aws

Guía del usuario

AWS Migration Hub Refactories

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Migration Hub Refactories: Guía del usuario

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas comerciales que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es AWS Migration Hub Refactor Spaces? 1
¿Es la primera vez que usa Refactor Spaces? 1
Pricing 2
Conceptos 2
Environment 2
Applications 3
Services 3
Route 3
Cómo funciona 3
Configuración 5
Registrarse en AWS 5
Crear usuarios de IAM 5
Creación de un usuario administrativo de IAM 6
Creación de un usuario no administrativo de IAM 6
Introducción 8
Prerequisites 8
Paso 1: Creación de un entorno 8
Paso 2: Cree una aplicación 9
Paso 3: Comparta su entorno 10
Paso 4: Crear un servicio 11
Paso 5: Creación de una ruta 12
Seguridad 14
Protección de los datos 15
Cifrado en reposo 16
Cifrado en tránsito 16
Identity and Access Management 16
Audience 16
Autenticación con identidades 17
Administración de acceso mediante políticas 20
Cómo funciona AWS Migration Hub Refactor Spaces con IAM 23
Políticas administradas por AWS 30
Ejemplos de políticas basadas en identidades 41
Solución de problemas 43
Uso de roles vinculados a servicios 46

Validación de conformidad 55
Trabajar con otros servicios de 57
Recursos de AWS CloudFormation 57
Plantillas de espacios de refactor y CloudFormation 57
Más información sobre CloudFormation 60
Registros de CloudTrail 60
Refactorizar la información de los espacios de CloudTrail 60
Descripción de las entradas de archivos de registro de Refactor de 61
Uso compartido de entornos medianteAWS RAM 62
Cuotas 63
Historial de documentos 64
..... lxv

¿Qué es AWS Migration Hub Refactor Spaces?

AWS Migration Hub Refactor Spaces se encuentra en la versión preliminar y está sujeta a cambios.

AWS Migration Hub Refactor Spaces es el punto de partida para la refactorización incremental de aplicaciones a microservicios enAWS. Refactor Spaces ayuda a reducir el levantamiento pesado indiferenciado de la construcción y la operaciónAWSinfraestructura para refactorización incremental. Puede utilizar Refactor Spaces para ayudar a reducir el riesgo al convertir aplicaciones en microservicios o ampliar las aplicaciones existentes con nuevas funciones escritas en microservicios.

El entorno de Refactor Spaces simplifica las redes entre cuentas mediante la orquestaciónAWS Transit Gateway,AWS Resource Access Managery las nubes privadas virtuales (VPC). Refactor Spaces une las redes a través deAWScuentas para permitir la comunicación de servicios anteriores y nuevos, manteniendo la independencia de los servicios separadosCuentas de AWS.

Refactor Spaces proporciona una aplicación que modela el patrón Strangler Fig para la refactorización incremental. Una aplicación Refactor Spaces orquesta Amazon API Gateway, Network Load Balancer y basada en recursosAWS Identity and Access Management(IAM) para que pueda agregar nuevos servicios de forma transparente a un extremo HTTP externo. También puede enrutar el tráfico de forma incremental a los nuevos servicios. Esto mantiene transparentes los cambios de arquitectura subyacentes para los consumidores de aplicaciones. Para obtener más información sobre el patrón Strangler Fig, consulte.Aplicación Strangler Fig.

Temas

- ¿Es la primera vez que usa Refactor Spaces?
- Pricing
- Conceptos de Refactor Spaces
- Cómo funciona Refactor Spaces

¿Es la primera vez que usa Refactor Spaces?

Si es la primera vez que usa Refactor Spaces, le recomendamos que empiece leyendo las siguientes secciones:

- Conceptos de Refactor Spaces
- Cómo funciona Refactor Spaces
- Configuración
- Introducción a Refactor Spaces

Pricing

Todos los recursos orquestados de Refactor Spaces (por ejemplo, Transit Gateway) se aprovisionan en suCuenta de AWS. Por lo tanto, paga por el uso de Refactor Spaces más los costes asociados con los recursos aprovisionados. Para obtener más información, consulteAWSMigration Hub.

> **Note**
>
> No se cobra ningún cargo por Refactor Spaces durante su período de vista previa.

Conceptos de Refactor Spaces

En esta sección se describen los componentes clave que puede crear y administrar al utilizar AWS Migration Hub Refactor Spaces.

Temas

- Environment
- Applications
- Services
- Route

Environment

El entorno de Refactor Spaces proporciona una vista unificada de redes, aplicaciones y servicios en variosAWScuentas.

Un entorno de Refactor Spaces contiene aplicaciones y servicios de Refactor Spaces. Es un tejido de red de varias cuentas que consiste en nubes privadas virtuales (VPC) conectadas en puente, que permite que los recursos de su interior interactúen a través de direcciones IP privadas. El entorno proporciona una vista unificada de redes, aplicaciones y servicios en variosCuentas de AWS.

LaEnvironment owneres la cuenta en la que se crea el entorno Refactor Spaces. El propietario del entorno tiene visibilidad entre cuentas de las aplicaciones, los servicios y las rutas creadas en el entorno, independientemente de la cuenta que cree el recurso.

Applications

Una aplicación Refactor Spaces contiene servicios y rutas y proporciona un único extremo externo para exponer la aplicación a personas que llaman externas. La aplicación proporciona un proxy Strangler Fig para la refactorización incremental de aplicaciones. Para obtener más información sobre Strangler Fig, consulte.Aplicación Strangler Fig.

La aplicación Refactor Spaces modela el patrón Strangler Fig y organiza Amazon API Gateway, enlaces de VPC de API Gateway, Network Load Balancer y basado en recursosAWS Identity and Access Management(IAM) para que pueda agregar nuevos servicios de forma transparente al extremo HTTP de la aplicación. También aleja el tráfico de forma incremental de la aplicación existente a los nuevos servicios. Esto mantiene transparentes los cambios de arquitectura subyacente para el consumidor de aplicaciones.

Services

Los servicios de Refactor Spaces proporcionan las capacidades empresariales de su aplicación y se puede acceder a ellos a través de puntos finales únicos. Los endpoints de servicio son de dos tipos: una URL HTTP/HTTPS o unAWS Lambdafunción.

Route

Una ruta de espacios de refactor es una regla de coincidencia de proxy que reenvía una solicitud a un servicio. Cada solicitud se ejecuta en el conjunto de rutas configuradas en la aplicación. Si una regla coincide, la solicitud se envía al servicio de destino configurado para esa regla. Las aplicaciones tienen una ruta predeterminada que reenvía solicitudes a un servicio predeterminado si no coinciden con ninguna de las reglas. Las rutas se configuran en el proxy de Amazon API Gateway de la aplicación.

Cómo funciona Refactor Spaces

Al empezar a utilizar AWS Migration Hub Refactor Spaces, puede utilizar uno o variosCuentas de AWS. Puede utilizar una sola cuenta para realizar pruebas. Sin embargo, una vez que esté listo para comenzar a refactorizar, le recomendamos que empiece por las siguientes tres cuentas:

- Una cuenta para la aplicación existente.
- Una cuenta para el primer microservicio nuevo.
- Una cuenta para actuar como refactorpropietario del entorno, en el que Refactor Spaces configura las redes multicuentas y enruta el tráfico.

En primer lugar, crea un entorno de Refactor Spaces en la cuenta elegida como propietario del entorno. A continuación, comparte el entorno con las otras dos cuentas medianteAWS Resource Access Manager(la consola de Refactor Spaces se encaja por usted). Después de compartir el entorno con otra cuenta, Refactor Spaces comparte automáticamente los recursos que crea dentro del entorno con las demás cuentas. Lo hace orquestandoAWS Identity and Access Management(IAM) de las políticas basadas en recursos de.

El entorno de refactor proporciona redes unificadas en todas las cuentas mediante la organizaciónAWS Transit Gateway,AWS Resource Access Managery nubes privadas virtuales (VPC). El entorno de refactor contiene la aplicación existente y los nuevos microservicios. Después de crear un entorno de refactor, crea una aplicación Refactor Spaces dentro del entorno. La aplicación Refactor Spaces contiene servicios y rutas y proporciona un único punto final para exponer la aplicación a personas que llaman externas.

Una aplicación admite el enrutamiento a servicios que se ejecutan en contenedores, informática sin servidor y Amazon Elastic Compute Cloud (Amazon EC2) con visibilidad pública o privada. Los servicios de una aplicación pueden tener uno de los dos tipos de endpoint: una URL (HTTP y HTTPS) en una VPC o unAWS Lambdafunción. Una vez que una aplicación contiene un servicio, agrega una ruta predeterminada para dirigir todo el tráfico desde el proxy de la aplicación al servicio que representa la aplicación existente. A medida que se desarrolla o agrega nuevas capacidades en contenedores o informática sin servidor, agrega nuevos servicios y rutas para redirigir el tráfico a los nuevos servicios.

Para los servicios con puntos finales de URL en una VPC, Refactor Spaces utiliza Transit Gateway para unir automáticamente todas las VPC de servicio dentro del entorno. Esto significa que cualquierAWSlos recursos que lanza en una VPC de servicio pueden comunicarse directamente con todas las demás VPC de servicio agregadas al entorno. Puede aplicar restricciones de enrutamiento multicuenta adicionales mediante grupos de seguridad de VPC. Al crear rutas que apuntan a servicios con puntos finales de Lambda, Refactor Spaces orquesta la integración Lambda de Amazon API Gateway para llamar a la funciónCuentas de AWS.

Configuración

AWS Migration Hub Refactor Spaces está en la versión preliminar y está sujeta a cambios.

Antes de usar AWS Migration Hub Refactor Spaces por primera vez, realice las siguientes tareas:

Registrarse en AWS

Crear usuarios de IAM

Registrarse en AWS

En esta sección, se registrará en una cuenta de AWS. Si ya tiene una cuenta de AWS, omita este paso.

