



Guía del usuario

AWS Application Discovery Service



AWS Application Discovery Service: Guía del usuario

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas 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 AWS Application Discovery Service?	1
Detección de VMware	2
detección de bases de datos	3
Compare Agentless Collector y Discovery Agent	3
Supuestos	4
Configuración	6
Registro en Amazon Web Services	6
Cree usuarios de IAM	6
Creación de un usuario administrativo de IAM	7
Creación de un usuario no administrativo de IAM	7
Inicia sesión en Migration Hub y elige una región de origen	8
Agente de descubrimiento	9
Requisitos previos	10
Instalación del en Linux	12
Requisitos de las plataformas Linux más antiguas	15
Administre el proceso de Discovery Agent en Linux	16
Desinstalar un agente	17
Solución de problemas de Linux Discovery Agent	18
Instalación de en Windows.	19
Package Signing y actualizaciones automáticas	23
Administre el proceso de Discovery Agent en Windows	23
Solución de problemas en Windows	25
Datos recopilados	26
Iniciar o detener la recopilación de datos	29
Recopilador sin agente	32
Introducción	33
Requisitos previos	33
Paso 1: Crear un usuario de IAM	36
Paso 2: Descarga el recopilador	38
Paso 3: Despliegue el recopilador	39
Paso 4: Acceda a la consola del recopilador	40
Paso 5: Configurar el recopilador	41
Paso 6: Configurar los módulos de recopilación de datos	47
Paso 7: Ver los datos recopilados	63

Datos recopilados	64
Datos recopilados por el módulo de VMware	65
Datos recopilados por la base de datos y el módulo de análisis	69
Con la consola	71
Panel para para colectores	71
Editar la configuración del recopilador	74
Edición de las credenciales de vCenter	75
Actualizaciones	75
Resolución de problemas	77
Reparación: no se puede acceder a Agentless Collector durante la configuración AWS	77
Solución de problemas de certificación autofirmada al conectarse al host proxy	79
Búsqueda de recopiladores en mal estado	80
Solucionar problemas con las direcciones IP	81
Solución de problemas de credenciales de vCenter	82
Solucionar problemas de reenvío de datos	82
Solucionar problemas de conexión	82
Soporte para hosts ESX independientes	84
Cómo contactar con AWS Support	84
Importación	86
Campos de archivo de importación admitidos	87
Configuración de los permisos de importación	92
Cargar el archivo importado en Amazon S3	95
Importación de datos	97
Seguimiento de solicitudes de importación de Migration Hub	99
Ver, exportar y explorar datos	101
Visualización de datos recopilados	101
Lógica de coincidencia	102
Exportación de datos recopilados	103
Exploración de datos en Athena	105
Permitir la exploración de datos en Amazon Athena	106
Uso de la exploración de datos en Amazon Athena	108
Tutoriales de la consola	119
Panel principal	119
Panel principal	119
Herramientas de recopilación de datos	120
Iniciar y detener los recopiladores de datos	120

Visualización y clasificación de recopiladores de datos	121
Ver, exportar y explorar datos	125
Visualización y clasificación de servidores	125
Etiquetado de servidores	126
Exportar datos del servidor	127
Exploración de datos en Athena	129
Aplicaciones	129
Uso de la API para consultar los elementos detectados	131
Uso de la DescribeConfigurations acción	131
Uso de la ListConfigurations acción	135
Consistencia final	151
Seguridad	152
Identity and Access Management	153
Público	153
Autenticación con identidades	154
Administración de acceso mediante políticas	157
¿Cómo AWS Application Discovery Service funciona con IAM	160
AWS políticas gestionadas	163
Ejemplos de políticas basadas en identidades	168
Descripción y uso de funciones vinculadas al servicio	175
IAM Solución de problemas	183
Registro y monitoreo en AWS Application Discovery Service	184
Registro de llamadas a la API de Application Discovery Service con AWS CloudTrail	184
Cuotas	188
Solución de problemas	189
Detenga la recopilación de datos mediante la exploración de datos	189
Elimine los datos recopilados mediante la exploración de datos	190
Solucione problemas comunes relacionados con la exploración de datos en Amazon Athena ..	192
La exploración de datos en Amazon Athena no se puede iniciar porque no se pueden crear las funciones vinculadas al servicio ni AWS los recursos necesarios	192
Los datos del nuevo agente no aparecen en Amazon Athena	192
No tiene permisos suficientes para acceder a Amazon S3, Amazon Data Firehose o AWS Glue	194
Solución de problemas de registros de importación fallidos	194
Historial de documento	197
Glosario de AWS	201

Apéndice	202
.....	202
Apéndice: Discovery Connector	202
Datos recopilados por Discovery Connector	203
Recopilación de datos sobre conectores	207
Solución de problemas del Discovery Connector	209
.....	ccxiv

¿Qué es AWS Application Discovery Service?

AWS Application Discovery Service con este, puede planificar su migración a la AWS nube de mediante la recopilación de datos de uso y de configuración de sus servidores y de bases de datos locales. El Application Discovery Service está integrado con AWS Migration Hub AWS Database Migration Service Fleet Advisor. Migration Hub simplifica el seguimiento de la migración, ya que agrega la información del estado de la migración en una sola consola. Puede ver los servidores detectados, agruparlos en aplicaciones y, a continuación, realizar un seguimiento del estado de migración de cada aplicación desde la consola de Migration Hub de su región de origen. Puede usar DMS Fleet Advisor para evaluar las opciones de migración para las cargas de trabajo de bases de datos.

Todos los datos descubiertos se almacenan en su región de AWS Migration Hub origen. Por lo tanto, debe configurar su región de origen en la consola de Migration Hub o con los comandos de la CLI antes de realizar cualquier actividad de detección y migración. Los datos se pueden exportar para su análisis en Microsoft Excel o en herramientas de AWS análisis como Amazon Athena y Amazon QuickSight.

Con las API de Application Discovery Service, puede exportar los datos de uso y rendimiento del sistema de los servidores detectados. Introduzca estos datos en su modelo de costos para calcular el costo de funcionamiento de esos servidores AWS. Además, puede exportar datos sobre las conexiones de red existentes entre servidores. Esto le ayudará a determinar las dependencias de red entre los servidores y agruparlas en aplicaciones para planear la migración.

Note

Debe configurar su región de origen AWS Migration Hub antes de comenzar el proceso de detección, ya que sus datos se almacenarán en su región de origen. Para obtener más información sobre cómo trabajar con una región de origen, consulte [Región de origen](#).

El servicio de detección de aplicaciones ofrece dos formas de detectar y recopilar datos sobre sus servidores locales:

- La detección sin agente se puede realizar mediante la implementación del recopilador sin agente de Application Discovery Service (recopilador sin agente) (archivo OVA) a través de VMware vCenter. Una vez configurado Agentless Collector, identifica las máquinas virtuales (VM) y los

hosts asociados a vCenter. Agentless Collector recopila los siguientes datos de configuración estática: nombres de servidor, direcciones IP, direcciones MAC, asignaciones de recursos de disco, versiones de motores de bases de datos y esquemas de bases de datos. Además, recopila los datos de uso de cada máquina virtual y base de datos y proporciona el uso promedio y máximo de métricas como la CPU, la RAM y la E/S del disco.

- La detección basada en agentes se puede realizar mediante la implementación del agente de detección de AWS aplicaciones en cada una de las máquinas virtuales y servidores físicos. El instalador del agente está disponible para sistemas operativos Windows y Linux. Recopila datos de configuración estáticos, información detallada del desempeño del sistema a lo largo del tiempo, las conexiones de red de entrada y salida y los procesos que se ejecutan.

El Application Discovery Service se integra con las soluciones de descubrimiento de aplicaciones de los socios de AWS Partner Network (APN). Estas soluciones de terceros pueden ayudarlo a importar detalles sobre su entorno local directamente a Migration Hub, sin utilizar ningún recopilador o agente de detección sin agentes. Las herramientas de descubrimiento de aplicaciones de terceros pueden consultar el AWS Application Discovery Service y escribir en la base de datos del Application Discovery Service mediante la API pública. De esta forma, puede importar datos en Migration Hub y consultarlos, de modo que pueda asociar aplicaciones con servidores y realizar un seguimiento de las migraciones.

Detección de VMware

Si tiene máquinas virtuales (VM) que se ejecutan en el entorno VMware vCenter, puede utilizar el recopilador sin agente para recopilar información del sistema sin tener que instalar un agente en cada máquina virtual. En lugar de ello, cargue esta aplicación local en vCenter y permita que detecte todos sus hosts y máquinas virtuales.

Agentless Collector captura la información sobre el rendimiento del sistema y la utilización de los recursos de cada máquina virtual que se ejecuta en vCenter, independientemente del sistema operativo que se utilice. Sin embargo, no puede examinar cada una de las máquinas virtuales y, por tanto, no puede averiguar qué procesos se están ejecutando en cada máquina virtual ni qué conexiones de red existen. Por lo tanto, si necesita este nivel de detalle y desea analizar más de cerca algunas de sus máquinas virtuales existentes para ayudarlo a planificar la migración, puede instalar el Discovery Agent según sea necesario.

Además, en el caso de las máquinas virtuales alojadas en VMware, puede utilizar tanto Agentless Collector como Discovery Agent para realizar el descubrimiento simultáneamente. Para obtener

más información acerca de los tipos de datos exactos que recopila cada herramienta de detección, consulte [Datos recopilados por Agentless Collector](#) y [Datos recopilados por Discovery Agent](#).

detección de bases de datos

Si tiene servidores de bases de datos y análisis en su entorno local, puede utilizar el recopilador sin agente para descubrir e inventariar estos servidores. A continuación, puede recopilar métricas de rendimiento para cada servidor de base de datos sin necesidad de instalar Agentless Collector en cada equipo de su entorno.

El módulo de recopilación de datos analíticos y bases de datos de Agentless Collector captura metadatos y métricas de rendimiento que proporcionan información sobre su infraestructura de datos. El módulo de recopilación de datos de bases de datos y análisis utiliza LDAP en Microsoft Active Directory para recopilar información sobre el sistema operativo, las bases de datos y los servidores de análisis de la red. A continuación, el módulo de recopilación de datos ejecuta consultas periódicamente para recopilar métricas de uso reales de la capacidad de la CPU, la memoria y el disco para las bases de datos y los servidores de análisis. Para obtener más información sobre las métricas recopiladas, consulte [Datos recopilados por la base de datos y el módulo de análisis](#).

Cuando Agentless Collector complete la recopilación de datos de su entorno, podrá utilizar la AWS DMS consola para realizar un análisis más detallado y planificar la migración. Por ejemplo, para elegir un destino de migración óptimo en Nube de AWS, puede generar recomendaciones de destinos para sus bases de datos de origen. Para obtener más información, consulte [Módulo de recopilación de datos analíticos y de bases de datos](#).

Compare Agentless Collector y Discovery Agent

La siguiente tabla proporciona una comparación rápida de las herramientas de recopilación de datos de Application Discovery Service.

	Recopilador sin agente	Application Discovery Service
Supported server types		
Máquina virtual de VMware	Sí	Sí
Servidor físico	No	Sí
Deployment		

	Recopilador sin agente	Application Discovery Service
Por servidor	No	Sí
Por vCenter	Sí	No
Collected data		
Datos de configuración de servidores estáticos	Yes	Yes
Datos de configuración de bases de datos	Yes	No
Métricas de utilización de máquina virtual	Yes	No
Métricas de uso de la base	Yes	No
Información de desempeño a lo largo del tiempo	No	Yes (Export only)
Conexiones de entrada/salida de red	No	Yes (Export only)
Procesos en ejecución	No	Yes (Export only)
Sistema operativo admitido	Any OS running in VMware vCenter V5.5+	Para ver la lista de los sistemas operativos Linux y Windows compatibles, consulte Requisitos previos para Discovery Agent .
Bases de datos compatibles	Oracle, SQL Server, MySQL, and PostgreSQL	Ninguno

Supuestos

Para utilizar Application Discovery Service, se asume lo siguiente:

- Se ha registrado en AWS. Para obtener más información, consulte [Configuración de Application Discovery Service](#).
- Ha seleccionado una región de origen de Migration Hub. Para obtener más información, consulte [la documentación de las regiones de origen](#).

Esto es lo que puede esperar:

- La región de origen de Migration Hub es la única región en la que Application Discovery Service almacena sus datos de descubrimiento y planificación.
- Los agentes de descubrimiento, los conectores y las importaciones solo se pueden usar en la región de origen de Migration Hub seleccionada.
- Para obtener una lista de AWS las regiones en las que puede utilizar Application Discovery Service, consulte la [Referencia general de Amazon Web Services](#).

Configuración de Application Discovery Service

Antes de usarlo AWS Application Discovery Service por primera vez, complete las siguientes tareas:

[Registro en Amazon Web Services](#)

[Cree usuarios de IAM](#)

[Inicia sesión en la consola de Migration Hub y elige una región de origen](#)

Registro en Amazon Web Services

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

Para suscribirse a una Cuenta de AWS

1. Abra <https://portal.aws.amazon.com/billing/signup>.
2. Siga las instrucciones que se le indiquen.

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

Cuando te registras en una Cuenta de AWS, Usuario raíz de la cuenta de AWS se crea una. 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 al usuario root para realizar [tareas que requieran dicho acceso](#).

Cree usuarios de IAM

Al crear una AWS cuenta, obtiene una identidad de inicio de sesión única con acceso completo a todos los AWS servicios y recursos de la cuenta. Esta identidad se denomina usuario raíz de la AWS cuenta. Al iniciar sesión AWS Management Console con la dirección de correo electrónico y la contraseña que utilizó para crear la cuenta, tendrá acceso completo a todos los AWS recursos de la cuenta.

Le recomendamos fuertemente que no utilice el usuario raíz en sus tareas cotidianas, incluso las tareas administrativas. En su lugar, siga las prácticas recomendadas de seguridad: [cree usuarios individuales de IAM](#) y cree un usuario administrador AWS Identity and Access Management (IAM).

A continuación, guarde las credenciales del usuario raíz en un lugar seguro y utilícelas tan solo para algunas tareas de administración de cuentas y servicios.

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

Temas

- [Creación de un usuario administrativo de IAM](#)
- [Creación de un usuario no administrativo de IAM](#)

Creación de un usuario administrativo de IAM

De forma predeterminada, una cuenta de administrador hereda todas las políticas necesarias para acceder a Application Discovery Service.

Para crear un usuario administrador

- Cree un usuario administrador en su AWS cuenta. Para obtener instrucciones, consulte [Creación del primer grupo de administradores y usuarios de IAM](#) en la Guía del usuario de IAM.

Creación de un usuario no administrativo de IAM

Al crear usuarios de IAM no administrativos, siga la práctica recomendada de seguridad de conceder [privilegios mínimos, que consiste en conceder a los usuarios permisos mínimos](#).

Utilice políticas gestionadas por IAM para definir el nivel de acceso a Application Discovery Service por parte de los usuarios de IAM no administrativos. Para obtener información sobre las políticas administradas de Application Discovery Service, consulte [AWS políticas gestionadas para AWS Application Discovery Service](#).

Para crear un usuario de IAM que no sea administrador

1. En AWS Management Console, navegue hasta la consola de IAM.
2. Cree un usuario de IAM que no sea administrador siguiendo las instrucciones para crear un usuario con la consola, tal y como se describe en la sección [Creación de un usuario de IAM en su AWS cuenta de la Guía del usuario](#) de IAM.

Siguiendo las instrucciones de la Guía del usuario de IAM:

- Cuando estés en el paso de seleccionar el tipo de acceso, selecciona Acceso programático. Tenga en cuenta que, si bien no se recomienda, seleccione el acceso a la consola de AWS administración únicamente si planea usar las mismas credenciales de usuario de IAM para acceder a la AWS consola.
- Cuando esté en el paso de la página Establecer permisos, elija la opción de adjuntar las políticas existentes directamente al usuario. A continuación, seleccione una política de IAM gestionada para Application Discovery Service de la lista de políticas. Para obtener información sobre las políticas administradas de Application Discovery Service, consulte [AWS políticas gestionadas para AWS Application Discovery Service](#).
- Cuando desee ver las claves de acceso del usuario (ID de clave de acceso y claves de acceso secretas), siga las instrucciones de la nota importante sobre cómo guardar el nuevo identificador de clave de acceso y clave de acceso secreta del usuario en un lugar seguro y protegido.

Inicia sesión en la consola de Migration Hub y elige una región de origen

Debe elegir una región de AWS Migration Hub origen en la AWS cuenta que está utilizando para AWS Application Discovery Service.

Para elegir la región de origen

1. Con tu AWS cuenta, inicia sesión en la consola de Migration Hub AWS Management Console y ábrela en <https://console.aws.amazon.com/migrationhub/>.
2. En el panel de navegación de la consola de Migration Hub, elija Configuración y, a continuación, elija una región de origen.

Los datos de Migration Hub se almacenan en su región de origen con fines de descubrimiento, planificación y seguimiento de la migración. Para obtener más información, consulte [la región de origen de The Migration Hub](#).

AWS Agente de descubrimiento de aplicaciones

El agente de detección de AWS aplicaciones (Discovery Agent) es un software que se instala en servidores y máquinas virtuales locales y está destinado a la detección y la migración. Los agentes capturan la configuración del sistema, el desempeño del sistema, los procesos en ejecución y detalles de las conexiones de red entre los sistemas. Los agentes son compatibles con la mayoría de los sistemas operativos Linux y Windows, y puede implementarlos en servidores físicos locales, instancias de Amazon EC2 y máquinas virtuales.

Note

Antes de implementar el Discovery Agent, debe elegir una [región de origen de Migration Hub](#). Debe registrar a su agente en su región de origen.

El Discovery Agent se ejecuta en su entorno local y requiere privilegios de root. Al iniciar el Discovery Agent, se conecta de forma segura con su región de origen y se registra en Application Discovery Service.

- Por ejemplo, si `eu-central-1` es su región de origen, se registra `arsenal-discovery.eu-central-1.amazonaws.com` en Application Discovery Service.
- O sustituya su región de origen por cualquier otra región, excepto `us-west-2`.
- Si `us-west-2` es su región de origen, se registra `arsenal.us-west-2.amazonaws.com` en Application Discovery Service.

Cómo funciona

Tras el registro, el agente comienza a recopilar datos para el host o la máquina virtual en la que reside. El agente hace ping al Application Discovery Service a intervalos de 15 minutos para obtener información de configuración.

Los datos recopilados incluyen especificaciones del sistema, datos de utilización o rendimiento a lo largo del tiempo, conexiones de red y datos de los procesos. Puede utilizar esta información para asignar sus recursos de TI y sus dependencias de red. Todos estos puntos de datos pueden ayudarlo a determinar el costo de ejecutar estos servidores AWS y también a planificar la migración.

Los Discovery Agents transmiten los datos de forma segura a Application Discovery Service mediante el cifrado Transport Layer Security (TLS). Los agentes están configurados para actualizarse automáticamente cuando se publican nuevas versiones. Esta configuración puede cambiarse si así lo desea.

 Tip

Antes de descargar e iniciar la instalación de Discovery Agent, asegúrese de leer todos los requisitos previos necesarios en [Requisitos previos para Discovery Agent](#)

Temas

- [Requisitos previos para Discovery Agent](#)
- [Instale Discovery Agent en Linux](#)
- [Instalación de en Windows.](#)
- [Datos recopilados por Discovery Agent](#)
- [Iniciar o detener la recopilación de datos de Discovery Agent](#)

Requisitos previos para Discovery Agent

Los siguientes son los requisitos previos y las tareas que debe realizar para poder instalar correctamente el AWS Application Discovery Agent (Discovery Agent).

- Debe establecer una [región de AWS Migration Hub origen](#) antes de empezar a instalar Discovery Agent.
- Si tiene instalada la versión 1.x del agente, debe eliminarla antes de instalar otra versión más reciente.
- Si el host en el que se va a instalar el agente ejecuta Linux, compruebe que el host sea compatible al menos con la arquitectura de CPU Intel i686 (también conocida como microarquitectura P6).
- 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 2003 R2 SP2

Windows Server 2008 R1 SP2, 2008 R2 SP1

Windows Server 2012 R1, 2012 R2

Windows Server 2016

Windows Server 2019

Windows Server 2022

- Si las conexiones salientes de la red están restringidas, tendrá que actualizar la configuración del firewall. Los agentes requieren acceso a `arsenal` a través del puerto TCP 443. No requieren ningún puerto de entrada abierto.

Por ejemplo, si su región de origen es `eu-central-1`, usaría `https://arsenal-discovery.eu-central-1.amazonaws.com:443`

- Para que la actualización automática funcione, es necesario tener acceso a Amazon S3 en su región de origen.
- Cree un usuario AWS Identity and Access Management (IAM) en la consola y adjunte la política gestionada de `AWSApplicationDiscoveryAgentAccess` IAM existente. Esta política permite al usuario realizar las acciones necesarias del agente en su nombre. Para obtener más información sobre las políticas administradas, consulte [AWS políticas gestionadas para AWS Application Discovery Service](#).
- Compruebe la diferencia horaria de sus servidores NTP (Network Time Protocol) y corríjala si es necesario. Si la sincronización de tiempo no se realiza correctamente, se producirá un error en la llamada de registro del agente.

Note

El Discovery Agent tiene un agente ejecutable de 32 bits, que funciona en sistemas operativos de 32 y 64 bits. Al tener un único ejecutable, se reduce el número de paquetes de instalación necesarios para la implementación. Este agente ejecutable funciona tanto

con sistemas operativos Linux como con sistemas operativos Windows. Lo veremos a continuación en las secciones de instalación correspondientes.

Instale Discovery Agent en Linux

Realice el siguiente procedimiento en Linux. Asegúrese de que la [región de origen de Migration Hub](#) esté configurada antes de iniciar este procedimiento.

Note

Si utiliza una versión no actual de Linux, consulte [Requisitos de las plataformas Linux más antiguas](#).

Para instalar AWS Application Discovery Agent en su centro de datos

1. Inicie sesión en su máquina virtual o servidor basado en Linux y cree un nuevo directorio que contenga los componentes del agente.
2. Vaya al nuevo directorio y descargue el script de instalación desde la línea de comandos o la consola.
 - a. Para descargarlo desde la línea de comandos, ejecute el siguiente comando.

```
curl -o ./aws-discovery-agent.tar.gz https://s3-us-west-2.amazonaws.com/aws-discovery-agent.us-west-2/linux/latest/aws-discovery-agent.tar.gz
```

- b. Para realizar la descarga desde la consola de Migration Hub, haga lo siguiente:
 - i. Abra la consola y vaya a la página [Discovery Tools \(Herramientas de detección\)](#).
 - ii. En el cuadro Discovery Agent (Agente de detección), elija Download agent (Descargar agente) y, a continuación, elija Linux en el cuadro de lista que aparece. La descarga comienza inmediatamente.
3. Verifique la firma criptográfica del paquete de instalación con estos tres comandos:

```
curl -o ./agent.sig https://s3.us-west-2.amazonaws.com/aws-discovery-agent.us-west-2/linux/latest/aws-discovery-agent.tar.gz.sig
```

```
curl -o ./discovery.gpg https://s3.us-west-2.amazonaws.com/aws-discovery-agent.us-west-2/linux/latest/discovery.gpg
```

```
gpg --no-default-keyring --keyring ./discovery.gpg --verify agent.sig aws-discovery-agent.tar.gz
```

La huella de la clave pública del agente de (discovery.gpg) es 7638 F24C 6717 F97C 4F1B 3BC0 5133 255E 4DF4 2DA2.

4. Realice la extracción desde el tarball como se muestra a continuación.

```
tar -xzf aws-discovery-agent.tar.gz
```

5. Para instalar el agente, elija uno de los siguientes métodos de instalación.

Para...	Haga lo siguiente...
Instale Discovery Agent	<p>Para instalar el agente, ejecute el comando <code>agent install</code> como se muestra en el siguiente ejemplo. En el ejemplo, <i>your-home-region</i> sustitúyalo por el nombre de la región de origen, <i>aws-access-key-id</i> por el identificador de la clave de acceso y <i>aws-secret-access-key</i> por la clave de acceso secreta.</p> <pre>sudo bash install -r <i>your-home-region</i> -k <i>aws-access-key-id</i> -s <i>aws-secret-access-key</i></pre> <p>De forma predeterminada, los agentes descargan y aplican automáticamente las actualizaciones a medida que están disponibles.</p> <p>Le recomendamos que utilice esta configuración predeterminada.</p>

Para...	Haga lo siguiente...
	<p>Sin embargo, si no desea que los agentes descarguen y apliquen las actualizaciones automáticamente, incluya el <code>-u false</code> parámetro al ejecutar el comando <code>agent install</code>.</p>
<p>(Opcional) Instale Discovery Agent y configure un proxy no transparente</p>	<p>Para configurar un proxy no transparente, añada los siguientes parámetros al comando <code>agent install</code>:</p> <ul style="list-style-type: none">• <code>-e</code> La contraseña del proxy.• <code>-f</code> El número de puerto del proxy.• <code>-g</code> El esquema de proxy.• <code>-i</code> El nombre de usuario del proxy. <p>A continuación, se muestra un ejemplo del comando <code>agent install</code> que utiliza parámetros de proxy no transparentes.</p> <pre>sudo bash install -r <i>your-home-region</i> -k <i>aws-access-key-id</i> -s <i>aws-secret-access-key</i> -d <i>myproxy.mycompany.com</i> -e <i>mypassword</i> -f <i>proxy-port-number</i> -g <i>https</i> -i <i>myusername</i></pre> <p>Si el proxy no requiere autenticación, omita los <code>-i</code> parámetros <code>-e</code> y.</p> <p>El comando <code>install</code> de ejemplo usa <code>https</code>, si tu proxy usa HTTP, especificar <code>http</code> el valor del <code>-g</code> parámetro.</p>

6. Si las conexiones salientes de la red están restringidas, tendrá que actualizar la configuración del firewall. Los agentes requieren acceso a `arsenal` a través del puerto TCP 443. No requieren ningún puerto de entrada abierto.

Por ejemplo, si su región de origen es `eu-central-1`, usaría `https://arsenal-discovery.eu-central-1.amazonaws.com:443`

Temas

- [Requisitos de las plataformas Linux más antiguas](#)
- [Administre el proceso de Discovery Agent en Linux](#)
- [Desinstale Discovery Agent en Linux](#)
- [Solución de problemas de Linux Discovery Agent](#)

Requisitos de las plataformas Linux más antiguas

Algunas plataformas de Linux antiguas como SUSE 10, CentOS 5 y RHEL 5, se encuentran al final de su ciclo de vida o solo reciben un soporte mínimo. Estas plataformas pueden tener conjuntos de out-of-date cifrado que impiden que el script de actualización del agente descargue los paquetes de instalación.

Curl

El agente Application Discovery es necesario `curl` para una comunicación segura con el AWS servidor. Algunas versiones anteriores de `curl` no pueden comunicarse de forma segura con un servicio web moderno.

Para utilizar la versión de `curl` incluida con Application Discovery Agent para todas las operaciones, ejecute el script de instalación con el parámetro `-c true`.

Paquete de entidades de certificación

Los sistemas Linux más antiguos pueden tener un paquete de autoridad de out-of-date certificación (CA), lo cual es fundamental para garantizar la comunicación por Internet.

Para utilizar el paquete de CA incluido con el Application Discovery Agent para todas las operaciones, ejecute el script de instalación con el parámetro `-b true`.

Estas opciones del script de instalación se pueden usar juntas. En el siguiente comando de ejemplo, ambos parámetros del script se pasan al script de instalación:

```
sudo bash install -r your-home_region -k aws-access-key-id -s aws-secret-access-key -c true -b true
```

Administre el proceso de Discovery Agent en Linux

Puede administrar el comportamiento del Discovery Agent a nivel del sistema mediante las System V `init` herramientas `systemd` `Upstart`, o. En las siguientes pestañas, se describen los comandos para las tareas que se admiten en cada una de las herramientas.

systemd

Comandos de administración de Application Discovery Agent

Tarea	Comando
Verificar que se está ejecutando un agente	<code>sudo systemctl status aws-discovery-daemon.service</code>
Iniciar un agente	<code>sudo systemctl start aws-discovery-daemon.service</code>
Detener un agente	<code>sudo systemctl stop aws-discovery-daemon.service</code>
Reiniciar un agente	<code>sudo systemctl restart aws-discovery-daemon.service</code>

Upstart

Comandos de administración del Application Discovery Agent

Tarea	Comando
Verificar que se está ejecutando un agente	<code>sudo initctl status aws-discovery-daemon</code>

Tarea	Comando
Iniciar un agente	<code>sudo initctl start aws-discovery-daemon</code>
Detener un agente	<code>sudo initctl stop aws-discovery-daemon</code>
Reiniciar un agente	<code>sudo initctl restart aws-discovery-daemon</code>

System V init

Comandos de administración para el Application Discovery Agent

Tarea	Comando
Verificar que se está ejecutando un agente	<code>sudo /etc/init.d/aws-discovery-daemon status</code>
Iniciar un agente	<code>sudo /etc/init.d/aws-discovery-daemon start</code>
Detener un agente	<code>sudo /etc/init.d/aws-discovery-daemon stop</code>
Reiniciar un agente	<code>sudo /etc/init.d/aws-discovery-daemon restart</code>

Desinstale Discovery Agent en Linux

En esta sección se describe cómo desinstalar Discovery Agent en Linux.

Para desinstalar un agente si utiliza el administrador de paquetes yum

- Use el siguiente comando para desinstalar un agente si usa yum.

```
rpm -e --nodeps aws-discovery-agent
```

Para desinstalar un agente si utiliza el administrador de paquetes apt-get

- Use el siguiente comando para desinstalar un agente si usa apt-get.

```
apt-get remove aws-discovery-agent:i386
```

Para desinstalar un agente si utiliza el administrador de paquetes zypper

- Use el siguiente comando para desinstalar un agente si usa zypper.

```
zypper remove aws-discovery-agent
```

Solución de problemas de Linux Discovery Agent

Si tiene problemas al instalar o utilizar el Discovery Agent en Linux, consulte la siguiente guía sobre el registro y la configuración. Para ayudar a solucionar posibles problemas con el agente o su conexión con Application Discovery Service, AWS Support suele solicitar estos archivos.

- Archivos de registro

Los archivos de registro de Discovery Agent se encuentran en el siguiente directorio.

```
/var/log/aws/discovery/
```

Los archivos de registro se denominan para indicar si los genera el daemon principal, el actualizador automático o el instalador.

- Archivos de configuración

Los archivos de configuración de la versión 2.0.1617.0 o posterior de Discovery Agent se encuentran en el siguiente directorio.

```
/etc/opt/aws/discovery/
```

Los archivos de configuración de las versiones de Discovery Agent anteriores a la 2.0.1617.0 se encuentran en el siguiente directorio.


```
/var/opt/aws/discovery/
```

- Para obtener instrucciones sobre cómo eliminar versiones anteriores del Discovery Agent, consulte. [Requisitos previos para Discovery Agent](#)

Instalación de en Windows.

Complete el procedimiento siguiente para instalar un agente en Windows. Asegúrese de que la [región de origen de Migration Hub](#) esté configurada antes de iniciar este procedimiento.

Para instalar AWS Application Discovery Agent en su centro de datos

1. Descargue el [instalador del agente de Windows](#), pero no haga doble clic para ejecutarlo en Windows.

Important


No haga doble clic para ejecutar el instalador en Windows, ya que no se instalará. La instalación del agente solo funciona desde el símbolo del sistema. (Si ya ha hecho doble clic en el instalador, debe ir a Agregar o quitar programas y desinstalar el agente antes de continuar con los pasos de instalación restantes).

Si el instalador del agente de Windows no detecta ninguna versión del motor de ejecución x86 de Visual C++ en el host, instalará automáticamente el motor de ejecución de Visual C++ x86 2015—2019 antes de instalar el software del agente.

2. Abra una línea de comandos como administrador y vaya a la ubicación en la que guardó el paquete de instalación.
3. Para instalar el agente, elija uno de los siguientes métodos de instalación.

Para...	Haga lo siguiente...
Instale Discovery Agent	Para instalar el agente, ejecute el comando <code>agent install</code> como se muestra en el siguiente ejemplo. En el ejemplo, <i>your-home-region</i> sustitúyalo por el nombre de la región de origen, <i>aws-access-key-id</i> por

Para...	Haga lo siguiente...
	<p>el ID de la clave de acceso y <i>aws-secret-access-key</i> por la clave de acceso secreta.</p> <p>Si lo desea, puede establecer la ubicación de instalación del agente especificando la ruta de la carpeta <i>C:\install-location</i> para el parámetro INSTALLLOCATION. Por ejemplo, INSTALLLOCATION=" <i>C:\install-location</i> ". La jerarquía de carpetas resultante será [ruta INSTALLLOCATION]\AWS Discovery. De forma predeterminada, la ubicación de instalación es la Program Files carpeta.</p> <p>Si lo desea, puede LOGANDCONFIGLOCATION reemplazar el directorio predeterminado (ProgramData) para la carpeta de registros del agente y el archivo de configuración. La jerarquía de carpetas resultante es [<i>LOGANDCONFIGLOCATION path</i>]\AWS Discovery .</p> <pre data-bbox="862 1255 1507 1495">.\AWSDiscoveryAgentInstaller.exe REGION=" <i>your-home-region</i> " KEY_ID=" <i>aws-access-key-id</i> " KEY_SECRET=" <i>aws-secret-access-key</i> " /quiet</pre> <p>De forma predeterminada, los agentes descargan y aplican automáticamente las actualizaciones a medida que están disponibles.</p> <p>Le recomendamos que utilice esta configuración predeterminada.</p>

Para...	Haga lo siguiente...
	<p>Sin embargo, si no desea que los agentes descarguen y apliquen las actualizaciones automáticamente, incluya el siguiente parámetro al ejecutar el comando <code>agent install</code>: <code>AUTO_UPDATE=false</code></p> <div data-bbox="862 478 1511 793" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Warning</p><p>La desactivación de las actualizaciones automáticas impedirá que se instalen los parches de seguridad más recientes.</p></div>

Para...	Haga lo siguiente...
(Opcional) Instale Discovery Agent y configure un proxy no transparente	<p data-bbox="862 226 1500 359">Para configurar un proxy no transparente, añada las siguientes propiedades públicas al comando <code>agent install</code>:</p> <ul data-bbox="862 401 1479 856" style="list-style-type: none">• <code>PROXY_HOST</code>: el nombre del host del proxy• <code>PROXY_SCHEME</code>: el esquema de proxy• <code>PROXY_PORT</code>: el número de puerto del proxy• <code>PROXY_USER</code>: el nombre de usuario del proxy• <code>PROXY_PASSWORD</code>: la contraseña del usuario proxy <p data-bbox="862 932 1500 1108">A continuación, se muestra un ejemplo del comando de instalación del agente que utiliza las propiedades del proxy no transparentes.</p> <pre data-bbox="862 1150 1500 1545">.\AWSDiscoveryAgentInstall.exe REGION=" <i>your-home-region</i> " KEY_ID=" <i>aws-access-key-id</i> " KEY_SECRET=" <i>aws-secret-access-key</i> " PROXY_HOST=" <i>myproxy.mycompany.com</i> " PROXY_SCHEME="http s" PROXY_PORT=" <i>proxy-port-number</i> " PROXY_USER=" <i>myusername</i> " PROXY_PASSWORD=" <i>mypassword</i> " /quiet</pre> <p data-bbox="862 1583 1500 1808">Si el proxy no requiere autenticación, omita las propiedades <code>PROXY_USER</code> y <code>PROXY_PASSWORD</code>. El ejemplo del comando <code>install</code> usa <code>https</code>. Si el proxy usa HTTP, especifique <code>http</code> el <code>PROXY_SCHEME</code> valor.</p>

4. Si las conexiones salientes de la red están restringidas, debe actualizar la configuración del firewall. Los agentes requieren acceso a `arsenal` a través del puerto TCP 443. No requieren ningún puerto de entrada abierto.

