticas de confianza en línea. En el siguiente ejemplo, se muestra cómo conceder al director del AWS Resilience Hub servicio el permiso para que asuma su función.

> **Note**
>
> El requisito de estar por fuera de las comillas (`'  '`) en la cadena JSON puede variar en función de la versión de intérprete de comandos.

Ejemplo de **`create-role`**

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-role-policy-
document '{"Version": "2012-10-17","Statement": [{"Effect": "Allow","Principal":
 {"AWS": ["arn:aws:iam::primary_account_id:role/InvokerRoleName"]},"Action":
 "sts:AssumeRole"}]}'
```

También puede definir la política de confianza para el rol con un archivo JSON aparte. En el siguiente ejemplo, `trust-policy.json` es un archivo que se encuentra en el directorio actual.

Definir la política de confianza mediante un archivo JSON

Puede definir la política de confianza para el rol utilizando un archivo JSON independiente y luego ejecutar el comando `create-role`. En el siguiente ejemplo, se muestra un archivo **`trust-policy.json`** que contiene la política de confianza en el directorio actual. Esta política se asocia a un rol mediante la ejecución del comando **`create-role`**. El resultado del comando **`create-role`** se muestra en el Ejemplo de salida. Para añadir permisos a un rol, 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.
```

Usar permisos de usuario de IAM actuales

Utilice este método si quiere usar sus permisos de usuario de IAM actuales para crear y ejecutar una evaluación. Puede adjuntar la política administrada por `AWSResilienceHubAsssessmentExecutionPolicy` a su usuario de IAM o un rol asociado a su usuario.

Configuración de cuenta única

El uso de la política administrada mencionada anteriormente es suficiente para ejecutar una evaluación en una aplicación que se administra en la misma cuenta que el usuario de IAM.

Configuración de la evaluación programada

Debe crear un nuevo rol de `AwsResilienceHubPeriodicAssessmentRole` para que AWS Resilience Hub pueda realizar las tareas relacionadas con la evaluación programada.

> **Note**
>
> - Si utiliza el acceso basado en roles (con el rol de invocador mencionado anteriormente), este paso no es obligatorio.
> - El nombre de rol debe ser `AwsResilienceHubPeriodicAssessmentRole`.

Para 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 permisos de IAM son obligatorias si utiliza AWS Resilience Hub con varias cuentas. Es posible que cada AWS cuenta necesite permisos diferentes según su caso de uso. Al configurar AWS Resilience Hub para el acceso entre cuentas, se tienen en cuenta las siguientes cuentas y roles:

- Cuenta principal: cuenta de AWS en la que desea crear la aplicación y ejecutar las evaluaciones.
- 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 su clúster de Amazon EKS”.

Configuración de cuenta principal

Debe crear un nuevo rol `AwsResilienceHubAdminAccountRole` en la cuenta principal y permitir el AWS Resilience Hub acceso para asumirlo. Esta función se utilizará para acceder a otra función de su AWS cuenta que contenga sus recursos. No debe tener permisos para leer los recursos.