Al inscribirse en Amazon Web Services (AWS), suAWSLa cuenta de se inscribe automáticamente en todosAWSservicios, incluidos los espacios de refactor de AWS Migration Hub. Solo se le cobrará por los servicios que utilice.

Si no dispone de una Cuenta de AWS, siga los pasos que figuran a continuación para crear una.

Para registrarse en Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones en línea.

   Parte del procedimiento de inscripción consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

Crear usuarios de IAM

Al crear unAWS, obtiene una identidad de inicio de sesión único que tiene acceso completo a todos losAWSservicios y recursos de la cuenta. Esta identidad recibe el nombre en la cuenta de AWS de usuario raíz. Inicio de sesión en laConsola de administración de AWSSi utiliza la dirección de correo electrónico y la contraseña que utilizó para crear la cuenta, disponga de acceso completo a todos losAWSrecursos de su cuenta de.

Le recomendamos fehacientemente que no utilice el usuario raíz en sus tareas cotidianas, incluso las tareas administrativas. En su lugar, siga las prácticas recomendadas de seguridadCrear usuarios de IAM de individualesy crea unAWS Identity and Access Management(IAM) usuario administrador de. A continuación, guarde las credenciales del usuario raíz en un lugar seguro y utilíelas únicamente para algunas tareas de administración de cuentas y servicios.

Además de crear un usuario administrativo, también debe crear usuarios de IAM que no sean administrativos. En los temas siguientes se explica cómo crear ambos tipos de usuarios de IAM.

Temas

- Creación de un usuario administrativo de IAM
- Creación de un usuario no administrativo de IAM

Creación de un usuario administrativo de IAM

De forma predeterminada, una cuenta de administrador hereda la`AWSMigrationHubRefactorSpacesFullAccess`política administrada necesaria para acceder a AWS Migration Hub Refactor Spaces.

Para crear un usuario administrador

- Cree un usuario administrador en su cuenta de AWS. Para obtener instrucciones, consulteCreación del primer grupo de usuarios y administradores de IAMen laIAM User Guide.

Creación de un usuario no administrativo de IAM

Esta sección describe cómo conceder los permisos necesarios solicitados para usar Refactorizar espacios para un usuario no administrativo.

Antes de utilizar Refactor Spaces, cree un usuario con el`AWSMigrationHubRefactorSpacesFullAccess`política administrada y, a continuación, adjunta la política que otorga los permisos adicionales necesarios para utilizar Refactor Spaces al usuario. Esta política de permisos extra obligatoria se describe enPermisos adicionales necesarios para espacios de refactor.

Al crear usuarios de IAM no administrativos, siga las prácticas recomendadas de seguridadConceder privilegios mínimosy conceda a los usuarios permisos mínimos.

Para crear un usuario de IAM que no sea administrador que utilice con Refactor Spaces

1. EnConsola de administración de AWS, vaya a la consola de IAM.
2. Cree un usuario de IAM que no sea administrador siguiendo las instrucciones para crear un usuario con la consola, tal y como se describe enCreación de un usuario de IAM en laAWScuentaen laIAM User Guide.

   Siga las instrucciones que se detallan en laIAM User Guide:

   - Cuando estés en el paso de seleccionar el tipo de acceso, selecciona ambosAcceso programáticoyAWSAcceso a Management Console de.
   - Cuando esté en el escalón sobre elEstablecer permisopágina, elige la opción paraAdjuntar políticas existentes directamente al usuario. A continuación, seleccione la política de IAM administradaAcceso completo a los espacios del factor de migración de AWS.
   - Cuando esté en el paso sobre la visualización de las claves de acceso del usuario (ID de clave de acceso y claves de acceso secretas), siga las instrucciones que se detallan en laImportanteNota sobre cómo guardar el nuevo ID de clave de acceso del usuario y la clave de acceso secreta en un lugar seguro.
3. Después de crear el usuario, agregue la política de permisos adicional requerida al usuario siguiendo las instrucciones para insertar una política en línea para un usuario descritas enAdición de permisos de identidad de IAMen laIAM User Guide. Esta política de permisos extra obligatoria se describe enPermisos adicionales necesarios para espacios de refactor.

Introducción a Refactor Spaces

AWS Migration Hub Refactor Spaces está en la versión preliminar y está sujeta a cambios.

En esta sección se describe cómo comenzar a utilizar los espacios de refactor de AWS Migration Hub

Temas

- Prerequisites
- Paso 1: Creación de un entorno
- Paso 2: Cree una aplicación
- Paso 3: Comparta su entorno
- Paso 4: Crear un servicio
- Paso 5: Creación de una ruta

Prerequisites

A continuación se indican los requisitos previos para utilizar los espacios de refactor de AWS Migration Hub.

- Debe tener uno o másCuentas de AWS, yAWS Identity and Access Management(IAM) configurados para estas cuentas. Para obtener más información, consulte Configuración.
- Designe una de las cuentas de usuario de IAM como cuenta de propietario del entorno de Refactor Spaces.

En los siguientes pasos se describe cómo utilizar los espacios de refactor de AWS Migration Hub en la consola de Migration Hub.

Paso 1: Creación de un entorno

En este paso se describe cómo crear un entorno como parte de los espacios de refactor.Introduccióasistente de. También puede crear un entorno eligiendoEntornosUNDERRefactor de aplicaciónen el panel de navegación de Refactorizar espacios.

Un entorno de refactor simplifica los casos de uso de varias cuentas para acelerar la refactorización de aplicaciones. Cuando creas un entorno, orquestamosAWS Transit Gateway, nubes privadas virtuales (VPC) yAWS Resource Access Manageren su cuenta.

Después de crear un entorno, puede compartirlo con otrosCuentas de AWS, unidades organizativas (OUs) enAWS Organizations, o un todoAWSorganización. Compartiendo el entorno con otrosCuentas de AWS, los usuarios de esas cuentas pueden crear aplicaciones, servicios y rutas dentro del entorno, a menos que utilice IAM para restringir el acceso.

Para crear una de entorno

1. Uso deAWScuenta que creaste enConfiguración, inicie sesión en laConsola de administración de AWSy abra la consola de Migration Hub enhttps://console.aws.amazon.com/migrationhub/.
2. En el panel de navegación de Migration Hub de, elijaRefactorizar espacios.
3. Elija Getting Started (Empezar).
4. SelectCree un entorno de refactor para empezar a modernizarse gradualmente a microservicios en variosAWScuentas.
5. Elija Inicio.
6. Especifique un nombre para el entorno.
7. (Opcional) Añada una descripción del entorno.
8. Refactor Spaces utiliza un rol vinculado al servicio para conectarse aServicios de AWSpara orquestar en su nombre. Cuando utilice Refactorizar espacios por primera vez, el rol vinculado al servicio se creará con los permisos correctos. Para obtener más información sobre el rol vinculado a servicio, consulte Uso de roles vinculados a servicios para Refactorizar Espacios.
9. ElegirPróximopara desplazarse alCrear aplicación(Se ha creado el certificado).

Paso 2: Cree una aplicación

En este paso se describe cómo crear una aplicación como parte de los espacios de refactor.Introduccióasistente de. También puede crear una aplicación eligiendoCrear aplicaciónUNDERAcciones rápidasen el panel de navegación de Refactorizar espacios.

Las aplicaciones proporcionan enrutamiento de tráfico de varias cuentas para los servicios de la aplicación. Para cada aplicación, orquestamos un proxy mediante enlaces de VPC de Amazon API Gateway, un Network Load Balancer y políticas de recursos. Las aplicaciones son contenedores de servicios y rutas.

El proxy de una aplicación necesita una VPC. El equilibrador de carga de red del proxy se lanza en la VPC y se configura un enlace de VPC de API Gateway para la VPC y el Network Load Balancer.

Para crear una aplicación

1. En la páginaCrear aplicación, escriba un nombre para su aplicación.
2. UNDERVPC proxy, elija una nube virtual privada (VPC) proxy o elijaCreación de una VPC.

   El proxy de una aplicación necesita una VPC. El Network Load Balancer del proxy se lanza en la VPC y se configura un enlace de VPC de API Gateway para la VPC y el Network Load Balancer.
3. UNDERTipo de punto de enlace de proxyseleccionarregionaloPrivate.

   El endpoint del proxy puede ser regional o privado. Los endpoints de API Gateway regionales son accesibles a través de Internet pública y los endpoints de API Gateway privados solo son accesibles a través de las VPC.
4. ElegirPróximopara desplazarse aluso compartido del entorno(Se ha creado el certificado).

Paso 3: Comparta su entorno

En este paso se describe cómo compartir un entorno como parte de los espacios de refactor.Introducciónasistente de. También puede compartir un entorno eligiendouso compartido del entornoUNDERAcciones rápidasen el panel de navegación de Refactorizar espacios.

Los entornos se comparten con otrosCuentas de AWSconAWS Resource Access Manager(AWS RAM). La cuenta invitada debe aceptar una parte del entorno en un plazo de doce horas. De lo contrario, el entorno debe compartirse de nuevo. Si se encuentra en unaAWSorganización, a continuación, puede habilitar la aceptación automática de recursos compartidos.AWS RAMadmite entornos compartidos con otrosCuentas de AWS, unidades organizativas (OUs) enAWS Organizations, o un todoAWSorganización.

Dado que los entornos son contenedores de aplicaciones, servicios, rutas y orquestadosAWSrecursos, compartir el entorno proporciona cierto acceso a estos recursos desde las cuentas invitadas. Después de compartir con otras cuentas, los usuarios de esas cuentas pueden crear aplicaciones, servicios y rutas dentro del entorno, a menos que utilice IAM para restringir el acceso.

Al compartir un entorno con otroCuenta de AWS, Refactor Spaces también comparte el entornoAWS Transit Gatewaycon la otra cuenta orquestandoAWS RAM.