Por ejemplo, si tu región de origen es `eu-central-1`, utilizarías lo siguiente: `https://arsenal-discovery.eu-central-1.amazonaws.com:443`

Package Signing y actualizaciones automáticas

Para Windows Server 2008 y versiones posteriores, Amazon firma criptográficamente el paquete de instalación del agente Application Discovery Service con un certificado SHA256. Para las actualizaciones automáticas firmadas por SHA2 en Windows Server 2008 SP2, asegúrese de que los hosts tengan una revisión instalada para admitir la autenticación con firma SHA2. La [revisión de soporte más reciente de Microsoft ayuda a admitir la autenticación SHA2 en Windows Server 2008 SP2](#).

Note

Las revisiones de compatibilidad con SHA256 para Windows 2003 ya no están disponibles públicamente en Microsoft. Si estas correcciones aún no están instaladas en el host de Windows 2003, es necesario realizar actualizaciones manuales.

Para realizar las actualizaciones manualmente

1. Descargue el [Windows Agent Updater](#).
2. Abra la línea de comandos como administrador.
3. Navegue hasta la ubicación en la que se guardó el actualizador.
4. Ejecute el siguiente comando de la .

```
AWSDiscoveryAgentUpdater.exe /Q
```

Administre el proceso de Discovery Agent en Windows

Puede administrar el comportamiento del Discovery Agent a nivel del sistema mediante la consola de servicios de Windows Server Manager. En la tabla siguiente se describe cómo hacerlo.

Tarea	Nombre del servicio	Estado/acción del servicio
Verificar que se está ejecutando un agente	AWS Discovery Agent AWS Discovery Updater	Started
Iniciar un agente	AWS Agente de descubrimiento AWS Discovery Updater	Elija Inicio
Detener un agente	AWS Agente de descubrimiento AWS Discovery Updater	Elija Stop (Detener).
Reiniciar un agente	AWS Agente de descubrimiento AWS Discovery Updater	Elija Restart (Reiniciar).

Para desinstalar un agente de detección en Windows

1. Abra el panel de control en Windows.
2. Elija Programas.
3. Elija Programas y características.
4. Seleccione AWS Discovery Agent.
5. Elija Desinstalar.

Note

Si decide volver a instalar el agente después de desinstalarlo, ejecute el siguiente comando con las `/norestart` opciones `/repair` y.

```
.\AWSDiscoveryAgentInstaller.exe REGION="your-home-region" KEY_ID="aws-access-key-id" KEY_SECRET="aws-secret-access-key" /quiet /repair /norestart
```

Para desinstalar un agente de detección en Windows mediante la línea de comandos

1. Haga clic con el botón derecho en
2. Seleccione Símbolo del sistema.
3. Use el siguiente comando para desinstalar un agente de detección en Windows.

```
wmic product where name='AWS Discovery Agent' call uninstall
```

Solución de problemas de Discovery Agent en Windows

Si tiene problemas al instalar o utilizar el AWS Application Discovery Agent en Windows, consulte las siguientes instrucciones sobre el registro y la configuración. AWS Support a menudo solicita estos archivos para ayudar a solucionar posibles problemas con el agente o su conexión con Application Discovery Service.

- Registro de instalación

En algunos casos, el comando de instalación del agente parece fallar. Por ejemplo, podría parecer que se ha producido un error con el Administrador de servicios de Windows que indique que los servicios de detección no se han creado. En este caso, añada /log install.log al comando para generar un archivo de registro de instalación detallado.

- Registro de operaciones

En Windows Server 2008 y versiones posteriores, los archivos log del agente se encuentran en el siguiente directorio:

```
C:\ProgramData\AWS\AWS Discovery\Logs
```

En Windows Server 2003, los archivos log del agente se encuentran en el siguiente directorio:

```
C:\Documents and Settings\All Users\Application Data\AWS\AWS Discovery\Logs
```

Los archivos de registro se denominan para indicar si los ha generado el servicio principal, las actualizaciones automáticas o el instalador.

- Archivo de configuración

En Windows Server 2008 y versiones posteriores, el archivo log de configuración del agente se encuentra en la siguiente ubicación.

```
C:\ProgramData\AWS\AWS Discovery\config
```

En Windows Server 2003, el archivo log de configuración del agente se encuentra en la siguiente ubicación.

```
C:\Documents and Settings\All Users\Application Data\AWS\AWS Discovery\config
```

- Para obtener instrucciones sobre cómo eliminar versiones anteriores del Discovery Agent, consulte [Requisitos previos para Discovery Agent](#).

Datos recopilados por Discovery Agent

AWS El Application Discovery Agent (Discovery Agent) es un software que se instala en máquinas virtuales y servidores locales. Discovery Agent recopila la configuración del sistema, los datos de uso o rendimiento de las series temporales, los datos de proceso y las conexiones de red del Protocolo de control de transmisión (TCP). En esta sección se describen los datos que se recopilan.

Leyenda de la tabla sobre los datos recopilados por Discovery Agent:

- El término "host" hace referencia a un servidor físico o máquina virtual.
- Los datos recopilados se especifican en kilobytes (KB) a menos que se indique otra cosa.
- Los datos equivalentes de la consola de Migration Hub se muestran en megabytes (MB).
- El período de sondeo tiene intervalos de aproximadamente 15 segundos y se envía AWS cada 15 minutos.
- Los campos de datos marcados con un asterisco (*) solo están disponibles en los .csv archivos que se generan a partir de la función de exportación de la API del agente.

Campo de datos	Descripción
agentAssignedProcess ^{ID: *}	ID de los procesos detectados por el agente
agentId	ID único del agente
agentProvidedTimeSello [*]	Fecha y hora de observación del agente (mm/dd/aaaa hh:mm: ss am/pm)
cmdLine [*]	Proceso introducido en la línea de comandos
cpuType	Tipo de CPU (unidad de procesamiento central) utilizado en el host
destinationIp [*]	Dirección IP de dispositivo al que se envía el paquete
destinationPort [*]	Número de puerto al que se envíen los datos o la solicitud
family [*]	Protocolo de la familia de enrutamiento
freeRAM (MB)	RAM libre y RAM en caché que se puede poner inmediatamente a disposición de las aplicaciones, medida en MB
gateway [*]	Dirección del nodo de red
hostName	Nombre del host del que se recopilaron datos
hypervisor	Tipo de hipervisor
ipAddress	Dirección IP del host
ipVersion [*]	Número de versión de IP
isSystem [*]	Atributo booleano que indica si un proceso pertenece al sistema operativo
macAddress	Dirección MAC del host

Campo de datos	Descripción
name*	El nombre de los datos de host, red, métricas, etc. es recopilado por
netMask*	Prefijo de la dirección IP a la que pertenece un host de red
osName	Nombre del sistema operativo en el host
osVersion	Versión del sistema operativo en el host
ruta	Ruta del comando procedente de la línea de comandos
sourceIp*	Dirección IP del dispositivo que envía el paquete de direcciones IP
sourcePort*	Número de puerto desde el que se originan los datos o la solicitud
timestamp*	Fecha y hora del atributo notificado registrado por el agente
totalCpuUsagePacto	Porcentaje de utilización de la CPU en el host durante el periodo de sondeo
totalDiskBytesReadPerSecond (Kbps)	Kilobits totales leídos por segundo en todos los discos
totalDiskBytesWrittenPerSecond (Kbps)	Kilobits totales escritos por segundo en todos los discos
totalDiskFreeTamaño (GB)	Espacio disponible en el disco expresado en GB
totalDiskReadOpsPerSecond	Número total de operaciones de E/S de lectura por segundo
totalDiskSize (GB)	Capacidad total del disco expresada en GB

Campo de datos	Descripción
totalDiskWriteOpsPerSecond	Número total de operaciones de E/S de escritura por segundo
totalNetworkBytesReadPerSecond (Kbps)	Cantidad total de bytes leídos por segundo
totalNetworkBytesWrittenPerSecond (Kbps)	Cantidad total de bytes escritos por segundo
totalNumCores	Número total de unidades de procesamiento independientes en la CPU
totalNumCpus	Número total de unidades de procesamiento centrales
totalNumDisks	El número de discos duros físicos en un host
totalNumLogical ^{Procesadores *}	Cantidad total de núcleos físicos multiplicada por el número de subprocesos que se pueden ejecutar en cada núcleo
totalNumNetworkTarjetas	Número total de tarjetas de red en el servidor
totalRAM (MB)	Cantidad total de RAM disponible en el host
transportProtocol [*]	Tipo de protocolo de transporte utilizado

Iniciar o detener la recopilación de datos de Discovery Agent

Una vez implementado y configurado el Discovery Agent, si la recopilación de datos se detiene, puede reiniciarlo. Puede iniciar o detener la recopilación de datos a través de la consola o realizando llamadas a la API a través de AWS CLI. Ambos métodos se describen en los siguientes procedimientos.

Using the Migration Hub console

El siguiente procedimiento muestra cómo iniciar o detener el proceso de recopilación de datos de Discovery Agent, en la página Recopiladores de datos de la consola de Migration Hub.

Para iniciar o detener la recopilación de datos

1. En el panel de navegación, elija Data Collectors (Recopiladores de datos).
2. Elija la pestaña Agentes.
3. Seleccione la casilla del agente que desee iniciar o detener.

 Tip

Si ha instalado varios agentes pero solo quiere iniciar o detener la recopilación de datos en determinados hosts, la columna Nombre de host de la fila del agente identifica el host en el que está instalado el agente.

4. Elija Start data collection (Iniciar recopilación de datos) o Stop data collection (Detener recopilación de datos).

Using the AWS CLI

Para iniciar o detener el proceso de recopilación de datos de Discovery Agent desde AWS CLI, primero debe instalarlo AWS CLI en su entorno y, a continuación, debe configurar la CLI para que utilice la [región de origen de Migration Hub](#) seleccionada.

Para instalar AWS CLI e iniciar o detener la recopilación de datos

1. Si aún no lo ha hecho, instale el sistema AWS CLI apropiado para su tipo de sistema operativo (Windows o Mac/Linux). Consulte las [AWS Command Line Interface instrucciones en la Guía del usuario](#).
2. Abra el símbolo del sistema (Windows) o Terminal (MAC/Linux).
 - a. Escriba `aws configure` y pulse Intro.
 - b. Introduzca su ID de clave de AWS acceso y su clave de acceso AWS secreta.
 - c. Especifique la región de origen para el nombre de región predeterminado, por ejemplo, `us-west-2`. (En este ejemplo, se presupone que `us-west-2` es la región de origen).
 - d. Especifique `text` para el formato de salida predeterminado.
3. Para encontrar el ID del agente cuya recopilación de datos desea detener o iniciar, escriba el siguiente comando:

```
aws discovery describe-agents
```

4. Para iniciar la recopilación de datos por parte del agente, escriba el siguiente comando:

```
aws discovery start-data-collection-by-agent-ids --agent-ids <agent ID>
```

Para detener la recopilación de datos por parte del agente, escriba el siguiente comando:

```
aws discovery stop-data-collection-by-agent-ids --agent-ids <agent ID>
```

Recopilador sin agente de Application Discovery Service

Application Discovery Service Agentless Collector (Agentless Collector) es una aplicación local que recopila información a través de métodos sin agente sobre su entorno local, incluida la información del perfil del servidor (por ejemplo, el sistema operativo, la cantidad de CPU, la cantidad de RAM), los metadatos de la base de datos y las métricas de uso. Instala el Recopilador sin agente como una máquina virtual (VM) en su entorno VMware vCenter Server, utilizando un archivo de virtualización abierta (OVA).

El recopilador sin agente tiene una arquitectura modular que permite el uso de varios métodos de recopilación sin agente. Actualmente, Agentless Collector admite módulos para la recopilación de datos desde máquinas virtuales de VMware y desde servidores de bases de datos y análisis. Los módulos futuros admitirán la recopilación de conexiones de red, la recopilación desde plataformas de virtualización adicionales y la recopilación a nivel del sistema operativo.

Agentless Collector admite la recopilación de datos para el AWS Application Discovery Service (Application Discovery Service), lo que le ayuda a planificar la migración al Nube de AWS mediante la recopilación de datos de uso y configuración sobre sus servidores y bases de datos locales.

Application Discovery Service está integrado con AWS Migration Hub, lo que simplifica el seguimiento de la migración, ya que agrega la información del estado de la migración en una sola consola. Puede ver los servidores detectados, obtener recomendaciones de Amazon EC2, visualizar las conexiones de red, agrupar los servidores en aplicaciones y, a continuación, realizar un seguimiento del estado de migración de cada aplicación desde la consola de Migration Hub de su región de origen.

El módulo de recopilación de datos analíticos y de base de datos Agentless Collector está integrado con AWS Database Migration Service (AWS DMS). Esta integración le ayuda a planificar su migración a Nube de AWS. Puede utilizar el módulo de recopilación de datos de bases de datos y análisis para descubrir los servidores de bases de datos y análisis de su entorno y crear un inventario de los servidores a los que desee migrar a Nube de AWS. Este módulo de recopilación de datos recopila los metadatos de la base de datos y las métricas de uso real de la capacidad de la CPU, la memoria y el disco. Una vez recopiladas estas métricas, puede usar la AWS DMS consola para generar recomendaciones de destino para sus bases de datos de origen.

Temas

- [Primeros pasos con Agentless Collector](#)

- [Datos recopilados por Agentless Collector](#)
- [Uso de la consola Agentless Collector](#)
- [Actualización manual de Agentless Collector](#)
- [Solución de problemas de Agentless Collector](#)

Primeros pasos con Agentless Collector

En esta sección se describe cómo empezar a utilizar Application Discovery Service Agentless Collector (Agentless Collector).

Temas

- [Requisitos previos para Agentless Collector](#)
- [Paso 1: Cree un usuario de IAM para Agentless Collector](#)
- [Paso 2: Descargue el recopilador sin agente](#)
- [Paso 3: Implemente un recopilador sin agente](#)
- [Paso 4: Acceda a la consola de Agentless Collector](#)
- [Paso 5: Configurar el recopilador sin agente](#)
- [Paso 6: Configurar los módulos de recopilación de datos de Agentless Collector](#)
- [Paso 7: Ver los datos recopilados](#)

Requisitos previos para Agentless Collector

Los siguientes son los requisitos previos para utilizar Application Discovery Service Agentless Collector (Agentless Collector):

- Una o más cuentas. AWS
- Una AWS cuenta con la región de AWS Migration Hub origen configurada, consulte [Inicia sesión en la consola de Migration Hub y elige una región de origen](#). Los datos de Migration Hub se almacenan en su región de origen con fines de descubrimiento, planificación y seguimiento de la migración.
- Un usuario de IAM de AWS cuenta que está configurado para usar la política AWS `AWSApplicationDiscoveryAgentlessCollectorAccess` administrada. Para usar el módulo de recopilación de datos analíticos y de bases de datos, este usuario de IAM también

debe usar dos políticas de IAM administradas por el cliente: `y. DMSCollectorPolicy` y `FleetAdvisorS3Policy`. Para obtener más información, consulte [Paso 1: Cree un usuario de IAM para Agentless Collector](#). El usuario de IAM debe crearse en una AWS cuenta con la región de origen de Migration Hub configurada.

- VMware vCenter Server V5.5, V6, V6.5, 6.7 o 7.0.

Note

El recopilador sin agente es compatible con todas estas versiones de VMware, pero actualmente estamos realizando pruebas con las versiones 6.7 y 7.0.

- Para la configuración de VMware vCenter Server, asegúrese de que puede proporcionar las credenciales de vCenter con los permisos de lectura y visualización establecidos para el grupo de sistemas.
- Agentless Collector requiere acceso saliente a varios dominios a través del puerto TCP 443. AWS Para obtener una lista de estos dominios, consulte [Configure el firewall para el acceso saliente a los dominios AWS](#)
- Para usar el módulo de recopilación de datos de bases de datos y análisis, cree un bucket de Amazon S3 en la Región de AWS que haya establecido como región de origen de Migration Hub. Los módulos de recopilación de datos de bases de datos y análisis almacenan los metadatos del inventario en este depósito de Amazon S3. Para obtener más información, consulte [Creación de un bucket](#) en la Guía del usuario de Amazon S3.

Configure el firewall para el acceso saliente a los dominios AWS

Si las conexiones salientes de su red están restringidas, debe actualizar la configuración del firewall para permitir el acceso saliente a los AWS dominios que requiere Agentless Collector. AWS Los dominios que requieren acceso saliente dependen de si la región de origen de su Migration Hub es la región US West (Oregón), us-west-2 o alguna otra región.

Los siguientes dominios requieren acceso saliente si la región de origen de su AWS cuenta es us-west-2:

- `arsenal-discovery.us-west-2.amazonaws.com`— El recopilador utiliza este dominio para validar que está configurado con las credenciales de usuario de IAM requeridas. El recopilador también lo usa para enviar y almacenar los datos recopilados, ya que la región de origen es us-west-2.

- `migrationhub-config.us-west-2.amazonaws.com`— El recopilador utiliza este dominio para determinar a qué región de origen envía los datos el recopilador en función de las credenciales de usuario de IAM proporcionadas.
- `api.ecr-public.us-east-1.amazonaws.com`— El recopilador usa este dominio para descubrir las actualizaciones disponibles.
- `public.ecr.aws`— El recopilador usa este dominio para descargar las actualizaciones.
- `dms.your-migrationhub-home-region.amazonaws.com`— El recopilador usa este dominio para conectarse al recopilador AWS DMS de datos.
- `s3.amazonaws.com`— El recopilador utiliza este dominio para cargar los datos recopilados por la base de datos y el módulo de recopilación de datos analíticos a su bucket de Amazon S3.

Los siguientes dominios requieren acceso saliente si la región de origen de su AWS cuenta no **us-west-2** lo es:

- `arsenal-discovery.us-west-2.amazonaws.com`— El recopilador utiliza este dominio para validar que está configurado con las credenciales de usuario de IAM requeridas.
- `arsenal-discovery.your-migrationhub-home-region.amazonaws.com`— El recopilador utiliza este dominio para enviar y almacenar los datos recopilados.
- `migrationhub-config.us-west-2.amazonaws.com`— El recopilador usa este dominio para determinar a qué región de origen debe enviar los datos basándose en las credenciales de usuario de IAM proporcionadas.
- `api.ecr-public.us-east-1.amazonaws.com`— El recopilador usa este dominio para descubrir las actualizaciones disponibles.
- `public.ecr.aws`— El recopilador usa este dominio para descargar las actualizaciones.
- `dms.your-migrationhub-home-region.amazonaws.com`— El recopilador usa este dominio para conectarse al recopilador AWS DMS de datos.
- `s3.amazonaws.com`— El recopilador utiliza este dominio para cargar los datos recopilados por la base de datos y el módulo de recopilación de datos analíticos a su bucket de Amazon S3.

Al configurar Agentless Collector, es posible que recibas errores como un error en la configuración: comprueba tus credenciales e inténtalo de nuevo o AWSno puedes contactar con él. Compruebe la configuración de la red. Estos errores pueden deberse a un intento fallido del recopilador sin agente de establecer una conexión HTTPS con uno de los AWS dominios a los que necesita acceso saliente.

Si AWS no se puede establecer una conexión, Agentless Collector no podrá recopilar datos de su entorno local. Para obtener información sobre cómo arreglar la conexión aAWS, consulte.

[Reparación: no se puede acceder a Agentless Collector durante la configuración AWS](#)

Paso 1: Cree un usuario de IAM para Agentless Collector

Para usar Agentless Collector, en la AWS cuenta que utilizó [Inicia sesión en la consola de Migration Hub y elige una región de origen](#), debe crear un AWS Identity and Access Management usuario (IAM). A continuación, configure este usuario de IAM para que utilice la siguiente política administrada. AWS [AWSApplicationDiscoveryAgentlessCollectorAccess](#) Esta política de IAM se adjunta al crear el usuario de IAM.

Para usar el módulo de recopilación de datos analíticos y de bases de datos, cree dos políticas de IAM administradas por el cliente. Estas políticas proporcionan acceso a su bucket de Amazon S3 y a la AWS DMS API. Para obtener más información, consulte [Crear una política gestionada por el cliente](#) en la Guía del usuario de IAM.

- Utilice el siguiente código JSON para crear la **DMSCollectorPolicy** política.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "dms:DescribeFleetAdvisorCollectors",
      "dms:ModifyFleetAdvisorCollectorStatuses",
      "dms:UploadFileMetadataList"
    ],
    "Resource": "*"
  }]
}
```

- Utilice el siguiente código JSON para crear la **FleetAdvisorS3Policy** política.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject*"
      ]
    }
  ]
}
```

```
        "s3:GetBucket*",
        "s3:List*",
        "s3:DeleteObject*",
        "s3:PutObject*"
    ],
    "Resource": [
        "arn:aws:s3:::bucket_name",
        "arn:aws:s3:::bucket_name/*"
    ]
}
]
```

En el ejemplo anterior, *bucket_name* sustitúyalo por el nombre del bucket de Amazon S3 que creó en el paso de requisitos previos.

Le recomendamos que cree un usuario de IAM no administrativo para usarlo con Agentless Collector. Al crear usuarios de IAM no administrativos, siga la práctica recomendada de seguridad de conceder [privilegios mínimos, que consiste en conceder a los usuarios permisos](#) mínimos.

Para crear un usuario de IAM que no sea administrador y utilizarlo con Agentless Collector

1. En AWS Management Console, navegue hasta la consola de IAM con la AWS cuenta que utilizó para configurar la región de origen. [Inicia sesión en la consola de Migration Hub y elige una región de origen](#)
2. Cree un usuario de IAM que no sea administrador siguiendo las instrucciones para crear un usuario con la consola, tal y como se describe en la sección [Creación de un usuario de IAM en su AWS cuenta de la Guía del usuario](#) de IAM.

Siguiendo las instrucciones de la Guía del usuario de IAM:

- Cuando estés en el paso de seleccionar el tipo de acceso, selecciona Acceso programático. Tenga en cuenta que, si bien no se recomienda, seleccione el acceso a la consola de AWS administración únicamente si planea usar las mismas credenciales de usuario de IAM para acceder a la AWS consola.
- Cuando esté en el paso de la página Establecer permisos, elija la opción de adjuntar las políticas existentes directamente al usuario. A continuación, seleccione la política `AWSApplicationDiscoveryAgentlessCollectorAccess` AWS gestionada de la lista de políticas.

A continuación, seleccione las políticas `DMSCollectorPolicy` de IAM administradas por el `FleetAdvisorS3Policy` cliente.

- Cuando esté viendo las claves de acceso del usuario (ID de clave de acceso y claves de acceso secretas), siga las instrucciones de la nota importante sobre cómo guardar el nuevo identificador de clave de acceso y clave de acceso secreta del usuario en un lugar seguro y protegido. Necesitará introducir estas claves de acceso [Paso 5: Configurar el recopilador sin agente](#).

Rotar las claves de acceso es una práctica recomendada de AWS seguridad. Para obtener información sobre la rotación de claves, consulte [Rotar las claves de acceso con regularidad para los casos de uso que requieran credenciales de larga duración](#) en la Guía del usuario de IAM.

Paso 2: Descargue el recopilador sin agente

Para configurar el Application Discovery Service Agentless Collector (Agentless Collector), debe descargar e implementar el archivo Agentless Collector Open Virtualization Archive (OVA). El recopilador sin agente es un dispositivo virtual que se instala en su entorno VMware local. En este paso se describe cómo descargar el archivo OVA del recopilador y en el siguiente paso se describe cómo implementarlo.

Para descargar el archivo OVA del recopilador y comprobar su suma de comprobación

1. Inicie sesión en vCenter como administrador de VMware y cambie al directorio en el que desee descargar el archivo OVA de Agentless Collector.
2. Descargue el archivo OVA desde la siguiente URL:

[Collector sin agente \(OVA\)](#)

3. En función del algoritmo hash que utilice en su entorno, descargue [MD5](#) o [SHA256](#) para obtener el archivo que contiene el valor de la suma de comprobación. Utilice el valor descargado para verificar el `ApplicationDiscoveryServiceAgentlessCollector` archivo descargado en el paso anterior.
4. Dependiendo de su variación de Linux, ejecute el comando MD5 apropiado o el comando SHA256 para verificar que la firma criptográfica del archivo `ApplicationDiscoveryServiceAgentlessCollector.ova` coincida con el valor del archivo MD5/SHA256 correspondiente que ha descargado.

```
$ md5sum ApplicationDiscoveryServiceAgentlessCollector.ova
```

```
$ sha256sum ApplicationDiscoveryServiceAgentlessCollector.ova
```

Paso 3: Implemente un recopilador sin agente

Application Discovery Service Agentless Collector (Agentless Collector) es un dispositivo virtual que se instala en su entorno VMware local. En esta sección, se describe cómo implementar el archivo Open Virtualization Archive (OVA) que descargó en el paso anterior en su entorno de VMware.

Especificaciones de la máquina virtual Agentless Collector

- Sistema operativo — Amazon Linux 2
- RAM: 16 GB
- CPU: 4 núcleos

El siguiente procedimiento explica cómo implementar el archivo OVA de Agentless Collector en su entorno VMware.

Para implementar Agentless Collector

1. Inicie sesión en vCenter como administrador de VMware.
2. Utilice uno de los siguientes métodos para instalar el archivo OVA:
 - Utilice la interfaz de usuario: elija Archivo, elija Implementar plantilla de OVF, seleccione el archivo OVA recopilador que descargó en la sección anterior y, a continuación, complete el asistente.
 - Utilice la línea de comandos: para instalar el archivo OVA del recopilador desde la línea de comandos, descargue y utilice la herramienta de formato de virtualización abierta de VMware (ovftool). Para descargar ovftool, seleccione una versión de la página de documentación de la herramienta [OVF](#).

El siguiente es un ejemplo del uso de la herramienta de línea de comandos ovftool para instalar el archivo OVA del recopilador.

```
ovftool --acceptAllEulas --name=AgentlessCollector --datastore=datastore1  
-dm=thin ApplicationDiscoveryServiceAgentlessCollector.ova  
'vi://username:password@vcenterurl/Datacenter/host/esxi/'
```

A continuación se describen los valores *reemplazables* del ejemplo

- El nombre es el nombre que desea usar para su máquina virtual Agentless Collector.
 - El almacén de datos es el nombre del almacén de datos de su vCenter.
 - El nombre del archivo OVA es el nombre del archivo OVA del recopilador descargado.
 - El nombre de usuario y la contraseña son sus credenciales de vCenter.
 - La URL de vCenter es la URL de su vCenter.
 - La ruta vi es la ruta a su host VMware ESXi.
3. Localice el recopilador sin agente implementado en su vCenter. Haga clic con el botón derecho en la máquina virtual y, a continuación, seleccione Power, Power On.
 4. Transcurridos unos minutos, la dirección IP del recopilador aparece en vCenter. Esta dirección IP se utiliza para conectarse al recopilador.

Paso 4: Acceda a la consola de Agentless Collector

El siguiente procedimiento describe cómo acceder a la consola Application Discovery Service Agentless Collector (Agentless Collector).

Para acceder a la consola Agentless Collector

1. Abra un navegador web y, a continuación, escriba la siguiente URL en la barra de direcciones: **https://<ip_address>**, donde <ip_address> se encuentra la dirección IP del recopilador.
[Paso 3: Implemente un recopilador sin agente](#)
2. Seleccione Comenzar la primera vez que acceda a Agentless Collector. A partir de entonces, se le pedirá que inicie sesión.

Si es la primera vez que accedes a la consola de Agentless Collector, lo harás. [Paso 5: Configurar el recopilador sin agente](#) De lo contrario, verás a continuación. [El panel de control de Agentless Collector](#)

Paso 5: Configurar el recopilador sin agente

Application Discovery Service Agentless Collector (Agentless Collector) es una máquina virtual (VM) basada en Amazon Linux 2. La siguiente sección describe cómo configurar una máquina virtual recopiladora en la página Configurar un recopilador sin agente de la consola Agentless Collector.

Para configurar una máquina virtual recopiladora, consulte la página Configurar un recopilador sin agente

1. En Nombre del recopilador, introduzca un nombre para que el recopilador lo identifique. El nombre puede contener espacios pero no caracteres especiales.
2. En Sincronización de datos, introduzca la clave de AWS acceso y la clave secreta para que el usuario de IAM especifique la AWS cuenta como cuenta de destino para recibir los datos descubiertos por el recopilador. Para obtener información sobre los requisitos del usuario de IAM, consulte. [Paso 1: Cree un usuario de IAM para Agentless Collector](#)
 - a. Para la AWS clave de acceso, introduzca la clave de acceso del usuario de IAM de la AWS cuenta que está especificando como cuenta de destino.
 - b. En el AWS caso de la clave secreta, introduce la clave secreta del usuario de IAM de la AWS cuenta que estás especificando como cuenta de destino.
 - c. (Opcional) Si su red requiere el uso de un proxy para acceder a AWS, introduzca el host del proxy, el puerto del proxy y, si lo desea, las credenciales necesarias para autenticarse con el servidor proxy actual.
3. En Contraseña de Agentless Collector, configure una contraseña para autenticar el acceso a Agentless Collector.
 - Las contraseñas distinguen mayúsculas de minúsculas
 - Las contraseñas deben tener una longitud de entre 8 y 64 caracteres
 - También deben contener al menos un carácter de cada una de las siguientes cuatro categorías:
 - Letras minúsculas (a-z)
 - Letras mayúsculas (A-Z)
 - Números (0-9)
 - Caracteres no alfanuméricos (@\$! #%^*? &)
 - Las contraseñas no pueden contener caracteres especiales distintos de los siguientes: @\$! #%^*? &

- a. En el caso de la contraseña del recopilador sin agente, introduzca una contraseña para autenticar el acceso al recopilador.
 - b. Para volver a introducir la contraseña de Agentless Collector, para verificarla, vuelva a introducir la contraseña.
4. En Otros ajustes, lea el contrato de licencia. Si está de acuerdo en aceptarlo, active la casilla de verificación.
 5. Para activar las actualizaciones automáticas de Agentless Collector, en Otros ajustes, selecciona Actualizar automáticamente Agentless Collector. Si no selecciona esta casilla de verificación, tendrá que actualizar manualmente Agentless Collector como se describe en [Actualización manual de Agentless Collector](#)
 6. Seleccione Guardar configuraciones.

En los temas siguientes se describen las tareas opcionales de configuración del recopilador.

Tareas de configuración opcionales

- [\(Opcional\) Configure una dirección IP estática para la máquina virtual Agentless Collector](#)
- [\(Opcional\) Restablezca la máquina virtual Agentless Collector para que utilice DHCP](#)
- [\(Opcional\) Configure el protocolo de autenticación Kerberos](#)

(Opcional) Configure una dirección IP estática para la máquina virtual Agentless Collector

Los siguientes pasos describen cómo configurar una dirección IP estática para la máquina virtual Application Discovery Service Agentless Collector (Agentless Collector). Cuando se instala por primera vez, la máquina virtual recopiladora se configura para utilizar el Protocolo de configuración dinámica de host (DHCP).

Note

El recopilador sin agente es compatible con IPv4. No es compatible con IPv6.

Para configurar una dirección IP estática para la máquina virtual recopiladora

1. Recopile la siguiente información de red de VMware vCenter:
 - Dirección IP estática: una dirección IP sin firmar en la subred. Por ejemplo, 192.168.1.138.
 - Máscara de red: se puede obtener comprobando la configuración de la dirección IP del host VMware vCenter que aloja la máquina virtual recopiladora. Por ejemplo, 255.255.255.0.
 - Puerta de enlace predeterminada: se puede obtener comprobando la configuración de la dirección IP del host VMware vCenter que aloja la máquina virtual recopiladora. Por ejemplo, 192.168.1.1.
 - DNS principal: se puede obtener comprobando la configuración de la dirección IP del host VMware vCenter que aloja la máquina virtual recopiladora. Por ejemplo, 192.168.1.1.
 - DNS secundario (opcional)
 - (Opcional) Nombre de dominio local: permite al recopilador acceder a la URL del host de vCenter sin el nombre de dominio.
2. Abra la consola de máquina virtual del recopilador e inicie sesión **ec2-user** con la contraseña, **collector** como se muestra en el siguiente ejemplo.

```
username: ec2-user
password: collector
```

3. Inhabilite la interfaz de red introduciendo el siguiente comando en el terminal remoto.

```
sudo /sbin/ifdown eth0
```

4. Actualice la configuración de la interfaz eth0 mediante los siguientes pasos.

- a. Abra ifcfg-eth0 en el editor vi con el siguiente comando.

```
sudo vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

- b. Actualice los valores de la interfaz, como se muestra en el siguiente ejemplo, con la información que recopile en el paso Recopilar información de red.

```
DEVICE=eth0
BOOTPROTO=static
ONBOOT=yes
IPADDR=static-ip-value
```

```
NETMASK=netmask-value  
GATEWAY=gateway-value  
TYPE=Ethernet  
USERCTL=yes  
PEERDNS=no  
RES_OPTIONS="timeout:2 attempts:5"
```

5. Actualice el sistema de nombres de dominio (DNS) siguiendo estos pasos.
 - a. Abra el `resolv.conf` archivo en vi con el siguiente comando.

```
sudo vi /etc/resolv.conf
```

- b. Actualice el `resolv.conf` archivo en vi mediante el siguiente comando.

```
search localdomain-name  
options timeout:2 attempts:5  
nameserver dnserver-value
```

El siguiente ejemplo muestra un `resolv.conf` archivo editado.

```
search vsphere.local  
options timeout:2 attempts:5  
nameserver 192.168.1.1
```

6. Active la interfaz de red introduciendo el siguiente comando.

```
sudo /sbin/ifup eth0
```

7. Reinicie la máquina virtual como se muestra en el siguiente ejemplo.

```
sudo reboot
```

8. Compruebe la configuración de la red mediante los siguientes pasos.

- a. Compruebe si la dirección IP está configurada correctamente introduciendo los siguientes comandos.

```
ifconfig  
  
ip addr show
```

- b. Compruebe que la puerta de enlace se agregó correctamente introduciendo el siguiente comando.

```
route -n
```

El resultado debe ser similar al del siguiente ejemplo.

```
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0          192.168.1.1    0.0.0.0         UG    0     0      0 eth0
172.17.0.0       0.0.0.0        255.255.0.0     U     0     0      0 docker0
192.168.1.0      0.0.0.0        255.255.255.0   U     0     0      0
```

- c. Compruebe que puede hacer ping a una URL pública introduciendo el siguiente comando.

```
ping www.google.com
```

- d. Compruebe que puede hacer ping a la dirección IP o al nombre de host de vCenter, como se muestra en el siguiente ejemplo.

```
ping vcenter-host-url
```

(Opcional) Restablezca la máquina virtual Agentless Collector para que utilice DHCP

En los siguientes pasos, se describe cómo volver a configurar la máquina virtual recopiladora sin agente para que utilice DHCP.

Para configurar la máquina virtual recopiladora para que utilice DHCP

1. Inhabilite la interfaz de red introduciendo el siguiente comando en el terminal remoto.

```
sudo /sbin/ifdown eth0
```

2. Actualice la configuración de la red mediante los siguientes pasos.

- a. Abra el `ifcfg-eth0` archivo en el editor vi con el siguiente comando.

```
sudo /sbin/ifdown eth0
```

- b. Actualice los valores del `ifcfg-eth0` archivo como se muestra en el siguiente ejemplo.

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
TYPE=Ethernet
USERCTL=yes
PEERDNS=yes
DHCPV6C=yes
DHCPV6C_OPTIONS=-nw
PERSISTENT_DHCLIENT=yes
RES_OPTIONS="timeout:2 attempts:5"
```

3. Restablezca la configuración de DNS introduciendo el siguiente comando.

```
echo "" | sudo tee /etc/resolv.conf
```

4. Habilite la interfaz de red ingresando el siguiente comando.

```
sudo /sbin/ifup eth0
```

5. Reinicie la máquina virtual del recopilador como se muestra en el siguiente ejemplo.

```
sudo reboot
```

(Opcional) Configure el protocolo de autenticación Kerberos

Si el servidor del sistema operativo admite el protocolo de autenticación Kerberos, puede utilizar este protocolo para conectarse al servidor. Para ello, debe configurar la máquina virtual Application Discovery Service Agentless Collector.

Los siguientes pasos describen cómo configurar el protocolo de autenticación Kerberos en su máquina virtual Application Discovery Service Agentless Collector.