> **Note**
>
> - El nombre de rol debe ser `AwsResilienceHubAdminAccountRole`.
> - Debe crearse en la cuenta principal.
> - Su usuario o rol de IAM actual debe tener el permiso de `iam:assumeRole` 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 AWS cuenta:

```
{
  {
  "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 estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

AWSResilienceHubAsssessmentExecutionPolicy

Puede adjuntar la `AWSResilienceHubAsssessmentExecutionPolicy` a las identidades de IAM. Al ejecutar una evaluación, esta política otorga permisos de acceso a otros AWS servicios para ejecutar las evaluaciones.

Detalles del permiso

Esta política proporciona los permisos adecuados para publicar alarmas AWS FIS y plantillas de SOP en su bucket de Amazon Simple Storage Service (Amazon S3). El nombre del bucket de Amazon S3 debe comenzar por `aws-resilience-hub-artifacts-`. Si desea publicar en otro bucket de Amazon S3, puede hacerlo mientras llama a la API `CreateRecommendationTemplate`. Para obtener más información, consulte CreateRecommendationTemplate.

Esta política incluye los permisos siguientes:

- Amazon CloudWatch (CloudWatch): obtiene todas las alarmas implementadas que configuraste en Amazon CloudWatch para monitorear la aplicación. Además, publicamos CloudWatch las métricas de la puntuación de resiliencia de la aplicación en el `ResilienceHub` espacio de nombres. `cloudwatch:PutMetricData`
- Amazon Data Lifecycle Manager: obtiene y proporciona `Describe` permisos para los recursos de Amazon Data Lifecycle Manager 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 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 (Amazon EC2): enumera y proporciona permisos de `Describe` para los recursos de Amazon EC2 asociados a su cuenta de AWS .
- Amazon Elastic Container Registry (Amazon ECR): proporciona `Describe` permisos para los recursos de Amazon ECR asociados a su cuenta. AWS
- Amazon Elastic Container Service (Amazon ECS): `Describe` proporciona permisos para los recursos de Amazon ECS asociados AWS a su cuenta.
- Amazon Elastic File System (Amazon EFS): proporciona `Describe` permisos para los recursos de Amazon EFS asociados a su AWS cuenta.
- Amazon Elastic Kubernetes Service (Amazon EKS): enumera y proporciona permisos de `Describe` para los recursos de Amazon EKS asociados a su cuenta de AWS .
- Auto Scaling de Amazon EC2: muestra y proporciona `Describe` permisos para los recursos de Auto Scaling de Amazon EC2 asociados AWS a su cuenta.
- Amazon EC2 Systems Manager (SSM): `Describe` proporciona permisos para los recursos de SSM asociados a su cuenta. AWS
- 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 (Amazon FSx): muestra los recursos de Amazon FSx asociados a su cuenta y proporciona `Describe` permisos para ellos. AWS
- Amazon RDS: muestra los recursos de Amazon RDS asociados a su AWS cuenta y proporciona `Describe` permisos para ellos.
- Amazon Route 53 (Route 53): enumera y proporciona permisos de `Describe` para los recursos de Route 53 asociados a su cuenta de AWS .
- Amazon Route 53 Resolver — Enumera los Amazon Route 53 Resolver recursos asociados a su AWS cuenta y proporciona `Describe` permisos para ellos.
- Amazon Simple Notification Service (Amazon SNS): enumera y proporciona permisos de `Describe` para los recursos de Amazon SNS asociados a su cuenta de AWS .
- Amazon Simple Queue Service (Amazon SQS): enumera y proporciona permisos de `Describe` para los recursos de Amazon SQS asociados a su cuenta de AWS .

- Amazon Simple Storage Service (Amazon S3): enumera y proporciona permisos de `Describe` para los recursos de Amazon S3 asociados a su cuenta de AWS .

> **Note**
>
> Al ejecutar una evaluación, si falta algún permiso que deba actualizarse desde las políticas gestionadas, AWS Resilience Hub completará correctamente la evaluación con s3: GetBucketLogging permission. Sin embargo, AWS Resilience Hub mostrará un mensaje de advertencia con una lista de los permisos faltantes y proporcionará un período de gracia para añadirlos. Si no agrega los permisos que faltan dentro del período de gracia especificado, la evaluación fallará.

- AWS Backup — Muestra y obtiene `Describe` los permisos para los recursos de Auto Scaling de Amazon EC2 asociados a su AWS cuenta.
- AWS CloudFormation — Enumera los recursos de las AWS CloudFormation pilas asociadas a su AWS cuenta y obtiene los `Describe` permisos correspondientes.
- AWS DataSync — Muestra los AWS DataSync recursos asociados a tu AWS cuenta y proporciona `Describe` permisos para ellos.
- AWS Directory Service — Enumera los AWS Directory Service recursos que están asociados a su AWS cuenta y proporciona `Describe` permisos para ellos.
- AWS Elastic Disaster Recovery (Elastic Disaster Recovery): proporciona `Describe` permisos para los recursos de Elastic Disaster Recovery asociados a su AWS cuenta.
- AWS Lambda (Lambda): muestra los recursos de Lambda asociados a su cuenta y proporciona `Describe` permisos para ellos. AWS
- 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 los SOP configurados para su aplicación.

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "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",
        "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:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "fis:GetExperimentTemplate",
        "fis:ListExperimentTemplates",
        "fis:ListExperiments",
        "fsx:DescribeFileSystems",
        "lambda:GetFunctionConcurrency",
        "lambda:GetFunctionConfiguration",
        "lambda:ListAliases",
        "lambda:ListVersionsByFunction",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
```

```
        "rds:DescribeDBInstances",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBSnapshots",
        "rds:DescribeGlobalClusters",
        "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:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetMultiRegionAccessPointRoutes",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "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": "*"
```

```
    },
    {
      "Effect": "Allow",
      "Action": [
        "apigateway:GET"
      ],
      "Resource": [
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/usageplans"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource": "arn:aws:s3:::aws-resilience-hub-artifacts-*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudwatch:PutMetricData"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "cloudwatch:namespace": "ResilienceHub"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:GetParametersByPath"
      ],
      "Resource": "arn:aws:ssm:*:*:parameter/ResilienceHub/*"
    }
  ]
}
```

AWS Resilience Hub actualizaciones de las políticas gestionadas AWS

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 a la fuente RSS de la página del historial del AWS Resilience Hub documento.

Cambio	Descripción	Fecha
AWSResilienceHubAssessmentExecutionPolicy— AWS Resilience Hub amplía la compatibilidad con Amazon FSx for Windows File Server.	Esta AWS Resilience Hub política le permite leer la configuración de Amazon FSx for Windows File Server.	26 de marzo de 2024
AWSResilienceHubAssessmentExecutionPolicy— AWS Resilience Hub amplía el soporte para. AWS Step Functions	Esta AWS Resilience Hub política le permite leer la AWS Step Functions configuración.	30 de octubre de 2023
AWSResilienceHubAssessmentExecutionPolicy: AWS Resilience Hub mejora el soporte para Amazon Relational Database Service (Amazon RDS).	Esta AWS Resilience Hub política le permite acceder a los recursos de Amazon RDS mientras ejecuta las evaluaciones.	5 de octubre de 2023
AWSResilienceHubAssessmentExecutionPolicy: política nueva	Esta AWS Resilience Hub política proporciona acceso a otros AWS servicios para ejecutar las 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

Importando el archivo de estado de Terraform a AWS Resilience Hub

AWS Resilience Hub admite la importación de archivos de estado de Terraform cifrados mediante cifrado del lado del servidor (SSE) con claves administradas de Amazon Simple Storage Service (SSE-S3) o con claves AWS Key Management Service administradas (SSE-KMS). Si sus archivos de estado de Terraform están cifrados con claves de cifrado proporcionadas por el cliente (SSE-C), no podrá importarlos mediante AWS Resilience Hub.