Para compartir un entorno

1. Seleccione uno de los siguientes tipos principales para compartir su entorno:

   - Cuenta de AWS
   - Organización - enteraAWSorganización
   - Unidad organizativa (OU)

   AWS RAMadmite entornos compartidos con otrosCuentas de AWS, unidades organizativas (OUs) enAWS Organizations, o un todoAWSorganización.
2. Los entornos se comparten con otrosCuentas de AWSconAWS Resource Access Manager(AWS RAM).AWS RAMadmite entornos compartidos con otrosCuentas de AWS, unidades organizativas (OUs) enAWS Organizations, o un todoAWSorganización. Si quieres compartir un entorno con un todoAWSorganización u OU, debe habilitar el uso compartido con la organización enAWS RAMantes de intentar compartir en Refactor Spaces.
3. Escriba laCuenta de AWSdel director y, a continuación, elijaAñadir.
4. ElegirPróximopara desplazarse alReview (Revisar)(Se ha creado el certificado).
5. Revise la información que introdujo en los pasos anteriores.
6. Si todo parece estar correcto, elijaCreación de entorno. Si desea cambiar algo, elijaPREVIOUS.

Paso 4: Crear un servicio

Los servicios proporcionan las capacidades empresariales de la aplicación. La aplicación existente está representada por uno o varios servicios. Cada servicio tiene un endpoint (una URL HTTP (TTPS) o unAWS Lambdafunción).

Una vez creado el entorno, podrá ver información sobre el entorno en la página de detalles del entorno (la página con el nombre del entorno como encabezado). La página de detalles del entorno muestra un resumen del entorno y enumera las aplicaciones de su entorno.

El siguiente procedimiento describe cómo crear un servicio a partir de la página de detalles del entorno. También puede crear un servicio eligiendoCrear un servicioUNDERAcciones rápidasen el panel de navegación de Refactorizar espacios.

Para crear un servicio desde la página de detalles del entorno

1. En la lista de aplicaciones, elija el nombre de la aplicación a la que desea agregar el servicio.

2. En la página de detalles de la solicitud (la página con el nombre de la aplicación como encabezado), enServicios, eligeCrear un servicio.
3. Escriba el nombre del nuevo servicio.
4. (Opcional) Escriba una descripción del servicio.
5. Seleccione uno de los tipos de endpoint de servicio.
6. Seleccione VPC si el servicio es un extremo de URL de una VPC.

    a. Seleccione una VPC para agregarla al puente de red del entorno.

    b. Introduzca el extremo de la URL del servicio.

    Las URL de endpoint de VPC pueden contener nombres DNS resueltos públicamente (http://www.example.com) o una dirección IP. Los nombres DNS privados no se admiten en las URL de servicio, pero puede utilizar direcciones IP privadas que se encuentran en la VPC del servicio.

    c. (Opcional) Introduzca una URL de endpoint de comprobación de estado.

7. a. Seleccione Lambda si el servicio es una función Lambda.

    b. Elija una función Lambda de su cuenta.

8. (Opcional) EnDirigir tráfico a este servicio, si desea configurar este servicio como ruta predeterminada de la aplicación, active la casilla de verificación correspondiente.

    Al crear un servicio, puede enrutar opcionalmente el tráfico de aplicaciones a él al mismo tiempo. Si la aplicación en la que se está creando el servicio no tiene rutas, puede convertir el servicio en la ruta predeterminada de la aplicación para que todo el tráfico se enrute al servicio. Si la aplicación tiene rutas existentes, puede agregar una ruta con una ruta para apuntar al servicio.

Paso 5: Creación de una ruta

En esta sección se describe cómo crear una ruta de.

Una aplicación se utiliza para redirigir gradualmente el tráfico de una aplicación existente a nuevos servicios. También puede usarlo para lanzar nuevas funciones sin tocar la aplicación existente.

Si la aplicación seleccionada no tiene rutas, la nueva ruta se convierte en la ruta predeterminada de la aplicación y todo el tráfico se enruta al servicio seleccionado. Si la aplicación tiene rutas existentes, la ruta se ajusta a una combinación de ruta y verbos.

> **Note**
>
> Una ruta está activa inmediatamente después de crearse y el tráfico se redirige fuera de la ruta predeterminada o de una ruta principal existente.

Para crear una ruta

En la página de detalles de la solicitud (la página con el nombre de la aplicación como encabezado), enRutas, eligeCreación de ruta.

1. Elija un servicio para la ruta.
2. Elija Create route (Crear ruta).

Seguridad en los espacios de refactor de AWS Migration Hub

AWS Migration Hub Refactor Spaces se encuentra en la versión preliminar y está sujeta a cambios.

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficia de una arquitectura de red y un centro de datos que se han diseñado para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS 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 los servicios de AWS en la nube de AWS. AWS también proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWSProgramas de conformidad de . Para obtener más información acerca de los programas de conformidad que se aplican a los espacios de refactorización, consulteAWSServicios de en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad se determina según el servicio de AWS que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza AWS Migration Hub Refactor Spaces. Muestra cómo configurar Refactor Spaces para satisfacer sus objetivos de seguridad y conformidad. También puedes aprender a utilizar otrosAWSque le ayudan a supervisar y proteger los recursos de Refactor Spaces.

Contenido

- Protección de datos en AWS Migration Hub Refactor Spaces
- Identity and Access Management para AWS Migration Hub Refactor de
- Validación de la conformidad de AWS Migration Hub Refactor Spaces

Protección de datos en AWS Migration Hub Refactor Spaces

LaAWS Modelo de responsabilidad compartidase aplica a la protección de datos en AWS Migration Hub Refactor Spaces. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Este contenido incluye la configuración de seguridad y las tareas de administración de los servicios de AWS que usted 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 AWSShared Responsability Model and GDPR en el Blog de seguridad de AWS.

Para fines de protección de datos, recomendamos proteger las credenciales de Cuenta de AWS y configurar cuentas de usuario individuales con AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir con sus obligaciones laborales. También recomendamos proteger sus datos de las siguientes formas:

- Utilice Multi-Factor Authentication (MFA) con cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos de AWS. Recomendamos TLS 1.2 o una versión posterior.
- Configure la API y el registro de actividad del usuario con AWS CloudTrail.
- Utilice las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los servicios de AWS.
- Utilice avanzados servicios de seguridad administrados, como Amazon Macie, que lo ayuden a detectar y proteger los datos personales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados FIPS 140-2 al acceder a AWS a través de una interfaz de línea de comandos o una API, utilice un punto de enlace de FIPS. Para obtener más información sobre los puntos de enlace de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Recomendamos encarecidamente que nunca introduzca información de identificación confidencial, como, por ejemplo, direcciones de email de sus clientes, en etiquetas o en los campos de formato libre, como el campo Name (Nombre). Esto incluye cuando trabaje con Refactor Spaces u otrosAWSservicios que utilizan la consola, API,AWS CLI, o bienAWSSDK. Los datos que ingresa en etiquetas o campos de formato libre utilizados para los nombres se pueden utilizar para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, le recomendamos

encarecidamente que no incluya información de credenciales en la URL para validar la solicitud para ese servidor.

Cifrado en reposo

Refactor Spaces cifra todos los datos en reposo.

Cifrado en tránsito

Las comunicaciones entre redes de Refactor Spaces admiten el cifrado TLS 1.2 entre todos los componentes y clientes.

Identity and Access Management para AWS Migration Hub Refactor de

AWS Identity and Access Management (IAM) es un servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan quién puede serautenticado(iniciado sesión) yautorizado(tienen permisos) para utilizar los recursos de Refactor Spaces. IAM es un servicio de AWS que puede utilizar sin cargo adicional.

Temas

- Audience
- Autenticación con identidades
- Administración de acceso mediante políticas
- Cómo funciona AWS Migration Hub Refactor Spaces con IAM
- AWSPolíticas administradas de AWS Migration Hub Refactor Spaces
- Ejemplos de políticas basadas en identidades para AWS Migration Hub Refactor Spaces
- Solución de problemas de identidad y acceso de AWS Migration Hub Refactor Spaces
- Uso de roles vinculados a servicios para Refactorizar Espacios

Audience

Cómo utilizaAWS Identity and Access Management(IAM) difiere en función del trabajo que se realice en Refactorice Spaces.

Usuario de servicio: si utiliza el servicio Refactor Spaces para realizar su trabajo, su administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Refactor Spaces para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarle a solicitar los permisos correctos a su administrador. Si no puede acceder a una característica en Refactorizar espacios, consulteSolución de problemas de identidad y acceso de AWS Migration Hub Refactor Spaces.

Administrador de servicios— Si está a cargo de los recursos de Refactor Spaces en su empresa, probablemente tenga acceso completo a Refactor Spaces. Su trabajo consiste en determinar a qué características y recursos de Refactor Spaces deben acceder sus empleados. A continuación, 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 IAM con Refactor Spaces, consulteCómo funciona AWS Migration Hub Refactor Spaces con IAM.

Administrador de IAM— Si es un administrador de IAM, es posible que desee obtener información sobre cómo escribir políticas para administrar el acceso a Refactor Spaces. Para ver ejemplos de políticas basadas en identidades de Refactor Spaces que puede utilizar en IAM, consulteEjemplos de políticas basadas en identidades para AWS Migration Hub Refactor Spaces.

Autenticación con identidades

La autenticación es la manera de iniciar sesión en AWS mediante credenciales de identidad. Para obtener más información acerca de cómo iniciar sesión con la Consola de administración de AWS, consulte Inicio de sesión en la Consola de administración de AWS como usuario de IAM o usuario raíz en la Guía del usuario de IAM.

Debe estar autenticado (haber iniciado sesión en AWS) como el usuario raíz de la Cuenta de AWS, como un usuario de IAM o asumiendo un rol de IAM. También puede utilizar la autenticación de inicio de sesión único de la empresa o incluso iniciar sesión con Google o Facebook. En estos casos, su administrador habrá configurado previamente la federación de identidad mediante roles de IAM. Cuando obtiene acceso a AWS mediante credenciales de otra empresa, asume un rol indirectamente.

