Guía del usuario

Recomendaciones de estrategias de Migration Hub

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Recomendaciones de estrategias de Migration Hub: Guía del usuario

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

¿Qué es el servicio Recomendaciones de estrategias de Migration Hub? ... 1
¿Es la primera vez que utiliza Recomendaciones de estrategias? ... 1
Descripción general ... 2
Servicios relacionados ... 2
Configuración ... 4
Inscríbase en un Cuenta de AWS ... 4
Creación de un usuario con acceso administrativo ... 4
Usuarios y roles de Recomendaciones de estrategias ... 6
Introducción ... 8
Requisitos previos ... 8
Paso 1: descargar el recopilador ... 10
Paso 2: implementar el recopilador ... 11
Cómo implementar el recopilador en vCenter ... 12
Cómo implementar la AMI del recopilador ... 13
Paso 3: iniciar sesión en el recopilador ... 14
Cómo iniciar sesión en el recopilador implementado en vCenter ... 14
Inicia sesión en el recopilador implementado como EC2 instancia de Amazon ... 15
Paso 4: configurar el recopilador ... 15
Configuraciones de AWS ... 16
Configuraciones de vCenter ... 18
Configuraciones de servidor remoto ... 21
Configuraciones de control de versiones ... 23
Cómo preparar sus servidores remotos para la recopilación de datos ... 24
Cómo comprobar la configuración para la recopilación de datos ... 28
Paso 5: obtener recomendaciones ... 30
Recomendaciones ... 33
Cómo ver Recomendaciones de estrategias ... 33
Recomendaciones sobre los componentes de la aplicación ... 34
Trabajo con componentes de la aplicación ... 35
Análisis del código fuente ... 37
Análisis de la base de datos ... 38
Análisis binario ... 40
Recomendaciones de servidores ... 41
Preferencias ... 42

Origen de datos ... 43
Visualización de los orígenes de datos ... 43
Recopilador de datos de aplicaciones ... 44
Datos recopilados por el recopilador ... 44
Actualización del recopilador ... 47
Importación de datos ... 48
Plantilla de importación ... 49
Cómo eliminar datos ... 54
Seguridad ... 55
Protección de los datos ... 56
Cifrado en reposo ... 57
Cifrado en tránsito ... 57
Identity and Access Management ... 57
Público ... 58
Autenticación con identidades ... 59
Administración de acceso mediante políticas ... 62
Cómo funciona el servicio Recomendaciones de estrategias de Migration Hub con IAM ... 65
AWS políticas gestionadas ... 72
Ejemplos de políticas basadas en identidades ... 78
Solución de problemas ... 83
Uso de roles vinculados a servicios ... 86
Puntos de conexión de VPC (AWS PrivateLink) ... 89
Validación de conformidad ... 91
Trabajar con otros servicios de ... 93
AWS CloudTrail ... 93
Información sobre recomendaciones de estrategia en CloudTrail ... 93
Cómo comprender las entradas del archivo de registro de Recomendaciones de estrategias ... 95
Cuotas ... 97
Notas de la versión ... 98
17 de noviembre de 2023 ... 98
12 de octubre de 2023 ... 98
17 de abril de 2023 ... 99
17 de marzo de 2023 ... 99
7 de noviembre de 2022 ... 99
27 de septiembre de 2022 ... 99

30 de junio de 2022 100
18 de abril de 2022 100
25 de febrero de 2022 100
10 de febrero de 2022 100
28 de enero de 2022 101
14 de enero de 2022 101
21 de diciembre de 2021 101
15 de diciembre de 2021 101
25 de octubre de 2021 102
Historial de documentos 103
..... cvi

¿Qué es el servicio Recomendaciones de estrategias de Migration Hub?

El servicio Recomendaciones de estrategias de Migration Hub ayuda a planificar iniciativas de migración y modernización, ya que ofrece recomendaciones de estrategias en migración y modernización para rutas de transformación viables en sus aplicaciones.

El servicio Recomendaciones de estrategias puede analizar el inventario del servidor, el entorno del tiempo de ejecución y los binarios de aplicaciones para las aplicaciones de Microsoft IIS y Java Tomcat y Jboss a fin de generar informes antipatrones. Además, puede configurar su código fuente para permitir que el servicio Recomendaciones de estrategias analice tanto el código fuente como la base de datos de todas sus aplicaciones. El servicio Recomendaciones de estrategias compara este análisis con sus objetivos empresariales y las preferencias de transformación de las aplicaciones y bases de datos que proporcionó para recomendar:

- La estrategia de migración más eficaz para cada una de sus aplicaciones.
- Herramientas o servicios de migración y modernización que puede utilizar.
- Incompatibilidades y antipatrones de aplicaciones para resolver una opción específica.

El servicio Recomendaciones de estrategias de Migration Hub recomienda estrategias de migración y modernización para volver a alojar, redefinir la plataforma y refactorizar con los destinos, herramientas y programas de implementación asociados. Para obtener información sobre cómo volver a alojar, redefinir la plataforma y refactorizar, consulte los Términos de migración: 7 R en el glosario de Recomendaciones prescriptivas de AWS .

Las recomendaciones de estrategia pueden recomendar opciones sencillas, como el realojamiento en Amazon Elastic Compute Cloud (Amazon EC2) mediante AWS Application Migration Service (AWS MGN). Las recomendaciones más optimizadas podrían incluir el cambio de plataforma a contenedores mediante AWS App2Container o la refactorización a tecnologías de código abierto como .NET Core y PostgreSQL.

¿Es la primera vez que utiliza Recomendaciones de estrategias?

De ser así, le recomendamos que comience por leer las siguientes secciones:

- Información general sobre Recomendaciones de estrategias

- Configuración de Recomendaciones de estrategias
- Introducción a Recomendaciones de estrategias

Información general sobre Recomendaciones de estrategias

Puede iniciar la evaluación de su cartera de servidores y aplicaciones mediante las recomendaciones estratégicas de Migration Hub desde la AWS Migration Hub consola. Utilice la consola para configurar y realizar una evaluación. Luego de la evaluación, puede utilizar la consola para ver los datos de evaluación de cada servidor y aplicación, junto con la herramienta de transformación recomendada.

A fin de recibir recomendaciones para refactorizar y una lista de incompatibilidades, puede utilizar Recomendaciones de estrategias para evaluar el código fuente y las bases de datos de su aplicación.

También puede descargar los datos de las recomendaciones en un archivo de Microsoft Excel.

Servicios relacionados

- AWS Migration Hub: usted utiliza la consola de AWS Migration Hub para acceder a la consola de Recomendaciones de estrategias de Migration Hub. También muestra información sobre los servidores desde los que está recopilando datos.
- AWS Application Discovery Service— Utiliza Application Discovery Service para recopilar datos sobre sus servidores y aplicaciones en la AWS Migration Hub consola antes de utilizar Strategy Recommendations.
- AWS Servicio de migración de AWS aplicaciones: el servicio de migración de aplicaciones es el principal servicio de migración recomendado para lift-and-shift las migraciones a AWS.
- AWS Database Migration Service— AWS Database Migration Service es un servicio web que puede utilizar para migrar datos de una base de datos local, de una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) o de una base de datos de una instancia de Amazon Elastic Compute Cloud (EC2Amazon) a una base de datos de un servicio. AWS
- AWS App2Container: AWS App2Container (A2C) es una herramienta de línea de comandos para modernizar las aplicaciones de.NET y Java y convertirlas en aplicaciones contenerizadas.
- Asistente de portabilidad para .NET: se utiliza para analizar el código fuente de .NET. El asistente de portabilidad para .NET es un escáner de compatibilidad que reduce el esfuerzo manual

necesario para transferir aplicaciones de Microsoft .NET Framework a .NET Core. El asistente de portabilidad para .NET evalúa el código fuente de la aplicación.NET e identifica los paquetes incompatibles y de terceros. APIs

- End-of-Support Programa de migración para Windows Server: el programa de End-of-Support migración (EMP) para Windows Server incluye herramientas para migrar las aplicaciones antiguas de Windows Server 2003, 2008 y 2008 R2 a versiones más recientes y compatibles AWS, sin necesidad de refactorizarlas.
- AWS Herramienta de conversión de esquemas: puede utilizar la herramienta de conversión de AWS esquemas (AWS SCT) para convertir el esquema de base de datos existente de un motor de base de datos a otro.
- Asistente de migración de aplicaciones web de Windows: el Asistente de migración de aplicaciones web de Windows AWS Elastic Beanstalk es una PowerShell utilidad interactiva que migra aplicaciones ASP.NET y ASP.NET Core desde servidores Windows IIS locales a Elastic Beanstalk.
- Babelfish para Aurora PostgreSQL: Babelfish para Aurora PostgreSQL es una nueva capacidad para la edición compatible de Amazon Aurora PostgreSQL que permite a Aurora comprender los comandos de las aplicaciones escritas para el servidor Microsoft SQL.

Configuración de Recomendaciones de estrategias

Antes de utilizar Recomendaciones de estrategias de Migration Hub por primera vez, realice las siguientes tareas:

Temas

- Inscríbase en un Cuenta de AWS
- Creación de un usuario con acceso administrativo
- Usuarios y roles de Recomendaciones de estrategias

Inscríbase en un Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirse a una Cuenta de AWS

1. Abrir https://portal.aws.amazon.com/billing/registro.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica o mensaje de texto e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. En cualquier momento, puede ver la actividad de su cuenta actual y administrarla accediendo a https://aws.amazon.com/y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In .

2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

   Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .

2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Inicio de sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, use la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center .

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center .

Usuarios y roles de Recomendaciones de estrategias

Le recomendamos crear dos roles para Recomendaciones de estrategias:

- Para acceder a la consola, cree un rol con `AWSMigrationHubFullAccess` y con las políticas administradas de `AWSMigrationHubStrategyConsoleFullAccess` adjuntas.
- Para acceder al recopilador de datos de la aplicación de Recomendaciones de estrategias, cree un rol con la política administrada de `AWSMigrationHubStrategyCollector` adjunta.

Las políticas administradas de IAM definen el nivel de acceso a un servicio por los usuarios. La política AWS Migration Hub `AWSMigrationHubFullAccess` gestionada otorga acceso a la consola de Migration Hub. Para obtener más información, consulte Roles y políticas de Migration Hub. Para obtener más información sobre `AWSMigrationHubStrategyConsoleFullAccess` y las políticas administradas de `AWSMigrationHubStrategyCollector`, consulte AWS políticas gestionadas para las recomendaciones estratégicas de Migration Hub.

Para proporcionar acceso, agregue permisos a sus usuarios, grupos o roles:

- Usuarios y grupos en AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center .
- Usuarios gestionados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones descritas en Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.
- Usuarios de IAM:

- Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
- (No recomendado) Adjunte una política directamente a un usuario o añada un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Introducción a Recomendaciones de estrategias

En esta sección, se describe cómo comenzar a utilizar Recomendaciones de estrategias de Migration Hub.

Temas

- Requisitos previos para Recomendaciones de estrategias
- Paso 1: descargar el recopilador de Recomendaciones de estrategias
- Paso 2: implementar el recopilador de Recomendaciones de estrategias
- Paso 3: iniciar sesión en el recopilador de Recomendaciones de estrategias
- Paso 4: configurar el recopilador de Recomendaciones de estrategias
- Paso 5: utilizar Recomendaciones de estrategias en la consola de Migration Hub para obtener recomendaciones

Requisitos previos para Recomendaciones de estrategias

A continuación, se indican los requisitos previos para utilizar Recomendaciones de estrategias de Migration Hub.

- Debe tener una o más AWS cuentas y los usuarios deben configurarlas. Para obtener más información, consulte Configuración de Recomendaciones de estrategias.
- El cliente recopilador de datos de la aplicación de Recomendaciones de estrategias debe poder recopilar los datos de forma remota desde los servidores. Esto requiere que utilice un conjunto de credenciales que funcionen para todos sus servidores Windows y un conjunto de credenciales que funcionen para todos sus servidores Linux. Las credenciales deben tener permisos para crear y eliminar directorios en los servidores.
- La versión del recopilador que se implementa en vCenter es compatible con VMware vCenter Server V6.0, V6.5, 6.7 o 7.0.

  También puedes implementar el recopilador en una EC2 instancia de Amazon mediante la AMI del recopilador.
- Compruebe que el entorno del sistema operativo (SO) sea compatible:
  - Linux

    - Amazon Linux 2012.03, 2015.03
    - Amazon Linux 2 (actualización del 25/9/2018 y posterior)
    - Ubuntu 12.04, 14.04, 16.04, 18.04, 20.04
    - Red Hat Enterprise Linux 5.11, 6.10, 7.3, 7.7, 8.1
    - CentOS 5.11, 6.9, 7.3
    - SUSE 11 SP4, 12 SP5
  - Windows
    - Windows Server 2008 R1 SP2, 2008 R2 SP1
    - Windows Server 2012 R1, 2012 R2
    - Windows Server 2016
    - Windows Server 2019
- Para el análisis del código fuente, tus repositorios GitHub y los de tu GitHub empresa deben tener un token de acceso personal con el alcance del repositorio que se pueda compartir con el cliente recopilador de Strategy Recommendations. Para obtener más información sobre cómo crear un token de acceso personal con el alcance del repositorio, consulta Cómo crear un token de acceso personal en los documentos. GitHub

  A fin de analizar los repositorios de .NET para ver las recomendaciones del Asistente de portabilidad para .NET, usted debe proporcionar una máquina Windows que esté configurada con la herramienta de evaluación de portabilidad del Asistente de portabilidad para .NET. Para obtener más información, consulte Introducción al Asistente de portabilidad para .NET en la Guía del usuario del Asistente de portabilidad para .NET.
- A fin de activar Recomendaciones de estrategias para el análisis de bases de datos, debe introducir las credenciales en AWS Secrets Manager. Para obtener más información, consulte Análisis de la base de datos de Recomendaciones de estrategias.
- Debes utilizar AWS Application Discovery Service la AWS Migration Hub consola para recopilar datos sobre tus servidores y aplicaciones antes de utilizar las recomendaciones de estrategia. Puede utilizar uno de los siguientes métodos para recopilar los datos.
  - Importación de Migration Hub: con la importación de Migration Hub, puede importar a Migration Hub información sobre sus servidores y aplicaciones en las instalaciones. Para obtener más información, consulte Importación de Migration Hub en la Guía del usuario de Application Discovery Service.
  - AWS Application Discovery Service Recopilador sin agente: el recopilador sin agente es un VMware dispositivo que recopila información sobre máquinas VMware virtuales (). VMs Para

obtener más información, consulte Recopilador sin agente en la Guía del usuario de Application Discovery Service.

- AWS Agente de detección de aplicaciones: el agente de detección es un AWS software que se instala en los servidores locales y que permite capturar la información del sistema y VMs los detalles de las conexiones de red entre los sistemas. Para obtener más información, consulte Agente de detección de aplicaciones de AWS en la Guía del usuario de Application Discovery Service.

- Recopilador de datos de recomendaciones de estrategia: si sus servidores están alojados en VMware vCenter y usted proporciona acceso, Strategy Recommendations puede recuperar automáticamente el inventario de servidores. La consola de Recomendaciones de estrategias utilizará la información recopilada para facilitar la evaluación.

> **Note**
>
> Para comprobar que la importación de Migration Hub se completó correctamente, en el panel de navegación de la consola de Migration Hub, en Detección, elija Servidores. Deberían aparecer todos los servidores importados.

Paso 1: descargar el recopilador de Recomendaciones de estrategias

El recopilador de datos de la aplicación Migration Hub Strategy Recommendations es un dispositivo virtual que puede instalar en su VMware entorno local. El recopilador de datos de la aplicación de Recomendaciones de estrategias también está disponible como Imagen de máquina de Amazon (AMI). Si desea utilizar la versión AMI del recopilador para evaluar AWS las solicitudes o por algún otro motivo, no necesita descargar el recopilador. Puede omitir esta sección e ir a Implemente el recopilador de recomendaciones de estrategia en una EC2 instancia de Amazon.