La importación de archivos de estado de Terraform a archivos de estado AWS Resilience Hub requiere las siguientes políticas de IAM, según la ubicación del archivo de estado.

Importar archivos de estado de Terraform desde un bucket de Amazon S3 ubicado en la cuenta principal

Se requieren las siguientes políticas de bucket de Amazon S3 y de IAM para permitir a AWS Resilience Hub el acceso de solo lectura a los archivos de estado de Terraform ubicados en un bucket de Amazon S3 de la cuenta principal.

- Política de bucket: política de bucket en el bucket de Amazon S3 de destino, que se encuentra en la cuenta principal. Para obtener más información, consulte el siguiente ejemplo.

```
{
  "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 a la función de invocador definida para esta aplicación o a la función de IAM AWS actual de AWS Resilience Hub la cuenta principal. AWS Para obtener más información, consulte el siguiente ejemplo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<s3-bucket-name>/<path-to-state-file>"
    },
    {
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<s3-bucket-name>"
    }
  ]
}
```

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

> **Note**
>
> Si sus archivos de estado de Terraform están cifrados mediante KMS, debe añadir el siguiente permiso de `kms:Decrypt`.

```
{
      "Effect": "Allow",
      "Action": [
              "kms:Decrypt",
      ],
```

```
      "Resource": "<arn_of_kms_key>"
}
```

Importar archivos de estado de Terraform desde un bucket de Amazon S3 ubicado en una cuenta secundaria

- Política de bucket: política de bucket en el bucket de Amazon S3 de destino, que se encuentra en una de las cuentas secundarias. Para obtener más información, consulte el siguiente ejemplo.

```
 {
  "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 cuenta principal AWS . 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 mediante KMS, debe añadir el siguiente permiso de `kms:Decrypt`.

```
{
      "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 (Amazon EKS) mediante el análisis de la infraestructura de su clúster de Amazon EKS. AWS Resilience Hub utiliza la configuración de control de acceso basado en roles (RBAC) de Kubernetes para evaluar otras cargas de trabajo de Kubernetes (K8), que se implementan como parte del clúster de Amazon EKS. AWS Resilience Hub Para consultar su clúster de Amazon EKS para analizar y evaluar la carga de trabajo, debe completar lo siguiente:

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

El acceso al clúster Amazon EKS mediante las entidades de AWS IAM está habilitado por el Autenticador de IAM para Kubernetes, que se ejecuta en el plano de control de Amazon EKS. El autenticador obtiene la información de la configuración de `aws-auth ConfigMap`.

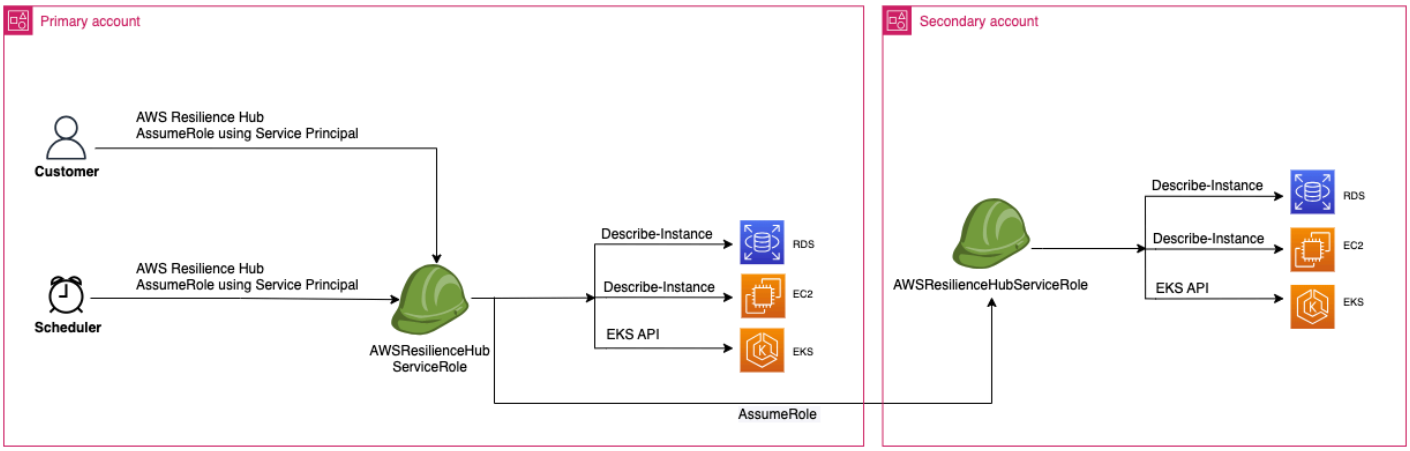
> **Note**
>
> - Para obtener más información sobre todos los `aws-auth ConfigMap` ajustes, consulte Formato de configuración completo en GitHub.
> - Para obtener más información acerca de las diferentes identidades de IAM, consulte Identidades (usuarios, grupos y roles) en la Guía del usuario de IAM.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

AWS Resilience Hub consulta los recursos de su clúster de Amazon EKS mediante un rol de IAM en su cuenta. Para acceder AWS Resilience Hub a los recursos de su clúster de Amazon EKS, la función de IAM utilizada por AWS Resilience Hub debe asignarse a un grupo de Kubernetes con suficientes permisos de solo lectura para los recursos de su clúster de Amazon EKS.