Para iniciar sesión directamente en la Consola de administración de AWS, utilice la contraseña con su dirección de email de usuario raíz o con su nombre de usuario de IAM. Puede acceder a AWS mediante programación utilizando sus claves de acceso de usuario raíz o usuario de IAM. AWS proporciona SDK y herramientas de línea de comandos para firmar criptográficamente su solicitud con sus credenciales. Si no utiliza las herramientas de AWS, debe firmar usted mismo la solicitud.

Para ello, utilice Signature Version 4, un protocolo para autenticar solicitudes de API de entrada. Para obtener más información acerca de cómo autenticar solicitudes, consulte Proceso de firma de Signature Version 4 en la Referencia general de AWS.

Independientemente del método de autenticación que utilice, es posible que también deba proporcionar información de seguridad adicional. Por ejemplo, AWS le recomienda el uso de la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de IAM.

Cuenta de AWS usuario raíz

Cuando se crea por primera vez una Cuenta de AWS, se comienza con una única identidad de inicio de sesión que tiene acceso completo a todos los servicios y recursos de AWS de la cuenta. Esta identidad recibe el nombre de usuario raíz de la Cuenta de AWS y se accede a ella iniciando sesión con el email y la contraseña que utilizó para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz en sus tareas cotidianas, ni siquiera en las tareas administrativas. En lugar de ello, es mejor ceñirse a la práctica recomendada de utilizar el usuario final exclusivamente para crear al primer usuario de IAM. A continuación, guarde las credenciales del usuario raíz en un lugar seguro y utilícelas tan solo para algunas tareas de administración de cuentas y servicios.

Usuarios y grupos de IAM

Un usuario de IAM es una identidad de la Cuenta de AWS que dispone de permisos específicos para una sola persona o aplicación. Un usuario de IAM puede tener credenciales a largo plazo, como un nombre de usuario y una contraseña o un conjunto de claves de acceso. Para obtener información sobre cómo generar claves de acceso, consulte Administración de claves de acceso de los usuarios de IAM en la Guía del usuario de IAM. Al generar claves de acceso para un usuario de IAM, asegúrese de ver y guardar de forma segura el par de claves. No puede recuperar la clave de acceso secreta en el futuro. En su lugar, debe generar un nuevo par de claves de acceso.

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 obtener más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

IAM roles

Un rol de IAM es una identidad de la Cuenta de AWS que dispone de permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente un rol de IAM en la Consola de administración de AWScambiando de roles. Puede asumir un rol llamando a una operación de la AWS CLI o de la API de AWS, o utilizando una URL personalizada. Para obtener más información acerca de 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:

- 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 de usuarios federados: en lugar de crear un usuario de IAM, puede utilizar identidades existentes de Directory Service, del directorio de usuarios de su empresa o de un proveedor de identidades web. A estas identidades se les llama usuarios federados. AWS asigna una función a un usuario federado cuando se solicita acceso a través de un proveedor de identidad. Para obtener más información acerca de los usuarios federados, consulte Usuarios federados y roles en la Guía del usuario de IAM.
- 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 algunos servicios de AWS, puede asociar una política directamente a un recurso (en lugar de utilizar 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 características de 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 a servicios.
  - Permisos principales: cuando utiliza un usuario o un rol de IAM para llevar a cabo acciones en AWS, se lo considera una entidad principal. Las políticas conceden permisos a una entidad

principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. En este caso, debe tener permisos para realizar ambas acciones. Para ver si una acción requiere acciones dependientes adicionales en una política, consulteClaves de condición, recursos y acciones de AWS Migration Hub Refactor Spacesen laReferencia de autorizaciones de servicio.

- 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.
- Rol vinculado a un servicio: un rol vinculado a un servicio es un tipo de función del servicio que está vinculado a un servicio de AWS. El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados a servicios aparecen en la cuenta de IAM y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puede utilizar un rol de IAM que le permita administrar credenciales temporales para las aplicaciones que se ejecutan en una instancia EC2 y realizan solicitudes a la AWS CLI o a la API de AWS. Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia EC2. Para asignar un rol de AWS a una instancia EC2 y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia asociado a la misma. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para obtener 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

Para controlar el acceso en AWS, se crean políticas y se adjuntan a identidades de IAM o recursos de AWS. Una política es un objeto de AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. Puede iniciar sesión como usuario raíz o usuario de IAM o puede asumir un rol de IAM. Cuando realiza una solicitud, AWS evalúa las políticas relacionadas basadas en identidades o en recursos. Los permisos en las políticas determinan si la solicitud se permite o se deniega. Las mayoría de las políticas se almacenan en 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 utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y bajo qué condiciones.

Cada entidad de IAM (usuario o rol) comienza sin permisos. En otras palabras, de forma predeterminada, los usuarios no pueden hacer nada, ni siquiera cambiar sus propias contraseñas. Para conceder permiso a un usuario para hacer algo, el administrador debe asociarle una política de permisos. O bien el administrador puede agregar al usuario a un grupo que tenga los permisos necesarios. Cuando el administrador concede permisos a un grupo, todos los usuarios de ese grupo obtienen los permisos.

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 dicha política puede obtener información del usuario de la Consola de administración de AWS, la AWS CLI o la API de AWS.

Políticas basadas en identidad

Las políticas basadas en identidades 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 bajo qué condiciones. Para obtener más información sobre cómo crear una política basada en identidades, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidad 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 asociar a varios usuarios, grupos y roles de su Cuenta de AWS. Las políticas administradas incluyen las políticas administradas por AWS y las políticas administradas por el cliente. Para obtener más información acerca de 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 basada en recursos. Las entidades 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 se puede utilizar políticas de IAM administradas por AWS 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 política JSON.

Amazon S3, AWS WAF y Amazon VPC son ejemplos de servicios que admiten las ACL. 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 otros tipos de políticas adicionales menos frecuentes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le otorgan.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidades puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una identidad. Los permisos resultantes son la intersección de las políticas basadas en identidades de la entidad y los límites de sus 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 servicio (SCP): las SCP son políticas de JSON que especifican los permisos máximos de una organización o una unidad organizativa (OU) en AWS Organizations. AWS Organizations es un servicio que le permite agrupar y administrar de manera centralizada varias Cuentas de AWS que posea su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o todas sus cuentas. Las SCP limitan los permisos de las entidades de las cuentas miembro, incluido cada 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 basada en recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para obtener información acerca de cómo AWS decide si permitir o no una solicitud cuando hay varios tipos de políticas implicados, consulte Lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funciona AWS Migration Hub Refactor Spaces con IAM

Antes de utilizar IAM para administrar el acceso a los espacios de refactor, conozca qué características de IAM están disponibles para su uso con Refactor Spaces.

Funciones de IAM que puede utilizar con los espacios de refactor de AWS Migration Hub

Características de IAM	Compatibilidad con Refactor Spaces
Políticas basadas en identidad	Sí
Políticas basadas en recursos	Sí
Acciones de política	Sí
Recursos de políticas	Sí
Claves de condición de	Sí
ACL	No
ABAC (etiquetas en las políticas)	Parcial

Características de IAM	Compatibilidad con Refactor Spaces
Credenciales temporales	Sí
Permisos principales	Sí
Roles de servicio	No
Roles vinculados a servicios	Sí

Para obtener una perspectiva general de cómo Refacturar espacios y otrosAWSlos servicios funcionan con la mayoría de las funciones de IAM, consulteAWSServicios que funcionan con IAMen laIAM User Guide.

Políticas basadas en identidades para espacios de refactor

Compatibilidad con las políticas basadas en identidad	Sí

Las políticas basadas en identidades 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 bajo qué condiciones. Para obtener más información sobre cómo crear una política basada en identidades, 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 recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No puede especificar el principal en una política basada en identidades porque se aplica al usuario o al rol al que está asociado. Para obtener más información acerca de 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 identidades para Refactor Spaces

Para ver ejemplos de políticas basadas en identidades de Refactor Spaces, consulteEjemplos de políticas basadas en identidades para AWS Migration Hub Refactor Spaces.

Políticas basadas en recursos en recursos de Refactor Spaces

Compatibilidad con las políticas basadas en recursos	Sí

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 basada en recursos. Las entidades principales pueden incluir cuentas, usuarios, roles, usuarios federados o servicios de AWS.

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

Acciones políticas para espacios de refactor

Compatibilidad con las acciones de política	Sí

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

El elemento `Action` de una política JSON describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones de la política generalmente tienen el mismo nombre que la operación de API de AWS 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 Refactorizar espacios, consulteAcciones definidas por AWS Migration Hub Refactor Spacesen laReferencia de autorizaciones de servicio.

Las acciones de políticas en espacios de refacturador de utilizan el siguiente prefijo antes de la acción:

```
refactor-spaces
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "refactor-spaces:action1",
      "refactor-spaces:action2"
         ]
```

Para ver ejemplos de políticas basadas en identidades de Refactor Spaces, consulteEjemplos de políticas basadas en identidades para AWS Migration Hub Refactor Spaces.

Recursos de políticas para espacios de refactor

Compatibilidad con los recursos de políticas	Sí

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y bajo 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 Refactor Spaces y sus ARN, consulteRecursos definidos por AWS Migration Hub Refactor Spacesen laReferencia de autorizaciones de servicio. Para obtener información acerca de con qué acciones puede especificar los ARN de cada recurso, consulteAcciones definidas por AWS Migration Hub Refactor Spaces.

Para ver ejemplos de políticas basadas en identidades de Refactor Spaces, consulteEjemplos de políticas basadas en identidades para AWS Migration Hub Refactor Spaces.

Claves de condición de política para espacios de refactor

Compatibles con las claves de condición de política	Sí

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y bajo 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 con una operación lógica `OR`. 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 obtener 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 globales de AWS, consulte Claves de contexto de condición globales de AWS en la Guía del usuario de IAM.