En esta sección se describe cómo descargar el archivo Open Virtualization Archive (OVA) del recopilador que se utiliza para implementar el recopilador como una máquina virtual (VM) en su VMware entorno.

Cómo descargar el archivo OVA del recopilador

1. Con la AWS cuenta que creóConfiguración de Recomendaciones de estrategias, inicie sesión en la consola de Migration Hub AWS Management Console y ábrala en https://console.aws.amazon.com/migrationhub/.
2. En el panel de navegación de la consola Migration Hub, elija Estrategias.
3. En la página Recomendaciones de estrategias de Migration Hub, elija Descargar recopilador de datos.
4. Como alternativa, puede elegir Descargar la plantilla de importación si desea importar los datos de la aplicación. Para obtener más información sobre cómo importar los datos, consulte Importación de datos en Recomendaciones de estrategias.
5. Haga clic en el botón Obtener recomendaciones y elija Aceptar para permitir que Migration Hub cree un rol vinculado a servicios (SLR) en su cuenta. La primera vez que configura Recomendaciones de estrategias debe crear el SLR. Para obtener más información, consulte Uso de roles vinculados a servicios para Recomendaciones de estrategias.

Paso 2: implementar el recopilador de Recomendaciones de estrategias

En esta sección se describe cómo implementar el recopilador de datos de aplicación de Recomendaciones de estrategias. Un recopilador de datos de aplicaciones es un recopilador de datos sin agente que identifica las aplicaciones en ejecución en los servidores, analiza el código fuente y las bases de datos.

Existen dos formas de implementar el recopilador:

- Implemente como una máquina virtual (VM) en su VMware vCenter Server. Para obtener más información, consulte Cómo implementar el recopilador de las Recomendaciones de estrategias en vCenter.
- Si tiene AWS aplicaciones que quiere evaluar, puede utilizar el recopilador de recomendaciones de estrategia Amazon Machine Image (AMI). Para obtener más información, consulte Implemente el recopilador de recomendaciones de estrategia en una EC2 instancia de Amazon.

Cómo implementar el recopilador de las Recomendaciones de estrategias en vCenter

El recopilador de datos de la aplicación Migration Hub Strategy Recommendations es un dispositivo virtual que puede instalar en su VMware entorno local. En esta sección, se describe cómo implementar el archivo recopilador Open Virtualization Archive (OVA) como una máquina virtual (VM) en su VMware entorno.

El siguiente procedimiento describe cómo implementar el recopilador de recomendaciones de estrategia en el entorno de VMware vCenter Server.

Cómo implementar el recopilador en vCenter

1. Inicie sesión en vCenter como administrador. VMware
2. Implemente el archivo OVA que descargó en el paso 1. El archivo OVA incluye el recopilador y una CLI que se puede utilizar para acceder a la API de Recomendaciones de estrategias.

   También puede descargar el archivo OVA desde el siguiente enlace:

   https://application-data-collector-release.s3.us-west-2.amazonaws.com/ova/latest/AWSMHubApplicationDataCollector.ova

Le recomendamos las siguientes especificaciones para la máquina virtual.

Especificaciones de la máquina virtual del recopilador de Recomendaciones de estrategias

- RAM: 8 GB como mínimo
- CPUs— al menos 4

> **Note**
>
> Para asegurarse de que está utilizando la última versión del recopilador con todas las nuevas características y correcciones de errores, actualice el recopilador después de implementar el archivo OVA del recopilador. Para obtener instrucciones sobre cómo actualizar, consulte Actualización del recopilador de Recomendaciones de estrategias.

Implemente el recopilador de recomendaciones de estrategia en una EC2 instancia de Amazon

Si tiene AWS aplicaciones que desee evaluar, puede utilizar el recopilador de datos de aplicaciones Amazon Machine Image (AMI) de Strategy Recommendations.

El siguiente procedimiento describe cómo lanzar una EC2 instancia de Amazon desde la AMI del recopilador.

Para implementar la EC2 instancia recopiladora de Amazon

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación de la parte superior de la pantalla, se muestra la región actual (por ejemplo, Este de EE. UU. [Ohio]). Elija una región que se adapte a sus necesidades entre las regiones que utiliza Recomendaciones de estrategias. Para obtener una lista de estas regiones, consulte los Puntos de conexión de Recomendaciones de estrategias en Referencia general de AWS.
3. En el panel de navegación, en Imágenes, selecciona AMIs.
4. Seleccione Imágenes públicas en el menú desplegable de Mi propiedad.
5. Elija la barra de búsqueda y seleccione Nombre de AMI en el menú.
6. Introduzca el nombre AWSMHubApplicationDataCollector.
7. Para asegurarse de que la AMI proviene de una fuente segura, compruebe que el propietario de la cuenta es 703163444405.
8. Para lanzar una instancia desde esta AMI, selecciónela y elija Lanzar. Para obtener más información sobre el lanzamiento de una instancia mediante la consola, consulte Lanzar la instancia desde una AMI en la Guía del EC2 usuario de Amazon.

   Recomendamos las siguientes especificaciones para la EC2 instancia de Amazon.

   Especificaciones de las EC2 instancias de Amazon del recopilador de recomendaciones estratégicas

   - RAM: 8 GB como mínimo
   - CPUs— Al menos 4

La AMI de Recomendaciones de estrategias incluye el recopilador y una CLI que se puede utilizar para acceder a la API de Recomendaciones de estrategias.

> **Note**
>
> Para asegurarse de que está utilizando la última versión del recopilador con todas las nuevas funciones y correcciones de errores, actualice el recopilador después de implementar el recopilador de recomendaciones de estrategia como una EC2 instancia de Amazon. Para obtener instrucciones sobre cómo actualizar, consulte Actualización del recopilador de Recomendaciones de estrategias.

Paso 3: iniciar sesión en el recopilador de Recomendaciones de estrategias

En esta sección, se describe cómo iniciar sesión en el recopilador de datos de la aplicación desplegada de Recomendaciones de estrategias de Migration Hub. La forma de iniciar sesión en el recopilador depende de cómo lo haya implementado.

- Cómo iniciar sesión en el recopilador implementado en el entorno basado en vCenter
- Inicia sesión en el recopilador implementado como EC2 instancia de Amazon

Cómo iniciar sesión en el recopilador implementado en el entorno basado en vCenter

Para iniciar sesión en el recopilador implementado de Recomendaciones de estrategias en el entorno basado en vCenter

1. Utilice el siguiente comando para conectarse al recopilador mediante un cliente SSH.

   ```
   ssh ec2-user@CollectorIPAddress
   ```

2. Cuando se te pida una contraseña, introduce la contraseña predeterminada aq1@ WSde3. La primera vez que inicia sesión debe cambiar la contraseña.

Inicia sesión en el recopilador implementado como EC2 instancia de Amazon

Para iniciar sesión en el recopilador de recomendaciones de estrategia implementado como una EC2 instancia de Amazon

- Utilice el siguiente comando para conectarse al recopilador mediante un cliente SSH.

  ```
  ssh -i "Keyname.pem" ec2-user@CollectorIPAddress
  ```

  Keyname.pem es la clave privada que se generó al lanzar la EC2 instancia de Amazon desde la AMI del recopilador.

Paso 4: configurar el recopilador de Recomendaciones de estrategias

En esta sección, se describe cómo utilizar los comandos `collector setup` de la línea de comandos para configurar el recopilador de datos de la aplicación de Recomendaciones de estrategias de Migration Hub. Estas configuraciones se almacenan de forma local.

Antes de poder utilizar los comandos `collector setup`, debe crear una sesión del intérprete de comandos bash en el contenedor de Docker del recopilador mediante el siguiente comando `docker exec`.

```
docker exec -it application-data-collector bash
```

El comando `collector setup` ejecuta todos los siguientes comandos de forma consecutiva, pero puedes ejecutarlos de forma individual:

- `collector setup --aws-configurations`: establecer las configuraciones de AWS .
- `collector setup --vcenter-configurations`: establecer las configuraciones de vCenter.

> **Note**
>
> La configuración de vCenter solo está disponible si el recopilador está alojado en vCenter. Sin embargo, puede forzar la configuración de vCenter mediante el comando `collector setup --vcenter-configurations`.

- `collector setup --remote-server-configurations`: establecer las configuraciones del servidor remoto.
- `collector setup --version-control-configurations`: establecer las configuraciones de control de versiones.

Para establecer todas las configuraciones del recopilador al mismo tiempo

1. Escriba el siguiente comando.

   ```
   collector setup
   ```

2. Introduzca la información de las AWS configuraciones tal y como se describe enConfigure AWS las configuraciones.
3. Ingrese la información para las configuraciones de vCenter tal y como se describe en Cómo establecer las configuraciones de vCenter.
4. Ingrese la información para las configuraciones de servidores remotos tal y como se describe en Cómo establecer las configuraciones del servidor remoto.
5. Ingrese la información para las configuraciones de control de versiones tal y como se describe en Cómo establecer las configuraciones de control de versiones.
6. Prepare sus servidores Windows y Linux para la recopilación de datos siguiendo las instrucciones que se indican en Cómo preparar sus servidores Windows y Linux remotos para la recopilación de datos.

Configure AWS las configuraciones

Para configurar AWS las configuraciones, al usar el `collector setup` comando o el `collector setup --aws-configurations` comando.

1. Ingrese S si la respuesta a la pregunta ¿Configuró los permisos de IAM...? es afirmativa. Estos permisos se configuraron al crear un usuario para acceder al recopilador mediante la política administrada de `AWSMigrationHubStrategyCollector` según los pasos que se indican en Usuarios y roles de Recomendaciones de estrategias.
2. Introduzca la clave de acceso y la clave secreta de la AWS cuenta que tiene el usuario que creó para acceder al recopilador siguiendo los pasos que se indican a continuaciónUsuarios y roles de Recomendaciones de estrategias.
3. Ingrese una región, por ejemplo, `us-west-2`. Elija una región que se adapte a sus necesidades entre las regiones que usan Recomendaciones de estrategias. Para obtener una lista de estas regiones, consulte los Puntos de conexión de Recomendaciones de estrategias en Referencia general de AWS.
4. Introduzca S si la respuesta a ¿Cargar métricas relacionadas con el recopilador al servicio de estrategias de Migration Hub? es afirmativa. La información sobre las métricas ayuda a AWS proporcionarle el soporte adecuado.
5. Introduzca S si la respuesta a la pregunta ¿Quiere cargar registros relacionados con el recopilador al servicio de estrategias de Migration Hub? es afirmativa. La información de los registros ayuda a AWS proporcionarle el soporte adecuado.

En el siguiente ejemplo, puede ver lo que se muestra, incluidas las entradas de ejemplo para las configuraciones de AWS .

```
Have you setup IAM permissions in you AWS account as per the user guide? [Y/N]: Y
Choose one of the following options for providing user credentials:
1. Long term AWS credentials
2. Temporary AWS credentials
Enter your options [1-2]: 2
AWS session token:
AWS access key ID [None]:
AWS secret access Key [None]:
AWS region name [us-west-2]:
AWS configurations are saved successfully
Upload collector related metrics to migration hub strategy service? By default
 collector will upload metrics. [Y/N]: Y
Upload collector related logs to migration hub strategy service? By default collector
 will upload logs. [Y/N]: Y
Application data collector configurations are saved successfully
Start registering application data collector
```

```
Application data collector is registered successfully.
```

Cómo establecer las configuraciones de vCenter

Para establecer las configuraciones de vCenter con los comandos `collector setup` o `collector setup --vcenter-configurations`:

1. Introduzca Y si es afirmativo en la pregunta ¿Desea autenticarse con las credenciales de VMware vCenter?, si desea autenticarse VMware con las credenciales de vCenter.

   > **Note**
   >
   > La autenticación mediante credenciales de VMware vCenter requiere VMware que las herramientas estén instaladas en los servidores de destino.

   Ingrese la URL del host, que puede ser la dirección IP o la URL de vCenter. A continuación, introduzca el nombre de usuario y la contraseña de VMware vCenter.
2. Escriba Y si es afirmativo en la pregunta ¿Tiene máquinas Windows administradas por VMware vCenter?, si desea configurar servidores Windows.

   Ingrese el nombre de usuario y la contraseña de Windows.

   > **Note**
   >
   > Si su servidor remoto de Windows pertenece a un dominio de Active Directory, debe introducir el nombre de usuario como*domain-name*\ *username* cuando utilice la CLI para proporcionar configuraciones de servidor remoto. Por ejemplo, si el nombre de su dominio es ejemplodominio y su nombre de usuario es Administrador, el nombre de usuario que introduce en la CLI es ejemplodominio\Administrador.
3. Introduzca Y como respuesta afirmativa a la pregunta Configuración para Linux mediante VMware vCenter si desea configurar servidores Linux.

   Ingrese el nombre de usuario y la contraseña de Linux.
4. Ingrese S si la respuesta a la pregunta ¿Desea configurar las credenciales para servidores externos a vCenter mediante NTLM para Windows y basadas en SSH/Cert para Linux? es

afirmativa, es decir, si desea configurar las credenciales de servidor remoto para servidores externos de vCenter.

5. En la pregunta ¿Desea utilizar las mismas credenciales de Windows que se usaron durante la configuración de vCenter?, ingrese S para indicar que las credenciales de las máquinas Windows administradas fuera de vCenter son las mismas que las credenciales proporcionadas al configurar las credenciales de las máquinas Windows con vCenter. De lo contrario, ingrese N.

   Si responde S, se formularán las siguientes preguntas.

   a. Ingrese S si la respuesta a la pregunta ¿Está de acuerdo con que el recopilador acepte y almacene localmente los certificados de servidor en su nombre durante la primera interacción con los servidores Windows? es afirmativa.

   b. Ingrese 1 para la pregunta Ingrese sus opciones si desea configurar la autenticación SSH.

      Si decide utilizar la autenticación SSH, debe copiar las credenciales de clave generadas en sus servidores Linux. Para obtener más información, consulte Configure la autenticación basada en claves en los servidores Linux.