AWS Resilience Hub permite acceder a los recursos de su clúster de Amazon EKS mediante una de las siguientes opciones de rol de IAM:

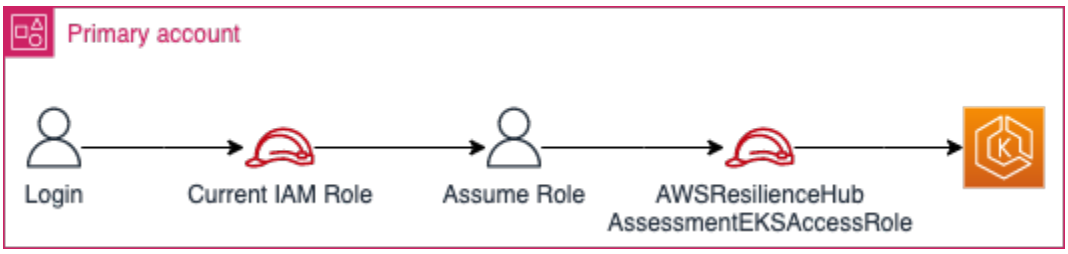
- Si su aplicación está configurada para utilizar el acceso basado en roles para acceder a los recursos, el rol de invocador o el rol de cuenta secundaria transferido a AWS Resilience Hub al crear una aplicación se utilizarán para acceder a su clúster de Amazon EKS durante la evaluación.

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

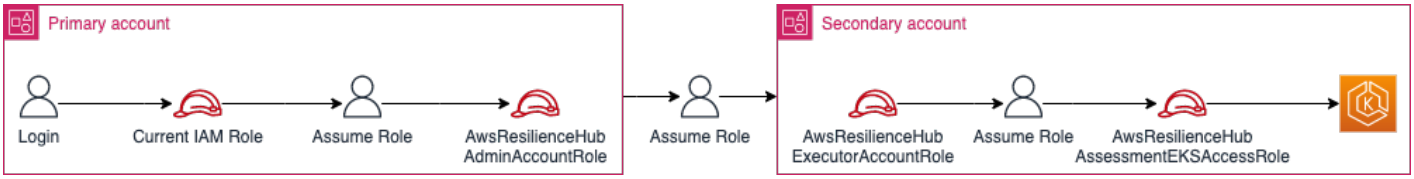


- Si su aplicación está configurada para utilizar el usuario de IAM actual para acceder al recurso, debe crear un nuevo rol de IAM con el nombre `AwsResilienceHubAssessmentEKSAccessRole` en la misma cuenta que el del clúster de Amazon EKS. Este rol de IAM se utilizará entonces para acceder a su clúster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

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



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



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

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

Para conceder los permisos necesarios AWS Resilience Hub para descubrir y evaluar los recursos del clúster Amazon EKS

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

   Si ha configurado la aplicación mediante el acceso basado en roles, puede omitir este paso y continuar con el paso 2 y usar el rol que utilizó para crear la aplicación. Para obtener más información acerca de cómo AWS Resilience Hub utiliza roles de IAM, consulte the section called “Cómo funciona AWS Resilience Hub con IAM”.

   Si ha configurado la aplicación con los permisos de usuario de IAM actuales, debe crear el rol de IAM `AwsResilienceHubAssessmentEKSAccessRole` en la misma cuenta que la del clúster de Amazon EKS. Este rol de IAM se utilizará entonces al acceder a su clúster de Amazon EKS.

   Al importar y evaluar su aplicación, AWS Resilience Hub utiliza una función de IAM para acceder a los recursos de su clúster de Amazon EKS. Esta función debe crearse en la misma cuenta que su clúster de Amazon EKS y se asignará a un grupo de Kubernetes que incluya los permisos necesarios AWS Resilience Hub para evaluar su clúster de Amazon EKS.

   Si su clúster de Amazon EKS está en la misma cuenta que la cuenta de AWS Resilience Hub llamada, el rol debe crearse mediante la siguiente política de confianza de IAM. En esta política de confianza de IAM, `caller_IAM_role` se utiliza en la cuenta corriente para solicitar las API. AWS Resilience Hub

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

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

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

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

```
{
  "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` (o`RoleBinding`) roles para la AWS Resilience Hub aplicación.

   Creando `ClusterRole` y `ClusterRoleBinding` concediendo los permisos de solo lectura necesarios AWS Resilience Hub para analizar y evaluar los recursos que forman parte de determinados espacios de nombres de su clúster de Amazon EKS.

   AWS Resilience Hub le permite limitar su acceso a sus espacios de nombres para generar evaluaciones de resiliencia realizando una de las siguientes acciones:

   a. Conceder a la aplicación de AWS Resilience Hub acceso de lectura a todos los espacios de nombres.

      AWS Resilience Hub Para evaluar la resiliencia de los recursos en todos los espacios de nombres de un clúster de Amazon EKS, debe crear los siguientes y. `ClusterRole` `ClusterRoleBinding`

      - `resilience-hub-eks-access-cluster-role`(`ClusterRole`): define los permisos necesarios AWS Resilience Hub para evaluar su clúster de Amazon EKS.
      - `resilience-hub-eks-access-cluster-role-binding` (`ClusterRoleBinding`): define un grupo denominado `resilience-hub-eks-access-group` en su clúster de Amazon EKS que concede a sus usuarios los permisos necesarios para ejecutar evaluaciones de resiliencia en AWS Resilience Hub.

      La plantilla para conceder a la aplicación de AWS Resilience Hub acceso de lectura en todos los espacios de nombres es la siguiente:

```
cat << EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: resilience-hub-eks-access-cluster-role
rules:
- apiGroups:
```

```
    - ""
  resources:
    - pods
    - replicationcontrollers
    - nodes
  verbs:
    - get
    - list
- apiGroups:
    - apps
  resources:
    - deployments
    - replicasets
  verbs:
    - get
    - list
- apiGroups:
    - policy
  resources:
    - poddisruptionbudgets
  verbs:
    - get
    - list
- apiGroups:
    - autoscaling.k8s.io
  resources:
    - verticalpodautoscalers
  verbs:
    - get
    - list
- apiGroups:
    - autoscaling
  resources:
    - horizontalpodautoscalers
  verbs:
    - get
    - list
- apiGroups:
    - karpenter.sh
  resources:
    - provisioners
  verbs:
    - get
    - list
```

```
- apiGroups:
    - karpenter.k8s.aws
  resources:
    - awsnodetemplates
  verbs:
    - get
    - list
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: resilience-hub-eks-access-cluster-role-binding
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-cluster-role
  apiGroup: rbac.authorization.k8s.io
---
EOF
```

b. AWS Resilience Hub Otorga el acceso para leer espacios de nombres específicos.

Puede limitar el acceso AWS Resilience Hub a los recursos dentro de un conjunto específico de espacios de nombres utilizando. `RoleBinding` Para ello, debe crear los siguientes roles:

- `ClusterRole`— Para acceder AWS Resilience Hub a los recursos en espacios de nombres específicos dentro de un clúster de Amazon EKS y evaluar su resiliencia, debe crear las siguientes funciones. `ClusterRole`
  - `resilience-hub-eks-access-cluster-role`: especifica los permisos necesarios para evaluar los recursos dentro de espacios de nombres específicos.
  - `resilience-hub-eks-access-global-cluster-role`— Especifica los permisos necesarios para evaluar los recursos con ámbito de clúster, que no están asociados a un espacio de nombres específico, dentro de sus clústeres de Amazon EKS. AWS Resilience Hub requiere permisos para acceder a los recursos del ámbito del clúster (como los nodos) de su clúster de Amazon EKS a fin de evaluar la resiliencia de la aplicación.

La plantilla para crear el rol de `ClusterRole` es la siguiente:

```
cat << EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: resilience-hub-eks-access-cluster-role
rules:
  - apiGroups:
      - ""
    resources:
      - pods
      - replicationcontrollers
    verbs:
      - get
      - list
  - apiGroups:
      - apps
    resources:
      - deployments
      - replicasets
    verbs:
      - get
      - list
  - apiGroups:
      - policy
    resources:
      - poddisruptionbudgets
    verbs:
      - get
      - list
  - apiGroups:
      - autoscaling.k8s.io
    resources:
      - verticalpodautoscalers
    verbs:
      - get
      - list
  - apiGroups:
      - autoscaling
    resources:
      - horizontalpodautoscalers
```

```
    verbs:
      - get
      - list

---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: resilience-hub-eks-access-global-cluster-role
rules:
  - apiGroups:
      - ""
    resources:
      - nodes
    verbs:
      - get
      - list
  - apiGroups:
      - karpenter.sh
    resources:
      - provisioners
    verbs:
      - get
      - list
  - apiGroups:
      - karpenter.k8s.aws
    resources:
      - awsnodetemplates
    verbs:
      - get
      - list

---
EOF
```

- `RoleBinding`rol: este rol otorga los permisos necesarios para acceder AWS Resilience Hub a los recursos dentro de espacios de nombres específicos. Es decir, debes crear un `RoleBinding` rol en cada espacio de nombres para poder acceder AWS Resilience Hub a los recursos dentro del espacio de nombres determinado.

> **Note**
>
> Si utiliza `ClusterAutoscaler` para el ajuste de escala automático, también debe crear `RoleBinding` en el `kube-system`. Esto es necesario para evaluar su `ClusterAutoscaler`, que forma parte del espacio de nombres de `kube-system`.
> De este modo, concederá AWS Resilience Hub los permisos necesarios para evaluar los recursos dentro del espacio de `kube-system` nombres mientras evalúa su clúster de Amazon EKS.

La plantilla para crear el rol de `RoleBinding` es la siguiente:

```
cat << EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: resilience-hub-eks-access-cluster-role-binding
  namespace: <namespace>
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-cluster-role
  apiGroup: rbac.authorization.k8s.io

---
EOF
```

- `ClusterRoleBinding`rol: este rol otorga los permisos necesarios para acceder AWS Resilience Hub a los recursos del ámbito del clúster.

  La plantilla para crear el rol de `ClusterRoleBinding` es la siguiente:

```
cat << EOF | kubectl apply -f -
```

```
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: resilience-hub-eks-access-global-cluster-role-binding
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-global-cluster-role
  apiGroup: rbac.authorization.k8s.io