Para ver una lista de claves de condición de Refactor de espacios, consulteClaves de condición de AWS Migration Hub Refactor deen laReferencia de autorizaciones de servicio. Para obtener información acerca de con qué acciones y recursos puede utilizar una clave de condición, consulteAcciones definidas por AWS Migration Hub Refactor Spaces.

Para ver ejemplos de políticas basadas en identidades de Refactor Spaces, consulteEjemplos de políticas basadas en identidades para AWS Migration Hub Refactor Spaces.

Listas de control de acceso (ACL) en espacios de refactor

Compatible con 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 política JSON.

Control de acceso basado en atributos (ABAC) con espacios de refactor

Compatible con ABAC (etiquetas en políticas)	Parcial

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos basados en atributos. En AWS, estos atributos se denominan etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a muchos recursos de AWS. 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 del 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`.

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 Usar el control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con espacios de refactor

Compatible con el uso de credenciales temporales.	Sí

Alguno servicios de AWS no funcionan cuando inicia sesión con credenciales temporales. Para obtener más información, incluido qué servicios de AWS funcionan con credenciales temporales, consulte Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en la Consola de administración de AWS con cualquier método, excepto un nombre de usuario y contraseña. Por ejemplo, cuando accede a AWS con el enlace de inicio de sesión único (SSO) de su empresa, ese proceso crea de forma automática credenciales temporales. También crea de forma automática credenciales temporales cuando inicia sesión en la consola como usuario y, a continuación, cambia de rol. Para obtener más información acerca del cambio de roles, consulte Cambio de rol (consola) en la Guía del usuario de IAM.

Puede crear de forma manual credenciales temporales con la API de AWS CLI o de AWS. A continuación, puede usar esas credenciales temporales para acceder a AWS. AWS recomienda que genere de manera dinámica credenciales temporales, en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM.

Permisos principales entre servicios para espacios de refactor

Compatible con permisos principales	Sí

Cuando utiliza un usuario o un rol de IAM para llevar a cabo acciones en AWS, se lo considera una entidad principal. Las políticas conceden permisos a una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. En este caso, debe tener permisos para realizar ambas acciones. Para ver si una acción requiere acciones dependientes adicionales en una política, consulteClaves de condición, recursos y acciones de AWS Migration Hub Refactor Spacesen laReferencia de autorizaciones de servicio.

Funciones de servicio para espacios de refactor

Compatible con funciones del servicio	No

Una función del 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 Refactorizar espacios. Edite los roles de servicio solo cuando Refactor Spaces proporciona orientación para hacerlo.

Roles vinculados a servicios de espacios de refactor

Compatible con roles vinculados a servicios	Sí

Una función vinculada a un servicio es un tipo de función del servicio que está vinculado a un servicio de AWS. El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados a servicios aparecen en la cuenta de IAM y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener más información acerca de cómo crear o administrar roles vinculados a servicios de, consulteAWSServicios que funcionan con IAM. Busque un servicio en la tabla que incluya unYesen laFunción vinculada al serviciocolumn. Elija el vínculo Sí para ver la documentación acerca del rol vinculado al servicio en cuestión.

AWSPolíticas administradas de AWS Migration Hub Refactor Spaces

Para agregar permisos a usuarios, grupos y roles, es más fácil utilizar las políticas administradas por AWS que escribirlas uno mismo. Se necesita tiempo y experiencia para crear políticas de IAM administradas por el cliente que proporcionen a su equipo solo los permisos necesarios. Para

comenzar a hacerlo con rapidez, puede utilizar nuestras políticas administradas por AWS. Estas políticas cubren casos de uso comunes y están disponibles en su Cuenta de AWS. Para obtener más información sobre las políticas administradas por AWS, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

Los servicios de AWS mantienen y actualizan las políticas administradas por AWS. No puede cambiar los permisos en las políticas administradas por AWS. En ocasiones, los servicios agregan permisos adicionales a una política administrada por AWS para admitir características nuevas. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Es más probable que los servicios actualicen una política administrada por AWS cuando se lanza una nueva característica o cuando se ponen a disposición nuevas operaciones. Los servicios no quitan permisos de una política administrada por AWS, por lo que las actualizaciones de políticas no deteriorarán los permisos existentes.

AWSpolítica administrada: Acceso completo a los espacios del factor de migración de AWS

Puede adjuntar la política `AWSMigrationHubRefactorSpacesFullAccess` a las identidades de IAM.

La`AWSMigrationHubRefactorSpacesFullAccess`otorga acceso completo a los espacios de refactor de AWS Migration Hub, las funciones de la consola de Refactor Spaces y otros relacionados`AWS`Servicios de .

Detalles sobre los permisos

La`AWSMigrationHubRefactorSpacesFullAccess`La política incluye los permisos siguientes.

- `refactor-spaces`— Permite a la cuenta de usuario de IAM acceso completo a Refactor Spaces.
- `ec2`Permite a la cuenta de usuario de IAM realizar operaciones de Amazon Elastic Compute Cloud (Amazon EC2) utilizadas por Refactor Spaces.
- `elasticloadbalancing`: permite que la cuenta de usuario de IAM realice operaciones de Elastic Load Balancing utilizadas por Refactor Spaces.
- `apigateway`— Permite que la cuenta de usuario de IAM realice operaciones de Amazon API Gateway utilizadas por Refactor Spaces.

- `organizations`— Permite que la cuenta de usuario de IAM puedaAWS Organizationsoperaciones utilizadas por Refactor Spaces.
- `cloudformation`— Permite que la cuenta de usuario de IAM realiceAWS CloudFormationoperaciones para crear un entorno de ejemplo con un solo clic desde la consola.
- `iam`: permite crear un rol vinculado a servicios para la cuenta de usuario de IAM, que es un requisito para utilizar espacios de refactor.

Permisos adicionales necesarios para espacios de refactor

Antes de poder utilizar espacios de refactor, además de la`AWSMigrationHubRefactorSpacesFullAccess`La política administrada proporcionada por Refactor Spaces, los siguientes permisos adicionales necesarios deben asignarse a un usuario, un grupo o un rol de IAM en su cuenta.

- Conceder permiso para crear un rol vinculado a servicios deAWS Transit Gateway.
- Conceda permiso para adjuntar una nube privada virtual (VPC) a una puerta de enlace de tránsito para la cuenta de llamada de todos los recursos.
- Concede permiso para modificar los permisos de un servicio de punto de enlace de VPC para todos los recursos.
- Conceda permiso para devolver recursos etiquetados o etiquetados anteriormente para la cuenta de llamada para todos los recursos.
- Concede permiso para realizar todas lasAWS Resource Access Manager(AWS RAM) para la cuenta de llamada en todos los recursos.
- Concede permiso para realizar todas lasAWS Lambdaacciones de la cuenta de llamada en todos los recursos de.

Puede obtener estos permisos adicionales añadiendo políticas en línea a su usuario, grupo o rol de IAM. Sin embargo, en lugar de utilizar políticas en línea, puede crear una política de IAM utilizando el siguiente JSON de política y adjuntarla al usuario, grupo o rol de IAM.

La siguiente política otorga los permisos necesarios adicionales necesarios para poder utilizar espacios de refactor.

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

```
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "transitgateway.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTransitGatewayVpcAttachment"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyVpcEndpointServicePermissions"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ram:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "lambda:*"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

A continuación se muestra el`AWSMigrationHubRefactorSpacesFullAccess`política.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RefactorSpaces",
            "Effect": "Allow",
            "Action": [
                "refactor-spaces:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcs",
                "ec2:DescribeTransitGatewayVpcAttachments",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeTags",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeInternetGateways"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTransitGateway",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTransitGatewayVpcAttachment"
            ],
            "Resource": "*",
```

```
            "Condition": {
                "Null": {
                    "aws:RequestTag/refactor-spaces:environment-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTransitGateway",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTransitGatewayVpcAttachment"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/refactor-spaces:environment-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateVpcEndpointServiceConfiguration"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteTransitGateway",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteTransitGatewayVpcAttachment",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DeleteTags"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/refactor-spaces:environment-id": "false"
                }
```

```
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteVpcEndpointServiceConfigurations",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/refactor-spaces:application-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:CreateLoadBalancer"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/refactor-spaces:application-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTags",
                "elasticloadbalancing:DescribeTargetHealth",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeListeners"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:CreateLoadBalancerListeners",
                "elasticloadbalancing:CreateListener",
                "elasticloadbalancing:DeleteListener",
                "elasticloadbalancing:DeleteTargetGroup"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/refactor-spaces:route-id": [
                        "*"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:DeleteLoadBalancer",
            "Resource": "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-
spaces-nlb-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:CreateListener"
            ],
            "Resource": "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-
spaces-nlb-*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/refactor-spaces:route-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:DeleteListener",
            "Resource": "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-
nlb-*"
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "elasticloadbalancing:DeleteTargetGroup",
                "elasticloadbalancing:RegisterTargets"
            ],
            "Resource": "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-
*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:CreateTargetGroup"
            ],
            "Resource": "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-
*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/refactor-spaces:route-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "apigateway:GET",
                "apigateway:DELETE",
                "apigateway:PATCH",
                "apigateway:POST",
                "apigateway:PUT",
                "apigateway:UpdateRestApiPolicy"
            ],
            "Resource": [
                "arn:aws:apigateway:*::/restapis",
                "arn:aws:apigateway:*::/restapis/*",
                "arn:aws:apigateway:*::/vpclinks",
                "arn:aws:apigateway:*::/vpclinks/*",
                "arn:aws:apigateway:*::/tags",
                "arn:aws:apigateway:*::/tags/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/refactor-spaces:application-id": "false"
                }
            }
```

```
        },
        {
            "Effect": "Allow",
            "Action": "apigateway:GET",
            "Resource": [
                "arn:aws:apigateway:*::/vpclinks",
                "arn:aws:apigateway:*::/vpclinks/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "refactor-spaces.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "elasticloadbalancing.amazonaws.com"
                }
            }
        }
    ]
```

```
}
```

Actualizaciones de Refactor Spaces aAWSPolíticas administradas de

Ver detalles sobre las actualizaciones deAWSLas políticas administradas de Refactor Spaces desde que este servicio comenzó a registrar estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de historial de documentos de Refactor Spaces.