Para configurar el protocolo de autenticación Kerberos en su máquina virtual recopiladora

1. Abra la consola de máquina virtual del recopilador e inicie sesión **ec2-user** con la contraseña, **collector** como se muestra en el siguiente ejemplo.

```
username: ec2-user
password: collector
```

2. Abre el archivo `krb5.conf` de configuración de la `/etc` carpeta. Para ello, puede utilizar el siguiente ejemplo de código.

```
cd /etc
sudo nano krb5.conf
```

3. Actualice el archivo de `krb5.conf` configuración con la siguiente información.

```
[libdefaults]
    forwardable = true
    dns_lookup_realm = true
    dns_lookup_kdc = true
    ticket_lifetime = 24h
    renew_lifetime = 7d
    default_realm = default_Kerberos_realm

[realms]
default_Kerberos_realm = {
    kdc = KDC_hostname
    server_name = server_hostname
    default_domain = domain_to_expand_hostnames
}

[domain_realm]
    .domain_name = default_Kerberos_realm
    domain_name = default_Kerberos_realm
```

Guarde el archivo y salga del editor de texto.

4. Reinicie la máquina virtual del compilador como se muestra en el siguiente ejemplo.

```
sudo reboot
```

Paso 6: Configurar los módulos de recopilación de datos de Agentless Collector

En la página del panel de control de la consola Application Discovery Service Agentless Collector (Agentless Collector), en Recopilación de datos, configura el módulo de recopilación de datos para recopilar datos de inventario, perfil y utilización de sus servidores.

Actualmente, Agentless Collector admite la recopilación de datos desde máquinas virtuales de VMware y desde servidores de bases de datos y análisis. Los módulos futuros admitirán la recopilación desde plataformas de virtualización adicionales y la recopilación a nivel del sistema operativo.

Temas

- [Módulo de recopilación de datos VMware vCenter Agentless Collector](#)
- [Módulo de recopilación de datos analíticos y de bases de datos](#)

Módulo de recopilación de datos VMware vCenter Agentless Collector

En esta sección se describe el módulo de recopilación de datos de VMware vCenter de Application Discovery Service (Agentless Collector), que se utiliza para recopilar datos de inventario, perfil y utilización de los servidores de sus máquinas virtuales de VMware.

Temas

- [Cómo configurar el módulo de recopilación de datos Agentless Collector para VMware vCenter](#)
- [Detalles de la recopilación de datos de VMware](#)
- [Controle el alcance de la recopilación de datos de vCenter](#)

Cómo configurar el módulo de recopilación de datos Agentless Collector para VMware vCenter

En esta sección se describe cómo configurar el módulo de recopilación de datos de VMware vCenter de Agentless Collector para recopilar datos de inventario, perfil y utilización de los servidores de sus máquinas virtuales de VMware.

Note

Antes de iniciar la configuración de vCenter, asegúrese de que puede proporcionar las credenciales de vCenter con los permisos de lectura y visualización establecidos para el grupo Sistema.

Para configurar el módulo de recopilación de datos de VMware vCenter

1. En la página del panel de control de Agentless Collector, en Recopilación de datos, seleccione Configurar en la sección VMware vCenter.

2. En la página Configurar la recopilación de datos de VMware vCenter, realice lo siguiente:
 - a. En las credenciales de vCenter:
 - i. Para la URL/IP de vCenter, introduzca la dirección IP de su host de VMware vCenter Server.
 - ii. Para el nombre de usuario de vCenter, introduzca el nombre de un usuario local o de dominio que el recopilador utilice para comunicarse con vCenter. Para usuarios del dominio, utilice el formato dominio\nombre de usuario o nombre de usuario@dominio.
 - iii. En vCenter Password (Contraseña de vCenter), escriba la contraseña de usuario local o del dominio.
 - b. En Preferencias de recopilación de datos:
 - Para empezar a recopilar datos automáticamente inmediatamente después de una configuración correcta, seleccione Iniciar la recopilación de datos automáticamente.
 - c. Elija Set up (Configurar).

A continuación, verá la página de detalles sobre la recopilación de datos de VMware, que se describe en el tema siguiente.

Detalles de la recopilación de datos de VMware

La página de detalles de recopilación de datos de VMware muestra detalles sobre el vCenter en el que se configuró [Cómo configurar el módulo de recopilación de datos Agentless Collector para VMware vCenter](#).

En Servidores vCenter detectados, el vCenter que configuró aparece con la siguiente información sobre el vCenter:

- Dirección IP del servidor vCenter.
- La cantidad de servidores de vCenter.
- El estado de la recopilación de datos.
- Cuánto tiempo ha pasado desde la última actualización.

Elija Eliminar servidor vCenter para eliminar el servidor vCenter que se muestra y volver a la página Configurar la recopilación de datos de VMware vCenter.

Si no eligió iniciar la recopilación de datos automáticamente, puede iniciar la recopilación de datos mediante el botón Iniciar la recopilación de datos de esta página. Una vez iniciada la recopilación de datos, el botón de inicio cambia a Detener la recopilación de datos.

Si la columna Estado de la recopilación muestra Recopilación, se ha iniciado la recopilación de datos.

Puede ver los datos recopilados en la AWS Migration Hub consola. Si está recopilando datos para un inventario de servidores VMware vCenter, puede acceder a los datos que aparecen en la consola aproximadamente 15 minutos después de activar la recopilación de datos.


Puede elegir Ver servidores en Migration Hub en esta página para abrir la consola de Migration Hub, si su acceso a Internet no está bloqueado. Tanto si elige este botón como si no, para obtener información sobre cómo acceder a la consola de Migration Hub, consulte [Paso 7: Ver los datos recopilados](#).

Las siguientes son las pautas sobre la duración recomendada de la recopilación de datos de acuerdo con las actividades de planificación de la migración:

- TCO (coste total de propiedad): de 2 a 4 semanas
- Planificación de la migración: de 2 a 6 semanas

Controle el alcance de la recopilación de datos de vCenter

El usuario de vCenter necesita permisos de solo lectura en cada host o máquina virtual de ESX para realizar el inventario mediante Application Discovery Service. Con la configuración de permisos puede controlar qué hosts y máquinas virtuales se incluyen en la recopilación de datos. Puede permitir que se inventarién todos los hosts y máquinas virtuales de la vCenter actual o conceder permisos de case-by-case forma escalonada.

 Note

Como práctica recomendada de seguridad, le aconsejamos que no proporcione permisos adicionales e innecesarios al usuario de vCenter del Application Discovery Service de Discovery.

En los procedimientos siguientes se describen las situaciones de configuración ordenadas de menos a más exhaustivas. Estos procedimientos son para vSphere Client v6.7.0.2. Los procedimientos para otras versiones del cliente pueden ser diferentes, según la versión del cliente de vSphere que utilice.

Para detectar datos de todos los hosts ESX y máquinas virtuales de la instancia de vCenter actual

1. En el cliente de VMware vSphere, elija vCenter y, a continuación, elija Hosts and Clusters o VMs and Templates.
2. Elija un recurso de centro de datos y, a continuación, elija Permisos.
3. Elija el usuario de vCenter y, a continuación, el símbolo para agregar, editar o eliminar un rol de usuario.
4. Seleccione Solo lectura en el menú Funciones.
5. Elija Propagar a niños y, a continuación, elija Aceptar.

Para detectar datos de un determinado host ESX y de todos sus objetos secundarios

1. En el cliente de VMware vSphere, elija vCenter y, a continuación, elija Hosts and Clusters o VMs and Templates.
2. Elija Related Objects, Hosts.
3. Abra el menú contextual (haga clic con el botón derecho) del nombre de host y elija All vCenter Actions, Add Permission.
4. En Add Permission, añada el usuario de vCenter al host. En Assigned Role, elija Read-only.
5. Elija Propagate to children, OK.

Para descubrir datos sobre un host ESX específico o una máquina virtual secundaria

1. En el cliente de VMware vSphere, elija vCenter y, a continuación, elija Hosts and Clusters o VMs and Templates.
2. Elija Related Objects.
3. Elija Hosts (se muestra una lista de los hosts ESX que conoce vCenter) o Virtual Machines (se muestra una lista de todas las máquinas virtuales en todos los hosts ESX).
4. Abra el menú contextual (haga clic con el botón derecho) del nombre de host o máquina virtual y elija All vCenter Actions, Add Permission.
5. En Add Permission, añada el usuario de vCenter al host o máquina virtual. En Assigned Role, elija Read-only, .

6. Seleccione OK (Aceptar).

Note

Si elige Propagar a niños, aún puede eliminar el permiso de solo lectura de los hosts y máquinas virtuales de ESX de vez encase-by-case cuando. Esta opción no modifica la aplicación de permisos heredados a otros hosts ESX y máquinas virtuales.

Módulo de recopilación de datos analíticos y de bases de datos

En esta sección se describe cómo configurar, configurar y utilizar una base de datos y un módulo de recopilación de datos analíticos. Puede usar este módulo de recopilación de datos para conectarse a su entorno de datos y recopilar metadatos y métricas de rendimiento de sus bases de datos y servidores de análisis locales. Para obtener información sobre las métricas que puede recopilar con este módulo, consulte [Datos recopilados por la base de datos Agentless Collector y el módulo de recopilación de datos de análisis](#).

En un nivel superior, al utilizar el módulo de recopilación de datos analíticos y de bases de datos, debe seguir los siguientes pasos.

1. Complete los pasos previos, configure el IAM usuario y cree el recopilador AWS DMS de datos.
2. Configure el reenvío de datos para asegurarse de que su módulo de recopilación de datos pueda enviar los metadatos recopilados y las métricas de rendimiento a AWS.
3. Añada sus LDAP servidores y utilícelos para detectar los servidores del sistema operativo en su entorno de datos. Como alternativa, añada los servidores del sistema operativo manualmente o utilice el [Módulo de recopilación de datos de VMware](#).
4. Configure las credenciales de conexión a los servidores del sistema operativo y, a continuación, utilícelas para detectar los servidores de bases de datos.
5. Configure las credenciales de conexión a sus servidores de bases de datos y análisis y, a continuación, ejecute la recopilación de datos. Para obtener más información, consulte [Recopilación de datos de bases de datos y análisis](#).
6. Vea los datos recopilados en la AWS DMS consola y utilícelos para generar recomendaciones específicas para una migración a Nube de AWS. Para obtener más información, consulte [Recopilación de datos de bases de datos y análisis](#).

Temas

- [Servidores de sistemas operativos, bases de datos y análisis compatibles](#)
- [Cree el recopilador de datos AWS DMS](#)
- [Configure el reenvío de datos](#)
- [Agregue sus servidores LDAP y los del sistema operativo](#)
- [Descubra sus servidores de bases de datos](#)

Servidores de sistemas operativos, bases de datos y análisis compatibles

El módulo de recopilación de datos de bases de datos y análisis del Agentless Collector es compatible con los servidores Microsoft Active DirectoryLDAP.

Este módulo de recopilación de datos es compatible con los siguientes servidores del sistema operativo.

- Amazon Linux 2
- Centos Linux versión 6 y superior
- Debian versión 10 y superior
- Red Hat Enterprise Linux versión 7 y superior
- SUSELinux Enterprise Server versión 12 y superior
- Ubuntu versión 16.01 y superior
- Windows Server 2012 y versiones posteriores
- Windows XP y versiones posteriores

Además, el módulo de recopilación de datos de bases de datos y análisis es compatible con los siguientes servidores de bases de datos.

- Microsoft SQL Server versión 2012 y versiones posteriores a 2019
- Mi SQL versión 5.6 y versiones posteriores
- Oracle versión 11g, versión 2 y versiones posteriores hasta 12c, 19c y 21c
- Postgre SQL versión 9.6 y versiones posteriores

Cree el recopilador de datos AWS DMS

El módulo de recopilación de datos de bases de datos y análisis utiliza un recopilador de AWS DMS datos para interactuar con la AWS DMS consola. Puede ver los datos recopilados en la AWS DMS consola o utilizarlos para determinar el tamaño correcto del motor AWS objetivo. Para obtener más información, consulte [Uso de la función de recomendaciones de objetivos de AWS DMS Fleet Advisor](#).

Antes de crear un recopilador de AWS DMS datos, cree un IAM rol que el recopilador de AWS DMS datos utilice para acceder a su bucket de Amazon S3. Creó este bucket de Amazon S3 al completar los requisitos previos en [Requisitos previos para Agentless Collector](#).

Para crear un IAM rol para que su recopilador de AWS DMS datos acceda a Amazon S3

1. Inicie sesión en AWS Management Console y abra la IAM consola en <https://console.aws.amazon.com/iam/>.
2. En el panel de navegación, selecciona Roles y, a continuación, selecciona Crear rol.
3. En la página Seleccionar entidad de confianza, para Tipo de entidad de confianza, elija Servicio de AWS . Para ver los casos de uso de otros AWS servicios, elija DMS.
4. Seleccione la DMS casilla de verificación y elija Siguiente.
5. En la página Añadir permisos, elija FleetAdvisorS3Policy que haya creado anteriormente. Elija Next (Siguiente).
6. En la página Asignar nombre, revisar y crear, ingrese **FleetAdvisorS3Role** para el Nombre del rol y, a continuación, elija Crear rol.
7. Abra el rol que creó y elija la pestaña Relaciones de confianza. Elija Editar la política de confianza.
8. En la página Editar política de confianza, pegue lo siguiente JSON en el editor y sustituya el código existente.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "",
    "Effect": "Allow",
    "Principal": {
      "Service": [
        "dms.amazonaws.com",
        "dms-fleet-advisor.amazonaws.com"
      ]
    }
  ]
}
```

```
    ]  
  },  
  "Action": "sts:AssumeRole"  
}]  
}
```

9. Elija Actualizar política.

Ahora, cree un recopilador de datos en la AWS DMS consola.

Para crear un recopilador AWS DMS de datos

1. Inicie sesión en la AWS DMS consola AWS Management Console y ábrala en la versión <https://console.aws.amazon.com/dms/2/>.
2. Elige la Región de AWS que hayas establecido como región de origen de Migration Hub. Para obtener más información, consulte [Inicia sesión en Migration Hub y elige una región de origen](#).
3. En el panel de navegación, elija Recopiladores de datos en Detectar. Se abre la página de recopiladores de datos.
4. Elija Crear recopilador de datos. Se abre la página Crear recopiladores de datos.
5. Para Nombre en la sección de configuración general, escriba un nombre del recopilador de datos.
6. En la sección Conectividad, elija Examinar S3. Elija el bucket de Amazon S3 que creó anteriormente de la lista.
7. Para IAM el rol, elija FleetAdvisorS3Role el que haya creado anteriormente.
8. Elija Crear recopilador de datos.

Configure el reenvío de datos

Tras crear los AWS recursos necesarios, configure el reenvío de datos desde la base de datos y el módulo de recopilación de datos analíticos al recopilador. AWS DMS

Para configurar el reenvío de datos

1. Abra la consola Agentless Collector. Para obtener más información, consulte [Paso 4: Acceda a la consola del recopilador](#).
2. Seleccione Ver base de datos y recopilador de análisis.

3. En la página del panel de control, elija Configurar el reenvío de datos en la sección Reenvío de datos.
4. Para el Región de AWSIdentificador de clave de IAM acceso y la clave de acceso IAM secreta, su recopilador sin agente utiliza los valores que configuró anteriormente. Para obtener más información, consulte [Inicia sesión en Migration Hub y elige una región de origen](#) y [Paso 1: Crear un usuario de IAM](#).
5. En el caso del recopilador de DMS datos conectado, elija el recopilador de datos que creó en la AWS DMS consola.
6. Seleccione Guardar.

Después de configurar el reenvío de datos, consulte la sección Reenvío de datos en la página del panel de control. Asegúrese de que el módulo de recopilación de datos analíticos y de base de datos muestre

for Access to DMS y Access to S3.

Agregue sus servidores LDAP y los del sistema operativo


El módulo de recopilación de datos de bases de datos y análisis se utiliza LDAP en Microsoft Active Directory para recopilar información sobre el sistema operativo, la base de datos y los servidores de análisis de la red. El Protocolo ligero de acceso a directorios (LDAP) es un protocolo de aplicación estándar abierto. Puede utilizar este protocolo para acceder a los servicios de información de directorios distribuidos y mantenerlos a través de su red IP.

Puede añadir un LDAP servidor existente a su base de datos y al módulo de recopilación de datos analíticos para detectar automáticamente los servidores del sistema operativo de su red. Si no lo usaLDAP, puede agregar los servidores del sistema operativo manualmente.

Para añadir un LDAP servidor a su base de datos y al módulo de recopilación de datos analíticos

1. Abra la consola Agentless Collector. Para obtener más información, consulte [Paso 4: Acceda a la consola del recopilador](#).
2. Seleccione Ver recopilador de bases de datos y análisis y, a continuación, elija LDAPLos servidores en Discovery en el panel de navegación.
3. Seleccione Añadir LDAP servidor. Se abre la página Añadir LDAP servidor.
4. En Nombre de host, introduzca el nombre de host de su LDAP servidor.
5. En Puerto, introduzca el número de puerto que se utiliza para LDAP las solicitudes.

6. En Nombre de usuario, introduzca el nombre de usuario que utiliza para conectarse al LDAP servidor.
7. En Contraseña, introduzca la contraseña que utiliza para conectarse al LDAP servidor.
8. (Opcional) Seleccione Verificar conexión para asegurarse de que ha agregado las credenciales LDAP del servidor correctamente. Como alternativa, puede comprobar las credenciales de conexión al LDAP servidor más adelante, en la lista de la página de LDAPservidores.
9. Seleccione Añadir LDAP servidor.
10. En la página de LDAPservidores, seleccione su LDAP servidor de la lista y elija Discover OS servers.

 Important

Para detectar el sistema operativo, el módulo de recopilación de datos necesita credenciales para que el servidor de dominio ejecute las solicitudes mediante el LDAP protocolo.

El módulo de recopilación de datos analíticos y de bases de datos se conecta al LDAP servidor y descubre los servidores del sistema operativo. Una vez que el módulo de recopilación de datos complete la detección de los servidores del sistema operativo, puede ver la lista de servidores del sistema operativo detectados si selecciona los servidores View OS.

Como alternativa, puede agregar los servidores del sistema operativo manualmente o importar la lista de servidores desde un archivo de valores (CSV) separados por comas. Además, puede utilizar el módulo de recopilación de datos VMware vCenter Agentless Collector para detectar los servidores de su sistema operativo. Para obtener más información, consulte [Módulo de recopilación de datos de VMware](#).

Para añadir un servidor de sistema operativo a su base de datos y al módulo de recopilación de datos analíticos

1. En la página del recopilador de bases de datos y análisis, seleccione los servidores del sistema operativo en Discovery en el panel de navegación.
2. Seleccione Añadir servidor de sistema operativo. Se abre la página Añadir servidor OS.
3. Proporcione las credenciales del servidor del sistema operativo.
 - a. Para el tipo de sistema operativo, elija el sistema operativo de su servidor.

- b. En Nombre de host/IP, introduzca el nombre de host o la dirección IP del servidor del sistema operativo.
 - c. En Puerto, introduzca el número de puerto que se utiliza para las consultas remotas.
 - d. En el tipo de autenticación, elija el tipo de autenticación que utiliza el servidor del sistema operativo.
 - e. En Nombre de usuario, introduzca el nombre de usuario que utiliza para conectarse al servidor del sistema operativo.
 - f. En Contraseña, introduzca la contraseña que utiliza para conectarse al servidor del sistema operativo.
 - g. Seleccione Verificar para asegurarse de que ha agregado correctamente las credenciales del servidor del sistema operativo.
4. (Opcional) Agregue varios servidores de sistema operativo desde un CSV archivo.
 - a. Seleccione la importación masiva de servidores del sistema operativo desde CSV.
 - b. Seleccione Descargar plantilla para guardar un CSV archivo que incluya una plantilla que pueda personalizar.
 - c. Introduzca las credenciales de conexión de los servidores del sistema operativo en el archivo según la plantilla. El siguiente ejemplo muestra cómo puede proporcionar las credenciales de conexión del servidor del sistema operativo en un CSV archivo.

```
OS type,Hostname/IP,Port,Authentication type,Username,Password
Linux,192.0.2.0,22,Key-based authentication,USER-EXAMPLE,ANPAJ2UCCR6DPCEXAMPLE
Windows,203.0.113.0,,NTLM,USER2-EXAMPLE,AKIAIOSFODNN7EXAMPLE
```

Guarde CSV el archivo después de añadir las credenciales para todos los servidores del sistema operativo.

- d. Selecciona Examinar y, a continuación, selecciona tu CSV archivo.
5. Selecciona Añadir servidor de sistema operativo.
 6. Tras añadir las credenciales para todos los servidores del sistema operativo, seleccione los servidores del sistema operativo y elija Discover database servers.

Descubra sus servidores de bases de datos

Para descubrir bases de datos, cree usuarios para las bases de datos de origen con los permisos mínimos necesarios para el módulo de recopilación de datos. Para obtener más información,

consulte [Creación de usuarios de bases de datos para AWS DMS Fleet Advisor](#) en la Guía del AWS DMS usuario.

Para descubrir las bases de datos que se ejecutan en los servidores del sistema operativo agregados anteriormente, el módulo de recopilación de datos requiere acceso al sistema operativo y a los servidores de bases de datos. Asegúrese de que se pueda acceder a la base de datos en el puerto que especificó en la configuración de conexión. A continuación, active la autenticación remota en el servidor de base de datos. Además, proporcione a su módulo de recopilación de datos los siguientes permisos.

Para descubrir servidores de bases de datos en Windows

1. Proporcione credenciales con permisos para ejecutar consultas del Instrumento de administración de Windows (WMI) y WMI Query Language (WQL) y leer el registro.
2. Agregue el usuario de Windows que especificó en las credenciales de conexión del servidor del sistema operativo a los siguientes grupos: COM usuarios distribuidos, usuarios del registro de rendimiento, usuarios del monitor de rendimiento y lectores de registro de eventos. Para ello, use el siguiente ejemplo de código.

```
net localgroup "Distributed COM Users" username /ADD
net localgroup "Performance Log Users" username /ADD
net localgroup "Performance Monitor Users" username /ADD
net localgroup "Event Log Readers" username /ADD
```

En el ejemplo anterior, *username* sustitúyalo por el nombre del usuario de Windows que especificó en las credenciales de conexión del servidor del sistema operativo.

3. Otorgue los permisos necesarios al usuario de Windows que especificó en las credenciales de conexión del servidor del sistema operativo.
 - Para las propiedades de administración e instrumentación de Windows, seleccione Inicio local y activación remota.
 - En WMIControl, elija los permisos Ejecute Methods, Enable Account, Remote Enable y Read Security para los CIMV2 espacios de WMI nombres DEFAULTStandartCimv2,, y.
 - Para el WMIcomplemento, ejecute **winrm configsddl default** y, a continuación, seleccione Leer y ejecutar.
4. Configure el host de Windows mediante el siguiente ejemplo de código.

```
netsh advfirewall firewall add rule name="Open Ports for WinRM incoming traffic"
  dir=in action=allow protocol=TCP localport=5985, 5986 # Opens ports for WinRM
netsh advfirewall firewall add rule name="All ICMP V4" protocol=icmpv4:any,any
  dir=in action=allow # Allows ICMP traffic

Enable-PSRemoting -Force # Enables WinRM
Set-Service WinRM -StartMode Automatic # Allows WinRM service to run on host
  startup
Set-Item WSMan:\localhost\Client\TrustedHosts -Value {IP} -Force # Sets the
  specific IP from which the access to WinRM is allowed

winrm set winrm/config/service '{@Negotiation="true"}' # Allow Negotiate auth usage
winrm set winrm/config/service '{@AllowUnencrypted="true"}' # Allow unencrypted
  connection
```

Para descubrir servidores de bases de datos en Linux

1. Proporcione acceso de sudo a los netstat comandos ss y.

El siguiente ejemplo de código otorga acceso de sudo a los comandos ss y netstat.

```
sudo bash -c "cat << EOF >> /etc/sudoers.d/username
username ALL=(ALL) NOPASSWD: /usr/bin/ss
username ALL=(ALL) NOPASSWD: /usr/bin/netstat
EOF"
```

En el ejemplo anterior, *username* sustitúyalo por el nombre del usuario de Linux que especificó en las credenciales de conexión del servidor del sistema operativo.

En el ejemplo anterior, se utiliza la /usr/bin/ ruta de acceso a los netstat comandos ss y. Esta ruta puede ser diferente en su entorno. Para determinar la ruta de acceso a los netstat comandos ss y, ejecute los which netstat comandos which ss y.

2. Configure sus servidores Linux para permitir la ejecución de SSH scripts remotos y permitir el tráfico del Protocolo de Mensajes de Control de Internet (ICMP).

Para iniciar la detección de sus servidores de bases de datos

1. En la página del recopilador de bases de datos y análisis, seleccione los servidores del sistema operativo en Discovery en el panel de navegación.
2. Seleccione los servidores del sistema operativo que incluyen sus servidores de bases de datos y análisis y, a continuación, seleccione Verificar la conexión en el menú Acciones.
3. En el caso de los servidores cuyo estado de conectividad sea Fallido, edite las credenciales de conexión.
 - a. Seleccione uno o varios servidores cuando tengan credenciales idénticas y, a continuación, seleccione Editar en el menú Acciones. Se abre la página Editar servidor del sistema operativo.
 - b. En Puerto, introduzca el número de puerto que se utiliza para las consultas remotas.
 - c. En el tipo de autenticación, elija el tipo de autenticación que utiliza el servidor del sistema operativo.
 - d. En Nombre de usuario, introduzca el nombre de usuario que utiliza para conectarse al servidor del sistema operativo.
 - e. En Contraseña, introduzca la contraseña que utiliza para conectarse al servidor del sistema operativo.
 - f. Seleccione Verificar la conexión para asegurarse de que ha actualizado correctamente las credenciales del servidor del sistema operativo. A continuación, seleccione Guardar.
4. Tras actualizar las credenciales de todos los servidores del sistema operativo, seleccione los servidores del sistema operativo y elija Discover database servers.

El módulo de recopilación de datos de bases de datos y análisis se conecta a los servidores del sistema operativo y descubre los servidores de bases de datos y análisis compatibles. Una vez que el módulo de recopilación de datos complete la detección, podrá ver la lista de servidores de bases de datos y análisis detectados seleccionando Ver servidores de bases de datos.

Como alternativa, puede añadir su base de datos y sus servidores de análisis al inventario manualmente. Además, puede importar la lista de servidores desde un CSV archivo. Puede omitir este paso si ya ha añadido todos sus servidores de bases de datos y análisis al inventario.

Para añadir una base de datos o un servidor de análisis manualmente

1. En la página del recopilador de bases de datos y análisis, elija Recopilación de datos en el panel de navegación.
2. Seleccione Añadir servidor de base de datos. Se abre la página Agregar servidor de base de datos.
3. Proporcione las credenciales del servidor de bases de datos.
 - a. En Motor de base de datos, elija el motor de base de datos de su servidor. Para obtener más información, consulte [Servidores de sistemas operativos, bases de datos y análisis compatibles](#).
 - b. En Nombre de host/IP, introduzca el nombre de host o la dirección IP de su base de datos o servidor de análisis.
 - c. En Puerto, introduzca el puerto en el que se ejecuta el servidor.
 - d. En Tipo de autenticación, elija el tipo de autenticación que utiliza su base de datos o servidor de análisis.
 - e. En Nombre de usuario, introduzca el nombre de usuario que utiliza para conectarse al servidor.
 - f. En Contraseña, introduzca la contraseña que utiliza para conectarse al servidor.
 - g. Elija Verificar para asegurarse de haber agregado correctamente las credenciales de la base de datos o del servidor de análisis.
4. (Opcional) Agregue varios servidores desde un CSV archivo.
 - a. Seleccione Importar de forma masiva servidores de bases de datos desde CSV.
 - b. Seleccione Descargar plantilla para guardar un CSV archivo que incluya una plantilla que pueda personalizar.
 - c. Introduzca las credenciales de conexión de sus servidores de bases de datos y análisis en el archivo según la plantilla. El siguiente ejemplo muestra cómo puede proporcionar las credenciales de conexión a la base de datos o al servidor de análisis en un CSV archivo.

```
Database engine,Hostname/IP,Port,Authentication type,Username,Password,Oracle  
service name,Database,Allow public key retrieval,Use SSL,Trust server  
certificate  
Oracle,192.0.2.1,1521,Login/Password authentication,USER-  
EXAMPLE,AKIAI44QH8DHBEXAMPLE,orcl,,,,
```