El siguiente ejemplo muestra lo que se muestra, incluidas las entradas de ejemplo para las configuraciones de VMware vCenter.

```
Your Linux remote server configurations are saved successfully.
collector setup –vcenter-configurations
Start setting up vCenter configurations for remote execution
Note: Authenticating using VMware vCenter credentials requires VMware tools to be
 installed on the target servers
Would you like to authenticate using VMware vCenter credentials? [Y/N]: y

NOTE: Your vSphere user must have Guest Operations privileges enabled.

Host Url for VMware vCenter: domain-name
Username for VMware vCenter: username
Password for VMware vCenter: password
Reenter password for VMware vCenter: password
Successfully stored vCenter credentials...
Do you have Windows machines managed by VMware vCenter? [Y/N]: y

NOTE: For the best experience, we recommend that you create a new Active Directory user
 in the Domain Admins group.
```

```
Username for Windows (Domain\User): username
Password for Windows: password
Reenter password for Windows: password
Successfully stored windows credentials...
You can verify your setup for vCenter windows machines is correct with "collector diag-
check"
Do you have Linux machines managed by VMWare vCenter? [Y/N]: y
Username for Linux: username
Password for Linux: password
Reenter password for Linux: password
Successfully stored linux credentials...
You can verify your setup for vCenter linux machines is correct with "collector diag-
check"
Would you like to setup credentials for servers not managed by vCenter using NTLM for
 windows and SSH/Cert based for Linux? [Y/N]: y
Setting up target server for remote execution:
Would you like to setup credentials for servers not managed by vCenter using NLTM for
 Windows [Y/N]: y
Would you like to use the same Windows credentials used during vCenter setup? [Y/N]: y
Are you okay with collector accepting and locally storing server certificates on your
 behalf during first interaction with windows servers? These certificates will be used
 by collector for secure communication with windows servers [Y/N]: y
Successfully stored windows server credentials...
Please note that all windows server certificates are stored in directory /opt/amazon/
application-data-collector/remote-auth/windows/certs

Please note the IP address of the collector and run the script specified in the user
 documentation on all the windows servers in your inventory
You can verify your setup for remote windows machines is correct with "collector diag-
check"
Would you like to setup credentials for servers not managed by vCenter using SSH/Cert
 based for Linux? [Y/N]: y
Choose one of the following options for remote authentication:
1. SSH based authentication
2. Certificate based authentication
Enter your options [1-2]: 1
Would you like to use the same Linux credentials used during vCenter setup? [Y/N]: y
Generating SSH key on this machine...
Successfully generated SSH key pair

SSH key pair path: /opt/amazon/application-data-collector/remote-auth/linux/keys/
id_rsa_assessment
```

```
Please add the public key "id_rsa_assessment.pub" to the "$HOME/.ssh/authorized_keys"
 file in your remote machines.
You can verify your setup for remote linux machines is correct with "collector diag-
check
```

Cómo establecer las configuraciones del servidor remoto

Para configurar los servidores remotos con los comandos `collector setup` y `collector setup --remote-server-configurations`:

1. Ingrese S si la respuesta a la pregunta ¿Desea configurar las credenciales para servidores no administrados por vCenter mediante NLTM para Windows? es afirmativa y si desea configurar servidores Windows.

   Ingrese el nombre de usuario y la contraseña de WinRM.

   > **Note**
   >
   > Si su servidor remoto de Windows pertenece a un dominio de Active Directory, debe introducir el nombre de usuario como*domain-name*\ *username* cuando utilice la CLI para proporcionar configuraciones de servidor remoto. Por ejemplo, si el nombre de su dominio es ejemplodominio y su nombre de usuario es Administrador, el nombre de usuario que introduce en la CLI es ejemplodominio\Administrador.

   Ingrese S si la respuesta a la pregunta ¿Está de acuerdo con que el recopilador acepte y almacene localmente los certificados de servidor en nombre de usted durante la primera interacción con los servidores de Windows? es afirmativa. Los certificados de Windows Server se almacenan en el directorio `/opt/amazon/application-data-collector/remote-auth/windows/certs`.

   Debe copiar las credenciales de servidor generadas en sus servidores Windows. Para obtener más información, consulte Cómo establecer la configuración del servidor remoto en los servidores Windows.

2. Ingrese S si la respuesta a la pregunta ¿Configuración para Linux mediante SSH o Cert? es afirmativa, es decir, si desea configurar servidores Linux.

3. Ingrese 1 para la pregunta Ingrese sus opciones si desea configurar la autenticación basada en claves SSH.

Si decide utilizar la autenticación SSH, debe copiar las credenciales clave generadas en sus servidores Linux. Para obtener más información, consulte Configure la autenticación basada en claves en los servidores Linux.

4. Ingrese 2 para la pregunta Ingrese sus opciones si desea configurar la autenticación basada en certificados.

   Para obtener información acerca de la autenticación basada en certificados, consulte Configuración de la autenticación basada en certificados en servidores Linux.

En el siguiente ejemplo, puede ver lo que se muestra, incluidas las entradas de ejemplo para las configuraciones del servidor remoto.

```
Setting up target server for remote execution
Would you like to setup credentials for servers not managed by vCenter using NLTM for
 Windows [Y/N]: y

NOTE: For the best experience, we recommend that you create a new Active Directory user
 in the Domain Admins group.

Username for WinRM (Domain\User): username
Password for WinRM: password
Reenter password for WinRM: password
Are you okay with collector accepting and locally storing server certificates on your
 behalf during first interaction with windows servers? These certificates will be used
 by collector for secure communication with windows servers [Y/N]: Y
Successfully stored windows server credentials...
Please note that all windows server certificates are stored in directory /opt/amazon/
application-data-collector/remote-auth/windows/certs

Please note the IP address of the collector and run the script specified in the user
 documentation on all the windows servers in your inventory
Would you like to setup credentials for servers not managed by vCenter using SSH/Cert
 based for Linux? [Y/N]: Y
Choose one of the following options for remote authentication:
1. SSH based authentication
2. Certificate based authentication
Enter your options [1-2]: 1
User name for remote server: username
Generating SSH key on this machine...
```

```
SSH key pair path: /opt/amazon/application-data-collector/remote-auth/linux/keys/
id_rsa_assessment
Please add the public key "id_rsa_assessment.pub" to the "$HOME/.ssh/authorized_keys"
 file in your remote machines.
Your Linux remote server configurations are saved successfully.
```

Cómo establecer las configuraciones de control de versiones

Para establecer las configuraciones de control de versiones con los comandos `collector setup` o `collector setup --version-control-configurations`:

1. Ingrese S si la respuesta a la pregunta¿Configurar análisis del código fuente? es afirmativa.
2. Ingrese 1 para la pregunta Ingrese sus opciones si desea configurar el punto de conexión del servidor Git.

   Ingrese github.com para el punto de conexión del servidor GIT.
3. Introduzca 2 para la pregunta Introduzca sus opciones si desea configurar un servidor GitHub empresarial.

   Introduzca el punto final empresarial sin https://, de la siguiente manera: punto final del servidor GIT: *`git-enterprise-endpoint`*
4. Introduce tu Git *`username`* y tu acceso personal*`token`*.
5. Ingrese S si la respuesta a la pregunta¿Tiene algún repositorio de csharp que deba analizarse en un equipo Windows? es afirmativa y si desea analizar el código de C#.

   > **Note**
   >
   > Para analizar los repositorios de .NET con las recomendaciones del Asistente de portabilidad para .NET, debe proporcionar un equipo Windows que esté configurado con la herramienta de evaluación de portabilidad Asistente de portabilidad para .NET. Para obtener más información, consulte Introducción al Asistente de portabilidad para .NET en la Guía del usuario del Asistente de portabilidad para .NET.
6. Para la pregunta¿Desea reutilizar las credenciales de Windows existentes en este equipo?. Ingrese S si la máquina Windows para el análisis del código fuente de C# utiliza las mismas credenciales que las credenciales proporcionadas anteriormente como parte de la configuración `--remote-server-configurations` o `--vcenter-configurations`.

Ingrese N si desea introducir nuevas credenciales.

7. Para usar las credenciales de máquina Windows de VMWare vCenter, escriba 1 en Elija una de las siguientes opciones para las credenciales de Windows.
8. Ingrese la dirección IP del equipo Windows.

En el siguiente ejemplo, puede ver lo que se muestra, incluidas las entradas de ejemplo para las configuraciones del control de versiones.

```
Set up for source code analysis [Y/N]: y
Choose one of the following options for version control type:
1. GIT
2. GIT Enterprise
3. Azure DevOps - Git
Enter your options [1-3]: 3
Your server endpoint: dev.azure.com (http://dev.azure.com/)
Your DevOps Organization name: <Your organization name>
Personal access token [None]:
Your version control credentials are saved successfully.
Do you have any csharp repositories that should be analyzed on a windows machine? [Y/
N]: y
Would you like to reuse existing windows credentials on this machine? [Y/N]: y
Choose one of the following options for windows credentials:
1. VMWare vCenter Windows Machine
2. Standard Windows Machine
Enter your options [1-2]:
1
Windows machine IP Address: <Your windows machine IP address>
Using VMWare vCenter Windows Machine credentials
Successfully stored windows server credentials...
```

Cómo preparar sus servidores Windows y Linux remotos para la recopilación de datos

> **Note**
>
> Este paso no es necesario si configura el recopilador de datos de la aplicación de Recomendaciones de estrategias con credenciales de vCenter.

Después de establecer las configuraciones de los servidores remotos, si utiliza los comandos `collector setup command` o `collector setup --remote-server-configurations`, debe preparar los servidores remotos para que el recopilador de datos de la aplicación de Recomendaciones de estrategias pueda recopilar datos de ellos.

> **Note**
>
> Debe asegurarse de que se pueda acceder a los servidores mediante su dirección IP privada. Para obtener más instrucciones sobre cómo configurar el entorno a través de una nube privada virtual (VPC) AWS para su ejecución remota, consulte la Guía del usuario de Amazon Virtual Private Cloud.

Para preparar sus servidores Linux remotos, consulte Cómo preparar servidores Linux remotos.

Para preparar los servidores Windows remotos, consulte Cómo establecer la configuración del servidor remoto en los servidores Windows.

Cómo preparar servidores Linux remotos

Configure la autenticación basada en claves en los servidores Linux

Si decide configurar la autenticación basada en claves SSH para Linux al establecer las configuraciones de servidores remotos, debe cumplir con los siguientes pasos para configurar la autenticación basada en claves en sus servidores, de modo que el recopilador de datos de la aplicación de Recomendaciones de estrategias pueda recopilar datos.

Cómo configurar la autenticación basada en claves en sus servidores Linux

1. Copie la clave pública generada con el nombre id_rsa_assessment.pub de la siguiente carpeta del contenedor:

   /opt/amazon/application-data-collector/remote-auth/linux/keys.

2. Agregue la clave pública copiada en el archivo `$HOME/.ssh/authorized_keys` para todos los equipos remotos. Si no hay ningún archivo disponible, lo genera con los comandos `touch` o `vim`.
3. Asegúrese de que la carpeta principal del servidor remoto tenga un nivel de permisos `755` o inferior. Si tiene `777`, no funcionará. Puede usar el comando `chmod` para restringir los permisos.

Configuración de la autenticación basada en certificados en servidores Linux

Si decide configurar la autenticación basada en certificados para Linux al establecer las configuraciones de servidores remotos, debe cumplir con los siguientes pasos para que el recopilador de datos de la aplicación de Recomendaciones de estrategias pueda recopilar los datos.

Recomendamos esta opción si ya tiene Certificate Authority (CA) para sus servidores de aplicaciones.

Cómo configurar la autenticación basada en certificados en sus servidores Linux

1. Copie el nombre de usuario que funciona con todos sus servidores remotos.
2. Copie la clave pública del recopilador en CA.

   La clave pública del recopilador se encuentra en la siguiente ubicación:

   /_rsa_assessment.pub opt/amazon/application-data-collector/remote-auth/linux/keys/id

   Esta clave pública debe agregarse a su CA para generar el certificado.
3. Copie el certificado generado en el paso anterior en la siguiente ubicación del recopilador:

   /opt/amazon/application-data-collector/remote-auth/linux/keys

   El nombre del certificado debe ser id_rsa_assessment-cert.pub.
4. Proporcione el nombre del archivo del certificado durante el paso de configuración.

Cómo establecer la configuración del servidor remoto en los servidores Windows

Si decide instalar Windows al configurar los servidores remotos en la configuración del recopilador, debe realizar los siguientes pasos para que el servicio Recomendaciones de estrategias pueda recopilar los datos.

> Para obtener más información sobre el PowerShell script que se ejecuta en el servidor remoto, lea esta nota.
>
> El script habilita la autenticación PowerShell remota e inhabilita todos los métodos de autenticación distintos de la negociación. Se utiliza para el administrador LAN de Windows NT (NTLM) y establece el WSMan protocolo «AllowUnencrypted» en false para garantizar que el oyente recién creado acepte únicamente el tráfico cifrado. Con el script de Microsoft, `New-SelfSignedCertificateEx.ps1`, crea un certificado autofirmado.

Cualquier WSMan instancia que tenga un agente de escucha HTTP se elimina junto con los agentes de escucha HTTPS existentes. Luego, crea un nuevo oyente HTTPS. También crea una regla de firewall entrante para el puerto TCP 5986. En el último paso, se reinicia el servicio WinRM.

Para configurar la recopilación de datos mediante una conexión remota en sus servidores de Windows 2008

1. Usa el siguiente comando para comprobar la versión de PowerShell instalada en tu servidor.

   ```
   $PSVersionTable
   ```

2. Si la PowerShell versión no es 5.1, descargue e instale WMF 5.1 siguiendo las instrucciones de Instalación y configuración de WMF 5.1 en la documentación de Microsoft.
3. Utilice el siguiente comando en una PowerShell ventana nueva para asegurarse de que PowerShell 5.1 está instalado.

   ```
   $PSVersionTable
   ```

4. Siga estos pasos que describen cómo configurar la recopilación de datos a través de una conexión remota en Windows 2012 y versiones posteriores.

Para configurar la recopilación de datos mediante una conexión remota en sus servidores Windows 2012 y versiones más recientes

1. Descargue el script de configuración desde una de las siguientes URL:

   https://application-data-collector-release.s3.us-west-2.amazonaws.com/scripts/WinRMSetup .ps1

2. Descargue `New-SelfSignedCertificateEx.ps1` desde la siguiente URL y pegue el script en la misma carpeta en la que descargó `WinRMSetup.ps1`:

   https://github.com/Azure/azure-libraries-for-net/- .ps1 blob/master/Samples/Asset/NewSelfSignedCertificateEx

3. Para completar la configuración, ejecute el PowerShell script descargado en todos los servidores de aplicaciones.

```
.\WinRMSetup.ps1
```

> **Note**
>
> Si la administración remota de Windows (WinRM) no está configurada correctamente en el servidor remoto de Windows, se producirá un error al intentar recopilar datos de ese servidor. Si esto ocurre, debe eliminar el certificado correspondiente a ese servidor de la siguiente ubicación del contenedor: /opt/amazon/application-data-collector/remote-auth/windows/certs/***ads-server-id***.cer Tras eliminar el certificado, espere a que se vuelva a intentar el proceso de recopilación de datos.

Compruebe que el recopilador y los servidores estén configurados para la recopilación de datos

Compruebe que el recopilador y los servidores estén correctamente configurados para la recopilación de datos mediante el siguiente comando.

```
collector diag-check
```

Este comando realiza una serie de comprobaciones de diagnóstico en las configuraciones del servidor y proporciona información sobre las comprobaciones fallidas.

Cuando utiliza el comando en `-a` modo, obtiene el resultado en un DiagnosticCheckResultarchivo.txt una vez finalizadas las comprobaciones.

```
collector diag-check -a
```

Puede realizar una comprobación de diagnóstico en las configuraciones del servidor de un único servidor con la dirección IP del mismo.

Los siguientes ejemplos muestran el resultado de una configuración correcta.

Servidor Linux

```
            Provide your test server IP address: IP address
-----------------------------------------------------------------
Start checking connectivity & credentials...
Connectivity and Credential Checks succeeded
-----------------------------------------------------------------
Start checking permissions...
Permission Check succeeded
-----------------------------------------------------------------
Start checking OS version...
OS version check succeeded
-----------------------------------------------------------------
Start checking Linux Bash installation...
Linux Bash installation check succeeded
-----------------------------------------------------------------
All diagnostic checks complete successfully.
This server is correctly set up and ready for data collection.
```

Servidor Windows

```
            Windows PowerShell Version Check succeeded
Provide your test server IP address: IP address
-----------------------------------------------------------------
Start checking connectivity & credentials...
Connectivity and Credential Checks succeeded
-----------------------------------------------------------------
Start checking permissions...
Permission Check succeeded
-----------------------------------------------------------------
Start checking OS version...
OS version check succeeded
-----------------------------------------------------------------
Start checking Windows architecture type...
Windows Architecture Type Check succeeded
-----------------------------------------------------------------
All diagnostic checks complete successfully.
This server is correctly set up and ready for data collection.
```

En el siguiente ejemplo, se muestra un mensaje de error que aparece cuando sus credenciales de servidor remoto son incorrectas.

```
Unable to authenticate the server credentials with IP address ${IPAddress}.
Ensure that your credentials are accurate and the server is configured correctly.
Use the following command to reset incorrect credentials.
collector setup –remote-server-configurations
```

Paso 5: utilizar Recomendaciones de estrategias en la consola de Migration Hub para obtener recomendaciones

En esta sección se describe cómo utilizar Recomendaciones de estrategias en la consola de Migration Hub para obtener recomendaciones de migración por primera vez.