Cambio	Descripción	Fecha
Acceso completo a los espacios del factor de migración de AWS— Nueva política disponible en el lanzamiento	La`AWSMigrationHubRefactorSpacesFullAccess` otorga acceso completo a los espacios de Refactor, las funciones de la consola de Refactor Spaces y otras características relacionadasAWSServicios de .	29 de noviembre de 2021
Política de rol de servicio de espacios de factor de migración— Nueva política disponible en el lanzamiento	`MigrationHubRefactorSpacesServiceRolePolicy` proporciona acceso aAWSrecursos administrados o utilizados por AWS Migration Hub Refactor Spaces. La política la usa el rol vinculado al servicio AWSServiceRoleForMigrationHubreFactorSpaces.	29 de noviembre de 2021
Refactor Spaces comenzó a registrar los cambios	Refactor Spaces comenzó a registrar los cambios deAWSpolíticas administradas de.	29 de noviembre de 2021

Ejemplos de políticas basadas en identidades para AWS Migration Hub Refactor Spaces

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

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

Temas

- Prácticas recomendadas relativas a políticas
- Uso de la consola Refactor Spaces
- Permitir a los usuarios consultar sus propios permisos

Prácticas recomendadas relativas a políticas

Las políticas basadas en identidades son muy eficaces. Determinan si alguien puede crear, acceder o eliminar los recursos de Refactor Spaces en su cuenta. Estas acciones pueden generar costes adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Empiece a trabajar conAWSPolíticas administradas de— Para empezar a utilizar espacios de refactor rápidamente, utiliceAWSPolíticas administradas para proporcionar a los empleados los permisos que necesitan. Estas políticas ya están disponibles en su cuenta, y AWS las mantiene y actualiza. Para obtener más información, consulte Introducción sobre el uso de permisos con políticas administradas por AWS en la Guía del usuario de IAM.
- Conceder privilegios mínimos: al crear políticas personalizadas, conceda solo los permisos necesarios para llevar a cabo una tarea. Comience con un conjunto mínimo de permisos y conceda permisos adicionales según sea necesario. Por lo general, es más seguro que comenzar con permisos que son demasiado tolerantes e intentar hacerlos más estrictos más adelante. Para obtener más información, consulte Conceder privilegios mínimos en la Guía del usuario de IAM.

- Habilitar la MFA para operaciones confidenciales: para mayor seguridad, obligue a los usuarios de IAM a utilizar la autenticación multifactor (MFA) para acceder a recursos u operaciones de API confidenciales. Para obtener más información, consulte Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de IAM.
- Utilizar condiciones de política para mayor seguridad: en la medida en que sea práctico, defina las condiciones en las que las políticas basadas en identidades permitan el acceso a un recurso. Por ejemplo, puede escribir condiciones para especificar un rango de direcciones IP permitidas desde el que debe proceder una solicitud. También puede escribir condiciones para permitir solicitudes solo en un intervalo de hora o fecha especificado o para solicitar el uso de SSL o MFA. Para obtener más información, consulteElemento de la política de JSON de IAM: Condiciónen laIAM User Guide.

Uso de la consola Refactor Spaces

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

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

Para asegurarse de que los usuarios y roles puedan seguir utilizando la consola de Refactor de espacios, asocie también los espacios de refactor de`ConsoleAccessoReadOnly` AWSadministra la política de las entidades. Para obtener más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

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 llevar a cabo esta acción en la consola o mediante programación con la AWS CLI o la API de 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": "*"
        }
    ]
}
```

Solución de problemas de identidad y acceso de AWS Migration Hub Refactor Spaces

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que es posible que surjan cuando se trabaja con Refactor Spaces e IAM.

Temas

- No tengo autorización para realizar una acción en Refactor Spaces
- No tengo autorización para realizar la operación iam:PassRole

- Quiero ver mis claves de acceso
- Soy administrador y deseo permitir que otros obtengan acceso a Refactor Spaces
- Quiero permitir que personas se encuentren fuera de miCuenta de AWSpara acceder a mis recursos de Refactor Spaces

No tengo autorización para realizar una acción en Refactor Spaces

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

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 `refactor-spaces:`*`GetWidget`*.

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

En este caso, Mateo pide a su administrador que actualice sus políticas de forma que pueda obtener acceso al recurso *`my-example-widget`* mediante la acción `refactor-spaces:`*`GetWidget`*.

No tengo autorización para realizar la operación iam:PassRole

Si recibe un error que indica que no está autorizado para llevar a cabo la acción `iam:PassRole`, debe ponerse en contacto con su administrador para recibir ayuda. Su administrador es la persona que le facilitó su nombre de usuario y contraseña. Pida a la persona que actualice sus políticas de forma que pueda transferir un rol a Refactor Spaces.

Algunos servicios de AWS le permiten transferir un rol existente a dicho servicio en lugar de crear un nuevo rol de servicio o uno vinculado al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado`marymajor`intenta utilizar la consola para realizar una acción en Refactorizar espacios. Sin embargo, la acción requiere que el servicio cuente con permisos otorgados por 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, Mary pide a su administrador que actualice sus políticas para que pueda realizar la acción `iam:PassRole`.

Quiero ver mis claves de acceso

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

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

> **Important**
>
> No proporcione las claves de acceso a terceros, ni siquiera para que le ayuden a buscar el ID de usuario canónico. Si lo hace, podría conceder a otra persona acceso permanente a su cuenta.

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

Soy administrador y deseo permitir que otros obtengan acceso a Refactor Spaces

Para permitir que otros obtengan acceso a espacios de refactor, debe crear una entidad de IAM (usuario o rol) para la persona o aplicación que necesita acceso. Esta persona utilizará las credenciales de la entidad para acceder a AWS. A continuación, debe asociar una política a la entidad que le conceda los permisos correctos en Espacios de refactor.

Para comenzar de inmediato, consulte Creación del primer grupo y usuario delegado de IAM en la Guía del usuario de IAM.

Quiero permitir que personas se encuentren fuera de miCuenta de AWSpara acceder a mis recursos de Refactor Spaces

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 obtener más información, consulte lo siguiente:

- Para obtener información acerca de si Refactor Spaces admite estas características, consulteCómo funciona AWS Migration Hub Refactor Spaces con IAM.
- Para obtener información acerca de cómo proporcionar acceso a los recursos de las Cuentas de AWS de su propiedad, consulte Proporcionar acceso a un usuario de IAM a otra Cuenta de AWS de la que es propietario en la Guía del usuario de IAM.
- Para obtener información acerca de cómo proporcionar acceso a los recursos a Cuentas de AWS de terceros, consulte Proporcionar acceso a Cuentas de AWS que son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una identidad federada, 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.

Uso de roles vinculados a servicios para Refactorizar Espacios

AWS Migration Hub Refactor Spaces utilizaAWS Identity and Access Management(IAM)roles vinculados a servicios. Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Refactorizar Espacios. Los roles vinculados a servicios están predefinidos por Refactor Spaces e incluyen todos los permisos que el servicio requiere para llamar a otrosAWSservicios en su nombre.

Un rol vinculado a un servicio simplifica la configuración de espacios de refactor porque ya no tendrá que agregar manualmente los permisos necesarios. Refactor Spaces define los permisos de sus

roles vinculados a servicio y, a menos que esté definido de otra manera, solo Refactor Spaces puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo puede eliminar una función vinculada a un servicio después de eliminar sus recursos relacionados. De esta forma se protegen los recursos de Refactor Spaces, ya que evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Para obtener información acerca de otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Rol vinculado a servicios. Seleccione una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de rol vinculado a servicios en espacios de refactor

Refactor Spaces utiliza el rol vinculado al servicio denominadoFunción de servicio de AWS para espacios de factor de migracióny lo asocia con elPolítica de rol de servicio de espacios de factor de migraciónPolítica de IAM: proporciona acceso aAWSrecursos administrados o utilizados por AWS Migration Hub Refactor Spaces.

El rol vinculado al servicio AWSServiceRoleForMigrationHubreFatorSpaces confía en que los siguientes servicios asuman el rol:

- `refactor-spaces.amazonaws.com`

A continuación se muestra el nombre de recurso de Amazon (ARN) de AWSServiceRoleForMigrationHubreFactorSpaces.