```
PostgreSQL,198.51.100.1,1533,Login/Password authentication,USER2-  
EXAMPLE,bPxRfiCYEXAMPLE,,postgre,,TRUE,  
MSSQL,203.0.113.1,1433,Login/Password authentication,USER3-  
EXAMPLE,h3yCo8nvbEXAMPLE,,,,,TRUE  
MySQL,2001:db8:4006:812:ffff:200e,8080,Login/Password authentication,USER4-  
EXAMPLE,APKAEIVFHP46CEXAMPLE,,mysql,TRUE,TRUE,
```

Guarde CSV el archivo después de añadir las credenciales para todos sus servidores de bases de datos y análisis.

- d. Seleccione Examinar y, a continuación, elija su CSV archivo.
5. Selecciona Añadir servidor de base de datos.
6. Tras añadir las credenciales para todos los servidores del sistema operativo, seleccione los servidores del sistema operativo y elija Discover database servers.

Tras añadir todos los servidores de bases de datos y análisis al módulo de recopilación de datos, agréguelos al inventario. El módulo de recopilación de datos de bases de datos y análisis puede conectarse a los servidores del inventario y recopilar metadatos y métricas de rendimiento.

Para añadir sus servidores de bases de datos y análisis al inventario

1. En la página del recopilador de bases de datos y análisis, seleccione Servidores de bases de datos en Discovery en el panel de navegación.
2. Seleccione los servidores de bases de datos y análisis para los que desee recopilar metadatos y métricas de rendimiento.
3. Selecciona Añadir al inventario.

Tras añadir todos los servidores de bases de datos y análisis a tu inventario, puedes empezar a recopilar metadatos y métricas de rendimiento. Para obtener más información, consulte [Recopilación de datos de bases de datos y análisis](#).

Paso 7: Ver los datos recopilados

Puede ver los datos que su Application Discovery Service Agentless Collector (Agentless Collector) recopiló en la consola de Migration Hub. Puede ver las métricas recopiladas de los servidores de bases de datos y análisis en la consola. AWS DMS

Para ver los datos detectados por el módulo de recopilación de datos de VMware vCenter Agentless Collector

1. Inicie sesión en la consola de Migration Hub AWS Management Console y ábrala en <https://console.aws.amazon.com/migrationhub/>. Para esta tarea, le recomendamos que utilice una cuenta de usuario de IAM diferente a la del usuario de IAM que creó para configurar y acceder a Agentless Collector.
2. En el panel de navegación de la consola de Migration Hub, en Discover, elija Servidores.
3. Para ver los detalles de un servidor, elija el nombre de host del servidor en la columna Información del servidor. La página de detalles del servidor muestra información sobre el servidor, como el nombre de host, la dirección IP, las métricas de rendimiento, etc.

Para ver los datos descubiertos por la base de datos y el módulo de recopilación de datos analíticos

1. Inicie sesión AWS Management Console y abra la AWS DMS consola en <https://console.aws.amazon.com/dms/v2/>.
2. Seleccione Inventario en Discover. Se abre la página de inventario.
3. Elija Analizar inventarios para determinar las propiedades del esquema de la base de datos, como la similitud y la complejidad.
4. Seleccione la pestaña Esquemas para ver los resultados del análisis.

Puede usar la AWS DMS consola para identificar esquemas duplicados, determinar la complejidad de la migración y exportar la información del inventario para futuros análisis. Para obtener más información, consulte [Uso de inventarios para el análisis en AWS DMS Fleet Advisor](#).

Datos recopilados por Agentless Collector

Debe configurar el módulo de recopilación de datos Application Discovery Service Agentless Collector (Agentless Collector) para recopilar datos de inventario, perfil y utilización de sus servidores.

Actualmente, Agentless Collector admite la recopilación de datos desde máquinas virtuales de VMware y desde servidores de bases de datos y análisis. Los módulos futuros admitirán la recopilación desde plataformas de virtualización adicionales y la recopilación a nivel del sistema operativo. Para obtener información sobre cómo configurar la recopilación de datos, consulte [Paso 6: Configurar los módulos de recopilación de datos de Agentless Collector](#).

En los siguientes temas se describen los datos que recopilan los módulos de recopilación de datos de Application Discovery Service Agentless Collector (Agentless Collector).

Temas

- [Datos recopilados por el módulo de recopilación de datos VMware vCenter de Agentless Collector](#)
- [Datos recopilados por la base de datos Agentless Collector y el módulo de recopilación de datos de análisis](#)

Datos recopilados por el módulo de recopilación de datos VMware vCenter de Agentless Collector

La siguiente información describe los datos que recopila el módulo de recopilación de datos VMware vCenter de Application Discovery Service Agentless Collector (Agentless Collector). Para obtener información sobre cómo configurar la recopilación de datos, consulte [Cómo configurar el módulo de recopilación de datos Agentless Collector para VMware vCenter](#)

Leyenda de la tabla para los datos recopilados por VMware vCenter con Agentless Collector:

- Los datos recopilados se especifican en kilobytes (KB) a menos que se indique otra cosa.
- Los datos equivalentes de la consola de Migration Hub se muestran en megabytes (MB).
- Los campos de datos marcados con un asterisco (*) solo están disponibles en los archivos.csv que se generan a partir de la función de exportación de la API Application Discovery Service.

El recopilador sin agente admite la exportación de datos mediante la CLI AWS . Para exportar los datos recopilados mediante la AWS CLI, siga las instrucciones que se describen en Exportar datos de rendimiento del sistema para todos los servidores en la página [Exportar datos recopilados](#) de la Guía del usuario de Application Discovery Service.

- El período de sondeo se indica en intervalos de 60 minutos aproximadamente.
- Los campos de datos con un doble asterisco (**) devuelven actualmente un valor nulo.

Campo de datos	Descripción
applicationConfigurationId*	ID de la aplicación de migración en la que se agrupa la máquina virtual.

Campo de datos	Descripción
avgCpuUsagePct	Porcentaje medio de uso de la CPU durante el período de sondeo.
avgDiskBytesReadPerSecond	Número medio de bytes leídos del disco durante el período de sondeo.
avgDiskBytesWrittenPerSecond	Número medio de bytes escritos en el disco durante el período de sondeo.
avgDiskReadOpsPerSecond ^{**}	Número medio de operaciones de E/S de lectura por segundo nulo.
avgDiskWriteOpsPerSecond ^{**}	Número medio de operaciones de E/S de escritura por segundo.
avgFreeRAM	Memoria RAM libre media expresada en MB.
avgNetworkBytesReadPerSecond	Cantidad media de rendimiento de bytes leídos por segundo.
avgNetworkBytesWrittenPerSecond	Cantidad media de rendimiento de bytes escritos por segundo.
Fabricante de ordenadores	Proveedor informado por el host ESXi.
Modelo de ordenador	Modelo de computadora informado por el host ESXi.
configId	ID asignado por Application Discovery Service a la máquina virtual descubierta.
configType	Tipo de recurso descubierto.
connectorId	ID del dispositivo virtual.
cpuType	vCPU para una máquina virtual, modelo real para un host.

Campo de datos	Descripción
datacenterId	ID del vCenter.
hostId*	ID del host de la máquina virtual.
hostName	Nombre del host que ejecuta el software de virtualización.
hypervisor	Tipo de hipervisor.
id	ID del servidor.
lastModifiedTimeSello*	Fecha y hora de la última recopilación de datos antes de la exportación de los datos.
macAddress	Dirección MAC de la máquina virtual.
manufacturer	Fabricante del software de virtualización.
maxCpuUsagePacto	Porcentaje máximo de uso de la CPU durante el período de sondeo.
maxDiskBytesReadPerSecond	Número máximo de bytes leídos del disco durante el período de sondeo.
maxDiskBytesWrittenPerSecond	Número máximo de bytes escritos en el disco durante el período de sondeo.
maxDiskReadOpsPerSecond**	Número máximo de operaciones de E/S de lectura por segundo.
maxDiskWriteOpsPerSecond**	Número máximo de operaciones de E/S de escritura por segundo.
maxNetworkBytesReadPerSecond	Cantidad máxima de rendimiento de bytes leídos por segundo.
maxNetworkBytesWrittenPerSecond	Cantidad máxima de rendimiento de bytes escritos por segundo.

Campo de datos	Descripción
memoryReservation [*]	Límite para evitar un consumo excesivo de memoria en la máquina virtual.
moRefId	ID de referencia único de vCenter Managed Object.
name [*]	Nombre de la máquina virtual o la red (especificado por el usuario).
numCores	Número de núcleos de CPU asignados a la máquina virtual.
numCpus	Número de sockets de CPU en el host ESXi.
numDisks ^{**}	Número de discos en la máquina virtual.
numNetworkCards ^{**}	Número de tarjetas de red en la máquina virtual.
osName	Nombre del sistema operativo en la máquina virtual.
osVersion	Versión del sistema operativo en la máquina virtual.
portGroupId [*]	ID del grupo de puertos miembros de la VLAN.
portGroupName [*]	Nombre del grupo de puertos miembros de la VLAN.
powerState [*]	Estado de la alimentación.
serverId	Application Discovery Service asignó un ID a la máquina virtual descubierta.
smBiosId [*]	ID/versión de la BIOS de administración del sistema.

Campo de datos	Descripción
state *	Estado del dispositivo virtual.
toolsStatus	Estado operativo de las herramientas de VMware
totalDiskFreeTamaño	Espacio libre en disco expresado en MB. Disponible para vCenter Server 7.0 y versiones posteriores.
totalDiskSize	Capacidad total del disco expresada en MB.
totalRAM	Cantidad total de RAM disponible en la máquina virtual en MB.
type	Tipo de host.
vCenterId	Número de identificación único de una máquina virtual.
vCenterName *	Nombre del host de vCenter.
virtualSwitchName *	Nombre del conmutador virtual.
vmFolderPath	Ruta del directorio de los archivos de la máquina virtual.
vmName	Nombre de la máquina virtual.

Datos recopilados por la base de datos Agentless Collector y el módulo de recopilación de datos de análisis

La base de datos de Application Discovery Service Agentless Collector (Agentless Collector) y el módulo de recopilación de datos analíticos recopilan las siguientes métricas de su entorno de datos. Para obtener más información sobre la recopilación de datos, consulte [Módulo de recopilación de datos analíticos y de bases de datos](#).

Cuando utiliza el módulo de recopilación de datos de bases de datos y análisis para recopilar los metadatos y la capacidad de la base de datos, captura las siguientes métricas.

- Memoria disponible en los servidores de su sistema operativo
- Almacenamiento disponible en los servidores de su sistema operativo
- Versión y edición de la base de datos
- Cantidad de CPU en los servidores del sistema operativo
- Número de esquemas
- Número de procedimientos almacenados
- Número de tablas
- Número de disparadores
- Número de vistas
- Estructura del esquema

Tras iniciar el análisis de esquemas en la AWS DMS consola, el módulo de recopilación de datos analiza y muestra las siguientes métricas.

- Fechas de soporte de bases de
- Número de líneas de código
- Complejidad del esquema
- Similitud de esquemas

Cuando utiliza el módulo de recopilación de datos de bases de datos y análisis para recopilar metadatos, la capacidad de la base de datos y la utilización de los recursos, captura las siguientes métricas.

- Rendimiento de E/S en sus servidores de bases de datos
- El número de operaciones de entrada/salida por segundo (IOPS) en los servidores de bases de datos
- Cantidad de CPU que utilizan los servidores del sistema operativo
- Uso de memoria en los servidores de su sistema operativo
- Uso de almacenamiento en los servidores de su sistema operativo

Puede utilizar el módulo de recopilación de datos de bases de datos y análisis para recopilar metadatos, capacidad y métricas de uso de sus bases de datos de Oracle y SQL Server. Al mismo tiempo, para las bases de datos PostgreSQL y MySQL, el módulo de recopilación de datos solo puede recopilar metadatos.

Uso de la consola Agentless Collector

En esta sección se describe cómo utilizar la consola de Application Discovery Service Agentless Recopilador (Recopilador sin Agentless).

Temas

- [El panel de control de Agentless Collector](#)
- [Edición de la configuración de Agentless Collector](#)
- [Edición de credenciales de VMware vCenter](#)

El panel de control de Agentless Collector

En la página del panel de control del recopilador sin agente de Application Discovery Service (recopilador sin agente), puede ver el estado del recopilador y elegir un método de recopilación de datos, tal como se describe en los siguientes temas.

Temas

- [Estado del Recopilador](#)
- [Recopilación de datos](#)

Estado del Recopilador

El estado del recopilador le proporciona información sobre el estado del recopilador. El nombre del recopilador, el estado de la conexión del recopilador a AWS, la región de origen de Migration Hub y la versión.

Si tiene problemas de AWS conexión, es posible que tenga que editar la configuración de Agentless Recopilador.

Para editar la configuración del recopilador, elija Editar la configuración del recopilador y siga las instrucciones que se describen en [Edición de la configuración de Agentless Collector](#).

Recopilación de datos

En Recopilación de datos, puede elegir un método de recopilación de datos. Actualmente, Application Discovery Service Agentless Collector (Agentless Collector) admite la recopilación de datos de máquinas virtuales de VMware y de servidores de bases de datos y análisis. Los módulos futuros admitirán la recopilación desde plataformas de virtualización adicionales y la recopilación a nivel de sistema operativo.

Temas

- [Recopilador de datos de VMware vCenter](#)
- [Recopilación de datos de bases de datos y análisis](#)

Recopilador de datos de VMware vCenter

Para recopilar los datos de inventario, perfil y utilización de los servidores de las máquinas virtuales de VMware, configure las conexiones a los servidores vCenter. Para configurar las conexiones, seleccione Configurar en la sección VMware vCenter y siga las instrucciones que se describen en [Paso 6: Configurar los módulos de recopilación de datos de Agentless Collector](#).

Tras configurar la recopilación de datos de vCenter, desde el panel de control puede realizar lo siguiente:

- Ver el estado de para la recopilación de datos
- Comenzar la recopilación de datos
- Detener la recopilación de datos

Note

En la página del panel, después de configurar la recopilación de datos de vCenter, el botón Configurar de la sección VMware vCenter se sustituye por la información sobre el estado de la recopilación de datos, un botón para detener la recopilación de datos y un botón para ver y editar.

Recopilación de datos de bases de datos y análisis

Puede ejecutar el módulo de recopilación de datos de base de datos y análisis en los dos modos siguientes.

Capacidad de metadatos y bases de datos

El módulo de recopilación de datos recopila información como esquemas, versiones, ediciones, CPU, memoria y capacidad de disco de sus servidores de bases de datos y análisis. Puede utilizar esta información recopilada para calcular las recomendaciones de objetivos en la AWS DMS consola. Si la base de datos de origen está sobreaprovisionada o subaprovisionada, las recomendaciones de destino también estarán sobreaprovisionadas o subaprovisionadas.

Este es el modo predeterminado.

Metadatos, capacidad de bases de datos y utilización de recursos

Además de los metadatos y la información sobre la capacidad de la base de datos, el módulo de recopilación de datos recopila las métricas de uso reales de la capacidad de la CPU, la memoria y el disco para las bases de datos y los servidores de análisis. Este modo proporciona recomendaciones de objetivos más precisas que el modo predeterminado, ya que las recomendaciones se basan en las cargas de trabajo reales de la base de datos. En este modo, el módulo de recopilación de datos recopila métricas de rendimiento cada minuto.

Para empezar a recopilar metadatos y métricas de rendimiento de su base de datos y servidores de análisis

1. En la página Recopilador de bases de datos y análisis, seleccione Recopilación de datos en el panel de navegación.
2. En la lista de inventario de bases de datos, seleccione los servidores de base de datos y análisis para los que desea recopilar metadatos y métricas de rendimiento.
3. Elija Ejecutar recopilación de datos. Se abre el cuadro de diálogo Tipo de recopilación de datos.
4. Elija cómo recopilar los datos para su análisis.

Si elige la opción Metadatos, capacidad de base de datos y utilización de recursos, defina el período de recopilación de datos. Puede recopilar datos durante los próximos 7 días o establecer el intervalo personalizado de 1 a 60 días.

5. Elija Ejecutar recopilación de datos. Se abre la página Recopilación de datos.
6. Seleccione la pestaña Estado de la colección para ver el estado de la recopilación de datos.

Tras completar la recopilación de datos, el módulo de recopilación de datos carga los datos recopilados en su bucket de Amazon S3. A continuación, puede ver los datos recopilados tal y como se describe en [Paso 7: Ver los datos recopilados](#).

Edición de la configuración de Agentless Collector

Configuró el recopilador cuando configuró por primera vez el recopilador sin agente de Application Discovery Service (recopilador sin agente), tal como se describe en [Paso 5: Configurar el recopilador sin agente](#). En el procedimiento siguiente se describe cómo editar los ajustes de Agentless Recopilador.

Para editar los parámetros de configuración del recopilador

- Seleccione el botón Editar la configuración del recopilador en el panel de control de Agentless Collector.

En la página Editar la configuración del recopilador, realice lo siguiente:

- a. En Nombre del Recopilador, introduzca un nombre para identificar al Recopilador. El nombre puede contener espacios, pero no caracteres especiales.
- b. En AWSCuenta de destino para datos de descubrimiento, introduzca la clave deAWS acceso y la clave secreta de laAWS cuenta que desee especificar como cuenta de destino para recibir los datos descubiertos por el recopilador. Para obtener información sobre los requisitos del usuario de IAM, consulte [Paso 1: Cree un usuario de IAM para Agentless Collector](#).
 - i. Para la AWSclave de acceso, introduzca la clave de acceso del usuario de IAM de laAWS cuenta que está especificando como cuenta de destino.
 - ii. Para la AWSclave secreta, introduzca la clave secreta del usuario de IAM de laAWS cuenta que está especificando como cuenta de destino.
- c. En Contraseña del recopilador sin agente, cambie la contraseña que se utilizará para autenticar el acceso al recopilador sin agente.
 - i. Para la contraseña del recopilador sin agente, introduzca la contraseña que se utilizará para autenticar el acceso al recopilador sin agente.
 - ii. Para volver a introducir la contraseña de Agentless Collector, vuelva a introducirla para verificarla.
- d. Selecciona Guardar configuraciones.

A continuación, verá [El panel de control de Agentless Collector](#).

Edición de credenciales de VMware vCenter

Para recopilar los datos de inventario, perfil y utilización de los servidores de las máquinas virtuales de VMware, configure las conexiones a los servidores vCenter. Para obtener más información sobre la configuración de las conexiones de VMware vCenter, consulte [Paso 6: Configurar los módulos de recopilación de datos de Agentless Collector](#).

En esta sección se describe cómo editar las credenciales de vCenter.

Note

Antes de editar las credenciales de vCenter, asegúrese de que puede proporcionar las credenciales de vCenter con los permisos de lectura y visualización establecidos para el grupo Sistema.

Para editar las credenciales de VMware vCenter

En la [Detalles de la recopilación de datos de VMware](#) página, seleccione Editar servidores vCenter.

- En la página Editar vCenter, realice lo siguiente:
 - a. En las credenciales de vCenter:
 - i. Para la URL/IP de vCenter, introduzca la dirección IP de su host de VMware vCenter Server.
 - ii. En vCenter Username (Nombre de usuario de vCenter), escriba el nombre del usuario local o del dominio local que utiliza el conector para comunicarse con vCenter. Para usuarios del dominio, utilice el formato dominio\nombre de usuario o nombre de usuario@dominio.
 - iii. En vCenter Password (Contraseña de vCenter), escriba la contraseña de usuario local o del dominio.
 - b. Seleccione Guardar.

Actualización manual de Agentless Collector

Al configurar Application Discovery Service Agentless Collector (Agentless Collector), puede optar por habilitar las actualizaciones automáticas como se describe en. [Paso 5: Configurar el recopilador](#)

[sin agente](#) Si no habilita las actualizaciones automáticas, tendrá que actualizar manualmente Agentless Collector.

El siguiente procedimiento describe cómo actualizar manualmente Agentless Collector.

Para actualizar manualmente Agentless Collector

1. Obtenga el archivo OVA (Open Virtualization Archive) más reciente de Agentless Collector.
2. (Opcional) Se recomienda eliminar el archivo OVA anterior de Agentless Collector antes de implementar el último.
3. En la [Primeros pasos con Agentless Collector](#) sección, siga los pasos [Paso 3: Implemente un recopilador sin agente](#) que se indican a continuación. [Paso 6: Configurar los módulos de recopilación de datos de Agentless Collector](#)

El procedimiento anterior solo actualiza el recopilador sin agente. Es su responsabilidad mantener el sistema operativo actualizado.

Para actualizar su instancia de Amazon EC2

1. Obtenga la dirección IP del recopilador sin agente de VMware vCenter.
2. Abra la consola de máquina virtual del recopilador e inicie sesión **ec2-user** con la contraseña, **collector** como se muestra en el siguiente ejemplo.

```
username: ec2-user
password: collector
```

3. Siga las instrucciones de [Actualizar el software de la instancia en la instancia AL2](#) de la Guía del usuario de Amazon Linux 2.

Parcheo en vivo del kernel en Amazon Linux 2

La máquina virtual Agentless Collector utiliza Amazon Linux 2, tal y como se describe en. [Paso 3: Implemente un recopilador sin agente](#)

Para habilitar y usar la aplicación de parches en tiempo real para Amazon Linux 2, consulte [Kernel Live Patching en Amazon Linux 2](#) en la Guía del usuario de Amazon EC2.

Solución de problemas de Agentless Collector

Esta sección contiene temas que pueden ayudarle a solucionar problemas conocidos con Application Discovery Service Agentless Collector (Agentless Collector).

Temas

- [Reparación: no se puede acceder a Agentless Collector durante la configuración AWS](#)
- [Solución de problemas de certificación autofirmada al conectarse al host proxy](#)
- [Búsqueda de recopiladores en mal estado](#)
- [Solucionar problemas con las direcciones IP](#)
- [Solución de problemas de credenciales de vCenter](#)
- [Solución de problemas de reenvío de datos en el módulo de recopilación de datos de análisis y bases de datos](#)
- [Solucionar problemas de conexión en el módulo de recopilación de datos analíticos y de base de datos](#)
- [Soporte para hosts ESX independientes](#)
- [Contactar con AWS Support por problemas con Agentless Collector](#)

Reparación: no se puede acceder a Agentless Collector durante la configuración AWS

Agentless Collector requiere acceso saliente a varios dominios a través del puerto TCP 443. AWS AI configurar Agentless Collector en la consola, puede aparecer el siguiente mensaje de error.

No se pudo contactar AWS

AWS no se puede contactar. Compruebe la configuración de la red.

Este error se produce debido a un intento fallido por parte de Agentless Collector de establecer una conexión HTTPS con un AWS dominio con el que el recopilador necesita comunicarse durante el proceso de configuración. La configuración del recopilador sin agente falla si no se puede establecer una conexión.

Para corregir la conexión a AWS

1. Consulte con su administrador de TI si el firewall de su empresa bloquea el tráfico saliente en el puerto 443 hacia alguno de los AWS dominios que requieren acceso saliente. AWS Los dominios que requieren acceso saliente dependen de si tu región de origen es la región EE.UU. Oeste (Oregón), us-west-2 o alguna otra región.

Los siguientes dominios requieren acceso saliente si la región de origen de su AWS cuenta es us-west-2:

- `arsenal-discovery.us-west-2.amazonaws.com`
- `migrationhub-config.us-west-2.amazonaws.com`
- `api.ecr-public.us-east-1.amazonaws.com`
- `public.ecr.aws`

Los siguientes dominios requieren acceso saliente si la región de origen de la AWS cuenta no lo es: **us-west-2**

- `arsenal-discovery.us-west-2.amazonaws.com`
- `arsenal-discovery.your-home-region.amazonaws.com`
- `migrationhub-config.us-west-2.amazonaws.com`
- `api.ecr-public.us-east-1.amazonaws.com`
- `public.ecr.aws`

Si su firewall bloquea el acceso saliente a los AWS dominios con los que Agentless Collector necesita comunicarse, configure un host proxy en la sección Sincronización de datos de la sección Configuración de Collector.

2. Si la actualización del firewall no resuelve el problema de conexión, siga estos pasos para asegurarse de que la máquina virtual recopiladora tenga conectividad de red saliente con los dominios enumerados en el paso anterior.
 - a. Obtenga la dirección IP del recopilador sin agente de VMware vCenter.
 - b. Abra la consola de máquina virtual del recopilador e inicie sesión **ec2-user** con la contraseña, **collector** como se muestra en el siguiente ejemplo.

```
username: ec2-user
```

```
password: collector
```

- c. Pruebe la conexión a los dominios de la lista ejecutando telnet en los puertos 443, como se muestra en el siguiente ejemplo.

```
telnet migrationhub-config.us-west-2.amazonaws.com 443
```

3. Si telnet no puede resolver el dominio, intente configurar un servidor DNS estático [siguiendo las instrucciones de Amazon Linux 2](#).
4. Si el error continúa, para obtener más ayuda, consulte [Contactar con AWS Support por problemas con Agentless Collector](#).

Solución de problemas de certificación autofirmada al conectarse al host proxy

Si la comunicación con el proxy que se proporciona de forma opcional se realiza a través de HTTPS y el proxy tiene un certificado autofirmado, es posible que tengas que proporcionar un certificado.

1. Obtenga la dirección IP del recopilador sin agente de VMware vCenter.
2. Abra la consola de máquina virtual del recopilador e inicie sesión `ec2-user` con la contraseña, `collector` como se muestra en el siguiente ejemplo.

```
username: ec2-user  
password: collector
```

3. Pegue el cuerpo del certificado asociado al proxy seguro, incluidos ambos `-----BEGIN CERTIFICATE-----` y `-----END CERTIFICATE-----`, en el siguiente archivo:

```
/etc/pki/ca-trust/source/anchors/https-proxy-ca.pem
```

4. Para instalar el nuevo certificado, ejecute los siguientes comandos:

```
sudo update-ca-trust
```

5. Reinicie el recopilador sin agente ejecutando el siguiente comando:

```
sudo shutdown -r now
```

Búsqueda de recopiladores en mal estado

La información de estado de cada recopilador se encuentra en la página de [recopiladores de datos](#) de la consola AWS Migration Hub (Migration Hub). Para identificar a los recopiladores con problemas, busque los recopiladores cuyo estado sea Requiere atención.

El siguiente procedimiento describe cómo acceder a la consola de Agentless Collector para identificar problemas de estado.

Para acceder a la consola Agentless Collector

1. Con tu AWS cuenta, inicia sesión en la consola de Migration Hub AWS Management Console y ábrela en <https://console.aws.amazon.com/migrationhub/>.
2. En el panel de navegación de la consola de Migration Hub, en Discover, elija Recopiladores de datos.
3. En la pestaña Recopiladores sin agente, anote la dirección IP de cada conector cuyo estado sea Requiere atención.
4. Para abrir la consola de Agentless Collector, abra un navegador web. A continuación, escriba la siguiente URL en la barra de direcciones: **https://<ip_address>**, donde ip_address es la dirección IP de un recopilador en mal estado.
5. Seleccione Iniciar sesión y, a continuación, introduzca la contraseña del recopilador sin agente, que se configuró cuando se configuró el recopilador en. [Paso 5: Configurar el recopilador sin agente](#)
6. En la página del panel de control de Agentless Collector, en Recopilación de datos, elija Ver y editar en la sección VMware vCenter.
7. Siga las instrucciones [Edición de credenciales de VMware vCenter](#) para corregir la URL y las credenciales.

Tras corregir los problemas de estado, el recopilador restablecerá la conectividad con vCenter Server y el estado del recopilador cambiará al estado de recopilación. Si los problemas persisten, consulte.

[Contactar con AWS Support por problemas con Agentless Collector](#)

Las causas más comunes de que los recopiladores no funcionen correctamente son los problemas con las direcciones IP y las credenciales. [Solucionar problemas con las direcciones IP](#) y [Solución de problemas de credenciales de vCenter](#) puede ayudarlo a resolver estos problemas y devolver un colector a un estado saludable.

Solucionar problemas con las direcciones IP

Un recopilador puede pasar a un estado incorrecto si el punto final de vCenter proporcionado durante la configuración del recopilador tiene un formato incorrecto, no es válido o si el servidor vCenter está actualmente inactivo y no se puede acceder a él. En este caso, recibirá un mensaje de error de conexión.

El siguiente procedimiento puede ayudarle a resolver problemas de direcciones IP.

Para solucionar problemas con las direcciones IP del recopilador

1. Obtenga la dirección IP del recopilador sin agente de VMware vCenter.
2. Abra la consola de Agentless Collector abriendo un navegador web y, a continuación, escriba la siguiente URL en la barra de direcciones: **https://<ip_address>**, donde ip_address es la dirección IP del recopilador. [Paso 3: Implemente un recopilador sin agente](#)
3. Seleccione Iniciar sesión y, a continuación, introduzca la contraseña del recopilador sin agente, que se configuró cuando se configuró el recopilador en. [Paso 5: Configurar el recopilador sin agente](#)
4. En la página del panel de control de Agentless Collector, en Recopilación de datos, elija Ver y editar en la sección VMware vCenter.
5. En la página de detalles de la recopilación de datos de VMware, en Servidores vCenter descubiertos, anote la dirección IP en la columna vCenter.
6. Con una herramienta de línea de comandos independiente, como ping o traceroute, valide que el servidor vCenter asociado esté activo y que se pueda acceder a la IP desde la máquina virtual recopiladora.
 - Si la dirección IP es incorrecta y el servicio vCenter está activo, actualice la dirección IP en la consola del recopilador y seleccione Siguiente.
 - Si la dirección IP es correcta pero el servidor de vCenter está inactivo, actívelo.
 - Si la dirección IP es correcta y el servidor de vCenter está activo, compruebe si está bloqueando las conexiones de red de entrada debido a problemas del firewall. En caso afirmativo, actualice la configuración del firewall para permitir las conexiones entrantes desde la máquina virtual recopiladora.

Solución de problemas de credenciales de vCenter

Los recopiladores pueden pasar a un estado incorrecto si las credenciales de usuario de vCenter proporcionadas al configurar un recopilador no son válidas o no tienen privilegios de cuenta de vCenter Read and View.

Si tiene problemas relacionados con las credenciales de vCenter, asegúrese de que tiene configurados los permisos de lectura y visualización de vCenter para el grupo de sistema.

Para obtener información sobre la edición de las credenciales de vCenter, consulte [Edición de credenciales de VMware vCenter](#)

Solución de problemas de reenvío de datos en el módulo de recopilación de datos de análisis y bases de datos

La página de inicio del módulo de recopilación de datos analíticos y de bases de datos de Agentless Collector muestra el estado de conexión de Access to DMS y Access to S3. Si ve No hay acceso a DMS y Acceso a S3, configure el reenvío de datos. Para obtener más información, consulte [Configure el reenvío de datos](#).

Si experimenta este problema después de configurar el reenvío de datos, asegúrese de que su módulo de recopilación de datos pueda acceder a Internet. A continuación, asegúrese de haber añadido las políticas de DMS CollectorPolicy y FleetAdvisorS3Policy a su usuario de IAM. Para obtener más información, consulte [Paso 1: Cree un usuario de IAM para Agentless Collector](#).

Si su módulo de recopilación de datos no se puede conectar AWS, proporcione acceso saliente a los siguientes dominios.

- `dms.your-home-region.amazonaws.com`
- `s3.amazonaws.com`

Solucionar problemas de conexión en el módulo de recopilación de datos analíticos y de base de datos

El módulo de recopilación de datos analíticos y de bases de datos de Agentless Collector se conecta a los servidores LDAP para detectar los servidores del sistema operativo de su entorno de datos. A continuación, el módulo de recopilación de datos se conecta a los servidores del sistema operativo para detectar los servidores de bases de datos y análisis. Desde estos servidores de bases de datos,

el módulo de recopilación de datos recopila métricas de capacidad y rendimiento. Si el módulo de recopilación de datos no puede conectarse a estos servidores, compruebe que puede conectarse a ellos.

En los ejemplos siguientes, sustituya los valores *reemplazables* por sus valores.

- Para comprobar que puede conectarse al servidor LDAP, instale el `ldap-util` paquete. Para ello, ejecute el siguiente comando.

```
sudo apt-get install ldap-util
```

A continuación, ejecute el siguiente comando.

```
ldapsearch -x -D "CN=user,CN=Users,DC=example,DC=com" -w "password" -b  
"dc=example,dc=com" -h
```

- Para comprobar que puede conectarse a un servidor de sistema operativo Linux, utilice los siguientes comandos.

```
ssh -i C:\Users\user\private_key.pem -p 22 username@my-linux-host.domain.com
```

Ejecute el ejemplo anterior como administrador en Windows.

```
ssh username@my-linux-host.domain.com
```

Ejecute el ejemplo anterior en Linux.

- Para comprobar que puede conectarse a un servidor del sistema operativo Windows, utilice los siguientes comandos.

```
winrs -r:[hostname or ip] -u:username -p:password cmd
```

Ejecute el ejemplo anterior como administrador en Windows.

```
sudo apt install -y winrm  
winrm --user=username --password=password [http or https]://[hostname or ip]:[port]  
"[cmd.exe or any other CLI command]"
```

Ejecute el ejemplo anterior en Linux.

- Para comprobar que puede conectarse a una base de datos de SQL Server, utilice los siguientes comandos.

```
sqlcmd -S [hostname or IP] -U username -P 'password'  
SELECT GETDATE() AS sysdate
```

- Para comprobar que puede conectarse a una base de datos MySQL, utilice los siguientes comandos.

```
mysql -u username -p 'password' -h [hostname or IP] -P [port]  
SELECT NOW() FROM DUAL
```

- Para comprobar que puede conectarse a una base de datos Oracle, utilice los siguientes comandos.

```
sqlplus username/password@[hostname or IP]:port/servicename  
SELECT SYSDATE FROM DUAL
```

- Para comprobar que puede conectarse a una base de datos PostgreSQL, utilice los siguientes comandos.

```
psql -U username -h [hostname or IP] -p port -d database  
SELECT CURRENT_TIMESTAMP AS sysdate
```

Si no puede conectarse a sus servidores de bases de datos y análisis, asegúrese de proporcionar los permisos necesarios. Para obtener más información, consulte [Descubra sus servidores de bases de datos](#).

Soporte para hosts ESX independientes

El recopilador sin agente no admite un host ESX independiente. El host de ESX debe formar parte de la instancia de vCenter Server.

Contactar con AWS Support por problemas con Agentless Collector

Si tiene problemas con Application Discovery Service Agentless Collector (Agentless Collector) y necesita ayuda, póngase en contacto con [AWS Support](#). Nos pondremos en contacto con usted y es posible que se le pida que envíe los registros del recopilador.

Para obtener los registros de Agentless Collector

1. Obtenga la dirección IP del recopilador sin agente de VMware vCenter.
2. Abra la consola de máquina virtual del recopilador e inicie sesión **ec2-user** con la contraseña, **collector** como se muestra en el siguiente ejemplo.

```
username: ec2-user  
password: collector
```

3. Utilice el siguiente comando para ir a la carpeta de registro.

```
cd /var/log/aws/collector
```

4. Comprima los archivos de registro mediante los siguientes comandos.

```
sudo cp /local/agentless_collector/compose.log .  
docker inspect $(docker ps --format {{.Names}}) | sudo tee docker_inspect.log >/dev/null  
sudo tar czf logs_$(date '+%d-%m-%Y_%H.%M.%S').tar.gz * --exclude='db.mv*'
```

5. Copie el archivo de registro de la máquina virtual Agentless Collector.

```
scp logs*.tar.gz targetuser@targetaddress
```

6. Entregue el tar.gz archivo a AWS Enterprise Support.

Migration Hub

AWS Migration HubLa importación (Migration Hub) le permite importar detalles de su entorno on-premises directamente a Migration Hub sin utilizar Application Discovery Service Agentless Collector (Agentless Collector) oAWSApplication Discovery Agent (Discovery Agent) para que pueda realizar las evaluaciones de migración y la planificación directamente desde los datos importados. También puede agrupar los dispositivos como aplicaciones y realizar un seguimiento de su estado de migración.

Para iniciar una solicitud de importación

- Descargue la plantilla de importación de valores separados por comas (CSV) con formato especial.
- Rellénelo con los datos del servidor local existentes.
- Carguelo en Migration Hub mediante la consola de Migration Hub,AWS CLIo uno de losAWSSDK.

Puede enviar varias solicitudes de importación. Cada solicitud se procesa secuencialmente. Puede comprobar el estado de sus solicitudes de importación en cualquier momento, a través de la consola o de las API de importación.

Una vez completada una solicitud de importación, puede ver los detalles de los registros importados individuales. Consulte los datos de utilización, las etiquetas y los mapeos de aplicaciones directamente desde la consola Migration Hub. Si se producen errores durante la importación, puede revisar el recuento de registros correctos y con error, así como los detalles de cada registro con error.

Gestión de errores: Se proporciona un enlace para descargar el registro de errores y los archivos de registros con error como archivos CSV en un archivo comprimido. Utilice estos archivos para volver a enviar la solicitud de importación después de corregir los errores.

Existen límites en el número de registros importados, los servidores importados y los registros eliminados que puede mantener. Para obtener más información, consulte [Cuotas de AWS Application Discovery Service](#).

Campos de archivo de importación admitidos

La importación de Migration Hub le permite importar datos desde cualquier origen. Los datos proporcionados deben estar en el formato compatible con los archivos CSV y solo pueden contener los campos compatibles con los rangos admitidos en dichos campos.

Un asterisco junto a un nombre de campo de importación en la siguiente tabla indica que se trata de un campo obligatorio. Cada registro del archivo de importación debe tener al menos uno o más de esos campos obligatorios rellenos para identificar de forma única un servidor o una aplicación. De lo contrario, no se podrá importar un registro sin ninguno de los campos obligatorios.

Note


Si utiliza VMware.MoRefId o VMware.vCenterId, para identificar un registro, debe tener ambos campos en el mismo registro.

Nombre del campo de importación	Descripción	Ejemplos
ExternalId*	Un identificador personalizado que le permite marcar cada registro como único. Por ejemplo, ExternalId puede ser el ID de inventario correspondiente al servidor del centro de datos.	ID de inventario 1 Servidor 2 ID de CMBD 3
SMBiosId	ID de BIOS de administración del sistema (SMBIOS).	
IPAddress*	Una lista delimitada por comas de las direcciones IP del servidor, entre comillas.	192.0.0.2 "10.12.31.233, 10.12.32.11"
MACAddress*	Una lista delimitada por comas de las direcciones MAC del servidor, entre comillas.	00:1B:44:11:3A:B7

Nombre del campo de importación	Descripción	Ejemplos
		"00-15-E9-2B-99-3C, 00-14-22-01-23-45"
HostName*	El nombre de host del servidor. Recomendamos utilizar el nombre de dominio completo (FQDN) para este valor.	ip-1-2-3-4 localhost.domain
VMware.MoRefId*	El ID de referencia del objeto administrado. Se debe proporcionar con VMware.VC enterId.	
VMware.vCenterId*	Identificador único de la máquina virtual. Se debe proporcionar con un VMware.MoRefId.	
CPU.NumberOfProcessors	El número de CPU.	4
CPU.NumberOfCores	El número total de núcleos físicos.	8
CPU.NumberOfLogicalCores	El número total de subprocesos que se pueden ejecutar de forma simultánea en todas las CPU de un servidor. Algunas CPU permiten que varios subprocesos se ejecuten de forma simultánea en un solo núcleo de la CPU. En esos casos, este número será mayor que el número de núcleos físicos (o virtuales).	16

Nombre del campo de importación	Descripción	Ejemplos
OS.Name	Nombre del sistema operativo.	Linux Windows.Hat
OS.Version	Versión del sistema operativo.	16.04.3 NT 6.2.8
VMware.VMName	Nombre de la máquina virtual.	Corp1
RAM.TotalSizeInMB.	La RAM total disponible en el servidor, en MB.	64 128
RAM.UsedSizeInMB. AVG	La cantidad promedio de RAM utilizada en el servidor, en MB.	64 128
RAM.UsedSizeInMB.máx	La cantidad máxima de RAM utilizada disponible en el servidor, en MB.	64 128
CPU.UsagePct.AVG.	Utilización de CPU media cuando la herramienta de detección estaba recolectando datos.	45 23.9
CPU.UsagePct.Ancho de banda	Utilización de CPU máxima cuando la herramienta de detección estaba recolectando datos.	55.34 24
DiskReadsPerSecond InkB.promedio	Número medio de lecturas de disco por segundo, en KB.	1159 84506

Nombre del campo de importación	Descripción	Ejemplos
DiskWritesPerSecondInKB.promedio	Número medio de escrituras de disco por segundo, en KB.	199 6197
DiskReadsPerSecondInKb.máx	Número máximo de lecturas de disco por segundo, en KB.	37892 869962
DiskWritesPerSecondInKb.máx	Número máximo de escrituras de disco por segundo, en KB.	18436 1808
DiskReadsOpsPerSecond.AVG.	El número medio de operaciones de lectura en disco por segundo.	45 28
DiskWritesOpsPerSecond.AVG.	Número medio de operaciones de escritura en disco por segundo.	8 3
DiskReadsOpsPerSecond.Ancho de banda	Número máximo de operaciones de lectura en disco por segundo.	1083 176
DiskWritesOpsPerSecond.Ancho de banda	Número máximo de operaciones de escritura en disco por segundo.	535 71
NetworkReadsPerSecondInKB.promedio	Número medio de operaciones de lectura de red por segundo, en KB.	45 28
NetworkWritesPerSecondInKB.promedio	Número medio de operaciones de escritura de red por segundo, en KB.	8 3

Nombre del campo de importación	Descripción	Ejemplos
NetworkReadsPerSecondInKb.máx	Número máximo de operaciones de lectura de red por segundo, en KB.	1083 176
NetworkWritesPerSecondInKb.máx	Número máximo de operaciones de escritura de red por segundo, en KB.	535 71
Aplicaciones	Una lista delimitada por comas de las aplicaciones que incluye este servidor, entre comillas. Este valor puede incluir aplicaciones existentes o aplicaciones nuevas que se crean tras la importación.	Application1 "Application2, Application3"
Etiquetas	Una lista delimitada por comas de etiquetas con el formato nombre:valor. <div style="border: 1px solid #f08080; border-radius: 10px; padding: 10px; background-color: #fff9f9;"> <p> Important No guarde información confidencial (como datos personales) en etiquetas.</p> </div>	"zone:1, critical:yes" "zone:3, critical:no, zone:1"

Puede importar datos aunque no tenga datos rellenos para todos los campos definidos en la plantilla de importación, siempre y cuando cada registro contenga al menos uno de los campos obligatorios. Los duplicados se administran en varias solicitudes de importación mediante una clave de coincidencia externa o interna. Si rellena su propia clave de coincidencia, External ID, este campo se utiliza para identificar e importar los registros de forma única. Si no se especifica ninguna clave de coincidencia, la importación utiliza una generada internamente que se deriva de algunas de

las columnas de la plantilla de importación. Para obtener más información sobre esta coincidencia, consulte [Lógica de coincidencia para servidores y aplicaciones detectados](#).

Note

La importación Migration Hub no admite ningún campo aparte de los definidos en la plantilla de importación. Se ignorará cualquier campo personalizado suministrado y no se importará.

Configuración de los permisos de importación

Para poder importar los datos, debe asegurarse de que su usuario de IAM tiene los permisos de Amazon S3 de necesarios para cargar (`s3:PutObject`) el archivo de importación a Amazon S3 y leer el objeto (`s3:GetObject`). También debe establecer un acceso mediante programación (para la AWS CLI) o a través de la consola creando una política de IAM y asociándola al usuario de IAM que realiza las importaciones en su AWS account.

Console Permissions

Utilice el siguiente procedimiento para editar la política de permisos para el usuario de IAM que realizará las solicitudes de importación en su AWS cuenta con la consola de.

Para editar las políticas administradas asociadas a un usuario

1. Inicie sesión en la AWS Management Console y abra la consola de IAM en <https://console.aws.amazon.com/iam/>.
2. En el panel de navegación, seleccione Users.
3. Elija el nombre del usuario cuya política de permisos desea modificar.
4. Seleccione la pestaña Permissions (Permisos) y elija Add permissions (Añadir permisos).
5. Elija Attach existing policies directly (Asociar directamente las políticas existentes) y, a continuación, Create policy (Crear política).
 - a. En la página Create policy (Crear política) que aparece, elija JSON y pegue la siguiente política. Recuerde reemplazar el nombre de su bucket por el nombre real del bucket en el que el usuario de IAM cargará los archivos de importación.

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

```
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetBucketLocation",
      "s3:ListAllMyBuckets"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": ["s3:ListBucket"],
    "Resource": ["arn:aws:s3:::importBucket"]
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:PutObject",
      "s3:GetObject",
      "s3:DeleteObject"
    ],
    "Resource": ["arn:aws:s3:::importBucket/*"]
  }
]
```

- b. Elija Review policy (Revisar política).
 - c. Asigne un valor en Name (Nombre) para la política, así como una descripción opcional, antes de revisar el resumen de la política.
 - d. Elija Create Policy (Crear política).
6. Vuelva a la Concesión de permisos página de la consola de IAM correspondiente al usuario que realizará las solicitudes de importación en su AWS account.
 7. Actualice la tabla de políticas y busque el nombre de la política que acaba de crear.
 8. Seleccione Next (Siguiente): Consulte.
 9. Elija Add permissions (Agregar permisos).

Ahora que ha añadido la política a su usuario de IAM, está listo para comenzar el proceso de importación.

AWS CLI Permissions

Utilice el siguiente procedimiento para crear las políticas administradas necesarias para conceder a un usuario de IAM los permisos necesarios para realizar solicitudes de datos de importación mediante AWS CLI.

Para crear y adjuntar las políticas gestionadas

1. Use `aws iam create-policy` AWS CLI para crear una política de IAM con los siguientes permisos. Recuerde reemplazar el nombre de su bucket por el nombre real del bucket en el que el usuario de IAM cargará los archivos de importación.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::importBucket"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": ["arn:aws:s3:::importBucket/*"]
    }
  ]
}
```

Para obtener más información acerca del uso de este comando, consulte [create-policy](#) en la AWS CLI Referencia de los comandos.