Cómo obtener recomendaciones

1. Con la AWS cuenta que creóConfiguración de Recomendaciones de estrategias, inicie sesión en la consola de Migration Hub AWS Management Console y ábrala en https://console.aws.amazon.com/migrationhub/.
2. En el panel de navegación de la consola de Migration Hub, elija Estrategias.
3. En la página Recomendaciones de estrategias de Migration Hub, elija Obtener recomendaciones.
4. Elija Aceptar si quiere permitir que Migration Hub cree un rol vinculado a servicios (SLR) en su cuenta. Para obtener más información sobre el SLR, consulte Uso de roles vinculados a servicios para Recomendaciones de estrategias.
5. Configuración de orígenes de datos
   a. En la página Configuración de orígenes de datos, debe elegir el origen de sus servidores para analizar entre las siguientes opciones:
      i. Recopilador de datos de la aplicación Strategy Recommendations: puede utilizar el recopilador de recomendaciones de estrategia para recuperar automáticamente la información sobre la información VMs alojada en VMware vCenter. Con esta opción, no necesita realizar una configuración adicional.
      ii. Importación manual: si desea introducir los datos sobre sus servidores y aplicaciones de forma independiente, puede utilizar la plantilla de importación de Recomendaciones de estrategias. La plantilla de importación es un archivo JSON en el que puede rellenar la información disponible para su VMs.

iii. Application Discovery Service: puede utilizar Application Discovery Service para recopilar información sobre sus aplicaciones y servidores en las instalaciones. En la consola de Migration Hub, en la sección Herramientas, puede elegir entre varias opciones en Herramientas de detección. Por ejemplo, puede elegir Recopilador sin agente de Application Discovery Service, Agente de detección de AWS o Importar (para archivos CSV).

b. En la tabla Servidores, se muestran todos los servidores disponibles en función de su elección en la sección de origen de datos.

c. En Recopiladores de datos de aplicaciones registradas, aparecen los recopiladores de datos de aplicaciones que configuró. Si no configuró ningún recopilador de datos, puede descargar el recopilador de datos y, a continuación, implementarlo. Para obtener más información, consulte Paso 1: descargar el recopilador de Recomendaciones de estrategias y Paso 2: implementar el recopilador de Recomendaciones de estrategias.

> **Note**
>
> Para obtener recomendaciones de estrategias, debe configurar al menos un recopilador de datos de aplicaciones o realizar una importación de datos de aplicaciones. Si desea agregar los datos a nivel de aplicación sin configurar un recopilador, puede utilizar la plantilla de importación de datos de la aplicación. Puede agregar orígenes de datos adicionales más adelante.

d. Si seleccionó Importación manual en Detalles de importación, elija Agregar nueva importación.

e. En Nombre de importación, ingrese un nombre para su importación.

f. Para el URI del bucket de S3, introduzca el URI del bucket de S3 en el que se va a cargar el archivo JSON de importación.

> **Important**
>
> El nombre del bucket de S3 debe comenzar con el prefijo **`migrationhub-strategy`**.

g. Elija Next (Siguiente).

6. Especificación de preferencias

a. En la página Especificación de preferencias, configure sus objetivos empresariales y las preferencias de migración. El servicio de Recomendaciones de estrategias recomienda la estrategia óptima para migrar y modernizar sus aplicaciones y bases de datos en función de las preferencias que especifique. Puede cambiar estas preferencias luego.

b. Elija Next (Siguiente).

7. Revisar y enviar.

a. Revise los orígenes de datos configurados y las preferencias de migración.

b. Si todo parece correcto, elija Iniciar análisis de datos. Esto realizará un análisis del inventario de su servidor y del entorno del tiempo de ejecución, así como de los binarios de aplicaciones para sus aplicaciones de Microsoft IIS y Java.

> **Note**
>
> El estado del análisis binario no se muestra en la consola. Cuando se complete el análisis, verá un enlace al informe antipatrón o un mensaje que indica que el análisis no se realizó correctamente.

Recomendaciones de estrategias

En esta sección, se describe cómo ver las recomendaciones de migración y modernización de Recomendaciones de estrategias para los servidores y las aplicaciones en su cartera de migración.

Temas

- Cómo ver recomendaciones de estrategias en Recomendaciones de estrategias
- Recomendaciones sobre los componentes de la aplicación de Recomendaciones de estrategias
- Recomendaciones de estrategias: recomendaciones del servidor
- Preferencias del servicio Recomendaciones de estrategias

Cómo ver recomendaciones de estrategias en Recomendaciones de estrategias

En esta sección se describe cómo utilizar las recomendaciones de estrategia en la AWS Migration Hub consola para ver las recomendaciones de estrategias de migración.

Cómo ver Recomendaciones de estrategias

1. Con la AWS cuenta que creóConfiguración de Recomendaciones de estrategias, inicie sesión en la consola de Migration Hub AWS Management Console y ábrala en https://console.aws.amazon.com/migrationhub/.
2. En el panel de navegación de la consola de Migration Hub, elija Estrategias y, a continuación, elija Recomendaciones.
3. En la página Recomendaciones, puede ver y exportar las recomendaciones resumidas de su cartera y las recomendaciones detalladas de la estrategia “R” de migración. También puede ver las herramientas y los destinos de migración y modernización, así como los antipatrones de sus servidores y componentes de aplicaciones.

   Los antipatrones son una lista de problemas conocidos que se encuentran en su cartera y que se clasifican según su gravedad. Los antipatrones de gravedad alta representan incompatibilidades que deben resolverse, los antipatrones de gravedad media representan advertencias y los antipatrones de gravedad baja representan problemas informativos. Para obtener información sobre la estrategia “R”, consulte Términos de migración: 7 R en el glosario de Recomendaciones prescriptivas de AWS .

- Si se produce un cambio en su centro de datos o si actualizan sus preferencias, le recomendamos que vuelva a analizar los datos. Para volver a analizar los datos y obtener nuevas recomendaciones, seleccione Reanalizar los datos.

  Hasta que se complete el proceso de reanálisis, los resultados de los datos recomendados pueden ser una combinación de datos anteriores y datos nuevos.

  Para descargar un informe con las recomendaciones, seleccione Exportar recomendaciones.

4. En la pestaña Componentes de la aplicación, puede ver las recomendaciones para los componentes de la aplicación de su cartera de migración. Para obtener más información, consulte Recomendaciones sobre los componentes de la aplicación de Recomendaciones de estrategias.
5. En la pestaña Servidores, puede ver las recomendaciones para los servidores de su cartera de migración. Para obtener más información, consulte Recomendaciones de estrategias: recomendaciones del servidor.
6. En la pestaña Preferencias, puede editar las preferencias que especificó en Paso 5: obtener recomendaciones. Para obtener información sobre cómo editar sus preferencias, consulte Preferencias del servicio Recomendaciones de estrategias.

Recomendaciones sobre los componentes de la aplicación de Recomendaciones de estrategias

En esta sección, se describe cómo usar Recomendaciones de estrategias en la consola de Migration Hub para ver y analizar las recomendaciones de estrategias de migración para los componentes de la aplicación.

Temas

- Cómo trabajar con los componentes de la aplicación en Recomendaciones de estrategias
- Recomendaciones de estrategias y análisis del código fuente
- Análisis de la base de datos de Recomendaciones de estrategias
- Recomendaciones de estrategias: análisis binario

Cómo trabajar con los componentes de la aplicación en Recomendaciones de estrategias

En esta sección, se describe cómo usar Recomendaciones de estrategias de Migration Hub en la consola de Migration Hub para ver y configurar las recomendaciones de estrategias de migración y modernización.

Temas

- Visualización de las recomendaciones sobre componentes de la aplicación
- Configuración del análisis del código fuente para un componente de la aplicación
- Configuración del análisis de la base de datos para un componente de la aplicación

Visualización de las recomendaciones sobre componentes de la aplicación

En esta sección, se describe cómo usar Recomendaciones de estrategias en la consola de Migration Hub para ver las recomendaciones de estrategias de migración para los componentes de la aplicación.

Cómo ver los detalles de las recomendaciones para los componentes de la aplicación

1. Con la AWS cuenta que creóConfiguración de Recomendaciones de estrategias, inicie sesión en la consola de Migration Hub AWS Management Console y ábrala en https://console.aws.amazon.com/migrationhub/.
2. En el panel de navegación de la consola de Migration Hub, elija Estrategias y, a continuación, elija Recomendaciones.
3. En la página Recomendaciones, seleccione la pestaña Componentes de la aplicación.
    a. En Resumen de los componentes de la aplicación, encontrará una descripción general de los distintos tipos de componentes de la aplicación que ejecuta en su cartera de servidores.
    b. En Componentes de la aplicación, puede ver el nombre del componente, el tipo de componente y las recomendaciones de estrategia “R” de migración. También puede ver el destino de la migración y las herramientas de migración y modernización que se van a utilizar para los distintos componentes de la aplicación que se ejecutan en su cartera de servidores. Para obtener información sobre la estrategia “R”, consulte Términos de migración: 7 R en el glosario de Recomendaciones prescriptivas de AWS .

4. Para ver los detalles de un componente de la aplicación, seleccione un componente de la aplicación y, a continuación, elija Ver detalles.
5. En la página de detalles del componente de la aplicación (la página con el nombre del componente como encabezado), en el apartado Resumen de las recomendaciones, puede ver Recomendaciones para el componente de la aplicación. También puede ver los antipatrones identificados. Los antipatrones son una lista de problemas conocidos que se encuentran en su cartera y que se clasifican según su gravedad.
6. Seleccione la pestaña Opciones de estrategia a fin de ver la recomendación de migración para el componente de la aplicación. Para anular la estrategia recomendada, seleccione una estrategia diferente y, a continuación, elija Establecer como preferida.
7. Según el tipo de componente de la aplicación que esté viendo, hay una pestaña Configuración de origen o Configuración de la base de datos. Para obtener más información sobre Configuración de origen, consulte Configuración del análisis del código fuente para un componente de la aplicación. Para obtener más información sobre Configuración de la base de datos, consulte Configuración del análisis de la base de datos para un componente de la aplicación.

Configuración del análisis del código fuente para un componente de la aplicación

En esta sección, se describe cómo usar Recomendaciones de estrategias en la consola de Migration Hub para configurar el análisis del código fuente de un componente de la aplicación.

Para configurar el análisis de código fuente de un componente de la aplicación

1. En el panel de navegación de la consola de Migration Hub, elija Estrategias y, a continuación, elija Recomendaciones.
2. En la página Recomendaciones, elija la pestaña Componentes de la aplicación.
3. En la lista de componentes de la sección Componentes de la aplicación, seleccione un componente de la aplicación con un tipo de componente java, dotnetframework o IIS y después elija Ver detalles.
4. En la página de detalles del componente de la aplicación (la página que tiene como encabezado el nombre del componente), seleccione la pestaña Configuración del código fuente.
5. En Detalles de configuración del código fuente, elija Analizar código fuente.
6. En la página Analizar código fuente, proporcione el nombre del repositorio, el nombre de la rama y el nombre del proyecto (si corresponde) donde se almacena el código fuente del componente

de la aplicación. Seleccione el tipo de control de versiones del código GitHub fuente que quiere usar y, a continuación, elija Analizar.

Una vez finalizado el análisis, puede ver las recomendaciones actualizadas en la página de detalles de los componentes de la aplicación.

Para obtener más información sobre el análisis del código fuente, consulte Recomendaciones de estrategias y análisis del código fuente.

Configuración del análisis de la base de datos para un componente de la aplicación

En esta sección, se describe cómo usar Recomendaciones de estrategias en la consola de Migration Hub para configurar el análisis de la base de datos de un componente de la aplicación.

Cómo configurar el análisis de la base de datos de un componente de la aplicación

1. En el panel de navegación de la consola de Migration Hub, elija Estrategias y, a continuación, elija Recomendaciones.
2. En la página Recomendaciones, elija la pestaña Componentes de la aplicación.
3. En la lista de componentes de la sección Componentes de la aplicación, seleccione un componente de la aplicación con el tipo de componente SQLServery, a continuación, elija Ver detalles.
4. En la página de detalles del componente de la aplicación (la página que tiene como encabezado el nombre del componente), elija la pestaña Configuración de la base de datos.
5. En Detalles de configuración de la base de datos, elija Analizar los detalles de la base de datos.
6. Elija un nombre secreto en el menú desplegable que creó en AWS Secrets Manager para usarlo como credenciales de base de datos y, a continuación, elija Analizar.

   Una vez finalizado el análisis, podrá ver las recomendaciones actualizadas en la página de detalles de los componentes de la aplicación.

Para obtener más información sobre el análisis de bases de datos y la configuración de un nombre secreto, consulte Análisis de la base de datos de Recomendaciones de estrategias.

Recomendaciones de estrategias y análisis del código fuente

El servicio Recomendaciones de estrategias de Migration Hub identifica automáticamente las aplicaciones en su cartera y crea componentes de la aplicación para ellas. Por ejemplo, si hay una

aplicación Java en su cartera, se identifica como un componente de la aplicación con un tipo de componente java.

Si así lo configura, el servicio Recomendaciones de estrategias analiza el código fuente de los componentes de la aplicación. Para obtener información sobre la configuración de un componente de la aplicación para el análisis del código fuente, consulte Configuración del análisis del código fuente para un componente de la aplicación.

El servicio Recomendaciones de estrategias realiza un análisis del código fuente para los lenguajes de programación Java y C#.

A fin de obtener información sobre los requisitos previos para utilizar el análisis del código fuente de Recomendaciones de estrategias, consulte. Requisitos previos para Recomendaciones de estrategias

Análisis de la base de datos de Recomendaciones de estrategias

El servicio Recomendaciones de estrategias identifica automáticamente los servidores de la base de datos de su cartera y crea componentes de la aplicación para ellos. Por ejemplo, si hay una base de datos de SQL Server en su cartera, se identifica como el componente de aplicación sqlservr.exe.

Strategy Recommendations analiza las bases de datos individuales del componente de aplicación de SQL Server identificado, sqlservr.exe, mediante la herramienta AWS Schema Conversion Tool. Strategy Recommendations también identifica las incompatibilidades al migrar las bases de datos a AWS bases de datos como Amazon Aurora MySQL Compatible Edition, Amazon Aurora PostgreSQL Compatible Edition, Amazon RDS for MySQL y Amazon RDS for PostgreSQL.

En la actualidad, el análisis de la base de datos de Recomendaciones de estrategias solo está disponible para SQL Server.

A fin de configurar Recomendaciones de estrategias para analizar sus bases de datos, debe proporcionar las credenciales para que el recopilador de datos de la aplicación de Recomendaciones de estrategias se conecte a sus bases de datos. Para ello, crea un secreto en AWS Secrets Manager en tu AWS cuenta.

Para obtener información sobre los permisos y privilegios de las credenciales que proporcione, consulte Privilegios necesarios para las credenciales AWS de Schema Conversion Tool. Para obtener información sobre cómo generar una clave con las credenciales, consulte Creación de una clave en Secrets Manager para las credenciales de las bases de datos.

Tras configurar las credenciales y el secreto, puede configurar el análisis de AWS Schema Conversion Tool en el servidor de base de datos. Para obtener más información, consulte Configuración del análisis de la base de datos para un componente de la aplicación.