```
arn:aws:iam::111122223333:role/aws-service-role/refactor-spaces.amazonaws.com/
AWSServiceRoleForMigrationHubRefactorSpaces
```

Refactor Spaces utiliza elFunción de servicio de AWS para espacios de factor de migraciónfunción vinculada a servicios cuando se realizan cambios entre cuentas. Este rol debe estar presente en su cuenta para utilizar espacios de refactor. Si no está presente, Refactor Spaces lo crea durante las siguientes llamadas a la API:

- `CreateEnvironment`
- `CreateService`

- `CreateApplication`
- `CreateRoute`

Debe tener permisos de `iam:CreateServiceLinkedRole` para crear el rol vinculado a servicios. Si el rol vinculado al servicio no existe en su cuenta y no se puede crear, el`Create`las llamadas fallarán. Debe crear el rol vinculado a servicios en la consola de IAM antes de utilizar Refactor Spaces, a menos que esté utilizando la consola Refactor Spaces.

Refactor Spaces no utiliza el rol vinculado al servicio cuando realiza cambios en la cuenta de inicio de sesión actual. Por ejemplo, cuando se crea una aplicación, Refactor Spaces actualiza todas las VPC del entorno para que puedan comunicarse con la VPC recién agregada. Si las VPC se encuentran en otras cuentas, Refactor Spaces utiliza el rol vinculado a servicios y el`ec2:CreateRoute`permiso para actualizar las tablas de rutas de otras cuentas.

Para ampliar aún más el ejemplo de creación de aplicación, al crear una aplicación, Refactor Spaces actualiza las tablas de enrutamiento que se encuentran en la nube privada virtual (VPC) proporcionada en el`CreateApplication`Llame a. De esta forma, la VPC puede comunicarse con otras VPC del entorno.

La persona que llama debe tener el`ec2:CreateRoute`permiso que utilizamos para actualizar las tablas de ruta. Este permiso existe en el rol vinculado a servicios, pero Refactor Spaces no utiliza el rol vinculado a servicios en la cuenta de la persona que llama para obtener este permiso. En cambio, la persona que llama debe tener la`ec2:CreateRoute`permiso. De lo contrario, la solicitud envía un error.

No puede utilizar el rol vinculado a servicio para ampliar sus privilegios. Tu cuenta debe tener ya los permisos del rol vinculado al servicio para realizar los cambios en la cuenta que llama. La`AWSMigrationHubRefactorSpacesFullAccess`la política administrada, junto con una política que otorga los permisos adicionales necesarios, define todos los permisos necesarios para crear recursos de Refactor Spaces. El rol vinculado a servicios es un subconjunto de estos permisos que se utiliza para llamadas cruzadas específicas. Para obtener más información acerca de `AWSMigrationHubRefactorSpacesFullAccess`, consulte AWSPolítica administrada: Acceso completo a los espacios del factor de migración de AWS.

Tags

Cuando Refactor Spaces crea recursos en tu cuenta, se etiquetan con el identificador de recurso de Refactor Spaces adecuado. Por ejemplo, Transit Gateway creado a partir

de`CreateEnvironment`está etiquetado con el`refactor-spaces:environment-id`etiqueta con el ID de entorno como valor. La API de API Gateway creada desde`CreateApplication`está etiquetado con`refactor-spaces:application-id`con el ID de aplicación como valor. Estas etiquetas permiten a Refactor Spaces administrar estos recursos. Si edita o elimina las etiquetas, Refactor Spaces ya no podrá actualizar ni eliminar el recurso.

MigrationHubRefactorSpacesServiceRolePolicy

La política de permisos del rol denominada MigrationHubreFactorSpacesServiceRolePolicy permite que Refactor Spaces realice las siguientes acciones en los recursos especificados:

Acciones de Amazon API Gateway

- `apigateway:PUT`
- `apigateway:POST`
- `apigateway:GET`
- `apigateway:PATCH`
- `apigateway:DELETE`

Acciones de Amazon Elastic Compute Cloud

- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSubnets`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeVpcEndpointServiceConfigurations`
- `ec2:DescribeTransitGatewayVpcAttachments`
- `ec2:AuthorizeSecurityGroupIngress`
- `ec2:RevokeSecurityGroupIngress`
- `ec2:DeleteSecurityGroup`

```
ec2:DeleteTransitGatewayVpcAttachment

ec2:CreateRoute

ec2:DeleteRoute

ec2:DeleteTags

ec2:DeleteVpcEndpointServiceConfigurations
```

Acciones de AWS Resource Access Manager

```
ram:GetResourceShareAssociations

ram:DeleteResourceShare

ram:AssociateResourceShare

ram:DisassociateResourceShare
```

Elastic Load Balancing; acciones

```
elasticloadbalancing:DescribeTargetHealth

elasticloadbalancing:DescribeListener

elasticloadbalancing:DescribeTargetGroups

elasticloadbalancing:RegisterTargets

elasticloadbalancing:CreateLoadBalancerListeners

elasticloadbalancing:CreateListener

elasticloadbalancing:DeleteListener

elasticloadbalancing:DeleteTargetGroup

elasticloadbalancing:DeleteLoadBalancer

elasticloadbalancing:AddTags

elasticloadbalancing:CreateTargetGroup
```

A continuación se muestra la política completa que muestra los recursos a los que se aplican las acciones anteriores:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeTransitGatewayVpcAttachments",
                "elasticloadbalancing:DescribeTargetHealth",
                "elasticloadbalancing:DescribeListeners",
                "elasticloadbalancing:DescribeTargetGroups",
                "ram:GetResourceShareAssociations"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteTransitGatewayVpcAttachment",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DeleteTags",
                "ram:DeleteResourceShare",
                "ram:AssociateResourceShare",
                "ram:DisassociateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/refactor-spaces:environment-id": "false"
                }
            }
        },
```

```
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteVpcEndpointServiceConfigurations",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/refactor-spaces:application-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:CreateLoadBalancerListeners",
                "elasticloadbalancing:CreateListener",
                "elasticloadbalancing:DeleteListener",
                "elasticloadbalancing:DeleteTargetGroup"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/refactor-spaces:route-id": [
                        "*"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "apigateway:PUT",
                "apigateway:POST",
                "apigateway:GET",
                "apigateway:PATCH",
                "apigateway:DELETE"
            ],
            "Resource": [
                "arn:aws:apigateway:*::/restapis",
                "arn:aws:apigateway:*::/restapis/*",
                "arn:aws:apigateway:*::/vpclinks/*",
                "arn:aws:apigateway:*::/tags",
                "arn:aws:apigateway:*::/tags/*"
            ],
```

```
            "Condition": {
                "Null": {
                    "aws:ResourceTag/refactor-spaces:application-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "apigateway:GET",
            "Resource": "arn:aws:apigateway:*::/vpclinks/*"
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:DeleteLoadBalancer",
            "Resource": "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-
spaces-nlb-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:CreateListener"
            ],
            "Resource": "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-
spaces-nlb-*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/refactor-spaces:route-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:DeleteListener",
            "Resource": "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-
nlb-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:DeleteTargetGroup",
                "elasticloadbalancing:RegisterTargets"
            ],
```

```
            "Resource": "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-
*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:CreateTargetGroup"
            ],
            "Resource": "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-
*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/refactor-spaces:route-id": "false"
                }
            }
        }
    ]
}
```

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado a un servicio para Refactorizar Espacios

No necesita crear manualmente un rol vinculado a servicios. Al crear recursos de entorno, aplicación, servicio o enrutamiento de Refactor Spaces en elConsola de administración de AWS, elAWS CLI, o elAWSAPI, Refactor Spaces crea automáticamente el rol vinculado al servicio. Para obtener más información acerca de cómo crear un rol vinculado a servicios para Refactorizar Espacios, consultePermisos de rol vinculado a servicios en espacios de refactor.

Si elimina este rol vinculado al servicio y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al crear recursos de entorno, aplicación, servicio o ruta de Refactor Spaces, Refactor Spaces crea de nuevo el rol vinculado al servicio.

Modificación de un rol vinculado a un servicio para Refactorizar espacios

Refactor Spaces no le permite editar el rol vinculado al servicio AWSServiceRoleForMigrationHubreFactorSpaces. Después de crear un rol vinculado a servicios, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia al mismo. Sin

embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM..

Eliminación de un rol vinculado a un servicio para Refactorizar Espacios

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a un servicio, recomendamos que elimine dicho rol. De esta forma no tiene una entidad no utilizada que no se monitorice ni mantenga de forma activa. Sin embargo, debe limpiar los recursos del rol vinculado al servicio antes de eliminarlo manualmente.

> **Note**
>
> Si el servicio Refactor Spaces utiliza el rol cuando intenta eliminar los recursos, la eliminación podría producir un error. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos de Refactor Spaces utilizados por AWSServiceRoleForMigrationHubreFactorSpaces, utilice la consola de Refactor Spaces para eliminar los recursos o utilizar las operaciones de eliminación de API de los recursos. Para obtener más información acerca de las operaciones de eliminación de la API de, consulteReferencia de la API de Refactor Spaces.

Para eliminar manualmente el rol vinculado a un servicio mediante IAM

Utilice la consola de IAM, laAWS CLI, o elAWSAPI para eliminar el rol vinculado al servicio AWSServiceRoleForMigrationHubreFatorSpaces. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Regiones admitidas para roles vinculados a servicios de Refactor Spaces

Refactor Spaces admite el uso de roles vinculados a servicios en todas las regiones en las que el servicio está disponible. Para obtener más información, consulte Regiones y puntos de enlace de AWS.

Validación de la conformidad de AWS Migration Hub Refactor Spaces

Auditores externos evalúan la seguridad y la conformidad de AWS Migration Hub Refactor Spaces en distintosAWSProgramas de conformidad. Estos incluyen SOC, PCI, FedRAMP, HIPAA y otros.

Para obtener una lista de servicios de AWS en el ámbito de programas de conformidad específicos, consulte Servicios de AWS en el ámbito del programa de conformidad. Para obtener información general, consulte Programas de conformidad de AWS.

Puede descargar los informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact.

Su responsabilidad de conformidad al utilizar Refactor Spaces se determina en función de la confidencialidad de los datos, los objetivos de conformidad de su empresa, así como de la legislación y los reglamentos aplicables.AWSproporciona los siguientes recursos para ayudar con la conformidad:

- Security and Compliance Quick Start Guides (Guías de inicio rápido de seguridad y conformidad) (Guías de inicio rápido de seguridad y conformidad): Estas guías de implementación analizan consideraciones sobre arquitectura y proporcionan los pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.
- Documento técnico sobre arquitectura para seguridad y conformidad de HIPAA : en este documento técnico, se describe cómo las empresas pueden utilizar AWS para crear aplicaciones conformes con HIPAA.
- AWSRecursos de conformidad de: este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- Evaluación de recursos con reglas en la Guía para desarrolladores de AWS Config: AWS Config evalúa en qué medida las configuraciones de sus recursos cumplen las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub CSPM: este servicio de AWS proporciona una vista integral de su estado de seguridad en AWS que lo ayuda a verificar la conformidad con los estándares y las prácticas recomendadas del sector de seguridad.

Trabajar con otros servicios de

La versión de AWS Migration Hub Refactor Spaces está en la versión preliminar y está sujeta a cambios.