2. Use `aws iam create-policy` AWS CLI para crear una política de IAM adicional con los siguientes permisos.

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

```

    "Effect": "Allow",
    "Action": [
        "discovery:ListConfigurations",
        "discovery:CreateApplication",
        "discovery:UpdateApplication",
        "discovery:AssociateConfigurationItemsToApplication",
        "discovery:DisassociateConfigurationItemsFromApplication",
        "discovery:GetDiscoverySummary",
        "discovery:StartImportTask",
        "discovery:DescribeImportTasks",
        "discovery:BatchDeleteImportData"
    ],
    "Resource": "*"
}
]
}

```

3. Use `aws iam attach-user-policy` para asociar las políticas que creó en los dos pasos anteriores al usuario de IAM que realizará las solicitudes de importación en su cuenta de AWS mediante el CLI de AWS. Para obtener más información acerca del uso de este comando, consulte [attach-user-policy](#) en la Referencia de los comandos de AWS CLI.

Ahora que ha añadido las políticas a su usuario de IAM, está listo para comenzar el proceso de importación.

Recuerde que, cuando el usuario de IAM carga objetos al bucket de Amazon S3 que ha especificado, debe dejar establecidos los permisos predeterminados para los objetos para que el usuario pueda leer el objeto.

Cargar el archivo importado en Amazon S3

A continuación, debe cargar el archivo de importación con formato CSV en Amazon S3 para que se pueda importar. Antes de comenzar, debe tener un bucket de Amazon S3 que contenga su archivo de importación creado o elegido por adelantado.

Console S3 Upload

Para cargar el archivo importado en Amazon S3

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon S3 en <https://console.aws.amazon.com/s3/>.
2. En la lista Bucket name (Nombre del bucket), seleccione el nombre del bucket en el que desea cargar el objeto.
3. Seleccione Upload (Cargar).
4. En el cuadro de diálogo Upload (Cargar), seleccione Add files (Añadir archivos) para elegir el archivo que desea cargar.
5. Seleccione un archivo que cargar y luego seleccione Open (Abrir).
6. Seleccione Upload (Cargar).
7. Una vez que se ha cargado el archivo, elija el nombre del objeto de archivo de datos en el panel de buckets.
8. En la pestaña Overview (Información general) de la página de detalles de objeto, copie el valor de Object URL (URL de objeto). Lo necesitará cuando cree la solicitud de importación.
9. Vaya a la página de importación en la consola de Migration Hub, como se describe en [Importación de datos](#). A continuación, pega la URL del objeto en el URL del objeto de Amazon S3.

AWS CLI S3 Upload

Para cargar el archivo importado en Amazon S3

1. Abra una ventana de terminal y vaya al directorio donde está guardado su archivo de importación.
2. Escriba el siguiente comando:

```
aws s3 cp ImportFile.csv s3://BucketName/ImportFile.csv
```

3. Devolverá los siguientes resultados:

```
upload: .\ImportFile.csv to s3://BucketName/ImportFile.csv
```

4. Copiar la ruta completa del objeto de Amazon S3 que se ha devuelto. Lo necesitará cuando cree la solicitud de importación.

Importación de datos

Una vez que haya descargado la plantilla de importación desde la consola Migration Hub y la haya rellenado con los datos existentes del servidor local, estará listo para comenzar a importar los datos a Migration Hub. En las siguientes instrucciones se describen dos formas de hacer esto: utilizando la consola o mediante llamadas a la API a través de la AWS CLI.

Console Import

Comience la importación de datos en la Herramientas desde la consola de Migration Hub.

Para comenzar la importación de datos

1. En el panel de navegación, en Discover (Detectar), elija Tools (Herramientas).
2. Si aún no ha rellenado una plantilla de importación, puede descargarla seleccionando import template (importar plantilla) en el cuadro Import (Importar). Abra la plantilla descargada y rellénela con los datos del servidor local existente. También puede descargar la plantilla de importación de nuestro bucket de Amazon S3 en https://s3.us-west-2.amazonaws.com/templates-7cfff56-bd96-4b1c-b45b-a5b42f282e46/import_template.csv
3. Para abrir la importación, elija la importación en la importación.
4. Debajo Nombre de importación., especifique un nombre para la importación.
5. Rellene el URL del objeto de Amazon S3. Para realizar este paso, deberá cargar el archivo de datos de importación en Amazon S3. Para obtener más información, consulte [Cargar el archivo importado en Amazon S3](#).
6. Elija Import (Importar) en el área derecha inferior. Se abrirá la página Imports (Importaciones), donde puede ver su importación y su estado en la tabla.

Después de seguir el procedimiento anterior para comenzar la importación de datos, la página Imports (Importaciones) mostrará los detalles de cada solicitud de importación, incluyendo su estado de avance, el tiempo de finalización y el número de registros correctos o con error con la posibilidad de descargar dichos registros. Desde esta pantalla también puede ir a la página Servers (Servidores) en Discover (Detectar) para ver los datos reales importados.

En la página Servers (Servidores), puede ver una lista de todos los servidores (dispositivos) que se han detectado junto con el nombre de la importación. Al navegar desde la Importaciones (historial de importación) seleccionando el nombre de la importación que aparece en el Nombre, se dirige a la sección de Servidores en la que se aplica un filtro basado en

el conjunto de datos de la importación seleccionada. A continuación, solo verá los datos que pertenecen a esa importación en particular.

El archivo está en formato .zip y contiene dos archivos: `errors-file` y `failed-entries-file`. El archivo de errores contiene una lista de mensajes de error asociados con cada línea con error y el nombre de columna asociado del archivo de datos que tuvo errores en la importación. Puede utilizar este archivo para identificar rápidamente dónde se produjeron los problemas. El archivo de entradas con error incluye cada línea y todas las columnas con error. Puede realizar los cambios que se indican en el archivo de errores de este archivo e intentar importar el archivo de nuevo con la información corregida.

AWS CLI Import

Para comenzar el proceso de importación de datos desde la AWS CLI, primero tendrá que instalar la AWS CLI en su entorno. Para obtener más información, consulte [Instalación de AWS Command Line Interface](#) en la [AWS Command Line Interface Guía del usuario](#) de.

Note

Si todavía no ha rellenado una plantilla de importación, puede descargarla de nuestro bucket de Amazon S3 aquí: https://s3.us-west-2.amazonaws.com/templates-7cfcf56-bd96-4b1c-b45b-a5b42f282e46/import_template.csv

Para comenzar la importación de datos

1. Abra una ventana de terminal y escriba el siguiente comando:

```
aws discovery start-import-task --import-url s3://BucketName/ImportFile.csv --  
name ImportName
```

2. De esta manera, se creará su tarea de importación y le devolverá la siguiente información de estado:

```
{  
  "task": {  
    "status": "IMPORT_IN_PROGRESS",  
    "applicationImportSuccess": 0,  
    "serverImportFailure": 0,  
    "serverImportSuccess": 0,  
  }  
}
```



```
    "name": "ImportName",
    "importRequestTime": 1547682819.801,
    "applicationImportFailure": 0,
    "clientRequestToken": "EXAMPLE1-abcd-1234-abcd-EXAMPLE1234",
    "importUrl": "s3://BucketName/ImportFile.csv",
    "importTaskId": "import-task-EXAMPLE1229949eabfEXAMPLE03862c0"
  }
}
```

Seguimiento de solicitudes de importación de Migration Hub

Puede hacer un seguimiento del estado de sus solicitudes de importación Migration Hub utilizando la consola, AWS CLI, o uno de los AWSSDK.

Console Tracking

Desde el momento en que se crea una solicitud de importación en la consola Migration Hub, encontrará los siguientes elementos.

- Nombre: el nombre de la solicitud de importación.
- ID de importación: el ID único de la solicitud de importación.
- Hora de importación: la fecha y hora en que se creó la solicitud de importación.
- Estado de importación.: el estado de la solicitud de importación. Puede ser uno de los siguientes valores:
 - Importing (Importando): este archivo de datos se está importando actualmente.
 - Importado: todo el archivo de datos se ha importado correctamente.
 - Importado con errores: uno o más de los registros del archivo de datos no se han importado. Para resolver los registros con error, elija Download failed records (Descargar registros con error) para su tarea de importación, resuelva los errores en el archivo csv de entradas con error y vuelva a realizar la importación.
 - No se pudo importar: no se importó ninguno de los registros del archivo de datos. Para resolver los registros con error, elija Download failed records (Descargar registros con error) para su tarea de importación, resuelva los errores en el archivo csv de entradas con error y vuelva a realizar la importación.
- Registros importados: el número de registros de un archivo de datos específico que se han importado correctamente.
- Registros fallidos: los registros de un archivo de datos específico que no se han importado.

CLI Tracking

Puede hacer un seguimiento del estado de sus tareas de importación con el comando `aws discovery describe-import-tasks` de la AWS CLI.

1. Abra una ventana de terminal y escriba el siguiente comando:

```
aws discovery describe-import-tasks
```

2. Devolverá una lista de todas las tareas de importación en formato JSON, completa con el estado y otra información relevante. También puede filtrar los resultados para devolver un subconjunto de las tareas de importación.

Al realizar el seguimiento de las tareas de importación, es posible que el valor devuelto de `serverImportFailure` sea mayor que cero. Cuando esto sucede, significa que el archivo de importación tenía una o más entradas que no se han podido importar. Esto se puede resolver descargando el archivo de registros con error, revisando los archivos que contiene y realizando otra solicitud de importación con el archivo `failed-entries.csv` modificado.

Después de crear la tarea de importación, puede realizar acciones adicionales para administrar y realizar un seguimiento de la migración de datos. Por ejemplo, puede descargar un archivo de registros con error para una solicitud específica. Para obtener información sobre el uso del archivo de registros con errores para resolver problemas de importación, consulte [Solución de problemas de registros de importación fallidos](#).

Ver, exportar y explorar los datos descubiertos

Tanto Application Discovery Service Agentless Collector (Agentless Collector) como AWS Discovery Agent (Discovery Agent) proporciona datos de rendimiento del sistema basados en el uso promedio y máximo. Puede usar los datos de rendimiento del sistema que se recopilan para lograr un costo total de propiedad (TCO) de alto nivel. Los agentes de detección recopilan datos más detallados, incluidos datos de series temporales para la información de rendimiento del sistema, las conexiones de red entrantes y salientes y los procesos que se ejecutan en el servidor. Puede utilizar estos datos para conocer las dependencias de red entre los servidores y agrupar los servidores relacionados en aplicaciones para la planificación de la migración.

En esta sección encontrará instrucciones sobre cómo ver y trabajar con los datos descubiertos por Agentless Collector y Discovery Agent tanto desde la consola como desde el AWS CLI.

Temas

- [Ver los datos recopilados mediante la consola de Migration Hub](#)
- [Exportación de datos recopilados](#)
- [Exploración de datos en Amazon Athena](#)

Ver los datos recopilados mediante la consola de Migration Hub

Tanto para Application Discovery Service Agentless Collector (Agentless Collector) como para AWS Discovery Agent (Discovery Agent), una vez iniciado el proceso de recopilación de datos, puede utilizar la consola para ver los datos recopilados sobre sus servidores y máquinas virtuales. Los datos aparecen en la consola aproximadamente 15 minutos después del inicio de la recopilación de datos. También puede ver estos datos en formato CSV exportando los datos recopilados realizando llamadas a la API mediante el AWS CLI. La exportación de los datos recopilados se explica en la siguiente sección [Exportación de datos recopilados](#).

Para ver los datos recopilados sobre los servidores detectados

1. En el panel de navegación de la consola, elija Servers (Servidores). Los servidores detectados aparecen en la lista de servidores.
2. Para obtener más información de los datos recopilados, elija el enlace de nombre de servidor en la columna Server info (Información del servidor). Se mostrará una pantalla en la que se describe información detallada como la información del sistema, métricas de desempeño, etc.

Para obtener más información sobre el uso de la consola para ver, ordenar y etiquetar los servidores descubiertos por sus recopiladores o agentes de descubrimiento sin agente, consulte [AWS Application Discovery Service Tutoriales de la consola](#).

El módulo de recopilación de datos de análisis y base de datos de Agentless Collector carga los datos recopilados en el bucket de Amazon S3. Puede ver los datos de este bucket en la consola de AWS DMS.

Para ver los datos recopilados sobre los servidores de bases de datos y análisis detectados

1. Inicie sesión en la consola de AWS DMS AWS Management Console y ábrala en <https://console.aws.amazon.com/dms/v2/>.
2. Selecciona Inventario en Descubrir. Se abre la página Inventario y muestra una lista de los servidores de bases de datos y análisis detectados.

Lógica de coincidencia para servidores y aplicaciones detectados

AWS Application Discovery Service (Application Discovery Service) tiene una lógica de coincidencia integrada que identifica cuándo los servidores que descubre coinciden con las entradas existentes. Cuando esta lógica encuentra una coincidencia, actualiza la información del servidor ya existente detectado con nuevos valores.

Esta lógica de coincidencia gestiona servidores duplicados de múltiples fuentes, como la importación de AWS Migration Hub (Migration Hub), Application Discovery Service Agentless Collector (Agentless Collector), AWS Application Discovery Agent (Discovery Agent) y otras herramientas de migración. Para obtener más información sobre la importación de Migration Hub, consulte [Migration Hub Import](#).

Cuando se produce la detección de servidores, cada entrada se compara con registros importados previamente para asegurarse de que el servidor importado no exista ya. Si no se encuentra ninguna coincidencia, se crea un nuevo registro y se asigna un nuevo identificador de servidor único. Si se encuentra una coincidencia, se crea una nueva entrada, pero se le asigna el mismo identificador de servidor único que el servidor existente. Al ver este servidor en la consola de Migration Hub, solo encontrará una entrada única para el servidor.

Los atributos de servidor asociados a esta entrada se fusionan para mostrar los valores de atributo de un registro previamente disponible, así como el nuevo registro importado. Si hay más de un valor para un determinado atributo de servidor de múltiples orígenes, por ejemplo, dos valores diferentes

para Total RAM asociados con un servidor determinado detectado mediante importación y también por el agente de detección, el valor que se actualizó más recientemente se muestra en el registro coincidente del servidor.

Campos coincidentes

Los siguientes campos se utilizan para la coincidencia de servidores cuando se utilizan herramientas de detección.

- **ExternalId**— Este es el campo principal que se utiliza para hacer coincidir los servidores. Si el valor de este campo es idéntico al **ExternalId** de otra entrada, Application Discovery Service hace coincidir las dos entradas, independientemente de si los demás campos coinciden o no.
- **IPAddress**
- **HostName**
- **MacAddress**
- **VMware. MoRefId** y **VMware. vCenterId**— Ambos valores deben ser idénticos a los campos respectivos de otra entrada para que Application Discovery Service pueda realizar una coincidencia.

Exportación de datos recopilados

Tanto para el recopilador sin agente de Application Discovery Service (recopilador sin agente) como para el agente de descubrimiento de AWS aplicaciones (agente de descubrimiento), una vez iniciado el proceso de recopilación de datos, puede exportar los datos recopilados sobre sus servidores y máquinas virtuales. Estos datos se pueden exportar interactuando con la consola o realizando llamadas a la API a través de AWS CLI, según la herramienta de descubrimiento que haya utilizado para recopilar datos.

A continuación se proporcionan instrucciones para ambos métodos. Expandir el método de su elección:

Exporte los datos recopilados para todos los servidores mediante el AWS CLI

Los datos que se recopilan de todos los recopiladores y agentes de detección sin agentes que se ejecutan en sus hosts y máquinas virtuales se pueden exportar de forma masiva mediante AWS Command Line Interface (AWS CLI). AWS CLI debe estar instalado en su entorno antes de exportar los datos.

Para instalar la AWS CLI y exportar los datos recopilados

1. Si aún no lo ha hecho, descargue e instale la AWS CLI correspondiente a su tipo de sistema operativo (Windows o Mac/Linux). Para obtener instrucciones de instalación, consulte la [GuíaAWS Command Line Interface del usuario](#).
2. Abra el símbolo del sistema (Windows) o Terminal (MAC/Linux).
 - a. Escriba `aws configure` y pulse Intro.
 - b. Introduzca su ID de clave deAWS acceso y su clave de accesoAWS secreta.
 - c. Especifique `us-west-2` para el nombre de región predeterminado.
 - d. Especifique `text` para el formato de salida predeterminado.
3. Escriba el siguiente comando para generar un ID de exportación:

```
aws discovery start-export-task
```

4. Usando el ID de exportación generado en el paso anterior, escriba el siguiente comando para generar una URL de S3 como un valor para el parámetro "configurationsDownloadUrl":

```
aws discovery describe-export-tasks --export-ids <export ID>
```

5. Copie la URL generada en el paso anterior y péguela en un navegador para descargar el archivo zip con los datos recopilados de los servidores detectados.


El agente de exportación recopiló los datos mediante la consola

La exportación de los datos recopilados por el agente desde la consola se limita a un agente, cuando se encuentra en la página de detalles de un servidor específico. En la página de detalles, encontrará los trabajos de exportación del servidor listados en la parte inferior de la pantalla, debajo de Exportaciones. Si no existe ninguna página de exportación, la página estará vacía. Puede ejecutar hasta cinco exportaciones de datos de servidor a la vez.

Para exportar los datos recopilados sobre un servidor detectado

1. En el panel de navegación, seleccione Servers (Servidores).
2. En la columna Server info (Información del servidor), elija el enlace del servidor para el que desea exportar datos.

3. En la sección Exports (Exportaciones) situada en la parte inferior de la pantalla, elija Export server details (Exportar detalles del servidor).
4. En Export server details (Exportar detalles del servidor), especifique un valor en Start date (Fecha de inicio) y Time (Hora).


 Note

La hora de inicio no puede ser anterior a 72 horas de la hora actual.

5. Elija Export para iniciar el trabajo. El estado inicial será In-progress (En curso); para actualizar el estado, haga clic en el icono de actualización en la sección Exports (Exportaciones).
6. Cuando se complete el trabajo de exportación, elija Download (Descargar) y guarde el archivo .zip.
7. Descomprima el archivo guardado. Un conjunto de archivos.csv contiene los datos de exportación.

Puede abrir los archivos .csv en Microsoft Excel y revisar los datos de servidor exportados.

Entre los archivos, encontrará un archivo JSON que contiene datos sobre la tarea de exportación y sus resultados.

 Note

Para obtener información sobre cómo generar y exportar recomendaciones de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en laAWS Migration Hub consola, consulte las [recomendaciones de instancias de Amazon EC2](#) en la Guía delAWS Migration Hub usuario.

Exploración de datos en Amazon Athena

La exploración de datos en Amazon Athena le permite analizar los datos que Discovery Agents recopilan de todos los servidores locales descubiertos en un solo lugar. Una vez que se habilite la exploración de datos en Amazon Athena desde la consola de Migration Hub (o mediante StartContinuousExport API) y la recopilación de datos para los agentes está activada, los datos recopilados por los agentes se almacenan automáticamente en su depósito de S3 a intervalos regulares.

A continuación, puede visitar Amazon Athena para ejecutar consultas predefinidas a fin de analizar el rendimiento del sistema de series temporales para cada servidor, el tipo de procesos que se ejecutan en cada servidor y las dependencias de red entre los diferentes servidores. Además, puede escribir sus propias consultas personalizadas con Amazon Athena, cargar fuentes de datos existentes adicionales, como exportaciones de bases de datos de administración de configuración (CMDB), y asociar los servidores descubiertos con las aplicaciones empresariales reales. También puede integrar la base de datos de Athena con Amazon QuickSight para visualizar los resultados de la consulta y realizar análisis adicionales

Pasos

1. [Permitir la exploración de datos en Amazon Athena](#)
2. [Uso de la exploración de datos en Amazon Athena](#)

Permitir la exploración de datos en Amazon Athena

La exploración de datos en Amazon Athena se habilita activando la exportación continua mediante la consola de Migration Hub o una llamada a la API desde el AWS CLI. Debe activar la exploración de datos antes de poder ver y empezar a explorar los datos descubiertos en Amazon Athena.

Al realizar una operación de exportación continua, se encarga de crear una función vinculada al servicio `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` se usa automáticamente en tu cuenta. Para obtener más información sobre este rol vinculado a servicio, consulte [Permisos de roles vinculados a servicios para Application Discovery Service](#).

Las siguientes instrucciones muestran cómo habilitar la exploración de datos en Amazon Athena mediante la consola y el AWS CLI.

Enable with the console

La exploración de datos en Amazon Athena se habilita cuando la exportación continua se activa implícitamente al elegir «Iniciar recopilación de datos» o al hacer clic en el botón de alternancia denominado «Exploración de datos en Amazon Athena» en la Colectores de datos de la consola de Migration Hub.

Para habilitar la exploración de datos en Amazon Athena desde la consola

1. En el panel de navegación, elija Data Collectors (Recopiladores de datos).
2. Elija la pestaña Agents (Agentes).

3. Elegir Iniciar la recopilación de datos, o si ya tienes activada la recopilación de datos, haz clic en Exploración de datos en Amazon Athena alternar.
4. En el cuadro de diálogo generado desde el paso anterior, haga clic en la casilla de verificación para aceptar los costos asociados y elija Continue (Continuar) o Enable (Activar).

 Note

Sus agentes ahora se ejecutan en modo de «exportación continua», lo que le permitirá ver y trabajar con los datos descubiertos en Amazon Athena. La primera vez que se activa, los datos pueden tardar hasta 30 minutos en aparecer en Amazon Athena.

Enable with the AWS CLI

La exploración de datos en Amazon Athena se habilita mediante la activación explícita de la exportación continua a través de una llamada a la API desde AWS CLI. Para ello, la AWS CLI debe estar instalada en su entorno.

Para instalar AWS CLI y habilite la exploración de datos en Amazon Athena

1. Instale la AWS CLI correspondiente a su sistema operativo (Linux, macOS o Windows). Consultar el [AWS Command Line Interface Guía del usuario](#) de para obtener instrucciones.
2. Abra el símbolo del sistema (Windows) o Terminal (Linux o macOS).
 - a. Escriba `aws configure` y pulse Intro.
 - b. Ingrese tu AWS ID de clave de clave de clave AWS Clave de acceso secreta.
 - c. Especifique `us-west-2` para el nombre de región predeterminado.
 - d. Especifique `text` para el formato de salida predeterminado.
3. Escriba el siguiente comando:

```
aws discovery start-continuous-export
```

Note

Sus agentes ahora se ejecutan en modo de «exportación continua», lo que le permitirá ver y trabajar con los datos descubiertos en Amazon Athena. La primera vez que se activa, los datos pueden tardar hasta 30 minutos en aparecer en Amazon Athena.

Uso de la exploración de datos en Amazon Athena

Después de habilitar la exploración de datos en Amazon Athena, puede empezar a explorar y trabajar con los datos actuales detallados que descubrieron sus agentes consultando los datos directamente en Athena. Puede utilizar los datos para generar hojas de cálculo, ejecutar un análisis de costos, transferir la consulta a un programa de visualización para diagramar las dependencias de red, etc.

Los temas de esta sección describen las formas en que puede trabajar con sus datos en Athena para evaluar y planificar la migración de su entorno local a AWS.

Temas

- [Exploración de datos directamente en Amazon Athena](#)
- [Visualización de los datos de Amazon Athena](#)
- [Consultas predefinidas para usar en Athena](#)

Exploración de datos directamente en Amazon Athena

Las siguientes instrucciones explican cómo explorar los datos del agente directamente en la consola de Athena. Si no tiene ningún dato en Athena o no ha habilitado la exploración de datos en Amazon Athena, aparecerá un cuadro de diálogo para habilitar la exploración de datos en Amazon Athena, como se explica en [Permitir la exploración de datos en Amazon Athena](#).

Para explorar los datos descubiertos por agentes directamente en Athena

1. En la consola de AWS Migration Hub, elija Servers (Servidores) en el panel de navegación.
2. Para abrir la consola de Amazon Athena, seleccione Explorar datos en Amazon Athena.
3. En la página Editor de consulta, en el panel de navegación en Base de datos, asegúrese de que `application_discovery_service_database` está seleccionado.

Note

En Tablas, las tablas siguientes representan los conjuntos de datos agrupados por los agentes.

- os_info_agent
- network_interface_agent
- sys_performance_agent
- processes_agent
- inbound_connection_agent
- outbound_connection_agent
- id_mapping_agent

4. Consulte los datos en la consola de Amazon Athena escribiendo y ejecutando consultas SQL en el editor de consultas de Athena. Por ejemplo, puede utilizar la siguiente consulta para ver todas las direcciones IP del servidor detectadas.

```
SELECT * FROM network_interface_agent;
```

Para obtener más consultas de ejemplo, consulte [Consultas predefinidas para usar en Athena](#).

Visualización de los datos de Amazon Athena

Para visualizar sus datos, se puede transferir una consulta a un programa de visualización como Amazon QuickSight u otras herramientas de visualización de código abierto como Cytoscape, yEd o Gephi. Utilice estas herramientas para representar diagramas de red, gráficos de resumen y otras representaciones gráficas. Cuando se utiliza este método, se conecta a Athena a través del programa de visualización para que pueda acceder a los datos recopilados como fuente para producir la visualización.

Para visualizar los datos de Amazon Athena con Amazon QuickSight

1. Inicie sesión en [Amazon QuickSight](#).
2. Elija Connect to another data source or upload a file (Conectar con otro origen de datos o cargar un archivo).

3. Elegir Athena. La Nueva fuente de datos de Athena aparece el cuadro de diálogo.
4. Escriba un nombre en el campo Data source name (Nombre del origen de datos).
5. Elija Create data source.
6. Seleccione la UNAgents-servers-ostabla en la Elige tu tabla de y elija Select.
7. En el cuadro de diálogo Finalizar la creación del conjunto de datos, seleccione Importar a SPICE para un análisis más rápido y elija Visualizar.

Se mostrará la visualización.

Consultas predefinidas para usar en Athena

Esta sección contiene un conjunto de consultas predefinidas que realizan casos de uso típicos, como análisis de TCO y visualización de red. Puede utilizar estas consultas tal cual están o modificarlas para adaptarlas a sus necesidades.

Para utilizar una consulta predefinida

1. En la consola de AWS Migration Hub, elija Servers (Servidores) en el panel de navegación.
2. Para abrir la consola de Amazon Athena, seleccione Explorar datos en Amazon Athena.
3. En la página Editor de consulta, en el panel de navegación en Base de datos, asegúrese de que application_discovery_service_database está seleccionado.
4. Elija el signo más (+) en el editor de consultas para crear una pestaña para una nueva consulta.
5. Copie una de las consultas de [Consultas predefinidas](#).
6. Pegue la consulta en el panel de consultas de la nueva pestaña de consultas que acaba de crear.
7. Elija Run Query (Ejecutar consulta).

Consultas predefinidas

Elija un título para ver información sobre la consulta.

Obtener direcciones IP y nombres de host para los servidores

Esta función auxiliar de vista recupera las direcciones IP y los nombres de host de un servidor determinado. Puede utilizar esta función de vista en otras consultas. Para obtener información sobre cómo crear una vista, consulte [CREAR VISTA](#) en el Guía del usuario de Amazon Athena.

```
CREATE OR REPLACE VIEW hostname_ip_helper AS
SELECT DISTINCT
  "os"."host_name"
, "nic"."agent_id"
, "nic"."ip_address"
FROM
  os_info_agent os
, network_interface_agent nic
WHERE ("os"."agent_id" = "nic"."agent_id");
```

Identificar servidores con o sin agentes

Esta consulta puede ayudarle a realizar la validación de datos. Si ha implementado agentes en varios servidores de la red, puede utilizar esta consulta para saber si hay otros servidores en la red sin agentes implementados en ellos. En esta consulta, examinamos el tráfico de red entrante y saliente, y filtramos el tráfico solo para direcciones IP privadas. Es decir, las direcciones IP que comienzan por 192, 10 o 172.

```
SELECT DISTINCT "destination_ip" "IP Address" ,
  (CASE
    WHEN (
      (SELECT "count"(*)
      FROM network_interface_agent
      WHERE ("ip_address" = "destination_ip") ) = 0) THEN
      'no'
    WHEN (
      (SELECT "count"(*)
      FROM network_interface_agent
      WHERE ("ip_address" = "destination_ip") ) > 0) THEN
      'yes' END) "agent_running"
FROM outbound_connection_agent
WHERE (((("destination_ip" LIKE '192.%')
  OR ("destination_ip" LIKE '10.%'))
  OR ("destination_ip" LIKE '172.%'))
UNION
SELECT DISTINCT "source_ip" "IP ADDRESS" ,
  (CASE
    WHEN (
      (SELECT "count"(*)
      FROM network_interface_agent
      WHERE ("ip_address" = "source_ip") ) = 0) THEN
      'no'
```

```

    WHEN (
      (SELECT "count"(*)
       FROM network_interface_agent
       WHERE ("ip_address" = "source_ip")) ) > 0) THEN
      'yes' END) "agent_running"
FROM inbound_connection_agent
WHERE (((("source_ip" LIKE '192.%')
        OR ("source_ip" LIKE '10.%'))
       OR ("source_ip" LIKE '172.%'));

```

Analizar los datos de rendimiento del sistema para servidores con agentes

Puede utilizar esta consulta para analizar el rendimiento del sistema y los datos de patrón de uso de los servidores locales que tienen agentes instalados. La consulta combina la tabla `system_performance_agent` con la tabla `os_info_agent` para identificar el nombre de host de cada servidor. Esta consulta devuelve los datos de uso de series temporales (en intervalos de 15 minutos) de todos los servidores en los que se ejecutan los agentes.

```

SELECT "OS"."os_name" "OS Name" ,
      "OS"."os_version" "OS Version" ,
      "OS"."host_name" "Host Name" ,
      "SP"."agent_id" ,
      "SP"."total_num_cores" "Number of Cores" ,
      "SP"."total_num_cpus" "Number of CPU" ,
      "SP"."total_cpu_usage_pct" "CPU Percentage" ,
      "SP"."total_disk_size_in_gb" "Total Storage (GB)" ,
      "SP"."total_disk_free_size_in_gb" "Free Storage (GB)" ,
      ("SP"."total_disk_size_in_gb" - "SP"."total_disk_free_size_in_gb") "Used
Storage" ,
      "SP"."total_ram_in_mb" "Total RAM (MB)" ,
      ("SP"."total_ram_in_mb" - "SP"."free_ram_in_mb") "Used RAM (MB)" ,
      "SP"."free_ram_in_mb" "Free RAM (MB)" ,
      "SP"."total_disk_read_ops_per_sec" "Disk Read IOPS" ,
      "SP"."total_disk_bytes_written_per_sec_in_kbps" "Disk Write IOPS" ,
      "SP"."total_network_bytes_read_per_sec_in_kbps" "Network Reads (kbps)" ,
      "SP"."total_network_bytes_written_per_sec_in_kbps" "Network Write (kbps)"
FROM "sys_performance_agent" "SP" , "OS_INFO_agent" "OS"
WHERE ("SP"."agent_id" = "OS"."agent_id") limit 10;

```

Realice un seguimiento de la comunicación saliente entre servidores según el número de puerto y los detalles del proceso

Esta consulta obtiene los detalles del tráfico saliente de cada servicio, junto con el número de puerto y los detalles del proceso.

Antes de ejecutar la consulta, si aún no lo ha hecho, debe crear la tabla `iana_service_ports_import` que contiene la base de datos de registro de puertos IANA descargada de IANA. Para obtener información sobre cómo crear esta tabla, consulte [Creación de la tabla de importación del registro de puertos de la](#).

Después de crear la tabla `iana_service_ports_import`, cree dos funciones auxiliares de vista para realizar un seguimiento del tráfico saliente. Para obtener información sobre cómo crear una vista, consulte [CREAR VISTA](#) en el Guía del usuario de Amazon Athena.

Para crear funciones de ayuda de seguimiento de salida

1. Abra la consola de Athena en <https://console.aws.amazon.com/athena/>.
2. Cree el `valid_outbound_ips_helper`, mediante la siguiente función de ayuda que enumera todas las direcciones IP de destino de salida distintas.

```
CREATE OR REPLACE VIEW valid_outbound_ips_helper AS
SELECT DISTINCT "destination_ip"
FROM outbound_connection_agent;
```

3. Cree la vista `outbound_query_helper`, mediante la siguiente función auxiliar que determina la frecuencia de comunicación para el tráfico saliente.

```
CREATE OR REPLACE VIEW outbound_query_helper AS
SELECT "agent_id" ,
       "source_ip" ,
       "destination_ip" ,
       "destination_port" ,
       "agent_assigned_process_id" ,
       "count"(*) "frequency"
FROM outbound_connection_agent
WHERE (("ip_version" = 'IPv4')
      AND ("destination_ip" IN
          (SELECT *
           FROM valid_outbound_ips_helper )))
```

```
GROUP BY "agent_id", "source_ip", "destination_ip", "destination_port",
"agent_assigned_process_id";
```

- Después de crear la tabla `iana_service_ports_import` y sus dos funciones auxiliares, puede ejecutar la siguiente consulta para obtener los detalles sobre el tráfico saliente de cada servicio, junto con el número de puerto y los detalles del proceso.

```
SELECT hip1.host_name "Source Host Name",
       outbound_connections_results0.source_ip "Source IP Address",
       hip2.host_name "Destination Host Name",
       outbound_connections_results0.destination_ip "Destination IP Address",
       outbound_connections_results0.frequency "Connection Frequency",
       outbound_connections_results0.destination_port "Destination Communication
Port",
       outbound_connections_results0.servicename "Process Service Name",
       outbound_connections_results0.description "Process Service Description"
FROM
  (SELECT DISTINCT o.source_ip,
                  o.destination_ip,
                  o.frequency,
                  o.destination_port,
                  ianap.servicename,
                  ianap.description
   FROM outbound_query_helper o, iana_service_ports_import ianap
   WHERE o.destination_port = TRY_CAST(ianap.portnumber AS integer)) AS
outbound_connections_results0 LEFT OUTER
JOIN hostname_ip_helper hip1
  ON outbound_connections_results0.source_ip = hip1.ip_address LEFT OUTER
JOIN hostname_ip_helper hip2
  ON outbound_connections_results0.destination_ip = hip2.ip_address
```

Realice un seguimiento de la comunicación entrante entre servidores según el número de puerto y los detalles del proceso

Esta consulta obtiene información sobre el tráfico entrante de cada servicio, junto con el número de puerto y los detalles del proceso.