Tras configurar el análisis de la base de datos para el componente de la aplicación, se programa una tarea de inventario de la AWS Schema Conversion Tool. Una vez completada esta tarea, usted verá cómo se crean los nuevos componentes de la aplicación para cada base de datos individual de ese servidor de base de datos. Por ejemplo, si su SQL Server tiene dos bases de datos (exampledbs1 y exampledbs2), se crea un componente de la aplicación para cada una de las bases de datos con los nombres exampledbs1 y exampledbs2.

Si desea antipatrones a la hora de migrar cada base de datos identificada a las bases de datos de AWS , configure el análisis para cada base de datos siguiendo los pasos que se indican a continuación en Configuración del análisis de la base de datos para un componente de la aplicación.

Privilegios necesarios para las credenciales AWS de Schema Conversion Tool

Las credenciales de inicio de sesión que proporciones a AWS Secrets Manager solo necesitan `VIEW SERVER STATE` y tienen `VIEW ANY DEFINITION` privilegios.

Puede brindar el nombre de inicio de sesión y la contraseña que quiera al crear el inicio de sesión de SQL Server.

Creación de una clave en Secrets Manager para las credenciales de las bases de datos

Cuando las credenciales estén listas para que el recopilador de datos de la aplicación Strategy Recommendations se conecte a una base de datos, cree un secreto en AWS Secrets Manager en su AWS cuenta, tal y como se describe en el siguiente procedimiento.

Para crear un secreto con AWS Secrets Manager en tu AWS cuenta

1. Con la AWS cuenta en la que creóConfiguración de Recomendaciones de estrategias, inicie sesión en la consola de AWS Secrets Manager AWS Management Console y ábrala en https://console.aws.amazon.com/secretsmanager/.
2. Elija Almacenar un nuevo secreto.
3. Seleccione el tipo de secreto como Otro tipo de secreto.
4. En Pares clave/valor, escriba lo siguiente:

nombre de usuario - *your-username*

Luego, elija + Agregar regla e ingrese la siguiente información.

contraseña - *your-password*

5. Elija Siguiente.
6. Introduzca el nombre secreto como cualquier cadena con el prefijo migrationhub-strategy-. Por ejemplo, migrationhub-strategy-one.

> **Note**
> Guarde su nombre secreto en un lugar seguro para usarlo más adelante.

7. Elija Siguiente y después elija Siguiente otra vez.
8. Elija Almacenar.

Puede usar el secreto que creó para las credenciales de la base de datos al configurar el análisis de la base de datos en Recomendaciones de estrategias.

Recomendaciones de estrategias: análisis binario

El servicio Recomendaciones de estrategias de Migration Hub identifica automáticamente las aplicaciones de su cartera y los componentes de las aplicaciones que les pertenecen. Por ejemplo, si hay una aplicación Java en su cartera, el servicio Recomendaciones de estrategias la identifica como un componente de la aplicación con un componente de tipo java. Sin configurar el acceso al código fuente, Strategy Recommendations puede realizar análisis binarios, inspeccionando la aplicación IIS DLLs en Windows o los archivos JAR de la aplicación en Linux y proporcionar informes antipatrones o de incompatibilidad. Un informe antipatrón es una lista de problemas conocidos que el servicio Recomendaciones de estrategias encuentra en su cartera, clasificados según su gravedad. Un informe de incompatibilidad contiene un subconjunto de los antipatrones, que son la compatibilidad con API, Nuget Package y Porting Action.

El servicio Recomendaciones de estrategias analizan las aplicaciones Windows IIS, Java Tomcat y Jboss. Si tiene una aplicación IIS, el servicio Recomendaciones de estrategias generan un informe de incompatibilidad de forma predeterminada; debe configurar el acceso al código fuente para recibir el informe antipatrón completo. Si tiene una aplicación Java, el servicio Recomendaciones de estrategias genera el informe antipatrón completo de forma predeterminada.

El informe incompatible o antipatrón se muestra una vez finalizado el análisis. Si el análisis no se realiza correctamente, puede intentar ejecutar un análisis del código fuente proporcionando acceso al código fuente tal y como se describe en Cómo establecer las configuraciones de control de versiones.

Recomendaciones de estrategias: recomendaciones del servidor

En esta sección, se describe cómo utilizar el servicio Recomendaciones de estrategias de Migration Hub en la consola de Migration Hub para ver las recomendaciones de estrategias de migración para los servidores de su cartera de migración.

Cómo ver las recomendaciones de servidores

1. Con la AWS cuenta que creóConfiguración de Recomendaciones de estrategias, inicie sesión en la consola de Migration Hub AWS Management Console y ábrala en https://console.aws.amazon.com/migrationhub/.
2. En el panel de navegación de la consola de Migration Hub, elija Estrategias y, a continuación, elija Recomendaciones.
3. En la página de Recomendaciones, elija la pestaña Servidores.
   a. En Resumen de servidores, puede ver una descripción general de los distintos tipos de servidores que utiliza en su cartera.
   b. En Servidores, puede ver los detalles del servidor y el sistema operativo y las recomendaciones de estrategias de migración “R”. También puede ver el destino de la migración y el número de antipatrones identificados en sus servidores, que se basan en las recomendaciones. Para obtener información sobre la estrategia “R”, consulte Términos de migración: 7 R en el glosario de Recomendaciones prescriptivas de AWS .
4. Para ver los detalles de las recomendaciones de un servidor en profundidad, seleccione el servidor de la lista y, a continuación, elija Ver detalles. Puede ver los metadatos recopilados para el servidor, junto con los análisis detallados y las recomendaciones correspondientes, que se basan en los componentes de la aplicación que se encuentran ejecutándose en el servidor.
5. En la página de detalles del servidor (la página cuyo encabezado es el nombre del servidor), en el apartado Resumen de las recomendaciones, puede ver un resumen de Recomendaciones de estrategias para el servidor. También puede ver Antipatrones identificados. Los antipatrones son una lista de problemas conocidos que se encuentran en su cartera y que se clasifican según su gravedad.

6. Elija la pestaña Opciones de estrategia para ver la recomendación de migración del servidor. Puede anular la estrategia recomendada al seleccionar una estrategia diferente y, a continuación, elegir Establecer como preferida.
7. Elija la pestaña Componentes de la aplicación para ver la lista de componentes de la aplicación asociados al servidor.
8. Para ver los detalles del componente de la aplicación, seleccione el componente de la lista y, a continuación, elija Ver detalles. Para obtener más información sobre componentes de la aplicación, consulte Trabajo con componentes de la aplicación.

Preferencias del servicio Recomendaciones de estrategias

En esta sección, se describe cómo ver y editar las preferencias del servicio Recomendaciones de estrategias de Migration Hub en la consola de Migration Hub.

Usted elige sus preferencias de recomendación cuando configura Recomendaciones de estrategias por primera vez, tal como se describe en Paso 5: obtener recomendaciones. Puede editar estas preferencias.

Cómo editar las preferencias de recomendación

1. Con la AWS cuenta que creóConfiguración de Recomendaciones de estrategias, inicie sesión en la consola de Migration Hub AWS Management Console y ábrala en https://console.aws.amazon.com/migrationhub/.
2. En el panel de navegación de la consola de Migration Hub, elija Estrategias y, a continuación, elija Recomendaciones.
3. En la página de Recomendaciones, elija la pestaña Preferencias.
4. En Objetivos empresariales priorizados, puede arrastrar y soltar los objetivos empresariales para reorganizarlos.
5. Elija las Preferencias de la aplicación y las Preferencias de la base de datos que quiera y, a continuación, elija Guardar cambios.

Si cambia sus preferencias, aparecerá un cartel para recordarle que debe elegir Reanalizar los datos.

Orígenes de datos de Recomendaciones de estrategias

En esta sección se describen los orígenes de datos que utiliza el servicio Recomendaciones de estrategias.

Temas

- Visualización de los orígenes de datos de las Recomendaciones estrategias
- Recopilador de datos de la aplicación de Recomendaciones de estrategias
- Importación de datos en Recomendaciones de estrategias
- Cómo eliminar los datos de Recomendaciones de estrategias

Visualización de los orígenes de datos de las Recomendaciones estrategias

En esta sección se describe cómo ver las fuentes de datos de las recomendaciones de estrategia en AWS Management Console.

Cómo visualizar los orígenes de datos

1. Con la AWS cuenta que creóConfiguración de Recomendaciones de estrategias, inicie sesión en la consola de Migration Hub AWS Management Console y ábrala en https://console.aws.amazon.com/migrationhub/.
2. En el panel de navegación de la consola de Migration Hub, elija Estrategias y, a continuación, elija Orígenes de datos.
3. En la pestaña Recopiladores, puede ver los recopiladores de datos de la aplicación de Recomendaciones de estrategias que usted configuró. Para obtener más información sobre el recopilador, consulte Recopilador de datos de la aplicación de Recomendaciones de estrategias.
4. En la pestaña Importaciones, puede importar datos y ver sus importaciones de datos. Para obtener más información, consulte Importación de datos en Recomendaciones de estrategias.
5. En la pestaña Herramientas, puede descargar el recopilador y la plantilla de datos de importación de la aplicación.

Recopilador de datos de la aplicación de Recomendaciones de estrategias

En esta sección, se describe cómo utilizar el recopilador de datos de la aplicación de Recomendaciones de estrategias.

Para obtener información sobre la descarga y la configuración de un recopilador de datos de aplicaciones, consulte Paso 1: descargar el recopilador de Recomendaciones de estrategias.

Temas

- Datos recopilados por el recopilador de Recomendaciones de estrategias
- Actualización del recopilador de Recomendaciones de estrategias

Datos recopilados por el recopilador de Recomendaciones de estrategias

En esta sección, se describe el tipo de datos que recopila el recopilador de datos de la aplicación de Recomendaciones de estrategias de Migration Hub. Un recopilador de datos de aplicaciones es un recopilador de datos sin agente que identifica las aplicaciones en ejecución en los servidores, analiza el código fuente y las bases de datos.

Campo de datos	Descripción
Tipo de sistemas operativos	Windows o Linux
Versión del sistema operativo	La versión específica del sistema operativo. Por ejemplo, Windows Server 2003, RHEL 5.2.
Arquitecturas de los sistemas operativos	Sistemas operativos de 32 bits o 64 bits
¿El servidor es una máquina virtual?	El servidor es una máquina virtual o física.
Software de virtualización	Por ejemplo, vCenter, Hyper-V.
Ubicación	Por ejemplo, en la consola Amazon Elastic Compute Cloud (Amazon EC2) o en las instalaciones.
¿Es dualBoot?	Permite arrancar desde múltiples OSs

Campo de datos	Descripción
Tipo de firmware	BIOS, UEFI
Gestor de arranque	GRUB, GRUB 2
Tipos de tablas de particiones	MBR, GPT
Velocidad de la CPU	Velocidad de la CPU en GHz. Por ejemplo, 2.4 GHz.
Windows OS data	
Windows Edition	Estándar, centro de datos, empresa
Versión de .NET Framework	La versión de .NET Framework instalada.
Versión de .NET Core	La versión de .NET Core instalada.
Linux data	
Distribución del sistema operativo de Linux	RHEL, CentOS, SUSE, etc.
Versión del kernel	salida uname -r, como `4.9.217-0.1.ac.205.84.332.metal1.x86_64`
For each disk volume	
Tipo de sistema de archivos	FAT32, NTFS, ReFS, ext4, jfs, etc.
Tamaño y volumen del disco	Espacio total del disco
Espacio libre en el volumen del disco	Espacio libre en el disco
Formato de imagen del disco virtual	vmdk, vhd, vhdx
Tipo de disco (Windows)	Básico, dinámico
Application level data	

Campo de datos	Descripción
Nombre de la aplicación	El nombre del procedimiento que se ejecuta. Por ejemplo, SQLServr .exe, MSdtsservr .exe, etc.
Tipo de aplicación	IIS JBoss, Tomcat, etc.
Lenguaje y versión de programación	C#, Java
Versión de JDK	La versión de JDK instalada.
¿Está disponible el código fuente?	Si se proporciona un repositorio de código fuente, indica que el código fuente está disponible.
Tamaño de bits de la aplicación	16 bits, 32 bits, 64 bits
Windows	
Versión de .NET Framework utilizada por la aplicación	La versión de la DLL de .NET Framework que se carga en tiempo de ejecución para la aplicación.
Versión de .NET Core	La versión de la DLL de .NET Core que se carga en tiempo de ejecución para la aplicació n.
¿Utiliza estructura WPF?	Determina si la aplicación basada en .NET es un tipo de aplicación WPF o no.
¿Utiliza estructura WCF?	Determina si la aplicación basada en .NET es un tipo de aplicación WCF o no.
Versión ASP.NET	La versión de ASP.NET.
Versión IIS	La versión del servidor IIS instalada en el equipo Windows.

Campo de datos	Descripción
Tamaño en bits del controlador del sistema operativo de la aplicación	32 bits, 64 bits
Uso del registro de Windows	Consulta las claves de registro de la máquina para buscar información, como por ejemplo la versión de la base de datos, la versión de Java, la versión de .NET, etc.
Todos los DLLs utilizados por la aplicación	Obtiene la lista de todos los procesos DLLs cargados en tiempo de ejecución por un proceso de Windows.
PowerShell versión	Comprueba la PowerShell versión instalada en la máquina, que debería ser 5.1 o posterior.
Linux	
Tipo de estructura de las aplicaciones	Tomcat, Spring Boot,, JBoss, WebLogic WebSphere
Versión de la estructura de las aplicaciones	La versión de la estructura de la aplicación.
Database	
Tipo de base de datos	MS SQL, Oracle, MySQL, etc.
Versión de base de datos	La versión de la base de datos.

Cómo eliminar sus datos de Recomendaciones de estrategias

Para que se eliminen todos los datos de Recomendaciones de estrategias, comuníquese con AWS Support y solicite la eliminación completa de los datos.

Actualización del recopilador de Recomendaciones de estrategias

El recopilador de datos de la aplicación de Recomendaciones de estrategias de Migration Hub se actualiza automáticamente. Puede utilizar el siguiente procedimiento para actualizar de forma manual el recopilador, si es necesario.

Cómo actualizar el recopilador de Recomendaciones de estrategias

1. Utilice el siguiente comando para conectarse a la máquina virtual (VM) del recopilador mediante un cliente SSH.

```
ssh ec2-user@CollectorIPAddress
```

2. Cambie al directorio de actualización de la máquina virtual del recopilador, tal como se muestra en el siguiente ejemplo.

```
cd  /home/ec2-user/collector/upgrades
```

3. Ingrese el siguiente comando para ejecutar el script.

```
sudo bash application-data-collector-upgrade
```

Importación de datos en Recomendaciones de estrategias

Como alternativa al uso del recopilador de datos de aplicaciones, puede importar información sobre las aplicaciones y los servidores para los que desee recibir recomendaciones de migración y modernización.

Al importar datos, las recomendaciones no son tan detalladas como cuando se utiliza el recopilador de datos. Por ejemplo, no puede utilizar el análisis del código fuente en los datos importados.

En esta sección, se describe cómo utilizar la plantilla de importación de aplicaciones para importar datos a Recomendaciones de estrategias en la consola de Migration Hub.

Cómo importar datos

1. Con la AWS cuenta que creóConfiguración de Recomendaciones de estrategias, inicie sesión en la consola de Migration Hub AWS Management Console y ábrala en https://console.aws.amazon.com/migrationhub/.
2. En el panel de navegación de la consola de Migration Hub, elija Estrategias y, a continuación, elija Orígenes de datos.
3. Elija la pestaña Importaciones.
4. Elija Descargar la plantilla de importación para descargar la plantilla de importación de la aplicación.