En esta sección se describen otrosAWSservicios que interactúan con Refactor Spaces.

Creación de recursos de Refactor Spaces con CloudFormation

AWS Migration Hub Refactor Spaces se integra conAWS CloudFormation, un servicio que le ayuda a modelar y configurar suAWSpara que pueda dedicar menos tiempo a crear y administrar sus recursos e infraestructura. Crea una plantilla que describe todos losAWSrecursos que desea (tales como entornos, aplicaciones, servicios y rutas) yCloudFormationaprovisiona y configura dichos recursos.

Cuando utilizaCloudFormation, puede volver a utilizar la plantilla para configurar sus recursos de Refactor Spaces 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 espacios de refactor y CloudFormation

Para aprovisionar y configurar los recursos de Refactor Spaces y sus servicios relacionados, debe entenderCloudFormationPlantillas de. 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 CloudFormation. Si no está familiarizado con JSON o YAML, puede utilizar Designer de CloudFormation para comenzar a utilizar las plantillas de CloudFormation. Para obtener más información, consulte ¿Qué es Designer de CloudFormation? en la Guía del usuario de AWS CloudFormation.

Refactor Spaces admite la creación de entornos, aplicaciones, servicios y rutas enCloudFormation. Para obtener más información, incluidos ejemplos de plantillas JSON y YAML para entornos, aplicaciones, servicios y rutas, consulteAWS Migration Hub Refactorizaren laAWS CloudFormationGuía del usuario de.

Ejemplo de plantilla

En la siguiente plantilla de ejemplo se crea una nube virtual privada (VPC) y los recursos de Refactor Spaces. Cuando elige desplegar unCloudFormationplantilla para crear un entorno de refactor de demostración desde elIntroducción, la consola de Refactor Spaces implementa la siguiente plantilla.

Example Plantilla de espacios de refactor YAML

```
AWSTemplateFormatVersion: '2010-09-09'
Description: This creates resources in one account.
Resources:
  VPC:
    Type: AWS::EC2::VPC
    Properties:
      CidrBlock: 10.2.0.0/16
      Tags:
        - Key: Name
          Value: VpcForRefactorSpaces
  PrivateSubnet1:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref VPC
      AvailabilityZone: !Select [ 0, !GetAZs  '' ]
      CidrBlock: 10.2.1.0/24
      MapPublicIpOnLaunch: false
      Tags:
        - Key: Name
          Value: RefactorSpaces Private Subnet (AZ1)
  PrivateSubnet2:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref VPC
      AvailabilityZone: !Select [ 1, !GetAZs  '' ]
      CidrBlock: 10.2.2.0/24
      MapPublicIpOnLaunch: false
      Tags:
        - Key: Name
          Value: RefactorSpaces Private Subnet (AZ2)
  RefactorSpacesTestEnvironment:
    Type: AWS::RefactorSpaces::Environment
    DeletionPolicy: Delete
    Properties:
      Name: EnvWithMultiAccountServices
```

```
      NetworkFabricType: TRANSIT_GATEWAY
      Description: "This is a test environment"
  TestApplication:
    Type: AWS::RefactorSpaces::Application
    DeletionPolicy: Delete
    DependsOn:
      - PrivateSubnet1
      - PrivateSubnet2
    Properties:
      Name: proxytest
      EnvironmentIdentifier: !Ref RefactorSpacesTestEnvironment
      VpcId: !Ref VPC
      ProxyType: API_GATEWAY
      ApiGatewayProxy:
        EndpointType: "REGIONAL"
        StageName: "admintest"
  AdminAccountService:
    Type: AWS::RefactorSpaces::Service
    DeletionPolicy: Delete
    Properties:
      Name: AdminAccountService
      EnvironmentIdentifier: !Ref RefactorSpacesTestEnvironment
      ApplicationIdentifier: !GetAtt TestApplication.ApplicationIdentifier
      EndpointType: URL
      VpcId: !Ref VPC
      UrlEndpoint:
        Url: "http://aws.amazon.com"
  RefactorSpacesDefaultRoute:
    Type: AWS::RefactorSpaces::Route
    Properties:
      RouteType: "DEFAULT"
      EnvironmentIdentifier: !Ref RefactorSpacesTestEnvironment
      ApplicationIdentifier: !GetAtt TestApplication.ApplicationIdentifier
      ServiceIdentifier: !GetAtt AdminAccountService.ServiceIdentifier
  RefactorSpacesURIRoute:
    Type: AWS::RefactorSpaces::Route
    DependsOn: 'RefactorSpacesDefaultRoute'
    Properties:
      RouteType: "URI_PATH"
      EnvironmentIdentifier: !Ref RefactorSpacesTestEnvironment
      ApplicationIdentifier: !GetAtt TestApplication.ApplicationIdentifier
      ServiceIdentifier: !GetAtt AdminAccountService.ServiceIdentifier
      UriPathRoute:
        SourcePath: "/cfn-created-route"
```

```
        ActivationState: ACTIVE
        Methods: [ "GET" ]
```

Más información sobre CloudFormation

Para obtener más información acerca de CloudFormation, consulte los siguientes recursos:

- AWS CloudFormation
- Guía del usuario de AWS CloudFormation
- Referencia de la API de CloudFormation
- Guía del usuario de la interfaz de la línea de comandos de AWS CloudFormation

Registro de llamadas a la API de Refactor Spaces medianteAWS CloudTrail

AWS Migration Hub Refactor Spaces se integra conAWS CloudTrail, un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o unAWSservicio en Refactor Spaces. CloudTrail captura todas las llamadas a la API de Refactor Spaces como eventos. Las llamadas capturadas incluyen las llamadas realizadas desde la consola de Refactor Spaces y las llamadas de código realizadas a las operaciones de API de Refactor Spaces. Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos de Refactor Spaces. Si no configura un registro de seguimiento, puede ver los eventos más recientes de la consola de CloudTrail en el Event history (Historial de eventos). Mediante la información que recopila por CloudTrail, se puede determinar la solicitud que se envió a Refactor Spaces, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales.

Para obtener más información acerca de CloudTrail, consulte la Guía del usuario de AWS CloudTrail.

Refactorizar la información de los espacios de CloudTrail

CloudTrail se habilita en su cuenta de AWS cuando la crea. Cuando se produce una actividad en Refactor Spaces, esta se registra en un evento de CloudTrail junto con los demásAWSeventos de servicios enHistorial de eventos. Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte Ver eventos con el historial de eventos de CloudTrail.

Para mantener un registro continuo de los eventos deAWS, incluidos los eventos de Refactor Spaces, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. También es posible configurar otros servicios de AWS para analizar en profundidad y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- Servicios e integraciones compatibles con CloudTrail
- Configuración de notificaciones de Amazon SNS para CloudTrail
- Recepción de archivos de registro de CloudTrail de varias regiones
- Recepción de archivos de registro de CloudTrail desde varias cuentas

CloudTrail registra todas las acciones de Refactor Spaces, que se documentan enReferencia de la API de Refactor Spaces. Por ejemplo, las llamadas a las acciones `CreateEnvironment`, `GetEnvironment` y `ListEnvironments` generan entradas en los archivos de registros de CloudTrail.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario AWS Identity and Access Management (IAM) o credenciales de usuario raíz.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte el elemento userIdentity de CloudTrail.

Descripción de las entradas de archivos de registro de Refactor de

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registros en un bucket de Amazon S3 que especifique. Los archivos log de CloudTrail pueden

contener una o varias entradas de log. Un evento representa una solicitud específica realizada desde un origen y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

Uso compartido de entornos de espacios de refactor medianteAWS RAM

AWS Migration Hub Refactor Spaces se integra conAWS Resource Access Manager(AWS RAM) para habilitar el uso compartido de recursos.AWS RAMes un servicio que le permite compartir algunos recursos de Refactor Spaces con otrosCuentas de AWSo a través deAWS Organizations. Con AWS RAM, puede compartir recursos de su propiedad creando un uso compartido de recursos. Un uso compartido de recursos especifica los recursos que compartir y los consumidores con quienes compartirlos. Los consumidores pueden incluir:

- SCICCuentas de AWSdentro o fuera de su organización enAWS Organizations
- Una unidad organizativa dentro de la organización en AWS Organizations
- Toda la organización en AWS Organizations

Para obtener más información acerca de AWS RAM, consulte la Guía del usuario de AWS RAM.

Para obtener más información acerca del modo de compartir entornos de Refactor Spaces, consulte Paso 3: Comparta su entorno.

Cuotas de los espacios de AWS Migration Hub Refactor de

AWS Migration Hub Refactor Spaces se encuentra en una versión preliminar y está sujeta a cambios.

La cuenta de AWS tiene cuotas predeterminadas para cada servicio de AWS (estas cuotas anteriormente se denominaban "límites"). A menos que se indique otra cosa, cada cuota es específica de la región. Puede solicitar el aumento de algunas cuotas, pero otras no se pueden aumentar.

Para ver una lista de las cuotas de los espacios de refactor de AWS Migration Hub, consulteCuotas de servicio de Refactor Spaces.

También puede ver las cuotas de Espacios de Refactorización, abriendo laConsola de Service Quotas. En el panel de navegación, seleccioneAWSServicios dey seleccioneEspacios de AWS Migration Hub.

Para solicitar un aumento de cuota, consulte Solicitud de aumento de cuota en la Guía del usuario de Service Quotas. Si la cuota aún no se encuentra disponible en Service Quotas, utilice el formulario de aumento del límite.

Historial de revisión de la guía del usuario de Refactor Spaces

AWS Migration Hub Refactor Spaces está en la versión preliminar y está sujeta a cambios.

En la siguiente tabla se describen las versiones de la documentación de Refactor Spaces.

update-history-change	update-history-description	update-history-date
Versión inicial	Versión inicial de la guía del usuario de Refactor Spaces	29 de noviembre de 2021

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.