Antes de ejecutar esta consulta, si aún no lo ha hecho, debe crear la tabla `iana_service_ports_import` que contiene la base de datos de registro de puertos IANA descargada de IANA. Para obtener información sobre cómo crear esta tabla, consulte [Creación de la tabla de importación del registro de puertos de la](#).

Después de crear la tabla `iana_service_ports_import`, cree dos funciones auxiliares de vista para realizar un seguimiento del tráfico entrante. Para obtener información sobre cómo crear una vista, consulte [CREAR VISTA](#) en el Guía del usuario de Amazon Athena.

Para crear funciones de ayuda de seguimiento de la importación

1. Abra la consola de Athena en <https://console.aws.amazon.com/athena/>.
2. Cree la vista `valid_inbound_ips_helper`, utilizando la siguiente función auxiliar que muestra todas las direcciones IP de origen entrantes distintas.

```
CREATE OR REPLACE VIEW valid_inbound_ips_helper AS
SELECT DISTINCT "source_ip"
FROM inbound_connection_agent;
```

3. Cree la vista `inbound_query_helper`, utilizando la siguiente función auxiliar que determina la frecuencia de comunicación para el tráfico entrante.

```
CREATE OR REPLACE VIEW inbound_query_helper AS
SELECT "agent_id" ,
       "source_ip" ,
       "destination_ip" ,
       "destination_port" ,
       "agent_assigned_process_id" ,
       "count"(*) "frequency"
FROM inbound_connection_agent
WHERE (("ip_version" = 'IPv4')
       AND ("source_ip" IN
           (SELECT *
            FROM valid_inbound_ips_helper )))
GROUP BY "agent_id", "source_ip", "destination_ip", "destination_port",
         "agent_assigned_process_id";
```

4. Después de crear la tabla `iana_service_ports_import` y sus dos funciones auxiliares, puede ejecutar la siguiente consulta para obtener los detalles del tráfico entrante de cada servicio, junto con el número de puerto y los detalles del proceso.

```
SELECT hip1.host_name "Source Host Name",
       inbound_connections_results0.source_ip "Source IP Address",
       hip2.host_name "Destination Host Name",
       inbound_connections_results0.destination_ip "Destination IP Address",
       inbound_connections_results0.frequency "Connection Frequency",
```

```

        inbound_connections_results0.destination_port "Destination Communication
Port",
        inbound_connections_results0.servicename "Process Service Name",
        inbound_connections_results0.description "Process Service Description"
FROM
    (SELECT DISTINCT i.source_ip,
        i.destination_ip,
        i.frequency,
        i.destination_port,
        ianap.servicename,
        ianap.description
    FROM inbound_query_helper i, iana_service_ports_import ianap
    WHERE i.destination_port = TRY_CAST(ianap.portnumber AS integer)) AS
inbound_connections_results0 LEFT OUTER
JOIN hostname_ip_helper hip1
    ON inbound_connections_results0.source_ip = hip1.ip_address LEFT OUTER
JOIN hostname_ip_helper hip2
    ON inbound_connections_results0.destination_ip = hip2.ip_address

```

Identificar el software en ejecución desde el número

Esta consulta identifica el software en ejecución en función de los números de puerto.

Antes de ejecutar esta consulta, si aún no lo ha hecho, debe crear la tabla

`iana_service_ports_import` que contiene la base de datos de registro de puertos IANA descargada de IANA. Para obtener información sobre cómo crear esta tabla, consulte [Creación de la tabla de importación del registro de puertos de la](#).

Ejecute la siguiente consulta para identificar el software en ejecución en función de los números de puerto.

```

SELECT o.host_name "Host Name",
    ianap.servicename "Service",
    ianap.description "Description",
    con.destination_port,
    con.cnt_dest_port "Destination Port Count"
FROM (SELECT agent_id,
    destination_ip,
    destination_port,
    Count(destination_port) cnt_dest_port
    FROM inbound_connection_agent
    GROUP BY agent_id,

```

```

                destination_ip,
                destination_port) con,
        (SELECT agent_id,
                host_name,
                Max("timestamp")
        FROM    os_info_agent
        GROUP  BY agent_id,
                host_name) o,
        iana_service_ports_import ianap
WHERE  ianap.transportprotocol = 'tcp'
      AND con.destination_ip NOT LIKE '172%'
      AND con.destination_port = ianap.portnumber
      AND con.agent_id = o.agent_id
ORDER BY cnt_dest_port DESC;

```

Creación de la tabla de importación del registro de puertos de la

Algunas de las consultas predefinidas requieren una tabla denominada `iana_service_ports_import` que contenga información descargada de IANA (Internet Assigned Numbers Authority).

Para crear la tabla `iana_service_ports_import`

1. Descargue el archivo CSV de la base de datos de registro de puertos IANA desde el [Registro de número de puerto de nombre de servicio y protocolo de transporte](#) en [iana.org](#).
2. Cargue el archivo en Amazon S3. Para obtener más información, consulte [¿Cómo puedo cargar archivos y carpetas en un bucket de S3?](#)
3. Crea una nueva tabla en Athena llamada `iana_service_ports_import`. Para obtener instrucciones, consulte [Crear una tabla de](#) en el Guía del usuario de Amazon Athena. En el ejemplo siguiente, debe reemplazar `my_bucket_name` por el nombre del bucket de S3 en el que cargó el archivo CSV en el paso anterior.

```

CREATE EXTERNAL TABLE IF NOT EXISTS iana_service_ports_import (
    ServiceName STRING,
    PortNumber INT,
    TransportProtocol STRING,
    Description STRING,
    Assignee STRING,
    Contact STRING,
    RegistrationDate STRING,
    ModificationDate STRING,

```

```
Reference STRING,  
ServiceCode STRING,  
UnauthorizedUseReported STRING,  
AssignmentNotes STRING  
)  
ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.lazy.LazySimpleSerDe'  
WITH SERDEPROPERTIES (  
  'serialization.format' = ',',  
  'quoteChar' = '"',  
  'field.delim' = ','  
) LOCATION 's3://my_bucket_name/'  
TBLPROPERTIES ('has_encrypted_data'='false',"skip.header.line.count"="1");
```

AWS Application Discovery Service Tutoriales de la consola

AWS Application Discovery Service (Application Discovery Service) está integrado con AWS Migration Hub (Migration Hub) y los clientes pueden ver y administrar sus recopiladores de datos, servidores y aplicaciones dentro de Migration Hub. Cuando usa la consola del Application Discovery Service, se le redirige a la consola de Migration Hub. Trabajar con la consola de Migration Hub no requiere pasos ni configuraciones adicionales por su parte.

En esta sección, encontrará información sobre cómo administrar y supervisar Application Discovery Service Agentless Collector (Agentless Collector) y AWS Agente de detección de aplicaciones (agente de detección) mediante la consola.

Temas

- [Panel principal](#)
- [Herramientas de recopilación de datos](#)
- [Ver, exportar y explorar los datos del servidor](#)

Panel principal

Para ver el panel principal, seleccione **Salpicadero** desde las **AWS Migration Hub** Panel de navegación de la consola (Migration Hub). En el panel principal de Migration Hub, puede ver estadísticas de alto nivel sobre servidores, aplicaciones y recopiladores de datos, como Application Discovery Service Agentless Collector (Agentless Collector) y AWS Agente de detección de aplicaciones (agente de detección).

Panel principal

El panel principal recopila datos de los paneles **Discover (Detectar)** y **Migrate (Migrar)** en una ubicación central. Tiene cuatro paneles de estado e información y una lista de enlaces de acceso rápido. Mediante los paneles, puede ver un resumen del estado de sus aplicaciones actualizadas más recientemente. También puede obtener acceso rápido a cualquiera de sus aplicaciones, obtener una descripción general de las aplicaciones en los distintos estados y realizar un seguimiento del progreso de migración a lo largo del tiempo.

Para ver el panel principal, seleccione **Salpicadero** en el panel de navegación, que se encuentra en el lado izquierdo de la consola de Migration Hub.

Herramientas de recopilación de datos

Application Discovery Service Agentless Collector (Agentless Collector) y AWS Application Discovery Agent (Discovery Agent) son las herramientas de recopilación de datos que AWS Application Discovery Service (Application Discovery Service) lo utiliza para ayudarlo a descubrir su infraestructura existente. En los siguientes temas, se explica cómo descargar e implementar estas herramientas de recopilación de datos de descubrimiento, [Primeros pasos con Agentless Collector](#) y [AWS Agente de descubrimiento de aplicaciones](#).

Estas herramientas de recopilación de datos almacenan sus datos en el repositorio de Application Discovery Service y proporcionan detalles sobre cada servidor y los procesos que se ejecutan en ellos. Cuando se implementa cualquiera de estas herramientas, puede iniciar, detener y ver los datos recopilados desde el AWS Migration Hub Consola (Migration Hub).

Temas

- [Iniciar y detener los recopiladores de datos](#)
- [Visualización y clasificación de recopiladores de datos](#)

Iniciar y detener los recopiladores de datos

Después de la AWS se implementa el Agente de detección de aplicaciones (Discovery Agent), puede iniciar o detener el proceso de recopilación de datos en el Recopiladores de Página de la AWS Migration Hub Consola (Migration Hub).

Para iniciar o detener las herramientas de recopilación de datos

1. Uso de la AWS Inicie sesión en la cuenta de AWS Management Console y abra la consola de Migration Hub en <https://console.aws.amazon.com/migrationhub/>.
2. En el panel de navegación de la consola Migration Hub en Descubrir, elige Recopiladores de.
3. Elija la pestaña Agents (Agentes).
4. Seleccione la casilla de verificación de la herramienta de recopilación que desea iniciar o detener.
5. Elija Start data collection (Iniciar recopilación de datos) o Stop data collection (Detener recopilación de datos).

Visualización y clasificación de recopiladores de datos

Si implementó muchos recopiladores de datos, puede ordenar la lista de recopiladores implementados que se muestra en la Recopiladores de la consola de. Para ordenar la lista, aplique filtros en la barra de búsqueda. Puede buscar y filtrar por la mayoría de los criterios especificados en la lista Data Collectors (Recopiladores de datos).

En la tabla siguiente, se muestran los criterios de búsqueda que se pueden utilizar para Agentes, incluidos los operadores, los valores y una definición de los valores.

Criterio de búsqueda	"."	Valor: Definición
ID de agente	==	Cualquier ID de agente seleccionado de la lista rellena previamente en la que está instalada una herramienta de recopilación.
Hostname	== !=	Para los agentes, cualquier nombre de host seleccionado de la lista de hosts rellena automáticamente cuando se instala un agente.
Estado de recopilación	== !=	<p>Comenzó: Los datos se recopilan y se envían al Application Discovery Service</p> <p>Inicio programado: La recopilación de datos se ha programado que comience. Los datos se enviarán al Application Discovery Service en el siguiente ping y el estado cambiará a Comenzó.</p> <p>Stopped: Los datos no se recopilan ni se envían al Application Discovery Service.</p>

Criterio de búsqueda	". "	Valor: Definición
		<p>Detener programado: Está previsto que se detenga la recopilación de datos. Los datos dejarán de enviarse al Application Discovery Service en el siguiente ping y el estado cambiará a Stopped.</p>
Estado	<p>==</p> <p>!=</p>	<p>Buen estado: La recopilación de datos no está activada. La herramienta funciona con normalidad.</p> <p>Insalubre: La herramienta está en estado de error. No se están recopilando ni registrando datos.</p> <p>Desconocido: No se ha establecido ninguna conexión en más de una hora.</p> <p>Apagado: La herramienta comunicó por última vez «cierre» debido al cierre de un sistema, servicio o demonio. Si se ha producido un reinicio o actualización de la herramienta, el estado cambiará a otro estado en el primer ciclo de notificación.</p> <p>Ejecución: La recopilación de datos está activada. La herramienta funciona con normalidad.</p>

Criterio de búsqueda	":"	Valor: Definición
Dirección IP	== !=	Cualquier dirección IP seleccionada de la lista rellena automáticamente en la que se ha instalado una herramienta de recopilación.

En la tabla siguiente, se muestran los criterios de búsqueda que se pueden utilizar para Recopiladores sin agentes, incluidos los operadores, los valores y una definición de los valores.

Criterio de búsqueda	":"	Valor: Definición
ID	==	Cualquier ID de recopilador sin agente seleccionado de la lista rellena previamente en la que está instalada una herramienta de recopilación.
Hostname	== !=	Para los recopiladores sin agente, cualquier nombre de host seleccionado de la lista de hosts previamente completada en la que esté instalado un recopilador sin agente.
Estado	== !=	Recopilador de datos La recopilación de datos está activada. La herramienta funciona con normalidad. Listo para configurar: la recopilación de datos no está activada. La herramienta funciona con normalidad.

Criterio de búsqueda	"	Valor: Definición
		<p>Requiere atención: la herramienta está en estado de error y necesita atención.</p> <p>Desconocido: No se ha establecido ninguna conexión en más de una hora.</p> <p>Apagar: La herramienta comunicó por última vez «cierre» debido al cierre de un sistema, servicio o demonio. Si se ha producido un reinicio o actualización de la herramienta, el estado cambiará a otro estado en el primer ciclo de notificación.</p>
Dirección IP	<p>==</p> <p>!=</p>	Cualquier dirección IP seleccionada de la lista rellena automáticamente en la que se ha instalado una herramienta de recopilación.

Para ordenar los recopiladores de datos mediante la aplicación de filtros de búsqueda

1. Uso de lasAWSInicie sesión en la cuenta deAWS Management Consoley abra la consola de Migration Hub en<https://console.aws.amazon.com/migrationhub/>.
2. En el panel de navegación de la consola Migration Hub enDescubrir, eligeRecopiladores de.
3. Elija entre las opcionesRecopiladores sin agentesoAgentesTabulador.
4. Haga clic dentro de la barra de búsqueda y elija un criterio de búsqueda de la lista.
5. Elija un operador en la siguiente lista.
6. Elija un valor en la última lista.

Ver, exportar y explorar los datos del servidor

La página Servers (Servidores) proporciona información de configuración y desempeño del sistema sobre cada instancia de servidor de la que tengan constancia las herramientas de recopilación de datos. Puede ver información del servidor, ordenar los servidores con filtros, etiquetar los servidores con pares de clave-valor y exportar información detallada del servidor y del sistema.

Temas

- [Visualización y clasificación de servidores](#)
- [Etiquetado de servidores](#)
- [Exportar datos del servidor](#)
- [Exploración de datos en Athena](#)
- [Aplicaciones](#)

Visualización y clasificación de servidores

Puede ver información acerca de los servidores detectados por las herramientas de recopilación de datos y puede ordenar los servidores mediante filtros.

Visualización de servidores

Puede obtener una visión general y una visión detallada de los servidores detectados por las herramientas de recopilación de datos.

Para ver los servidores detectados

1. Uso de lasAWSInicie sesión en la cuenta deAWS Management Consoley abra la consola de Migration Hub en<https://console.aws.amazon.com/migrationhub/>.
2. En el panel de navegación de la consola Migration Hub enDescubrir, eligeServidores. Los servidores detectados aparecen en la lista de servidores.
3. Para obtener más información acerca de un servidor, elija su enlace de servidor en la columna Server info (Información del servidor). Se mostrará una pantalla que describe el servidor.

La pantalla de detalles del servidor muestra información del sistema y métricas de desempeño. También encontrará un botón para exportar la información de dependencias y procesos. Para exportar información detallada del servidor, consulte [Exportar datos del servidor](#).

Clasificación de servidores con filtros de búsqueda

Para encontrar fácilmente servidores específicos, aplique filtros de búsqueda para ordenar todos los servidores detectados por las herramientas de recopilación. Puede buscar y filtrar por numerosos criterios.

Para ordenar los servidores mediante la aplicación de filtros de búsqueda

1. Uso de lasAWSInicie sesión en la cuenta deAWS Management Consoley abra la consola de Migration Hub en<https://console.aws.amazon.com/migrationhub/>.
2. En el panel de navegación de la consola Migration Hub enDescubrir, eligeServidores.
3. Haga clic dentro de la barra de búsqueda y elija un criterio de búsqueda de la lista.
4. Elija un operador en la siguiente lista.
5. Escriba un valor que distinga entre mayúsculas y minúsculas para el criterio de búsqueda que ha seleccionado y, a continuación, pulse Intro.
6. Se pueden aplicar varios filtros repitiendo los pasos del 2 al 4.

Etiquetado de servidores

Para ayudarle a planificar la migración y mantener el orden, puede crear varias etiquetas para cada servidor. Las etiquetas son pares de clave-valor que pueden almacenar datos personalizados o metadatos de los servidores. Puede etiquetar un servidor individual o varios servidores en una sola operación.AWS Application Discovery Service (Application Discovery Service) son similares aAWS Etiquetas, pero los dos tipos de etiquetas no se pueden usar indistintamente.

Puede añadir o eliminar varias etiquetas para uno o varios servidores desde la página Servers (Servidores) principal. En la página de detalles de un servidor, puede añadir o eliminar una o varias etiquetas para el servidor seleccionado. Puede realizar cualquier tipo de tarea de etiquetado que incluya varios servidores o etiquetas en una sola operación. También puede eliminar etiquetas.

Para añadir etiquetas a uno o varios servidores

1. Uso de lasAWSInicie sesión en la cuenta deAWS Management Consoley abra la consola de Migration Hub en<https://console.aws.amazon.com/migrationhub/>.
2. En el panel de navegación de la consola Migration Hub enDescubrir, eligeServidores.

3. En la columna Server info (Información del servidor), elija el enlace del servidor al que desea añadir etiquetas. Para añadir etiquetas a más de un servidor a la vez, haga clic en las casillas de verificación de varios servidores.
4. Elegir Añada etiqueta y, a continuación, elija Añada una etiqueta nueva.
5. En el cuadro de diálogo, escriba una clave en el cuadro de diálogo Clave y, opcionalmente, un valor en el campo Valor.

Añade más etiquetas eligiendo Añada una etiqueta nueva y añadir más información.

6. Seleccione Save (Guardar).

Para eliminar etiquetas de uno o varios servidores

1. Uso de las AWS: Inicie sesión en la cuenta de AWS Management Console y abra la consola de Migration Hub en <https://console.aws.amazon.com/migrationhub/>.
2. En el panel de navegación de la consola Migration Hub en Descubrir, elige Servidores.
3. En la columna Server info (Información del servidor), elija el enlace del servidor del que desea eliminar etiquetas. Seleccione las casillas de verificación de varios servidores para eliminar etiquetas de más de un servidor a la vez.
4. Elegir Eliminación de etiquetas.
5. Seleccione cada etiqueta que desee eliminar.
6. Elija Confirm.

Exportar datos del servidor

Para exportar información de dependencias de red y procesos de un servidor cada vez, puede utilizar la pantalla de detalles de un servidor. Encontrará los trabajos de exportación de un servidor en una tabla incluida en la sección Exports (Exportaciones) de la pantalla de detalles del servidor. Si aún no existen trabajos de exportación, la tabla estará vacía. Puede exportar hasta cinco colecciones de datos a la vez.


Note

La exportación de datos del servidor desde la consola solo está disponible para los datos recopilados por un agente que se ejecuta en ese servidor. Si desea exportar datos masivos

para todos los servidores en los que se hayan instalado los agentes, consulte [Exploración de datos en Amazon Athena](#).

Para exportar datos detallados del servidor

1. Uso de lasAWSInicie sesión en la cuenta deAWS Management Consoley abra la consola de Migration Hub en<https://console.aws.amazon.com/migrationhub/>.
2. En el panel de navegación de la consola Migration Hub enDescubrir, eligeServidores.
3. En la columna Server info (Información del servidor), elija el ID del servidor para el que desea exportar datos.
4. En la sección Exports (Exportaciones) situada en la parte inferior de la pantalla, elija Export server details (Exportar detalles del servidor).
5. En Export server details (Exportar detalles del servidor), especifique un valor en Start date (Fecha de inicio) y Time (Hora).

 Note

La hora de inicio no puede ser anterior a 72 horas de la hora actual.

6. Elija Export para iniciar el trabajo. El estado inicial será In-progress (En curso); para actualizar el estado, haga clic en el icono de actualización en la sección Exports (Exportaciones).
7. Cuando se complete el trabajo de exportación, elija Download (Descargar) y guarde el archivo .zip.
8. Descomprima el archivo guardado. Un conjunto de archivos .csv contiene los datos de exportación, similar al siguiente:
 - *<AWSID de la cuenta de_*destinationProcessConnection.CSV
 - *<AWSID de la cuenta de_*networkInterface.csv
 - *<AWSID de la cuenta de_*osInfo.csv
 - *<AWSID de la cuenta de_*process.csv
 - *<AWSID de la cuenta de_*sourceProcessConnection.CSV
 - *<AWSID de la cuenta de_*systemPerformance.csv

Puede abrir los archivos .csv en Microsoft Excel y revisar los datos de servidor exportados.

Entre los archivos, encontrará un archivo JSON que contiene datos sobre la tarea de exportación y sus resultados.

Exploración de datos en Athena

La exploración de datos en Amazon Athena le permite analizar los datos que Discovery Agent recopila de todos los servidores locales descubiertos en un solo lugar. Una vez que se habilite la exploración de datos en Amazon Athena desde la consola de Migration Hub (o mediante StartContinuousExport API) y la recopilación de datos para los agentes está activada, los datos recopilados por los agentes se almacenan automáticamente en su depósito de S3 a intervalos regulares. Para obtener más información, consulte [Exploración de datos en Amazon Athena](#).

Aplicaciones

Es posible que tenga que migrar algunos de los servidores detectados para que sigan funcionando. En tal caso, puede definir y agrupar de forma lógica los servidores detectados en aplicaciones.

Como parte del proceso de agrupación, puede buscar, filtrar y añadir etiquetas.

Para agrupar servidores en una aplicación nueva o existente

1. Uso de lasAWSInicie sesión en la cuenta deAWS Management Consoley abra la consola de Migration Hub en<https://console.aws.amazon.com/migrationhub/>.
2. En el panel de navegación de la consola Migration Hub enDescubrir, eligeServidores.
3. En la lista de servidores, seleccione cada servidor que desea agrupar en una aplicación nueva o existente.

Para ayudar a elegir los servidores de su grupo, puede buscar y filtrar por cualquiera de los criterios que especifique en la lista de servidores. Haga clic en la barra de búsqueda y elija un elemento de la lista, seleccione un operador de la lista siguiente y, a continuación, especifique los criterios.

4. Opcional: Para cada servidor seleccionado, elijaAñada etiqueta, escriba un valor paraClavey, si lo desea, escriba un valor paraValor.
5. Elija Group as application (Agrupar como aplicación) para crear la aplicación o añadir los servidores a una aplicación existente.

6. En el cuadro de diálogo Group as application (Agrupar como aplicación), elija Group as a new application (Agrupar como nueva aplicación) o Add to an existing application (Añadir a una aplicación existente).
 - a. Si ha elegido Group as a new application (Agrupar como nueva aplicación), escriba un nombre en Application name (Nombre de aplicación). Si lo desea, puede especificar una descripción en Application description (Descripción de la aplicación).
 - b. Si ha elegido Add to an existing application (Añadir a una aplicación existente), seleccione el nombre de la aplicación a la que desea añadir servidores de la lista.
7. Seleccione Save (Guardar).

Uso de la API Application Discovery Service para consultar los elementos de configuración detectados

Un elemento de configuración es un activo de TI que un agente o una importación descubrió en su centro de datos. Cuando usa AWS Application Discovery Service (Application Discovery Service), usa la API para especificar filtros y consultar elementos de configuración específicos para los activos de servidor, aplicación, proceso y conexión. Para obtener información sobre la API, consulte la [referencia de la API de Application Discovery Service](#).

En las tablas de las siguientes secciones se enumeran los filtros de entrada y las opciones de clasificación de salida disponibles para dos acciones de Application Discovery Service:

- `DescribeConfigurations`
- `ListConfigurations`

Las opciones de filtrado y ordenación están organizadas por el tipo de recurso al que se aplican (servidor, aplicación, proceso o conexión).

Important

Los resultados devueltos por `DescribeConfigurations` y `ListConfigurations`, y es posible que `StartExportTask` no contengan actualizaciones recientes. Para obtener más información, consulte [Consistencia final](#).

Uso de la **DescribeConfigurations** acción

La acción `DescribeConfigurations` recupera los atributos de una lista de ID de configuración. Todos los ID suministrados deben ser para el mismo tipo de recurso (servidor, aplicación, proceso o conexión). Los campos de salida son específicos del tipo de activo seleccionado. Por ejemplo, la salida de un servidor elemento de configuración de servidor incluye una lista de atributos sobre el servidor, como, por ejemplo, nombre de host, sistema operativo y número de tarjetas de red. Para obtener más información sobre la sintaxis de los comandos, consulte [DescribeConfigurations](#).

La acción `DescribeConfigurations` no admite el filtrado.

Campos de salida para **DescribeConfigurations**

En las tablas siguientes, organizadas por tipo de recurso, se enumeran los campos de salida admitidos de la acción `DescribeConfigurations`. Los marcados como obligatorios están siempre presentes en la salida.

Recursos de servidor

Campo	Obligatorio
<code>server.agentId</code>	
<code>server.applications</code>	
<code>server.applications.hasMoreValues</code>	
<code>server.configurationId</code>	x
<code>server.cpuType</code>	
<code>server.hostName</code>	
<code>server.hypervisor</code>	
<code>server.networkInterfaceInfo</code>	
<code>server.networkInterfaceInfo.hasMoreValues</code>	
<code>server.osName</code>	
<code>server.osVersion</code>	
<code>server.tags</code>	
<code>server.tags.hasMoreValues</code>	
<code>server.timeOfCreation</code>	x
<code>server.type</code>	

Campo	Obligatorio
<code>server.performance.avgCpuUsagePct</code>	
<code>server.performance.avgDiskReadIOPS</code>	
<code>server.performance.avgDiskReadsPerSecondInKB</code>	
<code>server.performance.avgDiskWriteIOPS</code>	
<code>server.performance.avgDiskWritesPerSecondInKB</code>	
<code>server.performance.avgFreeRAMInKB</code>	
<code>server.performance.avgNetworkReadsPerSecondInKB</code>	
<code>server.performance.avgNetworkWritesPerSecondInKB</code>	
<code>server.performance.maxCpuUsagePct</code>	
<code>server.performance.maxDiskReadIOPS</code>	
<code>server.performance.maxDiskReadsPerSecondInKB</code>	
<code>server.performance.maxDiskWriteIOPS</code>	
<code>server.performance.maxDiskWritesPerSecondInKB</code>	

Campo	Obligatorio
<code>server.performance.maxNetworkReadsPerSecondInKB</code>	
<code>server.performance.maxNetworkWritesPerSecondInKB</code>	
<code>server.performance.minFreeRAMInKB</code>	
<code>server.performance.numCores</code>	
<code>server.performance.numCpus</code>	
<code>server.performance.numDisks</code>	
<code>server.performance.numNetworkCards</code>	
<code>server.performance.totalRAMInKB</code>	

Procesamiento de recursos

Campo	Obligatorio
<code>process.commandLine</code>	
<code>process.configurationId</code>	x
<code>process.name</code>	
<code>process.path</code>	
<code>process.timeOfCreation</code>	x

Recursos de aplicación

Campo	Obligatorio
<code>application.configurationId</code>	x
<code>application.description</code>	
<code>application.lastModifiedTime</code>	x
<code>application.name</code>	x
<code>application.serverCount</code>	x
<code>application.timeOfCreation</code>	x

Uso de la **ListConfigurations** acción

La acción `ListConfigurations` recupera una lista de elementos de configuración según los criterios especificados en un filtro. Para obtener más información sobre la sintaxis de los comandos, consulte [ListConfigurations](#).

Campos de salida para **ListConfigurations**

En las tablas siguientes, organizadas por tipo de recurso, se enumeran los campos de salida admitidos de la acción `ListConfigurations`. Los marcados como obligatorios están siempre presentes en la salida.

Recursos de servidor

Campo	Obligatorio
<code>server.configurationId</code>	x
<code>server.agentId</code>	
<code>server.hostName</code>	
<code>server.osName</code>	
<code>server.osVersion</code>	

Campo	Obligatorio
<code>server.timeOfCreation</code>	x
<code>server.type</code>	

Procesamiento de recursos

Campo	Obligatorio
<code>process.commandLine</code>	
<code>process.configurationId</code>	x
<code>process.name</code>	
<code>process.path</code>	
<code>process.timeOfCreation</code>	x
<code>server.agentId</code>	
<code>server.configurationId</code>	x

Recursos de aplicación

Campo	Obligatorio
<code>application.configurationId</code>	x
<code>application.description</code>	
<code>application.name</code>	x
<code>application.serverCount</code>	x
<code>application.timeOfCreation</code>	x
<code>application.lastModifiedTime</code>	x

Recursos de conexión

Campo	Obligatorio
<code>connection.destinationIp</code>	X
<code>connection.destinationPort</code>	X
<code>connection.ipVersion</code>	X
<code>connection.latestTimestamp</code>	X
<code>connection.occurrence</code>	X
<code>connection.sourceIp</code>	X
<code>connection.transportProtocol</code>	
<code>destinationProcess.configurationId</code>	
<code>destinationProcess.name</code>	
<code>destinationServer.configurationId</code>	
<code>destinationServer.hostName</code>	
<code>sourceProcess.configurationId</code>	
<code>sourceProcess.name</code>	
<code>sourceServer.configurationId</code>	
<code>sourceServer.hostName</code>	

Filtros compatibles para **ListConfigurations**

En las tablas siguientes, organizadas por tipo de recurso, se enumeran los filtros admitidos para la acción `ListConfigurations`. Los filtros y valores se encuentran en una relación clave/

valor definida por una de las condiciones lógicas admitidas. Puede ordenar la salida de los filtros indicados.

Recursos de servidor

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
<code>server.configurationId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	<ul style="list-style-type: none"> • Cualquier ID de configuración de servidor válido 	Ninguna
<code>server.hostName</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Cadena 	<ul style="list-style-type: none"> • ASC • DESC
<code>server.osName</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Cadena 	<ul style="list-style-type: none"> • ASC • DESC
<code>server.osVersion</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Cadena 	<ul style="list-style-type: none"> • ASC • DESC
<code>server.agentId</code>	<ul style="list-style-type: none"> • EQUALS 	<ul style="list-style-type: none"> • Cadena 	Ninguna

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
	<ul style="list-style-type: none"> • NOT_EQUALS • EQ • NE 		
<code>server.connectorId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	<ul style="list-style-type: none"> • Cadena 	Ninguna
<code>server.type</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	Cadena con uno de los siguientes valores: <ul style="list-style-type: none"> • EC2 • OTHER • VMWARE_VM • VMWARE_HOST • VMWARE_VM_TEMPLATE 	Ninguna
<code>server.vmWareInfo.morefId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Cadena 	Ninguna

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
<code>server.vmWareInfo.vcenterId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Cadena 	Ninguna
<code>server.vmWareInfo.hostId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Cadena 	Ninguna
<code>server.networkInterfaceInfo.portGroupId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Cadena 	Ninguna
<code>server.networkInterfaceInfo.portGroupName</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Cadena 	Ninguna

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
<code>server.networkInterfaceInfo.virtualSwitchName</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Cadena 	Ninguna
<code>server.networkInterfaceInfo.ipAddress</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Cadena 	Ninguna
<code>server.networkInterfaceInfo.macAddress</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Cadena 	Ninguna
<code>server.performance.avgCpuUsagePct</code>	<ul style="list-style-type: none"> • GE • LE • GT • LT 	<ul style="list-style-type: none"> • Porcentaje 	Ninguna
<code>server.performance.totalDiskFreeSizeInKB</code>	<ul style="list-style-type: none"> • GE • LE • GT • LT 	<ul style="list-style-type: none"> • Doble 	Ninguna

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
<code>server.performance.avgFreeRAMInKB</code>	<ul style="list-style-type: none"> • GE • LE • GT • LT 	<ul style="list-style-type: none"> • Doble 	Ninguna
<code>server.tag.value</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Cadena 	Ninguna
<code>server.tag.key</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Cadena 	Ninguna
<code>server.application.name</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Cadena 	Ninguna

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
<code>server.application.description</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Cadena 	Ninguna
<code>server.application.configurationId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	<ul style="list-style-type: none"> • Cualquier ID de configuración de aplicación válida 	Ninguna
<code>server.process.configurationId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	<ul style="list-style-type: none"> • ProcessId 	Ninguna
<code>server.process.name</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Cadena 	Ninguna
<code>server.process.commandLine</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Cadena 	Ninguna

Recursos de aplicación

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
<code>application.configurationId</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE 	<ul style="list-style-type: none"> ApplicationId 	Ninguna
<code>application.name</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> Cadena 	<ul style="list-style-type: none"> ASC DESC
<code>application.description</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> Cadena 	<ul style="list-style-type: none"> ASC DESC
<code>application.serverCount</code>	No se admite el filtrado.	No se admite el filtrado.	<ul style="list-style-type: none"> ASC DESC
<code>application.timeOfCreation</code>	No se admite el filtrado.	No se admite el filtrado.	<ul style="list-style-type: none"> ASC DESC

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
<code>application.lastModifiedTime</code>	No se admite el filtrado.	No se admite el filtrado.	<ul style="list-style-type: none"> • ASC • DESC
<code>server.configurationId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	<ul style="list-style-type: none"> • ServerId 	Ninguna

Procesamiento de recursos

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
<code>process.configurationId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	<ul style="list-style-type: none"> • ProcessId 	
<code>process.name</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Cadena 	<ul style="list-style-type: none"> • ASC • DESC
<code>process.commandLine</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	<ul style="list-style-type: none"> • Cadena 	<ul style="list-style-type: none"> • ASC • DESC

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
	<ul style="list-style-type: none"> CONTAINS NOT_CONTAINS 		
<code>server.configurationId</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE 	<ul style="list-style-type: none"> ServerId 	
<code>server.hostName</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> Cadena 	<ul style="list-style-type: none"> ASC DESC
<code>server.osName</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> Cadena 	<ul style="list-style-type: none"> ASC DESC
<code>server.osVersion</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> Cadena 	<ul style="list-style-type: none"> ASC DESC

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
<code>server.agentId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Cadena 	

Recursos de conexión

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
<code>connection.sourceIp</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • IP 	<ul style="list-style-type: none"> • ASC • DESC
<code>connection.destinationIp</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • IP 	<ul style="list-style-type: none"> • ASC • DESC
<code>connection.destinationPort</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	<ul style="list-style-type: none"> • Entero 	<ul style="list-style-type: none"> • ASC • DESC

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
sourceServer.configurationId	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	<ul style="list-style-type: none"> • ServerId 	
sourceServer.hostName	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Cadena 	<ul style="list-style-type: none"> • ASC • DESC
destinationServer.osName	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Cadena 	<ul style="list-style-type: none"> • ASC • DESC
destinationServer.osVersion	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Cadena 	<ul style="list-style-type: none"> • ASC • DESC

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
<code>destinationServer.agentId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Cadena 	
<code>sourceProcess.configurationId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	<ul style="list-style-type: none"> • ProcessId 	
<code>sourceProcess.name</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Cadena 	<ul style="list-style-type: none"> • ASC • DESC
<code>sourceProcess.commandLine</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Cadena 	<ul style="list-style-type: none"> • ASC • DESC
<code>destinationProcess.configurationId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	<ul style="list-style-type: none"> • ProcessId 	

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
<code>destinationProcess.name</code>	<ul style="list-style-type: none">• EQUALS• NOT_EQUALS• EQ• NE• CONTAINS• NOT_CONTAINS	<ul style="list-style-type: none">• Cadena	<ul style="list-style-type: none">• ASC• DESC
<code>destinationProcess.commandLine</code>	<ul style="list-style-type: none">• EQUALS• NOT_EQUALS• EQ• NE• CONTAINS• NOT_CONTAINS	<ul style="list-style-type: none">• Cadena	<ul style="list-style-type: none">• ASC• DESC

Coherencia eventual en la AWS Application Discovery Service API

Las siguientes operaciones de actualización son finalmente consistentes. Es posible que las actualizaciones no estén visibles inmediatamente para las operaciones de lectura [StartExportTask](#), [DescribeConfigurations](#), y [ListConfigurations](#).