5. Complete la plantilla y súbala a un bucket de Amazon S3. Asegúrese de que el nombre del bucket comience con el prefijo `migrationhub-strategy`.
6. Vuelva a la pestaña Importaciones y, a continuación, elija Importar.
7. Introduzca un nombre para la importación, introduzca el URI del objeto de Amazon S3 para la plantilla de datos completada y, a continuación, elija Iniciar importación.

Plantilla de importación de Recomendaciones de estrategias

La plantilla de importación que descarga es un archivo `.json`, tal como se muestra en el siguiente ejemplo.

```
{
    "ImportFormatVersion": 1,
    "Resources": [
        {
            "ResourceType": "SERVER",
            "ResourceName": "",
            "ResourceId": "",
            "IpAddress": "",
            "OSDistribution": "",
            "OSType": "",
            "HostName": "",
            "OSVersion": "",
            "CPUArchitecture": ""
        },
        {
            "ResourceType": "PROCESS",
            "ResourceName": "",
            "ResourceId": "",
            "ApplicationType": "",
            "DotNetFrameworkVersion": "",
            "ApplicationVersion": "",
            "DotNetCoreVersion": "",
            "JdkVersion": "",
            "ProgrammingLanguage": "",
            "DatabaseType": "",
            "DatabaseVersion": "",
            "DatabaseEdition": "",
            "AssociatedServerIds": []
        }
    ]
```

```
}
```

Para ayudarlo a rellenar la plantilla de importación, en las siguientes tablas se muestran los valores válidos de los campos de datos.

Los campos obligatorios de los servidores se indican en la siguiente tabla.

Nombre	Descripción	Tipo	Obligatorio/a	Valores válidos
ResourceId	Un ID único para el recurso	Cadena	Sí	Cualquier cadena única
ResourceName	El nombre del recurso	Cadena	Sí	Cualquier cadena
ResourceType	El tipo de recurso que se va a importar	Cadena	Sí	“Servidor”, “Procedimiento”
OSDistribution	Windows, Windows Server, Ubuntu	Cadena	Sí	Windows: “Windows PC”, “Windows Server” Linux: “Ubuntu”, “RHEL”, “Amazon Linux”, “DEBIAN”, “SLES”, “CENT_OS” , “ORACLE_LINUX”, “FEDORA”, “KALI”
OSType	El tipo de sistema operativo	Cadena	Sí	“Windows”, “Linux”
OSVersion	La versión del kernel	Cadena	Sí	Consulte la versión HTML de la documentación.

Nombre	Descripción	Tipo	Obligatorio/a	Valores válidos
CPUArchitecture	La arquitectura de la CPU	Cadena	No	“32 bits”, “64 bits”
IpAddress	La dirección IP del servidor	Matriz	No	En el formato xxx.xxx.xxx.xxx
MacAddresses	Las direcciones Mac asociadas al servidor	Matriz	No	En el formato xx:xx:xx:xx:xx:xx
Nombre del host	El nombre del host	Cadena	No	Cualquier cadena

Los campos obligatorios de los procesos se indican en la siguiente tabla.

Nombre	Descripción	Tipo	Obligatorio/a	Valores válidos
ResourceId	Un ID único para el recurso	Cadena	Sí	Cualquier cadena única
ResourceName	El nombre del recurso	Cadena	Sí	Cualquier cadena
ResourceType	El tipo de recurso que se va a importar	Cadena	Sí	“Servidor”, “Procedimiento”
AssociatedServerIds	Una lista de los servidores IDs en los que se	Cadena	Sí	ResourceId Del "Resource Type«: «SERVIDOR» que ha definido.

Nombre	Descripción	Tipo	Obligatorio/a	Valores válidos
	ejecuta el proceso.			
ApplicationType	El tipo de aplicación	Cadena	Sí	«Tomcat», JBoss «Spring», «IIS», «Mongo DB», "DB2«Maria DB», «MySQL», «Oracle», «Sybase», SQLServer «Postgre», «Cassandra», SQLServer «IBM «, «Oracle WebLogic», WebSphere «Java Generic»
ApplicationVersion	La versión de la aplicación	Cadena	Sí	“IIS 1.0”, “IIS 2.0”, “IIS 3.0”, “IIS 4.0”, “IIS 5.0”, “IIS 5.1”, “IIS 6.0”, “IIS 7.0”, “IIS 7.5”, “IIS 8.0”, “IIS 8.5“, “IIS 10.0”
ProgrammingLanguage	El lenguaje de programación de la aplicación	Cadena	No	«Java», "» CSharp

Nombre	Descripción	Tipo	Obligatorio/a	Valores válidos
DotNetFrameworkVersion	La versión de .NET Framework si la aplicación está basada en estructura .NET	Cadena	No	«DotnetFramework 1.0"," DotnetFramework 1.0 SP1 «," DotnetFramework 1.0 SP2 «," DotnetFramework 1.0 «," DotnetFramework 1.1 SP3 «," DotnetFramework DotnetFramework 2.0", "2.0 SP1 «," 2.0 «," DotnetFramework 2.0 SP1 «," DotnetFramework 3.0"DotnetFramework , "DotnetFramework 3.0 SP2 «," DotnetFramework 3.5", "DotnetFramework 3.5 SP1 SP1 «," DotnetFramework DotnetFramework 4.0", "4.5"," DotnetFramework 4.5", "DotnetFramework4.5.1"," 4.5.2», "DotnetFramework 4.6"," DotnetFramework 4.6.1», «DotnetFramework 4.6.2», «4.7"," 4.7.2 1 pulgada, DotnetFramework 4 7.2 pulgadas, SP2 DotnetFramework DotnetFramework DotnetFramework "DotnetFramework 4,8»
DotNetCoreVersion	La versión de .NET Core si la aplicación está basada en .NET Core	Cadena	No	".NET Core 1.0", ".NET Core 1.1", ".NET Core 2.0", ".NET Core 2.1", ".NET Core 2.2", ".NET Core 3.0", ".NET Core 3.1"

Nombre	Descripción	Tipo	Obligatorio/a	Valores válidos
JdkVersion	La versión del JDK, si la aplicación utiliza JDK	Cadena	No	«JDK1.0"," .0", "JDK2.0",...," JDK3 .0" JDK11
DatabaseType	El tipo de la base de datos	Cadena	No	«SQLServer«, «Oracle», «Sybase», «Mongo DB», «María DB», «Apache Cassandra», «MySQL», «IBM», « DB2Postgre» SQLServer
DatabaseEdition	La edición de la base de datos	Cadena	No	
DatabaseVersion	La versión de la base de datos	Cadena	No	Consulte la versión HTML de la documentación.

Cómo eliminar los datos de Recomendaciones de estrategias

Para eliminar todos sus datos de las Recomendaciones estrategias de Migration Hub, comuníquese con AWS Support.

Seguridad en Recomendaciones de estrategias de Migration Hub

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

La seguridad es una responsabilidad compartida entre AWS usted y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de cumplimiento que se aplican a las recomendaciones estratégicas de Migration Hub, consulte AWS Servicios dentro del alcance por programa de cumplimiento AWS .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También eres responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

En esta documentación, se ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Recomendaciones de estrategias. En los siguientes temas, se le mostrará cómo configurar Recomendaciones de estrategias para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus recursos de recomendaciones de estrategia.

Temas

- Protección de los datos en Recomendaciones de estrategias de Migration Hub
- Administración de identidades y accesos de Recomendaciones de estrategias de Migration Hub
- Validación de conformidad de Recomendaciones de estrategias de Migration Hub

Protección de los datos en Recomendaciones de estrategias de Migration Hub

El modelo de se aplica a protección de datos en las Recomendaciones Estratégicas de Migration Hub. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos los Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulta las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulta la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

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

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulta Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales

como el campo Nombre. Esto incluye cuando trabaja con Strategy Recommendations u otro tipo de Servicios de AWS uso de la consola, la API o. AWS CLI AWS SDKs Cualquier dato que ingrese en etiquetas o campos de texto de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya la información de las credenciales en la URL para validar la solicitud para ese servidor.

Cifrado en reposo

Todos los datos almacenados en la base de datos de Recomendaciones de estrategias están encriptados.

Cifrado en tránsito

Las comunicaciones entre redes de Recomendaciones de estrategias admiten encriptado TLS 1.2 entre todos los componentes y clientes.

Administración de identidades y accesos de Recomendaciones de estrategias de Migration Hub

AWS Identity and Access Management (IAM) es una Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién está autenticado (inició sesión) y autorizado (tiene permisos) para utilizar los recursos de Recomendaciones de estrategias. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Temas

- Público
- Autenticación con identidades
- Administración de acceso mediante políticas
- Cómo funciona el servicio Recomendaciones de estrategias de Migration Hub con IAM
- AWS políticas gestionadas para las recomendaciones estratégicas de Migration Hub
- Ejemplos de políticas basadas en identidad de Recomendaciones de estrategias de Migration Hub

- Identidad y acceso a la solución de problemas de Recomendaciones de estrategias de Migration Hub
- Uso de roles vinculados a servicios para Recomendaciones de estrategias
- Recomendaciones de estrategias de Migration Hub y los puntos de conexión de VPC de la interfaz (AWS PrivateLink)

Público

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

Usuario de servicio: si utiliza el servicio Recomendaciones de estrategias para realizar su trabajo, su administrador le brinda las credenciales y los permisos que necesita. A medida que utilice más características de Recomendaciones de estrategias para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ser útil para solicitar los permisos correctos a su administrador. Si no puede acceder a una característica en Recomendaciones de estrategias, consulte Identidad y acceso a la solución de problemas de Recomendaciones de estrategias de Migration Hub.

Administrador de servicio: si está a cargo de los recursos de Recomendaciones de estrategias en su empresa, es probable que tenga acceso completo a Recomendaciones de estrategias. Su trabajo consiste en determinar a qué características y recursos de Recomendaciones de estrategias deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su gestionador 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 Recomendaciones de estrategias, consulte Cómo funciona el servicio Recomendaciones de estrategias de Migration Hub con IAM.

Administrador de IAM: si es un administrador de IAM, es posible que quiera obtener más detalles sobre cómo escribir políticas para administrar el acceso a Recomendaciones de estrategias. Para consultar ejemplos de las políticas basadas en identidades de Recomendaciones de estrategias que puede utilizar en IAM, consulte Ejemplos de políticas basadas en identidad de Recomendaciones de estrategias de Migration Hub.

Autenticación con identidades

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

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su gestionador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

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

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre la firma de solicitudes, consulte AWS Signature Versión 4 para solicitudes API en la Guía del usuario de IAM.

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

Cuenta de AWS usuario root

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

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

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

Usuarios y grupos de IAM

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

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puedes iniciar sesión como grupo. Puedes usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos para administrar 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 de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una persona determinada. Para asumir temporalmente un rol de IAM en el AWS Management Console, puede cambiar de un rol de usuario a uno de IAM (consola). Puedes asumir un rol llamando a una operación de AWS API AWS CLI o usando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulta Métodos para asumir un rol en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles de federación, consulte Crear un rol para un proveedor de identidad de terceros (federación) en la Guía de usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulta Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulta Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en AWS ellas, se te considera principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los

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

- Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
- Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

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

Administración de acceso mediante políticas

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

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

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

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

Políticas basadas en identidades

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

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

Políticas basadas en recursos

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

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso () ACLs

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

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

Otros tipos de políticas

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

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puedes establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCPs): SCPs son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y administrar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una Usuario raíz de la cuenta de AWS. Para obtener más información sobre Organizations SCPs, consulte las políticas de control de servicios en la Guía del AWS Organizations usuario.
- Políticas de control de recursos (RCPs): RCPs son políticas de JSON que puedes usar para establecer los permisos máximos disponibles para los recursos de tus cuentas sin actualizar las políticas de IAM asociadas a cada recurso que poseas. El RCP limita los permisos de los recursos en las cuentas de los miembros y puede afectar a los permisos efectivos de las identidades, incluidos los permisos Usuario raíz de la cuenta de AWS, independientemente de si pertenecen a su organización. Para obtener más información sobre Organizations e RCPs incluir una lista de

Servicios de AWS ese apoyo RCPs, consulte Políticas de control de recursos (RCPs) en la Guía del AWS Organizations usuario.

- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

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

Cómo funciona el servicio Recomendaciones de estrategias de Migration Hub con IAM

Antes de utilizar IAM para administrar el acceso a Recomendaciones de estrategias, conozca qué características de IAM se pueden utilizar con las Recomendaciones de estrategias.

Características de IAM que puede utilizar con Recomendaciones de estrategias de Migration Hub

Característica de IAM	Compatibilidad de Recomendaciones de estrategias
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	No
Claves de condición de política	No
ACLs	No

Característica de IAM	Compatibilidad de Recomendaciones de estrategias
ABAC (etiquetas en políticas)	No
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	No
Roles vinculados al servicio	Sí

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

Políticas basadas en identidad para Recomendaciones de estrategias

Compatibilidad con las políticas basadas en identidad: sí

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

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

Ejemplos de políticas basadas en identidad de Recomendaciones de estrategias

Para ver ejemplos de políticas basadas en identidad de Recomendaciones de estrategias, consulte Ejemplos de políticas basadas en identidad de Recomendaciones de estrategias de Migration Hub.

Políticas basadas en recursos de Recomendaciones de estrategias

Admite políticas basadas en recursos: no

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

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política basada en recursos concede acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte Cross account resource access in IAM en la Guía del usuario de IAM.

Acciones de política para Recomendaciones de estrategias

Compatibilidad con las acciones de políticas: sí

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

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

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

Para ver una lista de las acciones de Recomendaciones de estrategias, consulte Acciones definidas por Recomendaciones de estrategias de Migration Hub en la Referencia de autorización de servicios.

Las acciones de políticas de Recomendaciones de estrategias utilizan el siguiente prefijo antes de la acción:

```
migrationhub-strategy
```

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

```
"Action": [
      "migrationhub-strategy:action1",
      "migrationhub-strategy:action2"
         ]
```

Para ver ejemplos de políticas basadas en identidad de Recomendaciones de estrategias, consulte Ejemplos de políticas basadas en identidad de Recomendaciones de estrategias de Migration Hub.

Recursos de políticas para Recomendaciones de estrategias

Compatibilidad con recursos de políticas: no

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

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puedes 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, utiliza 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 las recomendaciones de estrategia y sus tipos de recursos ARNs, consulte Recursos definidos por las recomendaciones de estrategia de

Migration Hub en la Referencia de autorización de servicios. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por Recomendaciones de estrategias de Migration Hub.

Para ver ejemplos de políticas basadas en identidad de Recomendaciones de estrategias, consulte Ejemplos de políticas basadas en identidad de Recomendaciones de estrategias de Migration Hub.

Claves de condición de política para Recomendaciones de estrategias

Compatibilidad con claves de condición de políticas específicas del servicio: no

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

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

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

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

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

Para ver una lista de las claves de condición de Recomendaciones de estrategias, consulte Claves de condición de Recomendaciones de estrategias de Migration Hub en la Referencia de autorización de servicios. Para obtener información sobre las acciones y los recursos con los que se puede utilizar una clave de condición, consulte Acciones definidas por Recomendaciones de estrategias.

Para ver ejemplos de políticas basadas en identidad de Recomendaciones de estrategias, consulte Ejemplos de políticas basadas en identidad de Recomendaciones de estrategias de Migration Hub.

Listas de control de acceso (ACLs) en las recomendaciones de estrategia

Soportes ACLs: No

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

Control de acceso basado en atributos (ABAC) con Recomendaciones de estrategias

Compatibilidad con ABAC (etiquetas en las políticas): no

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

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con Recomendaciones de estrategias

Compatibilidad con credenciales temporales: sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluidas las que Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

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

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM.