---
EOF
```

3. Actualice `aws-auth ConfigMap` para asignar el `resilience-hub-eks-access-group` al rol de IAM utilizado para acceder al clúster de Amazon EKS.

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

   > **Note**
   >
   > - `ROLE-NAME` hace referencia al rol de IAM que se utiliza para acceder al clúster de Amazon EKS.
   >   - Si la aplicación está configurada para usar el acceso basado en roles, el rol debe ser el rol de invocador o el rol de cuenta secundaria al que se transfiere al crear la aplicación. AWS Resilience Hub
   >   - Si su aplicación está configurada para utilizar el usuario de IAM actual para acceder a los recursos, debe ser el de `AwsResilienceHubAssessmentEKSAccessRole`.
   > - `ACCOUNT-ID`debe ser el ID de AWS cuenta del clúster de Amazon EKS.

   Puede crear el `aws-auth ConfigMap` utilizando una de las siguientes maneras:

- Uso de `eksctl`

  Use el siguiente comando para actualizar el `aws-auth ConfigMap`:

  ```
  eksctl create iamidentitymapping \
   --cluster <cluster-name> \
   --region=<region-code> \
   --arn arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>\
   --group resilience-hub-eks-access-group \
   --username AwsResilienceHubAssessmentEKSAccessRole
  ```

- Puede editar manualmente `aws-auth ConfigMap` añadiendo los datos del rol de IAM a la sección `mapRoles` de los datos secundarios de `ConfigMap`. Utilice el siguiente comando para editar el archivo `aws-auth ConfigMap`.

  ```
  kubectl edit -n kube-system configmap/aws-auth
  ```

  La sección `mapRoles` consta de los siguientes parámetros:

  - `rolearn`: el nombre de recurso de Amazon (ARN) del rol de IAM que se agregará.
    - Sintaxis del ARN: `arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>`.
  - `username`: nombre del usuario de Kubernetes al que se mapea el rol de IAM (`AwsResilienceHubAssessmentEKSAccessRole`).
  - `groups`: los nombres de los grupos deben coincidir con los nombres de los grupos creados en el Paso 2 (`resilience-hub-eks-access-group`).

  > **Note**
  >
  > Si la sección `mapRoles` no existe, debe añadirla manualmente.

  Utilice la siguiente plantilla para añadir la información del rol de IAM a la sección `mapRoles` de los datos secundarios de `ConfigMap`.

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

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 del Amazon Simple Notification Service (Amazon SNS). Para enviar notificaciones a un tema de Amazon SNS, asegúrese de tener lo siguiente:

- Una AWS Resilience Hub aplicación activa.
- Un tema de Amazon SNS existente al que se AWS Resilience Hub deben enviar notificaciones. Para obtener más información sobre la creación de un tema de Amazon SNS, consulte Creación de un tema de Amazon SNS.

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

```
{
  "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 AWS Resilience Hub mensajes de regiones con suscripción voluntaria en temas ubicados en regiones que están habilitadas de forma predeterminada, debes modificar la política de recursos creada para el tema de Amazon SNS. Cambie el valor de la entidad principal de `resiliencehub.amazonaws.com` a `resiliencehub.<opt-in-region>.amazonaws.com`.

Si utiliza un tema de Amazon SNS cifrado del servidor (SSE), debe asegurarse de que AWS Resilience Hub tiene el acceso `Decrypt` y `GenerateDataKey*` a la clave de cifrado de Amazon SNS.

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

```
{
  "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 confianza de IAM. En esta política de confianza de IAM, `caller_IAM_role` (asociada a su cuenta de AWS usuario) se utiliza en la cuenta corriente para AWS Resilience Hub solicitar las API.

```
{
  "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 red AWS global que se describen en el documento técnico Amazon Web Services: Overview of Security Processes.

Utiliza las llamadas a la API AWS publicadas para acceder a AWS Resilience Hub través de la red. Los clientes deben ser compatibles con Transport Layer Security (TLS) 1.2 o una versión posterior. Recomendamos TLS 1.3 o una versión posterior. Los clientes también deben ser compatibles con conjuntos de cifrado con confidencialidad directa total (PFS) tales como Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

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 a AWS Resilience Hub qué dirección IP 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 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 la carga de trabajo estimada (RTO) y la carga de trabajo estimada (RPO) 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 actualizar la detección

de la desviación de resiliencia del procedimiento de solicitud y active la casilla de verificación Evaluar automáticamente esta solicitud a diario).

- 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 aplicación AWS Resilience Hub a diario en su nombre, puede activarla marcando la casilla de verificación Evaluar automáticamente esta aplicación a diario en la detección de desviaciones de AWS Resilience Hub resiliencia. Para seleccionar la casilla de verificación Evaluar automáticamente esta solicitud a diario, complete la casilla Para actualizar la detección de desviaciones de resiliencia de su procedimiento de solicitud. ???

  > **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 Supportusuario.