- [AssociateConfigurationItemsToAplicación](#)
- [CreateTags](#)
- [DeleteApplications](#)
- [DeleteTags](#)
- [DescribeBatchDeleteConfigurationTarea](#)
- [DescribeImportTareas](#)
- [DisassociateConfigurationItemsFromSolicitud](#)
- [UpdateApplication](#)

Sugerencias para gestionar la coherencia eventual:

- Cuando invoque las operaciones de lectura [StartExportTask](#), [DescribeConfigurations](#), o [ListConfigurations](#) (o sus AWS CLI comandos correspondientes), utilice un algoritmo de retroceso exponencial para dejar tiempo suficiente para que cualquier operación de actualización anterior se propague por el sistema. Para ello, ejecute la operación de lectura varias veces, empezando con un tiempo de espera de dos segundos y aumentando gradualmente hasta cinco minutos.
- Añada el tiempo de espera entre las operaciones subsiguientes, incluso si una operación de actualización arroja una respuesta de 200 (OK). Aplique un algoritmo de retardo exponencial comenzando con un par de segundos de tiempo de espera y aumente gradualmente hasta unos cinco minutos de tiempo de espera.

Seguridad en AWS Application Discovery Service

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

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

- Seguridad de la nube – AWS es responsable de proteger la infraestructura que ejecuta los servicios de AWS en la nube de AWS. AWS también proporciona servicios que puede utilizar de forma segura. Auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los [programas de conformidad de AWS](#).
- Seguridad en la nube: su responsabilidad viene determinada por el servicio de AWS que utilice. Usted también es responsable de otros factores incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Para utilizar AWS Application Discovery Agent o Application Discovery Service Agentless Collector, debe proporcionar las claves de acceso a su AWS cuenta. Luego, esta información se almacena en su infraestructura local. Como parte del modelo de responsabilidad compartida, usted es responsable de proteger el acceso a su infraestructura.

Esta documentación le ayudará a entender cómo aplicar el modelo de responsabilidad compartida al utilizar Application Discovery Service. En los temas siguientes se muestra cómo configurar Application Discovery Service para cumplir sus objetivos de seguridad y conformidad. También aprenderá a usar otros AWS servicios que pueden ayudarlo a monitorear y proteger sus recursos de Application Discovery Service.

Temas

- [Identity and Access Management para AWS Application Discovery Service](#)
- [Registro y monitoreo en AWS Application Discovery Service](#)

Identity and Access Management para AWS Application Discovery Service

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

Temas

- [Público](#)
- [Autenticación con identidades](#)
- [Administración de acceso mediante políticas](#)
- [¿Cómo AWS Application Discovery Service funciona con IAM](#)
- [AWS políticas gestionadas para AWS Application Discovery Service](#)
- [AWS Application Discovery Service Ejemplos de políticas basadas en la identidad](#)
- [Uso de roles vinculados a servicios para Application Discovery Service](#)
- [Solución de problemas AWS Application Discovery Service de identidad y acceso](#)

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realice en Application Discovery Service.

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

Administrador de servicios: si está a cargo de los recursos de Application Discovery Service en su empresa, probablemente tenga acceso completo a Application Discovery Service. Es su trabajo determinar a qué funciones y recursos de Application Discovery Service deben acceder los usuarios del servicio. A continuación, debe enviar solicitudes al IAM administrador para cambiar los permisos de los usuarios del servicio. Revise la información de esta página para comprender los conceptos

básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM Application Discovery Service, consulte [¿Cómo AWS Application Discovery Service funciona con IAM?](#)

IAM administrador: si es IAM administrador, puede que desee obtener información detallada sobre cómo escribir políticas para administrar el acceso a Application Discovery Service. Para ver ejemplos de políticas basadas en la identidad de Application Discovery Service que puede utilizar IAM, consulte [AWS Application Discovery Service Ejemplos de políticas basadas en la identidad](#)

Autenticación con identidades

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

Usuario raíz de la cuenta de AWS

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

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

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

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

Cuenta de AWS usuario root

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

Usuarios y grupos de IAM

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

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

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

IAMFunciones

Un [IAMrol](#) es una identidad dentro de tu Cuenta de AWS que tiene permisos específicos. Es similar a un IAM usuario, pero no está asociado a una persona específica. Puede asumir temporalmente un IAM rol en el AWS Management Console [cambiando de rol](#). Puede asumir un rol llamando a

una AWS API operación AWS CLI o o utilizando una operación personalizada URL. Para obtener más información sobre los métodos de uso de roles, consulte [Uso de IAM roles](#) en la Guía del IAM usuario.

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

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

- **Función de servicio:** una función de servicio es una [IAMfunción](#) que un servicio asume para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentro IAM. Para obtener más información, consulte [Crear un rol para delegar permisos Servicio de AWS en un rol](#) en el IAMManual del usuario.
- **Función vinculada a un servicio:** una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un IAM administrador puede ver los permisos de los roles vinculados al servicio, pero no editarlos.
- **Aplicaciones que se ejecutan en Amazon EC2:** puedes usar un IAM rol para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y que realizan AWS CLI o AWS API solicitan. Esto es preferible a almacenar las claves de acceso 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 [Uso de un IAM rol para conceder permisos a aplicaciones que se ejecutan en EC2 instancias de Amazon](#) en la Guía del IAM usuario.

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

Administración de acceso mediante políticas

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

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

De forma predeterminada, los usuarios y los roles no tienen permisos. Para conceder a los usuarios permiso para realizar acciones en los recursos que necesitan, un IAM administrador puede crear

IAM políticas. A continuación, el administrador puede añadir las IAM políticas a las funciones y los usuarios pueden asumir las funciones.

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

Políticas basadas en identidad

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

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

Políticas basadas en recursos

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

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

Listas de control de acceso (ACLs)

Las listas de control de acceso (ACLs) controlan qué 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 JSON de las políticas.

Amazon S3, AWS WAF y Amazon VPC son ejemplos de servicios compatibles con ACLs. Para obtener más información sobre 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 función avanzada en la que se establecen los permisos máximos que una política basada en la identidad puede conceder a una entidad IAM (IAM Usuario o rol). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte los [límites de los permisos para IAM las entidades](#) en la Guía del IAM Usuario.
- **Políticas de control de servicios (SCPs):** SCPs son JSON políticas que especifican los permisos máximos para una organización o unidad organizativa (OU) AWS Organizations. AWS Organizations es un servicio para agrupar y administrar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus cuentas. 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 sesión:** las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información, consulte [las políticas de sesión](#) en la Guía del IAM usuario.

Varios tipos de políticas

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

¿Cómo AWS Application Discovery Service funciona con IAM

Antes de administrar el acceso IAM a Application Discovery Service, debe comprender qué IAM funciones están disponibles para su uso con Application Discovery Service. Para obtener una visión general de cómo funcionan Application Discovery Service y otros AWS servicios IAM, consulte [AWS Servicios con los que funcionan IAM](#) en la Guía del IAM usuario.

Temas

- [Políticas basadas en la identidad de Application Discovery Service](#)
- [Políticas basadas en recursos de Application Discovery Service](#)
- [Autorización basada en etiquetas de Application Discovery Service](#)
- [IAM Funciones de Application Discovery Service](#)

Políticas basadas en la identidad de Application Discovery Service

Con las políticas IAM basadas en la identidad, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. Application Discovery Service admite acciones, recursos y claves de condición específicos. Para obtener información sobre todos los elementos que se utilizan en una JSON política, consulte la [Referencia sobre los elementos de la IAM JSON política](#) en la Guía del IAM usuario.

Acciones

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

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

requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

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

Las acciones de política en Application Discovery Service utilizan el siguiente prefijo antes de la acción: `discovery:`. Las instrucciones de la política deben incluir un elemento `Action` o un elemento `NotAction`. Application Discovery Service define su propio conjunto de acciones que describen las tareas que puede realizar con este servicio.

Para especificar varias acciones en una única instrucción, sepárelas con comas del siguiente modo:

```
"Action": [  
    "discovery:action1",  
    "discovery:action2"
```

Puede utilizar caracteres comodín para especificar varias acciones (*). Por ejemplo, para especificar todas las acciones que comiencen con la palabra `Describe`, incluya la siguiente acción:

```
"Action": "discovery:Describe*"
```

Para ver una lista de las acciones de Application Discovery Service, consulte [Acciones definidas por AWS Application Discovery Service](#) en la Guía del IAM usuario.

Recursos

Application Discovery Service no admite la especificación de recursos ARNs en una política. Para separar el acceso, cree y utilícelo por separado Cuentas de AWS.

Claves de condición

Application Discovery Service no proporciona ninguna clave de condición específica del servicio, pero sí admite el uso de algunas claves de condición globales. Para ver todas las claves de condición AWS globales, consulte las claves de [contexto de condición AWS globales](#) en la Guía del IAM usuario.

Ejemplos

Para ver ejemplos de políticas basadas en la identidad de Application Discovery Service, consulte. [AWS Application Discovery Service Ejemplos de políticas basadas en la identidad](#)

Políticas basadas en recursos de Application Discovery Service

Application Discovery Service no admite políticas basadas en recursos.

Autorización basada en etiquetas de Application Discovery Service

Application Discovery Service no admite el etiquetado de recursos ni el control del acceso en función de las etiquetas.

IAMFunciones de Application Discovery Service

Un [IAMrol](#) es una entidad de su AWS cuenta que tiene permisos específicos.

Uso de credenciales temporales con Application Discovery Service

Application Discovery Service no admite el uso de credenciales temporales.

Roles vinculados a servicios

Las [funciones vinculadas al servicio](#) permiten a AWS los servicios acceder a los recursos de otros servicios para completar una acción en su nombre. Los roles vinculados al servicio aparecen en tu IAM cuenta y son propiedad del servicio. Un IAM administrador puede ver los permisos de los roles vinculados al servicio, pero no editarlos.

Application Discovery Service admite funciones vinculadas a servicios. Para obtener más información sobre la creación o administración de funciones vinculadas a servicios de Application Discovery Service, consulte. [Uso de roles vinculados a servicios para Application Discovery Service](#)

Roles de servicio

Esta característica permite que un servicio asuma un [rol de servicio](#) en su nombre. Este rol permite que el servicio obtenga acceso a los recursos de otros servicios para completar una acción en su nombre. Los roles de servicio aparecen en su IAM cuenta y son propiedad de la cuenta. Esto significa que un IAM administrador puede cambiar los permisos de este rol. Sin embargo, hacerlo podría deteriorar la funcionalidad del servicio.

Application Discovery Service apoya las funciones de servicio.

AWS políticas gestionadas para AWS Application Discovery Service

Para añadir permisos a usuarios, grupos y roles, es más fácil usar políticas AWS administradas que escribirlas usted 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 agregan permisos adicionales a una política administrada de AWS para admitir características nuevas. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Es más probable que los servicios actualicen una política administrada de AWS cuando se lanza una nueva característica o cuando se ponen a disposición nuevas operaciones. 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 descripción 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: `AWSApplicationDiscoveryServiceFullAccess`

La `AWSApplicationDiscoveryServiceFullAccess` política otorga a una cuenta de usuario de IAM acceso a las API Application Discovery Service y Migration Hub.

Una cuenta de usuario de IAM con esta política adjunta puede configurar Application Discovery Service, iniciar y detener agentes, iniciar y detener el descubrimiento sin agentes y consultar datos

de la base de datos de AWS Discovery Service. Para obtener un ejemplo de esta política, consulte [Concesión de acceso completo a Application Discovery Service](#).

AWS política gestionada: AWSApplicationDiscoveryAgentlessCollectorAccess

La política `AWSApplicationDiscoveryAgentlessCollectorAccess` gestionada otorga al Application Discovery Service Agentless Collector (Agentless Collector) acceso para registrarse y comunicarse con el Application Discovery Service y comunicarse con otros servicios. AWS

Esta política debe adjuntarse al usuario de IAM cuyas credenciales se utilizan para configurar el recopilador sin agente.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `arsenal`— Permite que el recopilador se registre en la aplicación Application Discovery Service. Esto es necesario para poder enviar los datos recopilados a AWS.
- `ecr-public`— Permite al recopilador realizar llamadas al Amazon Elastic Container Registry Public (Amazon ECR Public), donde se encuentran las actualizaciones más recientes del recopilador.
- `mgh`— Permite al recopilador llamar AWS Migration Hub para recuperar la región de origen de la cuenta utilizada para configurar el recopilador. Esto es necesario para saber a qué región deben enviarse los datos recopilados.
- `sts`— Permite al recopilador recuperar un token de portador del servicio para que pueda realizar llamadas a Amazon ECR Public para obtener las actualizaciones más recientes.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "arsenal:RegisterOnPremisesAgent"
      ],
      "Resource": "*"
    },
    {
```

```

    "Effect": "Allow",
    "Action": [
        "ecr-public:DescribeImages"
    ],
    "Resource": "arn:aws:ecr-
public::44637222237:repository/6e5498e4-8c31-4f57-9991-13b4b992ff7b"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ecr-public:GetAuthorizationToken"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "mgh:GetHomeRegion"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "sts:GetServiceBearerToken"
        ],
        "Resource": "*"
    }
    ]
}

```

AWS política gestionada: AWSApplicationDiscoveryAgentAccess

La `AWSApplicationDiscoveryAgentAccess` política otorga al Application Discovery Agent acceso para registrarse y comunicarse con Application Discovery Service.

Adjunta esta política a cualquier usuario cuyas credenciales utilice Application Discovery Agent.

Esta política también concede acceso al usuario a Arsenal. Arsenal es un servicio de agente administrado y alojado por AWS. El Arsenal reenvía los datos a Application Discovery Service en la nube. Para obtener un ejemplo de esta política, consulte [Otorgar acceso a los agentes de detección](#).

AWS política gestionada: AWSAgentlessDiscoveryService

La `AWSAgentlessDiscoveryService` política otorga al AWS Agentless Discovery Connector que se ejecuta en su VMware vCenter Server acceso para registrar, comunicarse y compartir las métricas de estado del conector con Application Discovery Service.

Asocie esta política a cualquier usuario cuyas credenciales utilicen el conector.

AWS política gestionada: política

`ApplicationDiscoveryServiceContinuousExportServiceRole`

Si su cuenta de IAM tiene la `AWSApplicationDiscoveryServiceFullAccess` política adjunta, `ApplicationDiscoveryServiceContinuousExportServiceRolePolicy` se adjunta automáticamente a su cuenta cuando activa la exploración de datos en Amazon Athena.

Esta política permite AWS Application Discovery Service crear transmisiones de Amazon Data Firehose para transformar y entregar los datos recopilados por los AWS Application Discovery Service agentes a un bucket de Amazon S3 de su AWS cuenta.

Además, esta política crea una AWS Glue Data Catalog nueva base de datos llamada `application_discovery_service_database` y tablas de esquemas para mapear los datos recopilados por los agentes. Para obtener un ejemplo de esta política, consulte [Otorgar permisos para la recopilación de datos de los agentes](#).

AWS política gestionada: `AWSDiscoveryContinuousExportFirehosePolicy`

La `AWSDiscoveryContinuousExportFirehosePolicy` política es obligatoria para utilizar la exploración de datos en Amazon Athena. Permite a Amazon Data Firehose escribir los datos recopilados desde Application Discovery Service en Amazon S3. Para obtener información sobre el uso de esta política, consulte [Crear el rol `AWSApplicationDiscoveryServiceFirehose`](#). Para obtener un ejemplo de esta política, consulte [Otorgar permisos para la exploración de datos](#).

Crear el rol `AWSApplicationDiscoveryServiceFirehose`

Un administrador adjunta las políticas gestionadas a su cuenta de usuario de IAM. Al usar la `AWSDiscoveryContinuousExportFirehosePolicy` política, el administrador primero debe crear un rol denominado `AWSApplicationDiscoveryServiceFirehoseFirehose` como entidad de confianza y, a continuación, adjuntar la `AWSDiscoveryContinuousExportFirehosePolicy` política al rol, como se muestra en el siguiente procedimiento.

Para crear el rol de IAM AWSApplicationDiscoveryServiceFirehose

1. En la consola de IAM, selecciona Roles en el panel de navegación.
2. Seleccione Crear rol.
3. Elija Kinesis.
4. Elija Kinesis Firehose como su caso de uso.
5. Elija Siguiente: permisos.
6. En Filtrar políticas, busque AWSDiscoveryContinuousExportFirehosePolicy.
7. Selecciona la casilla situada al lado y AWSDiscoveryContinuousExportFirehosePolicy, a continuación, selecciona Siguiente: Revisar.
8. Introduce AWSApplicationDiscoveryServiceFirehoseel nombre del rol y, a continuación, selecciona Crear rol.

Application Discovery Service actualiza las políticas AWS administradas

Vea los detalles sobre las actualizaciones de las políticas AWS administradas de Application Discovery Service desde que este servicio comenzó a rastrear estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de [Historial de documento de AWS Application Discovery Service](#).

Cambio	Descripción	Fecha
AWSApplicationDiscoveryAgentlessCollectorAccess — La nueva política está disponible con el lanzamiento de Agentless Collector	Application Discovery Service agregó la nueva política administrada AWSApplicationDiscoveryAgentlessCollectorAccess que otorga al recopilador sin agente acceso para registrarse y comunicarse con el Application Discovery Service y comunicarse con otros AWS servicios.	16 de agosto de 2022

Cambio	Descripción	Fecha
Application Discovery Service comenzó a rastrear los cambios	Application Discovery Service comenzó a rastrear los cambios en sus políticas AWS administradas.	1 de marzo de 2021

AWS Application Discovery Service Ejemplos de políticas basadas en la identidad

De forma predeterminada, IAM los usuarios y los roles no tienen permiso para crear o modificar los recursos de Application Discovery Service. Tampoco pueden realizar tareas con AWS Management Console AWS CLI, o AWS API. IAMEI administrador debe crear IAM políticas que concedan a los usuarios y roles permisos para realizar API operaciones específicas en los recursos específicos que necesitan. A continuación, el administrador debe adjuntar esas políticas a los IAM usuarios o grupos que requieran esos permisos.

Para obtener información sobre cómo crear una política IAM basada en la identidad con estos documentos de JSON política de ejemplo, consulte [Creación de políticas en la JSON pestaña de la Guía del IAMusuario](#).

Temas

- [Prácticas recomendadas sobre las políticas](#)
- [Concesión de acceso completo a Application Discovery Service](#)
- [Otorgar acceso a los agentes de detección](#)
- [Otorgar permisos para la recopilación de datos de los agentes](#)
- [Otorgar permisos para la exploración de datos](#)
- [Conceder permisos para usar el diagrama de red de la consola de Migration Hub](#)

Prácticas recomendadas sobre las políticas

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

- Comience con las políticas AWS administradas y opte por los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su Cuenta de AWS. Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Para obtener más información, consulte [las políticas AWS gestionadas](#) o [las políticas AWS gestionadas para las funciones laborales](#) en la Guía del IAM usuario.
- Aplique permisos con privilegios mínimos: cuando establezca permisos con IAM políticas, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Para obtener más información sobre cómo IAM aplicar permisos, consulte [Políticas y permisos IAM en](#) la IAM Guía del usuario.
- Utilice las condiciones en IAM las políticas para restringir aún más el acceso: puede añadir una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de política para especificar que todas las solicitudes deben enviarse mediante 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, como AWS CloudFormation. Para obtener más información, consulte [los elementos IAM JSON de la política: Condición](#) en la Guía del IAM usuario.
- Utilice IAM Access Analyzer para validar sus IAM políticas y garantizar permisos seguros y funcionales: IAM Access Analyzer valida las políticas nuevas y existentes para que se ajusten al lenguaje de las políticas (JSON) y IAM a las IAM mejores prácticas. IAM Access Analyzer proporciona más de 100 comprobaciones de políticas y recomendaciones prácticas para ayudarle a crear políticas seguras y funcionales. Para obtener más información, consulte la [validación de políticas de IAM Access Analyzer](#) en la Guía del IAM usuario.
- Requerir autenticación multifactorial (MFA): si se encuentra en una situación en la que se requieren IAM usuarios o un usuario raíz Cuenta de AWS, actívela MFA para aumentar la seguridad. Para solicitarlo MFA cuando se convoque a API las operaciones, añada MFA condiciones a sus políticas. Para obtener más información, consulte [Configuración del API acceso MFA protegido](#) en la Guía del IAM usuario.

Para obtener más información sobre las prácticas recomendadas IAM, consulte las [prácticas recomendadas de seguridad IAM en](#) la Guía del IAM usuario.

Concesión de acceso completo a Application Discovery Service

La política `AWSApplicationDiscoveryServiceFullAccess` gestionada concede a la cuenta IAM de usuario acceso a Application Discovery Service y a Migration Hub APIs.

Un IAM usuario con esta política asociada a su cuenta puede configurar Application Discovery Service, iniciar y detener agentes, iniciar y detener la detección sin agentes y consultar datos de la base de datos de AWS Discovery Service. Para obtener más información sobre esta política, consulte [AWS políticas gestionadas para AWS Application Discovery Service](#).

Example `AWSApplicationDiscoveryServiceFullAccess` política

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "mgh:*",
        "discovery:*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Action": [
        "iam:GetRole"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Otorgar acceso a los agentes de detección

La política `AWSApplicationDiscoveryAgentAccess` administrada otorga al Application Discovery Agent acceso para registrarse y comunicarse con Application Discovery Service. Para obtener más información sobre esta política, consulte [AWS políticas gestionadas para AWS Application Discovery Service](#).

Adjunte esta política a cualquier usuario cuyas credenciales utilice Application Discovery Agent.

Esta política también concede acceso al usuario a Arsenal. Arsenal es un servicio de agente administrado y alojado por AWS. El Arsenal reenvía los datos a Application Discovery Service en la nube.

Example AWSApplicationDiscoveryAgentAccessPolítica

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "arsenal:RegisterOnPremisesAgent"
      ],
      "Resource": "*"
    }
  ]
}
```

Otorgar permisos para la recopilación de datos de los agentes

La política `ApplicationDiscoveryServiceContinuousExportServiceRolePolicy` gestionada permite AWS Application Discovery Service crear transmisiones de Amazon Data Firehose para transformar y entregar los datos recopilados por los agentes de Application Discovery Service a un bucket de Amazon S3 de su AWS cuenta.

Además, esta política crea un catálogo de AWS Glue datos con una nueva base de datos denominada `application_discovery_service_database` y tablas de esquemas para mapear los datos recopilados por los agentes.

Para obtener información sobre el uso de esta política, consulte [AWS políticas gestionadas para AWS Application Discovery Service](#).

Example ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "glue:CreateDatabase",
        "glue:UpdateDatabase",

```

```

        "glue:CreateTable",
        "glue:UpdateTable",
        "firehose:CreateDeliveryStream",
        "firehose:DescribeDeliveryStream",
        "logs:CreateLogGroup"
    ],
    "Effect": "Allow",
    "Resource": "*"
},
{
    "Action": [
        "firehose>DeleteDeliveryStream",
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:UpdateDestination"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:firehose:*:*:deliverystream/aws-application-discovery-
service*"
},
{
    "Action": [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:PutBucketLogging",
        "s3:PutEncryptionConfiguration"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:s3:::aws-application-discovery-service*"
},
{
    "Action": [
        "s3:GetObject"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:s3:::aws-application-discovery-service*/*"
},
{
    "Action": [
        "logs:CreateLogStream",
        "logs:PutRetentionPolicy"
    ],
    "Effect": "Allow",

```

```

    "Resource": "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose*"
  },
  {
    "Action": [
      "iam:PassRole"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:iam:*:*:role/AWSApplicationDiscoveryServiceFirehose",
    "Condition": {
      "StringLike": {
        "iam:PassedToService": "firehose.amazonaws.com"
      }
    }
  },
  {
    "Action": [
      "iam:PassRole"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:iam:*:*:role/service-role/
AWSApplicationDiscoveryServiceFirehose",
    "Condition": {
      "StringLike": {
        "iam:PassedToService": "firehose.amazonaws.com"
      }
    }
  }
]
}

```

Otorgar permisos para la exploración de datos

La `AWSDiscoveryContinuousExportFirehosePolicy` política es obligatoria para utilizar la exploración de datos en Amazon Athena. Permite a Amazon Data Firehose escribir los datos recopilados desde Application Discovery Service en Amazon S3. Para obtener información sobre el uso de esta política, consulte [Crear el rol `AWSApplicationDiscoveryServiceFirehose`](#).

Example `AWSDiscoveryContinuousExportFirehosePolicy`

```

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

```

```

    {
      "Effect": "Allow",
      "Action": [
        "glue:GetTableVersions"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::aws-application-discovery-service-*",
        "arn:aws:s3:::aws-application-discovery-service-*/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose:log-stream:*"
      ]
    }
  ]
}

```

Conceder permisos para usar el diagrama de red de la consola de Migration Hub

Para conceder acceso al diagrama de red de la AWS Migration Hub consola al crear una política basada en la identidad que permita o deniegue el acceso a Application Discovery Service o a Migration Hub, puede que tenga que añadir la `discovery:GetNetworkConnectionGraph` acción a la política.

Debe utilizar la `discovery:GetNetworkConnectionGraph` acción en las políticas nuevas o actualizar las políticas anteriores si se cumplen las dos condiciones siguientes para la política:

- La política permite o deniega el acceso a Application Discovery Service o al Migration Hub.
- La política otorga permisos de acceso mediante una acción de descubrimiento más específica, como `discovery:action-name` en lugar de `discovery:*`.

El siguiente ejemplo muestra cómo utilizar la `discovery:GetNetworkConnectionGraph` acción en una IAM política.

Example

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["discovery:GetNetworkConnectionGraph"],
      "Resource": "*"
    }
  ]
}
```

Para obtener información sobre el diagrama de red de Migration Hub, consulte [Visualización de las conexiones de red en Migration Hub](#).

Uso de roles vinculados a servicios para Application Discovery Service

AWS Application Discovery Service utiliza roles [vinculados a servicios](#) de AWS Identity and Access Management (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Application Discovery Service. Los roles vinculados a servicios están predefinidos por Application Discovery Service e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios de en su nombre.

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

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

Temas

- [Permisos de roles vinculados a servicios para Application Discovery Service](#)
- [Creación de un rol vinculado a un servicio para Application Discovery Service](#)
- [Eliminación de un rol vinculado a un servicio para Application Discovery Service](#)

Para obtener información sobre otros servicios que son compatibles con los roles vinculados a servicios, consulte [Servicios de AWS que funcionan con IAM](#) y busque los servicios que muestran Yes (Sí) en la columna Service-Linked Role (Rol vinculado a servicios). Seleccione una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de roles vinculados a servicios para Application Discovery Service

Application Discovery Service usa el rol vinculado a servicios denominado `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport`— Permite el acceso a AWS Servicios y recursos utilizados o gestionados por AWS Application Discovery Service.

La `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` El rol vinculado a servicios confía en los siguientes servicios para asumir el rol:

- `continuousexport.discovery.amazonaws.com`

La política de permisos del rol permite que Application Discovery Service realice las siguientes acciones en los recursos:

glue

`CreateDatabase`

`UpdateDatabase`

`CreateTable`

`UpdateTable`

firehose

`CreateDeliveryStream`

DeleteDeliveryStream

DescribeDeliveryStream

PutRecord

PutRecordBatch

UpdateDestination

s3

CreateBucket

ListBucket

GetObject

registros

CreateLogGroup

CreateLogStream

PutRetentionPolicy

iam

PassRole

Esta es la política completa que muestra los recursos a los que se aplican las acciones anteriores:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:UpdateTable",
        "firehose:CreateDeliveryStream",
        "firehose:DescribeDeliveryStream",
        "logs:CreateLogGroup"
      ],
      "Effect": "Allow",
    }
  ]
}
```

```

    "Resource": "*"
  },
  {
    "Action": [
      "firehose:DeleteDeliveryStream",
      "firehose:PutRecord",
      "firehose:PutRecordBatch",
      "firehose:UpdateDestination"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:firehose:*:*:deliverystream/aws-application-discovery-
service*"
  },
  {
    "Action": [
      "s3:CreateBucket",
      "s3:ListBucket",
      "s3:PutBucketLogging",
      "s3:PutEncryptionConfiguration"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:s3:::aws-application-discovery-service*"
  },
  {
    "Action": [
      "s3:GetObject"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:s3:::aws-application-discovery-service/*/*"
  },
  {
    "Action": [
      "logs:CreateLogStream",
      "logs:PutRetentionPolicy"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose*"
  },
  {
    "Action": [
      "iam:PassRole"
    ],
    "Effect": "Allow",

```



```

    "Resource": "arn:aws:iam::*:role/AWSApplicationDiscoveryServiceFirehose",
    "Condition": {
      "StringLike": {
        "iam:PassedToService": "firehose.amazonaws.com"
      }
    }
  },
  {
    "Action": [
      "iam:PassRole"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:iam::*:role/service-role/
AWSApplicationDiscoveryServiceFirehose",
    "Condition": {
      "StringLike": {
        "iam:PassedToService": "firehose.amazonaws.com"
      }
    }
  }
]
}

```

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

Creación de un rol vinculado a un servicio para Application Discovery Service

No necesita crear manualmente un rol vinculado a servicios. La `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` la función vinculada al servicio se crea automáticamente cuando la exportación continua se activa implícitamente mediante a) la confirmación de las opciones en el cuadro de diálogo que se presenta en la página Recopiladores de datos después de elegir «Iniciar recopilación de datos» o hacer clic en el control deslizante denominado «Exploración de datos en Athena», o b) cuando llama al `StartContinuousExport` API que usa el `AWSCLI`.

⚠ Important

Este rol vinculado al servicio puede aparecer en su cuenta si se ha completado una acción en otro servicio que utilice las características compatibles con este rol. Para obtener más información, consulte [Un nuevo rol ha aparecido en mi cuenta de IAM](#).

Creación de la función vinculada al servicio desde la consola de Migration Hub

Puede utilizar la consola de Migration Hub para crear el `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` rol vinculado a servicios.

Para crear la función vinculada al servicio (consola)

1. En el panel de navegación, elija Data Collectors (Recopiladores de datos).
2. Elija la pestaña Agents (Agentes).
3. Alternar el Exploración de datos en Athenadeslizador a la posición Encendido.
4. En el cuadro de diálogo generado desde el paso anterior, haga clic en la casilla de verificación para aceptar los costos asociados y elija Continue (Continuar) o Enable (Activar).

Creación del rol vinculado a servicios a partir de laAWS CLI

Puede usar los comandos del Application Discovery Service desde laAWS Command Line Interfacepara crear el `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport`rol vinculado a servicios.

Esta función vinculada al servicio se crea automáticamente al iniciar la exportación continua desde elAWS CLI(elaWS CLIdebe instalarse primero en su entorno).

Para crear el rol vinculado a servicios (CLI), inicie la exportación continua desde elAWS CLI

1. Instale la AWS CLI correspondiente a su sistema operativo (Linux, macOS o Windows). Consulte el[AWS Command Line InterfaceGuía del usuario de](#)para obtener instrucciones.
2. Abra el símbolo del sistema (Windows) o Terminal (Linux o macOS).
 - a. Escriba `aws configure` y pulse Intro.
 - b. Ingresa tuAWSID de clave de acceso de yAWSClave de acceso secreta.
 - c. Especifique `us-west-2` para el nombre de región predeterminado.

- d. Especifique `text` para el formato de salida predeterminado.
3. Escriba el siguiente comando:

```
aws discovery start-continuous-export
```

También puede utilizar la consola de IAM para crear un rol vinculado a un servicio con la Discovery Service: exportación continuacaso de uso. En la CLI de IAM o la API de IAM, cree un rol vinculado a servicio con el nombre de servicio `continuousexport.discovery.amazonaws.com`. Para obtener más información, consulte [Crear un rol vinculado a un servicio](#) en la Guía del usuario de IAM. Si elimina este rol vinculado al servicio, puede utilizar este mismo proceso para volver a crear el rol.

Eliminación de un rol vinculado a un servicio para Application Discovery Service

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

Limpieza de la función vinculada al servicio

Antes de que pueda utilizar IAM para eliminar un rol vinculado a servicios, primero debe eliminar los recursos que utiliza el rol.

Note

Si Application Discovery Service está utilizando el rol cuando intenta eliminar los recursos, es posible que se produzcan errores en la operación de eliminación. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar recursos de Application Discovery Service utilizados por `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` rol vinculado a servicios desde la consola de Migration Hub

1. En el panel de navegación, elija Data Collectors (Recopiladores de datos).
2. Elija la pestaña Agents (Agentes).
3. Alternar elExploración de datos en Athenadeslizador a la posición Off.

Para eliminar recursos de Application Discovery Service utilizados por `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` rol vinculado a servicios de la AWS CLI

1. Instale la AWS CLI correspondiente a su sistema operativo (Linux, macOS o Windows). Consulte el [AWS Command Line Interface Guía del usuario](#) para obtener instrucciones.
2. Abra el símbolo del sistema (Windows) o Terminal (Linux o macOS).
 - a. Escriba `aws configure` y pulse Intro.
 - b. Ingresa tu `AWSID` de clave de acceso de y `AWSClave de acceso secreta`.
 - c. Especifique `us-west-2` para el nombre de región predeterminado.
 - d. Especifique `text` para el formato de salida predeterminado.
3. Escriba el siguiente comando:

```
aws discovery stop-continuous-export --export-id <export ID>
```

- Si no conoce el ID de la exportación continua que desea detener, escriba el siguiente comando para ver este ID:

```
aws discovery describe-continuous-exports
```

4. Introduzca el siguiente comando para asegurarse de que la exportación continua se ha detenido verificando que su estado de devolución sea «INACTIVO»:

```
aws discovery describe-continuous-export
```

Eliminar manualmente la función vinculada al servicio

Puede eliminar el `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` rol vinculado a servicios mediante la consola de IAM, la CLI de IAM o la API de IAM. Si ya no tiene que utilizar las funciones de Discovery Service - Continuous Export que requieren este rol vinculado a servicios, le recomendamos que elimine dicho rol. De esta forma no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa. Para obtener más información, consulte [Eliminación de un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Note

Primero debe limpiar la función vinculada al servicio antes de eliminarla. Consulte [Limpieza de la función vinculada al servicio](#).

Solución de problemas AWS Application Discovery Service de identidad y acceso

Utilice la siguiente información para ayudarle a diagnosticar y solucionar problemas comunes que pueden surgir al trabajar con Application Discovery Service y IAM.

Temas

- [No estoy autorizado a realizar iam: PassRole](#)

No estoy autorizado a realizar iam: PassRole

Si recibe un error que indica que no está autorizado a realizar la `iam:PassRole` acción, sus políticas deben actualizarse para permitirle transferir una función a Application Discovery Service.

Algunos 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.

El siguiente ejemplo de error se produce cuando un IAM usuario denominado `marymajor` intenta utilizar la consola para realizar una acción en Application Discovery Service. 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 AWS el administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Registro y monitoreo en AWS Application Discovery Service

AWS Application Discovery Service está integrado en AWS CloudTrail. Puede usar CloudTrail para registrar, supervisar y conservar continuamente la actividad de la cuenta para solucionar problemas y auditorías. CloudTrail proporciona un historial de eventos de suAWSactividad de cuenta, incluidas las acciones emprendidas a través delAWSConsola de administración,AWSLos SDK de y las herramientas de línea de comandos de. En el tema de esta sección se explica cómo utilizar CloudTrail con Application Discovery Service.

Temas

- [Registro de llamadas a la API de Application Discovery Service conAWS CloudTrail](#)

Registro de llamadas a la API de Application Discovery Service conAWS CloudTrail

AWS Application Discovery Service se integra conAWS CloudTrail, un servicio que proporciona un registro de las acciones que realiza un usuario, un rol o unAWSen Application Discovery Service. CloudTrail captura todas las llamadas a la API para Application Discovery Service como eventos. Las llamadas capturadas incluyen las llamadas desde la consola de Application Discovery Service y las llamadas desde el código a las operaciones API de Application Discovery Service.

Si crea un registro de seguimiento, puede habilitar la entrega continua de CloudTrail Eventos de a un bucket de Amazon S3, incluidos los eventos de Application Discovery Service. Si no configura un registro de seguimiento, puede ver los eventos más recientes en el CloudTrail Consola de estadoHistorial de eventos. Uso de la información recopilada por CloudTrail, se puede determinar la solicitud que se de al Application Discovery Service, la dirección IP desde la que se, quién la solicitud, cuándo la y los detalles adicionales.

Para obtener más información CloudTrail, consulte la[AWS CloudTrailGuía del usuario de](#).

Application Discovery Service en CloudTrail

CloudTrail está activado en tuAWSal crearla. Cuando se produce una actividad en Application Discovery Service, dicha se registra en un CloudTrail evento junto con otrosAWSEventos de servicio

de enHistorial de eventos. Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte [Visualización de eventos con CloudTrail Historial de eventos](#).

Para mantener un registro continuo de los eventos de laAWS, incluidos los eventos de Application Discovery Service, cree un registro de seguimiento. UNATrailpermite CloudTrail para entregar archivos de registros a un bucket de Amazon S3. De manera predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. Además, puede configurar otrosAWSpara analizar y actuar en función de los datos de eventos recopilados en CloudTrail troncos. Para obtener más información, consulte los siguientes enlaces:

- [Introducción a la creación de registros de seguimiento](#)
- [CloudTrail Servicios e integraciones compatibles con](#)
- [Configuración de notificaciones de Amazon SNS para CloudTrail](#)
- [Recepción de CloudTrail Archivos de registro de multirregionesyRecepción de CloudTrail Archivos de registro de varias cuentas](#)

Todas las acciones de Application Discovery Service CloudTrail y están documentados en el[Application Discovery Service](#). Por ejemplo, las llamadas a laCreateTags,DescribeTags, yGetDiscoverySummarylas acciones generan entradas en el CloudTrail archivos de registro.

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

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

Para obtener más información, consulte el [elemento userIdentity de CloudTrail](#) .

Descripción de las entradas del archivo de registro de Application

Un registro de seguimiento es una configuración que permite entregar eventos como archivos de registro al bucket de Amazon S3 que especifique. CloudTrail Los archivos de registro pueden

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

En el ejemplo siguiente se muestra un CloudTrail entrada de registro que demuestra laDescribeTagsacción.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAJBHMC4H6EKEXAMPLE:sample-user",
    "arn": "arn:aws:sts::444455556666:assumed-role/ReadOnly/sample-user",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDAJQABLZS4A3QDU576Q",
        "arn": "arn:aws:iam::444455556666:role/ReadOnly",
        "accountId": "444455556666",
        "userName": "sampleAdmin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2020-05-05T15:19:03Z"
      }
    }
  },
  "eventTime": "2020-05-05T17:02:40Z",
  "eventSource": "discovery.amazonaws.com",
  "eventName": "DescribeTags",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "20.22.33.44",
  "userAgent": "Coral/Netty4",
  "requestParameters": {
    "maxResults": 0,
    "filters": [
      {
        "values": [
```



```
        "d-server-0315rfdjreyqsq"
      ],
      "name": "configurationId"
    }
  ]
},
"responseElements": null,
"requestID": "mgh-console-eb1cf315-e2b4-4696-93e5-b3a3b9346b4b",
"eventID": "7b32b778-91c9-4c75-9cb0-6c852791b2eb",
"eventType": "AwsApiCall",
"recipientAccountId": "111122223333"
}
```

Cuotas de AWS Application Discovery Service

La consola de cuotas de servicio proporciona información sobre las cuotas de AWS Application Discovery Service. Puede utilizar la consola de Service Quotas para consultar las cuotas de servicio predeterminadas o para [aumento de la cuota de solicitud](#) para cuotas ajustables.