Permisos de entidad principal entre servicios de Recomendaciones de estrategias

Admite sesiones de acceso directo (FAS): sí

Cuando utilizas un usuario o un rol de IAM para realizar acciones en AWSél, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Roles de servicio para Recomendaciones de estrategias

Compatible con roles de servicio: No

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

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de Recomendaciones de estrategias. Edite los roles de servicio solo cuando en Recomendaciones de estrategias se proporcione orientación para hacerlo.

Roles vinculados a servicios de Recomendaciones de estrategias

Admite roles vinculados a servicios: sí

Un rol vinculado a un servicio es un tipo de rol de 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 al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener más información sobre cómo crear o administrar roles vinculados a servicios de Recomendaciones de estrategias, consulte Uso de roles vinculados a servicios para Recomendaciones de estrategias.

AWS políticas gestionadas para las recomendaciones estratégicas de Migration Hub

Para añadir permisos a usuarios, grupos y roles, es más fácil usar políticas AWS administradas que escribirlas tú mismo. Se necesita tiempo y experiencia para crear políticas administradas por el cliente de IAM que proporcionen a su equipo solo los permisos necesarios. Para empezar rápidamente, puedes usar nuestras políticas AWS gestionadas. Estas políticas cubren casos de uso comunes y están disponibles en su Cuenta de AWS. Para obtener más información sobre las políticas AWS administradas, consulte las políticas AWS administradas en la Guía del usuario de IAM.

AWS los servicios mantienen y AWS actualizan las políticas gestionadas. No puede cambiar los permisos en las políticas AWS gestionadas. En ocasiones, los servicios añaden permisos adicionales a una política AWS gestionada para admitir nuevas funciones. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Lo más probable es que los servicios actualicen una política AWS administrada cuando se lanza una nueva función o cuando

hay nuevas operaciones disponibles. Los servicios no eliminan los permisos de una política AWS administrada, por lo que las actualizaciones de la política no afectarán a los permisos existentes.

Además, AWS admite políticas administradas para funciones laborales que abarcan varios servicios. Por ejemplo, la política ReadOnlyAccess AWS gestionada proporciona acceso de solo lectura a todos los AWS servicios y recursos. Cuando un servicio lanza una nueva función, AWS agrega permisos de solo lectura para nuevas operaciones y recursos. Para obtener una lista y descripciones de las políticas de funciones de trabajo, consulte Políticas administradas de AWS para funciones de trabajo en la Guía del usuario de IAM.

AWS política gestionada: AWSMigration HubStrategyConsoleFullAccess

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

La política de `AWSMigrationHubStrategyConsoleFullAccess` concede acceso total al usuario del servicio de Recomendaciones de estrategias a través de la AWS Management Console.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `discovery`: otorga al usuario acceso para obtener un resumen del descubrimiento en Application Discovery Service.
- `iam`: permite crear un rol vinculado a servicios para el usuario, lo cual es un requisito para utilizar Recomendaciones de estrategias.
- `migrationhub-strategy`: otorga al usuario acceso completo a Recomendaciones de estrategias.
- `s3`: permite al usuario crear y leer los buckets de S3 que utiliza el servicio Recomendaciones de estrategias.
- `secretsmanager`: permite al usuario enumerar los secretos de acceso en el Secrets Manager.

Para ver los permisos de esta política, consulte AWSMigrationHubStrategyConsoleFullAccessen la Guía de referencia de políticas AWS gestionadas.

AWS política gestionada: AWSMigration HubStrategyCollector

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

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `application-transformation`— Otorga permisos para cargar datos de registro y métricas para las operaciones de transformación de aplicaciones y trabajar con las evaluaciones y recomendaciones de compatibilidad de portabilidad.
- `execute-api`: permite al usuario acceder a Amazon API Gateway para cargar registros y métricas en AWS.
- `migrationhub-strategy`— Concede al usuario acceso para registrar mensajes, enviar mensajes, cargar datos de registro y cargar datos de métricas a Strategy Recommendations.
- `s3`— Concede al usuario acceso a la lista de grupos y a sus ubicaciones. Los usuarios también tienen acceso para escribir, recuperar objetos, añadir objetos, devolver la lista de control de acceso (ACL), crear, acceder, configurar el cifrado, modificar la `PublicAccessBlock` configuración, establecer el estado del control de versiones y crear o reemplazar una configuración de ciclo de vida para los buckets de S3 utilizados en las recomendaciones de estrategia.
- `secretsmanager`: permite al usuario acceder a los secretos en Secrets Manager que utiliza el servicio Recomendaciones de estrategias.

Para ver los permisos de esta política, consulte AWSMigrationHubStrategyCollectoren la Guía de referencia de políticas AWS gestionadas.

Recomendaciones de estrategia: actualizaciones de las políticas AWS gestionadas

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas para Strategy Recommendations desde que este servicio comenzó a realizar un seguimiento de estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de historial de documentos de Recomendaciones de estrategias.

Cambio	Descripción	Fecha
AWSMigrationHubStrategyCollector: actualización de una política actual	Esta política se actualiza para incluir las acciones de transformación de las `GetPortingRecommendationAssessment` aplicaciones `PutLogData` `StartPortingCompatibilityAssessment` `GetPortingCompatibilityAssessment` , `StartPortingRecommendationAssessment` y permitir que el servicio de transformación de aplicaciones envíe registros y métricas al servicio. Los `ListBucket` y `GetBucketLocation` se agregaron para Amazon Simple Storage Service (Amazon S3) para admitir la carga de registros y métricas. También `PutMetricData` se agregaron para permitir que el recopilador de recomendaciones de estrategia enviara registros y métricas al punto final del servicio. `PutLogData`	1 de abril de 2024
AWSMigrationHubStrategyCollector: actualización de una política actual	Esta política se actualiza con las `PutLogData` acciones `PutMetricData` y. Estas acciones permiten cargar	5 de febrero de 2024

Cambio	Descripción	Fecha
	datos de registro y métricas para las operaciones de transformación de aplicaciones. Esta actualización también añade condiciones para garantizar que `aws:ResourceAccount` sea igual al permiso `aws:PrincipalAccount` para utilizar las AWS Secrets Manager acciones y el servicio Amazon Simple Storage incluidos.	
AWSMigrationHubStrategyCollector: actualización de una política actual	Esta política se actualiza con las siguientes versiones de Amazon S3 APIs : `CreateBucket` `PutEncryptionConfiguration` ,`PutBucketPublicAccessBlock` ,`PutBucketPolicy` ,`PutBucketVersioning` , y`PutLifecycleConfiguration` .	15 de septiembre de 2023
AWSMigrationHubStrategyCollector: actualización de una política actual	Esta actualización de la política otorga permisos para analizar el código fuente.	8 de marzo de 2023

Cambio	Descripción	Fecha
AWSMigrationHubStrategyConsoleFullAccess: actualización de una política actual	Esta política se actualiza con tres AWS Application Discovery Service APIs : `DescribeConfigurations` `DescribeTags` , `yListConfigurations` .	10 de noviembre de 2022
AWSMigrationHubStrategyCollector: actualización de una política actual	Esta política se actualiza con la `UpdateCollectorConfiguration` acción. Esta acción almacena la configuración del recopilador para poder recuperarla fácilmente.	7 de septiembre de 2022
AWSMigrationHubStrategyConsoleFullAccess— La nueva política estará disponible en el momento del lanzamiento	`AWSMigrationHubStrategyConsoleFullAccess` otorga al usuario acceso completo al servicio de Recomendaciones de estrategias a través de la AWS Management Console.	25 de octubre de 2021
AWSMigrationHubStrategyCollector— La nueva política estará disponible en el momento del lanzamiento	`AWSMigrationHubStrategyCollector` concede al usuario acceso al servicio de Recomendaciones de estrategias y acceso de lectura y escritura a los buckets de S3 relacionados con el servicio. También otorga acceso a Amazon API Gateway para cargar registros y métricas AWS, y acceso a AWS Secrets Manager para obtener credenciales.	25 de octubre de 2021

Cambio	Descripción	Fecha
AWSMigrationHubStrategyServiceRolePolicy— La nueva política estará disponible en el momento del lanzamiento	La política de funciones `AWSMigrationHubStrategyServiceRolePolicy` vinculadas al servicio proporciona acceso a AWS Migration Hub y. AWS Application Discovery Service Esta política también concede permisos para almacenar informes en Amazon Simple Storage Service (Amazon S3).	25 de octubre de 2021
comienzo de seguimiento de cambios de Recomendaciones de estrategias	Strategy Recommendations comenzó a rastrear los cambios en sus políticas AWS gestionadas.	25 de octubre de 2021

Ejemplos de políticas basadas en identidad de Recomendaciones de estrategias de Migration Hub

De forma predeterminada, los usuarios y los roles no tienen permiso para crear ni modificar los recursos de Recomendaciones de estrategias. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS la API. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puedes añadir las políticas de IAM a roles y los usuarios puedes asumirlos.

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

Para obtener más información sobre las acciones y los tipos de recursos definidos en las recomendaciones de estrategia, incluido el ARNs formato de cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de las recomendaciones estratégicas de Migration Hub en la Referencia de autorización de servicios.

Temas

- Prácticas recomendadas sobre las políticas
- Uso de la consola de Recomendaciones de estrategias
- Cómo permitir a los usuarios consultar sus propios permisos
- Acceso a un bucket de Amazon S3

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidad determinan si alguien puede crear, acceder o eliminar los recursos de Recomendaciones de estrategias de la cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulta las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulta Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulta Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas

recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.

- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

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

Uso de la consola de Recomendaciones de estrategias

Para acceder a la consola de Recomendaciones de estrategias, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de recomendaciones de estrategia que tiene en su cuenta. Cuenta de AWS Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

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

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

Cómo permitir a los usuarios consultar sus propios permisos

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

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

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

Acceso a un bucket de Amazon S3

En este ejemplo, quiere conceder a un usuario de IAM el Cuenta de AWS acceso a uno de sus buckets de Amazon S3,. `amzn-s3-demo-bucket` También desea permitir al usuario añadir, actualizar o eliminar objetos.

Además de conceder los permisos `s3:PutObject`, `s3:GetObject` y `s3:DeleteObject` al usuario, la política también concede los permisos `s3:ListAllMyBuckets`, `s3:GetBucketLocation` y `s3:ListBucket`. Estos son los permisos adicionales que requiere la consola. Las acciones `s3:PutObjectAcl` y `s3:GetObjectAcl` también son necesarias para poder copiar, cortar y pegar objetos en la consola. Para ver un tutorial de ejemplo en el que se