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

- Versión de la API: la más reciente
- Última actualización de la documentación: 28 de marzo de 2024

Cambio	Descripción	Fecha
AWS Trusted Advisor mejoras	AWS Resilience Hub ha ampliado la compatibilidad con la adición AWS Trusted Advisor de una comprobación para identificar los componentes de la aplicación irrecuperables (). AppComponents Para obtener más información, 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. Para obtener más información, consulte the section called “Administración de alarmas”.	26 de marzo de 2024

AWS Resilience Hub amplía la compatibilidad con Amazon FSx for Windows File Server	AWS Resilience Hub amplía el soporte de evaluación de los recursos de Amazon FSx for Windows File Server y, al mismo tiempo, evalúa la resiliencia de la aplicación. Para las aplicaciones que utilizan Amazon FSx for Windows File Server AWS Resilience Hub , proporcio na un nuevo conjunto de recomendaciones de resilienc ia, que abarca las implement aciones en zonas de disponibi lidad (AZ) y Multi-AZ y los planes de respaldo, así como la replicación de datos. AWS Resilience Hub es compatibl e 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. Para obtener más información, consulte los temas siguientes: • the section called “ AWS Resilience Hub Recursos compatibles” • the section called “AWSResilienceHubA sssessmentExecutionPolicy”	26 de marzo de 2024

	• the section called “Agrupar recursos en un AppComponent”	
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. Para obtener más información, consulte the section called “Comprender las puntuaciones de resiliencia”.	9 de noviembre de 2023
AWS Resilience Hub amplía el soporte para aplicaciones que incluyen recursos de Amazon Elastic Kubernetes Service (Amazon EKS)	AWS Resilience Hub amplía el soporte para las aplicaciones que incluyen recursos de Amazon EKS para incluir nuevas recomendaciones operativas. Mientras realizamos una evaluación que incluye recursos de los clústeres de Amazon EKS, ahora recomendaremos que se ejecuten pruebas y alarmas para ayudar a mejorar la resiliencia de las aplicaciones. Para obtener más información, consulte the section called “Experimentos del Servicio de inyección de errores de Amazon”.	9 de noviembre de 2023

AWS Resilience Hub proporciona información adicional a nivel de aplicación	AWS Resilience Hub proporciona información adicional a nivel de aplicación sobre el RTO de la carga de trabajo estimada y el RPO de la carga de trabajo estimada. Esta información adicional indica el máximo RTO de carga de trabajo estimado posible y el RPO de carga de trabajo estimado de su aplicación a partir de la última evaluación exitosa. Este valor es el RTO máximo estimado de la carga de trabajo y el RPO estimado de la carga de trabajo de todos los tipos de interrupciones. Para obtener más información, consulte the section called “Aplicaciones”.	30 de octubre de 2023

AWS Resilience Hub amplía el soporte de evaluación de los recursos AWS Step Functions	AWS Resilience Hub amplía el soporte de evaluación de los AWS Step Functions recursos y, al mismo tiempo, evalúa la resiliencia de su aplicación. AWS Resilienc e Hub analiza la AWS Step Functions configuración, incluido el tipo de máquina de estado (flujos de trabajo estándar o exprés). Además, también AWS Resilience Hub proporcionará recomenda ciones que le ayudarán a cumplir los objetivos de tiempo de recuperación (RTO) estimados de la carga de trabajo y los objetivos de punto de recuperación (RPO) estimados de la carga de trabajo. Para evaluar las aplicaciones, incluidos AWS Step Functions los recursos, debe configurar los permisos necesarios, ya sea mediante una política AWS administrada o añadiendo manualmente el permiso específico para poder leer la AWS Step Functions configuración. AWS Resilienc e Hub 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 (SOP) 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, los SOP y AWS FIS las pruebas recomendadas que no sean relevantes para ellos. El flujo de trabajo de exclusión es beneficioso si utiliza una plataforma distinta a la sugerida o si ya ha implementado la recomendación con un método alternativo. Para obtener más información, consulte los temas siguientes: • the section called “Incluir o excluir recomendaciones operativas” • the section called “Limitar los permisos para incluir o	9 de agosto de 2023

	excluir recomendaciones de AWS Resilience Hub ”	
Mejorar el diseño de los permisos para AWS Resilience Hub	AWS Resilience Hub presenta un nuevo diseño de permisos para brindar flexibilidad a la hora de configurar las funciones AWS Identity and Access Management (IAM) 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. 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 (Amazon SNS) reciba notificaciones cuando el objetivo de tiempo de recuperación (RTO) de la carga de trabajo o el objetivo de punto de recuperación (RPO) de la carga de trabajo estimado hayan pasado de cumplir el objetivo a dejar de cumplir los objetivos empresariales de la organización. Pasar de detectar problemas de resiliencia de forma reactiva al ejecutar una evaluación de forma manual a recibir notificaciones proactivas a través de los temas de Amazon SNS le permitirá anticipar las posibles interrupciones con antelación y le proporcionará una mayor confianza en el logro de los objetivos de recuperación. Para obtener más información, consulte los temas siguientes: • the section called “Paso 5: Configurar la detección de desviaciones de resiliencia”	2 de agosto de 2023

- 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 Amazon RDS, ahora distinguiremos entre diferentes motores de bases de datos para proporcionar una estimación más precisa de los objetivos de tiempo de recuperación de la carga de trabajo (RTO). AWS Resilienc e Hub también proporcio naremos acciones adicionales para implementar las mejores prácticas de resiliencia en su AWS entorno. Las prácticas recomendadas pueden incluir información sobre el rendimien to con DevOps Guru para Amazon RDS, una supervisi ón mejorada y una automatiz ación de la implementación azul/verde en los motores de bases de datos compatibles. 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 (Amazon EBS) para reconocer las instantáneas de Amazon EBS, que se toman dentro de la misma región de Amazon EBS mediante API directas. El soporte ampliado se suma al soporte actual para los clientes que utilizan Amazon Data Lifecycle Manager (Amazon Data Lifecycle Manager) o AWS Backup. Para obtener más información, consulte Amazon Elastic Block Store (Amazon EBS).	2 de agosto de 2023