En la actualidad, la única cuota que se puede aumentar es servidores importados por cuenta.

Application Discovery Service incluye las siguientes cuotas predeterminadas:

- 1 000 solicitudes por cuenta.

Si alcanza esta cuota y desea importar nuevas aplicaciones, puede eliminar las existentes con el `DeleteApplications` Acción de la API. Para obtener más información, consulte [DeleteApplications](#) en la Application Discovery Service Referencia de la API.

- El tamaño máximo de un archivo de importación es de 10 MB
- 25.000 registros de servidor importados por cuenta.
- 25.000 eliminaciones de registros de importación por día.
- 10.000 servidores importados por cuenta (puede solicitar aumentar esta cuota).
- 1 000 agentes activos, que recopilan y envían datos a Application Discovery Service.
- 10 000 agentes inactivos, que responden, pero que no recopilan datos.
- 400 servidores por aplicación.
- 30 etiquetas por servidor.

Solución de problemas AWS Application Discovery Service

En esta sección, encontrará información sobre cómo solucionar los problemas comunes con AWS Application Discovery Service.

Temas

- [Detenga la recopilación de datos mediante la exploración de datos](#)
- [Elimine los datos recopilados mediante la exploración de datos](#)
- [Solucione problemas comunes relacionados con la exploración de datos en Amazon Athena](#)
- [Solución de problemas de registros de importación fallidos](#)

Detenga la recopilación de datos mediante la exploración de datos

Para detener la exploración de datos, puede apagar el conmutador de la consola de Migration Hub, en la pestaña Discover > Data Collectors > Agents, o invocar el `StopContinuousExport` API. La recopilación de datos puede tardar hasta 30 minutos en detenerse y, durante esta etapa, el interruptor de la consola y la `DescribeContinuousExport` API invocación mostrarán el estado de la exploración de datos como «Parada en curso».

Note

Si tras actualizar la página de la consola, el conmutador no se apaga y aparece un mensaje de error o `DescribeContinuousExport` API devuelve el estado «`Stop_Failed`», puedes volver a intentarlo apagando el conmutador o llamando al `StopContinuousExport` API. Si la «exploración de datos» sigue mostrando un error y no se detiene correctamente, ponte en contacto con el servicio de asistencia. AWS

Si lo prefiere, puede detener manualmente la recopilación de datos tal y como se describe en los pasos que se indican a continuación.

Opción 1: Detener la recopilación de datos del agente

Si ya ha realizado el descubrimiento con ADS agentes y ya no desea recopilar datos adicionales en el repositorio de la ADS base de datos:

1. En la consola de Migration Hub, seleccione la pestaña Discover > Data Collectors > Agents.

2. Seleccione todos los agentes en ejecución existentes y elija Stop Data Collection (Detener recopilación de datos).

Esto garantizará que los agentes no recopilen datos nuevos ni en el repositorio de ADS datos ni en el depósito de S3. Los datos existentes siguen estando accesibles.

Opción 2: Eliminar Amazon Kinesis Data Streams de exploración de datos

Si desea seguir recopilando datos por parte de los agentes en el repositorio de ADS datos, pero no quiere recopilarlos en su bucket de Amazon S3 mediante la exploración de datos, puede eliminar manualmente las transmisiones de Amazon Data Firehose creadas por la exploración de datos:

1. Inicie sesión en Amazon Kinesis desde la AWS consola y elija Data Firehose en el panel de navegación.
2. Elimine las siguientes transmisiones creadas por la función de exploración de datos:
 - `aws-application-discovery-service-id_mapping_agent`
 - `aws-application-discovery-service-inbound_connection_agent`
 - `aws-application-discovery-service-network_interface_agent`
 - `aws-application-discovery-service-os_info_agent`
 - `aws-application-discovery-service-outbound_connection_agent`
 - `aws-application-discovery-service-processes_agent`
 - `aws-application-discovery-service-sys_performance_agent`

Elimine los datos recopilados mediante la exploración de datos

Para eliminar los datos recopilados mediante la exploración de datos

1. Elimine los datos del agente de detección almacenados en Amazon S3.

Los datos recopilados por AWS Application Discovery Service (ADS) se almacenan en un bucket de S3 denominado `aws-application-discovery-service-uniqueid`.

Note

Si se elimina el bucket de Amazon S3 o cualquiera de sus objetos mientras la exploración de datos en Amazon Athena está habilitada, se produce un error. Sigue

enviando nuevos datos del agente de detección a S3. Los datos borrados tampoco estarán accesibles en Athena.

2. Eliminar AWS Glue Data Catalog.

Cuando se activa la exploración de datos en Amazon Athena, se crea un bucket de Amazon S3 en su cuenta para almacenar los datos recopilados por los ADS agentes a intervalos de tiempo regulares. Además, también crea una que le AWS Glue Data Catalog permite consultar los datos almacenados en un bucket de Amazon S3 desde Amazon Athena. Al desactivar la exploración de datos en Amazon Athena, no se almacenan nuevos datos en el bucket de Amazon S3, pero los datos recopilados anteriormente se conservan. Si ya no necesita estos datos y quiere devolver su cuenta al estado anterior a la activación de la exploración de datos en Amazon Athena.

- a. Visite Amazon S3 desde la AWS consola y elimine manualmente el bucket con el nombre "aws-application-discover-discovery-service-uniqueid»
- b. Puede eliminar manualmente el catálogo de datos de AWS Glue Data Catalog de exploración de datos eliminando la application-discovery-service-databasebase de datos y todas estas tablas:
 - os_info_agent
 - network_interface_agent
 - sys_performance_agent
 - processes_agent
 - inbound_connection_agent
 - outbound_connection_agent
 - id_mapping_agent

Eliminar sus datos de AWS Application Discovery Service

Para eliminar todos sus datos de Application Discovery Service, póngase en contacto con [AWS Support](#) y solicite la eliminación total de los datos.

Solucione problemas comunes relacionados con la exploración de datos en Amazon Athena

En esta sección, encontrará información sobre cómo solucionar problemas comunes relacionados con la exploración de datos en Amazon Athena.

Temas

- [La exploración de datos en Amazon Athena no se puede iniciar porque no se pueden crear las funciones vinculadas al servicio ni AWS los recursos necesarios](#)
- [Los datos del nuevo agente no aparecen en Amazon Athena](#)
- [No tiene permisos suficientes para acceder a Amazon S3, Amazon Data Firehose o AWS Glue](#)

La exploración de datos en Amazon Athena no se puede iniciar porque no se pueden crear las funciones vinculadas al servicio ni AWS los recursos necesarios

Al activar la exploración de datos en Amazon Athena, se crea en su cuenta el rol vinculado al servicio `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport`, que le permite crear los AWS recursos necesarios para que los datos recopilados por el agente estén accesibles en Amazon Athena, incluidos un bucket de Amazon S3, Amazon Kinesis Streams y AWS Glue Data Catalog. Si su cuenta no tiene los permisos adecuados para la exploración de datos en Amazon Athena a fin de crear este rol, no se podrá inicializar. Consulte [AWS políticas gestionadas para AWS Application Discovery Service](#).

Los datos del nuevo agente no aparecen en Amazon Athena

Si los datos nuevos no llegan a Athena, han pasado más de 30 minutos desde que se inició un agente y el estado de exploración de datos es Activo, compruebe las soluciones que se indican a continuación:

- AWS Agentes de descubrimiento

Asegúrese de que el estado de Collection (Recopilación) del agente está marcado como Started (Iniciado) y de que el estado de Health (Estado) está marcado como Running (En ejecución).

- Función de Kinesis

Asegúrese de que tiene la función `AWSApplicationDiscoveryServiceFirehose` en su cuenta.

- Estado de la Firehose

Asegúrese de que los siguientes flujos de entrega de Firehose funcionen correctamente:

- `aws-application-discovery-service/os_info_agent`
- `aws-application-discovery-service-network_interface_agent`
- `aws-application-discovery-service-sys_performance_agent`
- `aws-application-discovery-service-processes_agent`
- `aws-application-discovery-service-inbound_connection_agent`
- `aws-application-discovery-service-outbound_connection_agent`
- `aws-application-discovery-service-id_mapping_agent`

- AWS Glue Data Catalog

Asegúrese de que la `application-discovery-service-database` base de datos esté activa. AWS Glue Asegúrese de que las siguientes tablas existen en AWS Glue:

- `os_info_agent`
- `network_interface_agent`
- `sys_performance_agent`
- `processes_agent`
- `inbound_connection_agent`
- `outbound_connection_agent`
- `id_mapping_agent`

- Bucket de Amazon S3

Asegúrese de tener un bucket de Amazon S3 nombrado `aws-application-discovery-service-uniqueid` en su cuenta. Si los objetos del cubo se han movido o eliminado, no se mostrarán correctamente en Athena.

Asegúrese de que sus servidores se están ejecutando para que los agentes pueden recopilar y enviar datos a AWS Application Discovery Service.

No tiene permisos suficientes para acceder a Amazon S3, Amazon Data Firehose o AWS Glue

Si está utilizando AWS Organizations Amazon Athena y la inicialización para la exploración de datos en Amazon Athena falla, puede deberse a que no tiene permisos para acceder a Amazon S3, Amazon Data Firehose, Athena o AWS Glue

Necesitará un IAM usuario con permisos de administrador para poder acceder a estos servicios. Un administrador puede utilizar su cuenta para conceder este acceso. Consulte [AWS políticas gestionadas para AWS Application Discovery Service](#).

Para garantizar que la exploración de datos en Amazon Athena funcione correctamente, no modifique ni elimine AWS los recursos creados por la exploración de datos en Amazon Athena, incluidos el bucket de Amazon S3, Amazon Data Firehose Streams y AWS Glue Data Catalog. Si elimina o modifica estos recursos por error, detenga e inicie Data Exploration; los recursos se volverán a crear automáticamente. Si elimina el depósito de Amazon S3 creado mediante la exploración de datos, puede perder los datos recopilados en el depósito.

Solución de problemas de registros de importación fallidos

La importación de Migration Hub le permite importar detalles de su entorno local directamente a Migration Hub sin usar Discovery Connector o Discovery Agent. De este modo, tiene la opción de realizar la evaluación y planificación de la migración directamente desde los datos importados. También puede agrupar los dispositivos como aplicaciones y realizar el seguimiento de su estado de migración.

Al importar datos, es posible que se produzcan errores. Normalmente, estos errores se deben a una de las siguientes razones:

- Se alcanzó una cuota relacionada con la importación: hay una cuota asociada a las tareas de importación. Si realizas una solicitud de tarea de importación que supere las cuotas, la solicitud fallará y devolverá un error. Para obtener más información, consulte [Cuotas de AWS Application Discovery Service](#).

- Se insertó una coma adicional (,) en el archivo de importación, con las comas dentro. CSVlos archivos se utilizan para diferenciar un campo del siguiente. No se admite que aparezca una coma en un campo, ya que siempre dividirá un campo. Esto puede provocar una cascada de errores de formato. Asegúrese de que las comas solo se utilicen entre campos y no se usen de otro modo en los archivos de importación.
- Un campo tiene un valor fuera del rango admitido: algunos campos, por ejemplo, CPU.NumberOfCores deben tener un rango de valores que admitan. Si tiene más o menos de este intervalo admitido, no se importará el registro.

Si se produce algún error en la solicitud de importación, puede resolverlo descargando los registros fallidos para la tarea de importación, resolver los errores del CSV archivo de entradas fallidas y volver a realizar la importación.

Console

Para descargar el archivo de registros con error

1. Inicie sesión en y abra la consola de Migration Hub en <https://console.aws.amazon.com/migrationhub>. AWS Management Console
2. En el panel de navegador izquierdo, en Discover (Detectar), elija Tools (Herramientas).
3. En Discovery Tools (Herramientas de detección), elija view imports (ver importaciones).
4. En el panel Imports (Importaciones), elija el botón de opción asociado a una solicitud de importación que tenga varios Failed records (Registros con error).
5. Elija Download failed records (Descargar registros con error) encima de la tabla del panel. Se abrirá el cuadro de diálogo de descarga del navegador para descargar el archivo.

AWS CLI

Para descargar el archivo de registros con error

1. Abra una ventana de terminal y escriba el siguiente comando, donde *ImportName* is the name of the import task with the failed entries that you want to correct.:

```
aws discovery describe-import-tasks - -name ImportName
```

2. De la salida, copie todo el contenido del valor devuelto por `errorsAndFailedEntriesZip`, sin las comillas que lo rodean.
3. Abra un navegador web, pegue el contenido en el cuadro de URL texto y presione `ENTER`. Esto descargará el archivo de registros con error, comprimido en formato `.zip`.

Ahora que ha descargado el archivo de registros con error, puede extraer los dos archivos que contiene y corregir los errores. Tenga en cuenta que si los errores están vinculados a límites basados en el servicio, tendrá que solicitar un aumento de límite o eliminar suficientes recursos asociados para que la cuenta esté por debajo del límite. El archivo tiene los dos archivos siguientes:

- `errors-file.csv`: este archivo es su registro de errores y rastrea la línea, el nombre de la columna y un mensaje de error descriptivo de cada registro fallido de cada entrada fallida. `ExternalId`
- `failed-entries-file.csv`: este archivo contiene solo las entradas fallidas del archivo de importación original.

Para corregir los `non-limit-based` errores encontrados, use `errors-file.csv` para corregir los problemas del `failed-entries-file.csv` archivo y, a continuación, importa ese archivo. Para obtener instrucciones sobre la importación de archivos, consulte [Importación de datos](#).

Historial de documento de AWS Application Discovery Service

Última actualización de la documentación de la Guía del usuario: 16 de mayo de 2023

En la siguiente tabla, se describen cambios importantes realizados en la Guía del usuario de Appation Appation Para obtener notificaciones sobre las actualizaciones de la documentación, puede suscribirse a la fuente RSS.

Cambio	Descripción	Fecha
Presentamos la base de datos Agentless Collector y el módulo de recopilación de datos de análisis	El módulo de recopilación de datos de bases de datos y análisis es el nuevo módulo de Application Discovery Service Agentless Collector (Agentless Collector). Puede utilizar este módulo de recopilación de datos para conectarse a su entorno y recopilar metadatos y métricas de rendimiento de sus servidores de análisis y bases de datos locales. Para obtener más información, consulte el módulo de recopilación de datos de bases de datos y análisis .	16 de mayo de 2023
Presentamos Application Discovery Service Agentless Collector	Application Discovery Service Agentless Collector (Agentless Collector) es la nueva aplicación AWS Application Discovery Service local que recopila información mediante métodos sin agentes sobre su entorno local para ayudarlo a	16 de agosto de 2022

planificar de manera eficaz su migración al. Nube de AWS
Para obtener más información, consulte [Agentation](#)

[Actualización de IAM](#)

La `discovery:GetNetworkConnectionGraph` acción AWS Identity and Access Management (IAM) ya está disponible para conceder acceso al diagrama de red de la AWS Migration Hub consola al crear una política basada en identidades. Para obtener más información, consulte [Concesión de permisos para usar el diagrama de red.](#)

24 de mayo de 2022

[Presentamos la región de origen](#)

La región de origen de Migration Hub proporciona un repositorio único de información de descubrimiento y planificación de la migración para toda su cartera, y una vista única de las migraciones a varias AWS regiones.

20 de noviembre de 2019

[Presentamos la función de importación de Migration Hub](#)

La importación de Migration Hub le permite importar información sobre sus servidores y aplicaciones locales a Migration Hub, incluidas las especificaciones del servidor y los datos de uso. También puede utilizar estos datos para realizar un seguimiento del estado de las migraciones de aplicaciones. Para obtener más información, [Migration Hub](#)

18 de enero de 2019

En la siguiente tabla se describen las versiones de documentación de la guía del usuario de Application Discovery Service anteriores al 18 de enero de 2019:

Cambio	Descripción	Fecha
Nueva característica	Se actualizaron los documentos para permitir la exploración de datos en Amazon Athena y se agregó un capítulo de solución de problemas.	09 de agosto de 2018
Revisión importante	Se ha reescrito la información de uso y salida; se ha reestructurado todo el documento.	25 de mayo de 2018
Discovery Agent 2.0	Se publicó una nueva versión de Application Discovery Agent mejorada.	19 de octubre de 2017
Consola	Se añadió la AWS Management Console.	19 de diciembre de 2016

Cambio	Descripción	Fecha
Detección sin agente	Esta versión describe cómo instalar y configurar la detección sin agente.	28 de julio de 2016
Se incluyeron nuevos datos sobre la resolución de problemas con Microsoft Windows Server y los comandos	Esta actualización añade información detallada acerca de Microsoft Windows Server. También documenta las soluciones a algunos problemas con los comandos.	20 de mayo de 2016
Publicación inicial	Esta es la primera versión de la Application Discovery Service	12 de mayo de 2016

Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el [Glosario de AWS](#) en la Referencia de Glosario de AWS.

Apéndice

Esta sección contiene información complementaria sobre AWS Application Discovery Service

Temas

- [Apéndice: Transición de Discovery Connector a Agentless Collector](#)
- [Apéndice: Conector AWS de detección sin agente](#)

Apéndice: Transición de Discovery Connector a Agentless Collector

En esta sección se describe cómo realizar la transición de AWS Agentless Discovery Connector (Discovery Connector) a Application Discovery Service Agentless Collector (Agentless Collector).

Recomendamos que los clientes que utilizan Discovery Connector actualmente hagan la transición al nuevo recopilador sin agente.

Para obtener información sobre cómo empezar a utilizar Agentless Collector, consulte [Primeros pasos con Agentless Collector](#)

Una vez implementado el recopilador sin agente, puede eliminar la máquina virtual Discovery Connector. Todos los datos recopilados anteriormente seguirán estando disponibles en AWS Migration Hub (Migration Hub).

Apéndice: Conector AWS de detección sin agente

Important

Recomendamos que los clientes que utilizan Discovery Connector actualmente hagan la transición al nuevo recopilador sin agente. Para obtener más información, consulte [Apéndice: Transición de Discovery Connector a Agentless Collector](#).

Temas

- [Datos recopilados por el Discovery Connector](#)
- [Recopilación de datos del conector Discovery](#)
- [Solución de problemas del Discovery Connector](#)

Datos recopilados por el Discovery Connector

El Discovery Connector recopila información sobre los hosts y máquinas virtuales de VMware vCenter Server. Sin embargo, solo puede registrar estos datos si se instalan las herramientas de VMware vCenter Server. Para asegurarse de que la AWS cuenta que está utilizando tiene los permisos necesarios para esta tarea, consulte [AWS políticas gestionadas para AWS Application Discovery Service](#)

A continuación, encontrará un inventario de la información recopilada por el Discovery Connector.

Leyenda de la tabla sobre los datos recopilados por Discovery Connector:

- Los datos recopilados se especifican en kilobytes (KB) a menos que se indique otra cosa.
- Los datos equivalentes de la consola de Migration Hub se muestran en megabytes (MB).
- Los campos de datos marcados con un asterisco (*) solo están disponibles en los archivos.csv que se generan a partir de la función de exportación de la API del conector.
- El período de sondeo se indica en intervalos de 60 minutos aproximadamente.
- Los campos de datos con un doble asterisco (**) devuelven actualmente un valor nulo.

Campo de datos	Descripción
applicationConfigurationId*	ID de la aplicación de migración en la que se agrupa la máquina virtual
avgCpuUsagePacto	Porcentaje medio de utilización de la CPU durante el periodo de sondeo
avgDiskBytesReadPerSecond	Número medio de bytes leídos del disco durante el periodo de sondeo
avgDiskBytesWrittenPerSecond	Número medio de bytes escritos en el disco durante el periodo de sondeo
avgDiskReadOpsPerSecond**	Número medio de operaciones de E/S de lectura por segundo (nulo)
avgDiskWriteOpsPerSecond**	Número medio de operaciones de E/S de escritura en disco por segundo

Campo de datos	Descripción
avgFreeRAM	Cantidad media de RAM disponible expresada en MB
avgNetworkBytesReadPerSecond	Cantidad media de bytes leídos por segundo
avgNetworkBytesWrittenPerSecond	Cantidad media de bytes escritos por segundo
configId	Application Discovery Service asignó un ID a la máquina virtual descubierta
configType	Tipo de recurso detectado
connectorId	ID del dispositivo virtual de Discovery Connector
cpuType	vCPU para una máquina virtual, modelo real para un host
datacenterId	ID de vCenter
hostId*	ID de host de la máquina virtual
hostName	Nombre de host que ejecuta el software de virtualización
hypervisor	Tipo de hipervisor
id	ID de servidor
lastModifiedTimeSello*	Última fecha y hora de recopilación de datos antes de la exportación de datos
macAddress	Dirección MAC de la máquina virtual
manufacturer	Marca del software de virtualización
maxCpuUsagePacto	Porcentaje máximo de utilización de la CPU durante el periodo de sondeo

Campo de datos	Descripción
maxDiskBytesReadPerSecond	Número máximo de bytes leídos del disco durante el periodo de sondeo
maxDiskBytesWrittenPerSecond	Número máximo de bytes escritos en el disco durante el periodo de sondeo
maxDiskReadOpsPerSecond ^{**}	Número máximo de operaciones de E/S de lectura por segundo
maxDiskWriteOpsPerSecond ^{**}	Número máximo de operaciones de E/S escritura por segundo
maxNetworkBytesReadPerSecond	Cantidad máxima de bytes leídos por segundo
maxNetworkBytesWrittenPerSecond	Cantidad máxima de bytes escritos por segundo
memoryReservation [*]	Límite para evitar la sobrecarga de memoria en la máquina virtual
moRefId	ID único de referencia de objeto administrado por vCenter
name [*]	Nombre de la máquina virtual o red (especificado por el usuario)
numCores	Número de unidades de procesamiento independientes en la CPU
numCpus	Número de unidades de procesamiento centrales en la máquina virtual
numDisks ^{**}	Número de discos en la máquina virtual
numNetworkCards ^{**}	Número de tarjetas de red en la máquina virtual
osName	Nombre del sistema operativo en la máquina virtual

Campo de datos	Descripción
osVersion	Versión del sistema operativo en la máquina virtual
portGroupld*	ID de grupo de puertos miembro de VLAN
portGroupName*	Nombre del grupo de puertos miembro de VLAN
powerState*	Estado de alimentación
serverId	Application Discovery Service asignó un ID a la máquina virtual descubierta
smBiosId*	ID/versión del BIOS de administración del sistema
state*	Estado del dispositivo virtual de Discovery Connector
toolsStatus	Estado operativo de las herramientas de VMware (consulte Visualización y clasificación de recopiladores de datos para ver una lista completa).
totalDiskSize	Capacidad total del disco expresada en MB
totalRAM	Cantidad total de RAM disponible en la máquina virtual en MB
type	Tipo de host
vCenterId	Número de identificación único de una máquina virtual
vCenterName*	Nombre del host de vCenter
virtualSwitchName*	Nombre del conmutador virtual

Campo de datos	Descripción
vmFolderPath	Ruta de directorio de los archivos de la máquina virtual
vmName	Nombre de la máquina virtual

Recopilación de datos del conector Discovery

Una vez implementado y configurado el Discovery Connector en su entorno VMware, si la recopilación de datos se detiene, puede reiniciarlo. Puede iniciar o detener la recopilación de datos a través de la consola o realizando llamadas a la API a través de AWS CLI. Ambos métodos se describen en los siguientes procedimientos.

Using the Migration Hub Console

El siguiente procedimiento muestra cómo iniciar o detener el proceso de recopilación de datos de Discovery Connector, en la página Recopiladores de datos de la consola de Migration Hub.

Para iniciar o detener la recopilación de datos

1. En el panel de navegación, elija Data Collectors (Recopiladores de datos).
2. Elija la pestaña Connectors (Conectores).
3. Seleccione la casilla del conector que desee iniciar o detener.
4. Elija Start data collection (Iniciar recopilación de datos) o Stop data collection (Detener recopilación de datos).

Note

Si no ve la información de inventario después de iniciar la recopilación de datos con el conector, confirme que ha registrado el conector con su instancia de vCenter Server.

Using the AWS CLI

Para iniciar el proceso de recopilación de datos de Discovery Connector desde AWS CLI, primero AWS CLI debe estar instalado en su entorno y, a continuación, debe configurar la CLI para que utilice la [región de origen de Migration Hub](#) seleccionada.

Para instalar AWS CLI e iniciar la recopilación de datos

1. Instálelo AWS CLI para su sistema operativo (Linux, macOS o Windows). Consulte las [AWS Command Line Interface instrucciones en la Guía](#) del usuario.
2. Abra el símbolo del sistema (Windows) o Terminal (Linux o macOS).
 - a. Escriba `aws configure` y pulse Intro.
 - b. Introduzca su ID de clave de AWS acceso y su clave de acceso AWS secreta.
 - c. Introduzca su región de origen como nombre de región predeterminado. Por ejemplo, `us-west-2`.
 - d. Especifique `text` para el formato de salida predeterminado.
3. Para encontrar el ID del conector para el que desea iniciar o detener la recopilación de datos, escriba el siguiente comando para ver el ID del conector:

```
aws discovery describe-agents --filters  
condition=EQUALS,name=hostName,values=connector
```

4. Para iniciar la recopilación de datos mediante el conector, escriba el siguiente comando:

```
aws discovery start-data-collection-by-agent-ids --agent-ids <connector ID>
```

Note

Si no ve la información de inventario después de iniciar la recopilación de datos con el conector, confirme que ha registrado el conector con su instancia de vCenter Server.

Para detener la recopilación de datos por parte del conector, escriba el siguiente comando:

```
aws discovery stop-data-collection-by-agent-ids --agent-ids <connector ID>
```

Solución de problemas del Discovery Connector

Esta sección contiene temas que pueden ayudarle a solucionar problemas conocidos con Application Discovery Service Discovery Connector.

Reparación: Discovery Connector no se puede alcanzar AWS durante la configuración

Al configurar el AWS Agentless Discovery Connector en la consola, puede aparecer el siguiente mensaje de error:

No se pudo contactar AWS

AWS no se puede contactar (se ha restablecido la conexión). Compruebe la configuración de red y proxy.

Este error se produce debido a un intento fallido del Discovery Connector de establecer una conexión HTTPS con un AWS dominio con el que el conector necesita comunicarse durante el proceso de configuración. La configuración del Discovery Connector falla si no se puede establecer una conexión.

Para corregir la conexión a AWS

1. Consulta con tu administrador de TI si el firewall de tu empresa bloquea el tráfico de salida en el puerto 443 hacia alguno de los AWS dominios a los que se necesita acceso saliente.

Los siguientes AWS dominios necesitan acceso saliente:

- `awsconnector.Migration Hub home Region.amazonaws.com`
- `sns.Migration Hub home Region.amazonaws.com`
- `arsenal-discovery.Migration Hub home Region.amazonaws.com`
- `iam.amazonaws.com`
- `aws.amazon.com`
- `ec2.amazonaws.com`

Si su firewall bloquea el tráfico de salida, desbloquéelo. Tras actualizar el firewall, vuelva a configurar el conector.

2. Si la actualización del firewall no resuelve el problema de conexión, asegúrese de que la máquina virtual del conector tenga conectividad de red saliente con los dominios de la lista. Si la máquina virtual tiene conectividad saliente, pruebe la conexión a los dominios de la lista ejecutando telnet en los puertos 443, como se muestra en el siguiente ejemplo.

```
telnet ec2.amazonaws.com 443
```

3. Si la conectividad saliente de la máquina virtual está habilitada, debe ponerse en contacto con [AWS Support](#) para obtener más información sobre la solución de problemas.

Reparación de conectores defectuosos

La información sobre el estado de cada Discovery Connector se encuentra en la página de [recopiladores de datos](#) de la consola de Migration Hub. Puede identificar los conectores con problemas buscando aquellos conectores cuyo Health (Estado) sea Unhealthy (Incorrecto). En el siguiente procedimiento se describe cómo obtener acceso a la consola del conector para identificar problemas de estado.

Acceso a la consola de un conector

1. Abra la consola de Migration Hub en un navegador web y selecciona Data Collectors en la barra de navegación de la izquierda.
2. En la pestaña Connectors (Conectores), anote el valor del campo IP address (Dirección IP) de cada conector que tenga un estado Unhealthy (Incorrecto).
3. Abra un navegador en cualquier ordenador que pueda conectarse a la máquina virtual del conector e introduzca la URL de la consola del conector `https://ip_address_of_connector`, donde `ip_address_of_connector` está la dirección IP de un conector en mal estado.
4. Escriba la contraseña de la consola de administración de conectores que especificó cuando configuró el conector.

Una vez que esté en la consola del conector, puede realizar acciones para resolver un estado incorrecto. Aquí puede elegir View Info (Ver información) en vCenter connectivity (Conectividad de vCenter); aparecerá un cuadro de diálogo con un mensaje de diagnóstico. El enlace View Info (Ver información) solo está disponible en conectores de la versión 1.0.3.12 o posterior.

Después de corregir los problemas de estado, el conector restablecerá la conectividad con el servidor de vCenter y el estado del conector cambiará a HEALTH (Correcto). Si los problemas persisten, ponte en contacto con [AWS Support](#).

Las causas más comunes de los conectores que no están en buen estado son problemas de direcciones IP y problemas de credenciales. Las siguientes secciones pueden ayudarle a resolver estos problemas y a devolver un conector a un estado correcto.

Temas

- [Problemas con la dirección IP](#)
- [Problemas con las credenciales](#)

Problemas con la dirección IP

Un conector puede tener un estado incorrecto si el punto de enlace de vCenter proporcionado durante la configuración del conector tiene un formato incorrecto, no es válido o si el servidor de vCenter está actualmente inactivo y no es accesible. En este caso, al elegir View Info (Ver información) en vCenter connectivity (Conectividad de vCenter) aparecerá un cuadro de diálogo con el mensaje "Confirm the operational status of your vCenter server, or choose Edit Settings to update the vCenter endpoint" (Confirme el estado operativo de su servidor de vCenter o elija Edit Settings para actualizar el punto de enlace de vCenter).

El siguiente procedimiento puede ayudarle a resolver problemas de direcciones IP.

1. En la consola del conector (https://ip_address_of_connector), elija Edit Settings (Editar configuración).
2. En el panel de navegación de la izquierda, seleccione Step 5: Discovery Connector Set Up (Paso 5: Configuración del conector de detección).
3. En Configure vCenter credentials (Configurar credenciales de vCenter), anote la dirección IP que figura en vCenter Host (Host de vCenter).
4. Con una herramienta de línea de comandos independiente, como ping o traceroute, valide que el servidor vCenter asociado esté activo y que se pueda acceder a la IP desde la máquina virtual del conector.
 - Si la dirección IP es incorrecta y el servicio vCenter está activo, actualice la dirección IP en la consola del conector y elija Next (Siguiente).
 - Si la dirección IP es correcta pero el servidor de vCenter está inactivo, actívelo.

- Si la dirección IP es correcta y el servidor de vCenter está activo, compruebe si está bloqueando las conexiones de red de entrada debido a problemas del firewall. Si es así, actualice la configuración del firewall para permitir conexiones entrantes desde la máquina virtual del conector.

Problemas con las credenciales

Los conectores pueden tener un estado incorrecto si las credenciales de usuario de vCenter proporcionadas durante la configuración del conector no son válidas o no tienen privilegios de cuenta de lectura y visualización de vCenter. En este caso, cuando elija View Info (Ver información) en vCenter connectivity (Conectividad de vCenter) aparecerá un cuadro de diálogo con el mensaje "Choose Edit Settings to update your vCenter username and password for your account with read and view privileges" (Elija Edit Settings para actualizar el nombre de usuario y la contraseña de vCenter de su cuenta con privilegios de lectura y visualización).

El procedimiento siguiente puede ayudarle a resolver problemas de credenciales. Como requisito previo, asegúrese de haber creado un usuario de vCenter que tenga permisos de cuenta de lectura y visualización en el servidor de vCenter.

1. En la consola del conector (https://ip_address_of_connector), elija Edit Settings (Editar configuración).
2. En el panel de navegación de la izquierda, seleccione Step 5: Discovery Connector Set Up (Paso 5: Configuración del conector de detección).
3. En Configure vCenter credentials (Configurar credenciales de vCenter), actualice los campos vCenter Username (Nombre de usuario de vCenter) y vCenter Password (Contraseña de vCenter) proporcionando las credenciales de un usuario de vCenter con permisos de lectura y visualización.
4. Seleccione Next (Siguiente) para completar la configuración.

Soporte para hosts ESX independientes

El Discovery Connector no admite un host ESX independiente. El host de ESX debe formar parte de la instancia de vCenter Server.

Obtener soporte adicional para problemas con los conectores

Si tiene problemas y necesita ayuda, póngase en contacto con [AWS Support](#). Nos pondremos en contacto con usted y le pediremos que nos envíe los logs del conector. Para obtener los logs, haga lo siguiente:

- Vuelva a iniciar sesión en la consola AWS Agentless Discovery Connector y seleccione Descargar paquete de registro.
- Una vez que el paquete de logs termine de descargarse, envíelo siguiendo las instrucciones de AWS Support.

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