conceden permisos a los usuarios y se prueban con la consola, consulte Tutorial de ejemplo: uso de las políticas del usuario para controlar el acceso al bucket.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"ListBucketsInConsole",
         "Effect":"Allow",
         "Action":[
            "s3:ListAllMyBuckets"
         ],
         "Resource":"arn:aws:s3:::*"
      },
      {
         "Sid":"ViewSpecificBucketInfo",
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket",
            "s3:GetBucketLocation"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket"
      },
      {
         "Sid":"ManageBucketContents",
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:GetObject",
            "s3:GetObjectAcl",
            "s3:DeleteObject"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*"
      }
   ]
}
```

Identidad y acceso a la solución de problemas de Recomendaciones de estrategias de Migration Hub

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con Recomendaciones de estrategias e IAM.

Temas

- No tengo autorización para realizar una acción en Recomendaciones de estrategias
- No estoy autorizado a realizar lo siguiente: PassRole
- Quiero ver mis claves de acceso
- Soy administrador y deseo permitir que otros obtengan acceso a Recomendaciones de estrategias
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de recomendaciones de estrategia

No tengo autorización para realizar una acción en Recomendaciones de estrategias

Si AWS Management Console le indica que no está autorizado a realizar una acción, debe ponerse en contacto con su administrador para obtener ayuda. Su administrador es la persona que le facilitó su nombre de usuario y contraseña.

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 `migrationhub-strategy:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 migrationhub-strategy: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 `migrationhub-strategy:`*`GetWidget`*.

No estoy autorizado a realizar lo siguiente: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, las políticas se deben actualizar para permitirle pasar un rol a Recomendaciones de estrategias.

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

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en Recomendaciones de estrategias. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

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

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

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

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 lo ayuden a buscar el ID de usuario canónico. De este modo, podrías dar a alguien acceso permanente a tu Cuenta de AWS.

Cuando crea un par de claves de acceso, se le pide que guarde el ID de clave de acceso y la clave de acceso secreta en un lugar seguro. La clave de acceso secreta solo está disponible en

el momento de su creación. Si 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 una nueva. 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 Recomendaciones de estrategias

Para permitir que otras personas accedan a las recomendaciones de estrategia, debes conceder permiso a las personas o aplicaciones que necesiten acceder. Si usa AWS IAM Identity Center para administrar las personas y las aplicaciones, debe asignar conjuntos de permisos a los usuarios o grupos para definir su nivel de acceso. Los conjuntos de permisos crean políticas de IAM y las asignan a los roles de IAM asociados a la persona o aplicación de forma automática. Para obtener más información, consulte la sección Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .

Si no utiliza IAM Identity Center, debe crear entidades de IAM (usuarios o roles) para las personas o aplicaciones que necesitan acceso. A continuación, debe asociar una política a la entidad que le conceda los permisos correctos en Recomendaciones de estrategias. Una vez concedidos los permisos, proporcione las credenciales al usuario o al desarrollador de la aplicación. Utilizarán esas credenciales para acceder a AWS. Para obtener más información sobre la creación de usuarios, grupos, políticas y permisos de IAM, consulte Identidades de IAM y Políticas y permisos en IAM en la Guía del usuario de IAM.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de recomendaciones de estrategia

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

Para obtener más información, consulte lo siguiente:

- Para obtener información acerca de si el servicio Recomendaciones de estrategias admite estas características, consulte Cómo funciona el servicio Recomendaciones de estrategias de Migration Hub con IAM.

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

Uso de roles vinculados a servicios para Recomendaciones de estrategias

Las recomendaciones de estrategia de Migration Hub utilizan AWS Identity and Access Management funciones vinculadas al servicio (IAM). Un rol vinculado a servicios es un tipo único de rol de IAM que está vinculado directamente a Recomendaciones de estrategias. Las funciones vinculadas al servicio están predefinidas en Strategy Recommendations e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Un rol vinculado a servicios simplifica la configuración de Recomendaciones de estrategias porque ya no tendrá que agregar manualmente los permisos necesarios. El servicio Recomendaciones de estrategias define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo el servicio Recomendaciones de estrategias puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda asociar a ninguna otra entidad de IAM.

Para obtener información sobre otros servicios que admiten funciones vinculadas a servicios, consulte AWS Servicios que funcionan con IAM y busque los servicios con la opción Sí en la columna Función vinculada a servicios. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

Permisos de roles vinculados a servicios para Recomendaciones de estrategias

Strategy Recommendations utiliza el rol vinculado al servicio denominado AWSServiceRoleForMigrationHubStrategyy lo asocia a la política de AWSMigrationHubStrategyServiceRolePolicyIAM: proporciona acceso a y. AWS Migration Hub AWS

Application Discovery Service Esta política también otorga permisos para almacenar informes en Amazon Simple Storage Service (Amazon S3).

El rol vinculado al servicio AWSServiceRoleForMigrationHubStrategy depende de los siguientes servicios para asumir el rol:

- `migrationhub-strategy.amazonaws.com`

La política de permisos de roles permite que el servicio Recomendaciones de estrategias completen las siguientes acciones.

AWS Application Discovery Service acciones

`discovery:ListConfigurations`

`discovery:DescribeConfigurations`

AWS Migration Hub acciones

`mgh:GetHomeRegion`

Acciones de Amazon S3

`s3:GetBucketAcl`

`s3:GetBucketLocation`

`s3:GetObject`

`s3:ListAllMyBuckets`

`s3:ListBucket`

`s3:PutObject`

`s3:PutObjectAcl`

Para ver los permisos de esta política, consulte AWSMigrationHubStrategyServiceRolePolicyen la Guía de referencia de políticas AWS gestionadas.

Para ver el historial de actualizaciones de esta política, consulte Recomendaciones de estrategia: actualizaciones de las políticas AWS gestionadas.

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 servicios para Recomendaciones de estrategias

No necesita crear manualmente un rol vinculado a servicios. Cuando aceptas permitir que Migration Hub cree un rol vinculado a un servicio (SLR) en tu cuenta en AWS Management Console, Strategy Recommendations crea el rol vinculado al servicio para ti.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando permite a Migration Hub crear un rol vinculado a servicios (SLR) en su cuenta, el servicio Recomendaciones de estrategias crea otra vez el rol vinculado a servicios por usted.

Edición de un rol vinculado a servicios para Recomendaciones de estrategias

Strategy Recommendations no le permite editar el rol vinculado al servicio. AWSServiceRoleForMigrationHubStrategy Después de crear un rol vinculado a un servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al mismo. Sin embargo, puede editar la descripción del rol mediante la consola de Recomendaciones de estrategias, la CLI o la API.

Eliminación de un rol vinculado a servicios para Recomendaciones de estrategias

Cómo eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al AWSServiceRoleForMigrationHubStrategyservicio. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Al eliminar los recursos de recomendaciones de estrategia utilizados por la AWSServiceRoleForMigrationHubStrategySLR, no puede tener ninguna evaluación en ejecución (tareas para generar recomendaciones). Tampoco se puede ejecutar ninguna evaluación en segundo plano. Si las evaluaciones se están ejecutando, se produce un error al eliminar el SLR en la consola de IAM. Si se produce este error, puede volver a intentarlo una vez que se hayan completado todas las tareas en segundo plano. No es necesario eliminar ningún recurso creado antes de eliminar el SLR.

Regiones admitidas para los roles vinculados a servicios de Recomendaciones de estrategias

El servicio Recomendaciones de estrategias admite el uso de roles vinculados a servicios en todas las regiones en las que el servicio esté disponible. Para obtener más información, consulte Regiones y puntos de conexión de AWS.

Recomendaciones de estrategias de Migration Hub y los puntos de conexión de VPC de la interfaz (AWS PrivateLink)

Puede establecer una conexión privada entre la VPC y Recomendaciones de estrategias de Migration Hub mediante la generación de un punto de conexión de VPC de la interfaz. Puntos de enlace de tipo interfaz con tecnología de AWS PrivateLink. Con AWS PrivateLink, puede acceder de forma privada a las operaciones de la API de Strategy Recommendations sin una pasarela de Internet, un dispositivo NAT, una conexión VPN o AWS Direct Connect una conexión. Las instancias de la VPC no necesitan direcciones IP públicas para comunicarse con las operaciones de la API de Recomendaciones de estrategias. El tráfico entre la VPC y Recomendaciones de estrategias permanece dentro de la red de Amazon.

Cada punto de conexión de la interfaz está representado por una o más interfaces de red elásticas en las subredes.

Para obtener más información, consulte Puntos de conexión de VPC de interfaz (AWS PrivateLink) en la Guía del usuario de Amazon VPC.

Consideraciones sobre los puntos de conexión de VPC de Recomendaciones de estrategias

Antes de configurar un punto de conexión de VPC de la interfaz de Recomendaciones de estrategias, asegúrese de revisar las propiedades y limitaciones del punto de conexión de la interfaz y las cuotas de AWS PrivateLink en la Guía del usuario de Amazon VPC.

La aplicación Recomendaciones de estrategias admite realizar llamadas a todas sus acciones de la API desde su VPC. Para utilizar por completo Recomendaciones de estrategias, debe crear un punto de conexión de VPC.

Creación de un punto de conexión de VPC de la interfaz para Recomendaciones de estrategias

Puede crear un punto de conexión de VPC para Recomendaciones de estrategias mediante la consola de Amazon VPC o la AWS Command Line Interface (AWS CLI). Para obtener más información, consulte Creación de un punto de conexión de interfaz en la Guía del usuario de Amazon VPC.

Genere un punto de conexión de VPC para Recomendaciones de estrategias mediante el siguiente nombre de servicio:

- `com.amazonaws.`*`region`*`.migrationhub-strategy`

Si habilita el DNS privado para el punto de conexión, puede efectuar solicitudes de API a Recomendaciones de estrategias utilizando su nombre de DNS predeterminado para la región. Por ejemplo, puede utilizar el nombre `migrationhub-strategy.us-east-1.amazonaws.com`.

Para más información, consulte Acceso a un servicio a través de un punto de conexión de interfaz en la Guía del usuario de Amazon VPC.

Creación de una política de punto de conexión de VPC para Recomendaciones de estrategias

Puede asociar una política de punto de conexión con su punto de conexión de VPC que controla el acceso a Recomendaciones de estrategias. La política especifica la siguiente información:

- La entidad principal que puede realizar acciones.
- Las acciones que se pueden realizar.
- Los recursos sobre los que se pueden realizar estas acciones.

Para obtener más información, consulte Control del acceso a los servicios con puntos de conexión de VPC en la Guía del usuario de Amazon VPC.

Ejemplo: política de punto de conexión de VPC para acciones de Recomendaciones de estrategias

A continuación, se muestra un ejemplo de una política de punto de conexión para Recomendaciones de estrategias. Cuando se asocia con un punto de conexión, esta política concede acceso a las acciones de Recomendaciones de estrategias mostradas para todas las entidades principales en todos los recursos.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "migrationhub-strategy:ListContacts",
         ],
         "Resource":"*"
      }
   ]
}
```

Validación de conformidad de Recomendaciones de estrategias de Migration Hub

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

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

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Cumplimiento de seguridad y gobernanza: en estas guías se explican las consideraciones de arquitectura y se proporcionan pasos para implementar las características de seguridad y cumplimiento.
- Referencia de servicios válidos de HIPAA: muestra una lista con los servicios válidos de HIPAA. No todos Servicios de AWS cumplen con los requisitos de la HIPAA.
- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos

el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).

- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulta la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Trabajar con otros servicios de

En esta sección se describen otros AWS servicios que interactúan con las recomendaciones estratégicas de Migration Hub.

Temas

- Registrar las llamadas a la API de recomendaciones de estrategia con AWS CloudTrail

Registrar las llamadas a la API de recomendaciones de estrategia con AWS CloudTrail

Las recomendaciones de estrategia de Migration Hub están integradas con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en las recomendaciones de estrategia. CloudTrail captura las llamadas a la API para las recomendaciones de estrategia como eventos. Las llamadas capturadas incluyen llamadas que se realizan desde la consola de Recomendaciones de estrategias, así como las llamadas de código que se realizan a las operaciones de API de Recomendaciones de estrategias.

Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos para las recomendaciones de estrategia. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a Strategy Recommendations, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

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

Información sobre recomendaciones de estrategia en CloudTrail

CloudTrail está habilitada en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en las recomendaciones de estrategia, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para tener un registro continuo de tus eventos Cuenta de AWS, incluidos los eventos de las recomendaciones de estrategia, crea una ruta. Un rastro permite CloudTrail entregar 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. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Strategy Recommendations permite registrar las siguientes acciones como eventos en los archivos de CloudTrail registro:

- GetApplicationComponentStrategies
- GetApplicationComponentDetails
- GetAssesment
- GetImportFileTask
- GetPortfolioPreferences
- GetPortfolioSummary
- GetServerDetails
- GetServerStrategies
- ListApplicationComponents
- ListCollectors
- ListImportFileTask
- ListServers
- PutPortfolioPreferences
- StartAssessment
- StartImportFileTask
- StopAssessment
- UpdateApplicationComponetConfig

- UpdateServerConfig

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 root o AWS Identity and Access Management (IAM)
- 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 AWS

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

Cómo comprender las entradas del archivo de registro de Recomendaciones de estrategias

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la GetServerDetailsacción.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "777777777777",
        "arn": "arn:aws:sts::111122223333:assumed-role/myUserName/...",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "777777777777",
                "arn": "arn:aws:iam::111122223333:role/myUserName",
```

```
                "accountId": "111122223333",
                "userName": "myUserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2021-09-20T01:07:16Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2021-09-20T01:07:43Z",
    "eventSource": "migrationhub-strategy.amazonaws.com",
    "eventName": "GetServerDetails",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "",
    "userAgent": "",
    "requestParameters": {
        "serverId": "ads-server-006"
    },
    "responseElements": null,
    "requestID": "07D681279BD94AED",
    "eventID": "cdc4b7ed-e171-4cef-975a-ad829d4123e8",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Cuotas para Recomendaciones de estrategias de Migration Hub

Tu AWS cuenta tiene cuotas predeterminadas, antes denominadas límites, para cada AWS servicio. A menos que se indique lo contrario, cada cuota es específica de la región de . Puede solicitar el aumento de algunas cuotas, pero otras no se pueden aumentar.

Para ver una lista de las cuotas de Recomendaciones de estrategias de Migration Hub, consulte las cuotas de servicio de Recomendaciones de estrategias.

También puede ver las cuotas de Recomendaciones de estrategias al abrir la consola Service Quotas. En el panel de navegación, elija servicios de AWS y seleccione Recomendaciones de estrategias de 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.

Notas de la versión

Temas

- 17 de noviembre de 2023
- 12 de octubre de 2023
- 17 de abril de 2023
- 17 de marzo de 2023
- 7 de noviembre de 2022
- 27 de septiembre de 2022
- 30 de junio de 2022
- 18 de abril de 2022
- 25 de febrero de 2022
- 10 de febrero de 2022
- 28 de enero de 2022
- 14 de enero de 2022
- 21 de diciembre de 2021
- 15 de diciembre de 2021
- 25 de octubre de 2021

17 de noviembre de 2023

Nuevas características

- Collector v1.1.47
- Support para aplicaciones.NET 8.

12 de octubre de 2023

Nuevas características

- Collector v1.1.45
- Support para fuentes de datos múltiples.

17 de abril de 2023

Nuevas características

- Collector v1.1.22
- Mejoras en los scripts de actualización. Esto requiere la última versión del recopilador.

17 de marzo de 2023

Nueva característica

Se agregó el análisis binario, que permite detectar antipatrones e incompatibilidades sin necesidad de un código fuente.

7 de noviembre de 2022

Nueva característica

- Filtro de aplicaciones
- Filtrado de servidores por AWS Application Discovery Service etiquetas

27 de septiembre de 2022

Nueva característica

- Collector v1.1.12
  - SCT versión 667
  - EMPAnalyzer 2.2.0.368
- Se agregaron comandos de `diag check` para obtener información sobre el servidor.
- Se agregó compatibilidad para posibles recomendaciones.
- Se mejoró la interfaz de usuario para evaluar el estado de configuración y evaluación.

Correcciones de errores

- Traductor asistente de portabilidad y otras correcciones.

30 de junio de 2022

Nueva característica

- Collector v1.1.11
  - Se agregó soporte VMware para API.
  - A2C solicitó cambios para agregar el encabezado de usuario al descargar el archivo binario.
  - Se agregó la ruta principal de Linux, el intérprete de comandos predeterminado y la terminal remota de todos los intérpretes de comandos.
- Binario público A2C v1.17
  - Se agregó compatibilidad con Azure DevOps como objetivo de implementación en proceso.

18 de abril de 2022

Nueva característica

- Collector v1.1.7
- Se agregó la posibilidad de descargar el binario A2C desde la URL pública de forma dinámica.

Correcciones de errores

- A2C v1.1.5

25 de febrero de 2022

Correcciones de errores

- SCT v5.6.9
- A2C v1.1.2
- Collector v1.1.4

10 de febrero de 2022

Correcciones de errores

- SCT v5.6.8
- A2C v1.1.1
  - Se agregó una verificación para el comando tar en Linux.
  - Se corrigió el problema para comprobar las imágenes de las aplicaciones en Amazon ECR.
  - Se corrigió el problema que obligaba a retirar el contenedor para su validación previa.
- Collector v1.1.3
  - Se corrigió el error 4xx en una máquina remota de 32 bits.
  - Se actualizaron los códigos de error A2C.
  - Se validó la dirección IP en `C#` para el análisis del código fuente de la máquina remota.

28 de enero de 2022

Nueva característica

- Collector v1.1.2
- Se agregó compatibilidad con el repositorio DevOps Git de Azure para el análisis del código fuente.

14 de enero de 2022

Nueva característica

- Collector v1.1.1
- Se agregaron recomendaciones de Babelfish para las bases de datos SQL.

21 de diciembre de 2021

Problema resuelto

- Collector v1.1.0
- Se restauró el análisis de la base de datos.

15 de diciembre de 2021

Problema conocido

- Collector v1.0.4
- Actualmente, no se admite el análisis de la base de datos (CVE-2021-44228).

25 de octubre de 2021

Nueva característica

- Collector v1.0.0
- Versión inicial de la Guía del usuario sobre Recomendaciones de estrategias de Migration Hub.

Historial de documentos y versiones

En la siguiente tabla se describen las versiones de la documentación de Recomendaciones de estrategias. Para obtener más información, consulte Notas de la versión.

Cambio	Descripción	Fecha
AWS actualizaciones de políticas gestionadas: actualización a AWSMigrationHubStrategyCollector	Se actualizó la AWSMigrationHubStrategyCollectorpolítica para incluir `migrationhub-strategy` acciones nuevas `s3` y. `application-transformation`	1 de abril de 2024
AWS actualizaciones de políticas gestionadas: actualización a AWSMigrationHubStrategyCollector	Se actualizó la AWSMigrationHubStrategyCollectorpolítica para incluir nuevas `application-transformation` acciones. Esta actualización también agrega condiciones para restringir varias acciones donde `aws:ResourceAccount` debe ser igual a`aws:PrincipalAccount` .	5 de febrero de 2024
Nueva característica	El cliente recopilador de datos de la aplicación Strategy Recommendations, versión 1.1.47, está disponible con soporte para aplicaciones.NET 8.	17 de noviembre de 2023
Nueva característica	El cliente recopilador de datos de la aplicación Strategy	12 de octubre de 2023

	Recommendations, versión 1.1.45, está disponible con soporte para múltiples fuentes de datos.	
AWS actualizaciones de políticas gestionadas: actualización a AWSMigrationHubStrategyCollector	Se actualizó la AWSMigrationHubStrategyCollectorpolítica para incluir la nueva Amazon S3 APIs.	15 de septiembre de 2023
AWS actualizaciones de políticas gestionadas: actualización a AWSMigrationHubStrategyCollector	Se actualizó la AWSMigrationHubStrategyCollectorpolítica para incluir nuevos analizadores para el código fuente.	8 de marzo de 2023
Actualizaciones de las prácticas recomendadas de IAM	Para obtener más información, consulta prácticas recomendadas de seguridad en IAM.	25 de febrero de 2023
AWS actualizaciones de políticas gestionadas: actualización de una política existente	Las recomendaciones de estrategia de Migration Hub AWS Application Discovery Service APIs agregaron tres a una política existente.	10 de noviembre de 2022
Actualizaciones de seguridad	Se establece una conexión privada con el punto de conexión de VPC de la interfaz.	7 de marzo de 2022
Nueva característica	Se agregó compatibilidad con el repositorio DevOps Git de Azure para el análisis del código fuente.	28 de enero de 2022

Nueva característica	Se agregaron las recomendaciones de Babelfish para las bases de datos SQL.	14 de enero de 2022
Versión inicial	Versión inicial de la Guía del usuario de Recomendaciones de estrategias de Migration Hub.	25 de octubre 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.