Mejoras de Amazon Elastic Compute Cloud	AWS Resilience Hub ha ampliado el soporte para Amazon Elastic Compute Cloud (Amazon EC2). Para aplicaciones de diferentes tamaños, AWS permite a sus clientes que utilizan Amazon EC2 seleccionar la configura ción adecuada para su caso de uso. AWS Resilience Hub admite la evaluación de las siguientes configuraciones de Amazon EC2: • Instancias bajo demanda. • Copia de seguridad de las instancias de forma AWS Backup automática. AWS Elastic Disaster Recovery • Soporte para grupos de escalado automático con el controlador de recuperación de aplicaciones de Amazon Route 53 (Route 53 ARC) A partir de ahora, el soporte de evaluación se ampliará para incluir instancias de spot, hosts dedicados, instancia s dedicadas, grupos de ubicación y flotas. Para obtener más informaci ón, consulte the section called “AWS Resilience Hub	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. 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 (de IAM) del rol que está utilizando. Para obtener más informaci ón, consulte the section called “AWS Resilience Hub referencia de permisos de acceso”.	2 de mayo de 2023

AWS Trusted Advisor mejoras	AWS Resilience Hub ha ampliado el soporte 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. 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), el control de versiones y el respaldo entre regiones (Amazon S3 CRR) y Amazon S3 en la misma región (SRR), el control de versiones y el AWS respaldo, ahora AWS Resilience Hub evaluará Amazon S3 para la configura ción de puntos de acceso multirregionales, control del tiempo de replicación de Amazon S3 (Amazon S3 RTC) y recuperación de copias de seguridad (PITR). AWS point-in-time Para obtener más información, consulte los temas siguientes: • the section called “AWS Resilience Hub referencia de permisos de acceso” • Gestionar el almacenam iento de Amazon S3	21 de marzo de 2023

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

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

Soporte para orígenes de entrada de aplicaciones	AWS Resilience Hub ahora 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. Para obtener más informaci ón, consulte the section called “Edición de recursos de aplicaciones”.	21 de febrero de 2023

Soporte para los parámetros de configuración de la aplicación	AWS Resilience Hub ahora proporciona un mecanismo de entrada para recopilar información adicional sobre los recursos asociados a sus aplicaciones. Con esta información, AWS Resilience Hub obtendrá una comprensión más profunda de sus recursos y proporcionará mejores recomendaciones de resiliencia. Para obtener más información, consulte los temas siguientes: • the section called “Parámetros de configuración de la aplicación” • the section called “Paso 7: configurar los parámetros de configuración de la aplicación” • the section called “Actualizar los parámetros de configuración de la aplicación”	21 de febrero de 2023

Soporte adicional para Amazon Elastic Block Store	Además de la compatibilidad actual con los volúmenes de Amazon Elastic Block Store (Amazon EBS) AWS Resilienc e Hub , ahora evaluará las instantáneas de Amazon EBS mediante Amazon Data Lifecycle Manager y Amazon EBS Fast Snapshot Restore (FSR). Para obtener más información, consulte los temas siguientes: • the section called “AWS Resilience Hub referencia de permisos de acceso” • Amazon Elastic Block Store (Amazon EBS)	21 de febrero de 2023

Integración con AWS Trusted Advisor	AWS Trusted Advisor los usuarios podrán ver las aplicaciones asociadas a su cuenta que hayan sido evaluadas por AWS Resilienc e Hub. AWS Trusted Advisor muestra la puntuación de resiliencia más reciente y proporciona un estado que indica si se ha cumplido o no la política de resilienc ia prevista (RTO y RPO). 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. Para obtener más informaci ón, consulte the section called “AWS Trusted Advisor”.	18 de noviembre de 2022

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

Soporte adicional para Amazon Route 53 Application Recovery Controller (Amazon Route 53 ARC)	AWS Resilience Hub ahora evalúa Amazon Route 53 ARC para Elastic Load Balancing y Amazon Relational Database Service (Amazon RDS), que incluye información sobre cuándo sería beneficioso Amazon Route 53 ARC. Ampliando AWS Resilience Hub el soporte de evaluació n de Amazon Route 53 ARC más allá de AWS Auto Scaling Group (AWS ASG) y Amazon DynamoDB. Amazon Route 53 ARC proporciona 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. Para obtener más información, consulte los temas siguientes: • the section called “ AWS Resilience Hub Recursos compatibles” • 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 (Amazon RDS), que incluye información sobre cuándo sería beneficioso Amazon Route 53 ARC. Ampliando AWS Resilience Hub el soporte de evaluació n de Amazon Route 53 ARC más allá de AWS Auto Scaling Group (AWS ASG) y Amazon DynamoDB. Amazon Route 53 ARC proporciona 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. Para obtener más información, consulte los temas siguientes: • the section called “ AWS Resilience Hub Recursos compatibles” • 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.