Guía del usuario

AWS Application Discovery Service

AWS Application Discovery Service: Guía del usuario

Table of Contents

¿Qué es AWS Application Discovery Service?

AWS Application Discovery Service le ayuda a planificar la migración a la AWS nube 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 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 AWS Migration Hub región de origen. Por lo tanto, debe configurar su región de origen en la consola de Migration Hub o mediante comandos CLI antes de realizar cualquier actividad de detección y migración. Los datos se pueden exportar para analizarlos en Microsoft Excel o en herramientas de AWS análisis como Amazon Athena y Amazon. QuickSight

Con Application Discovery Service APIs, puede exportar los datos de rendimiento y utilización del sistema para los servidores descubiertos. Introduzca estos datos en su modelo de costes para calcular el coste 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**
>
> Su región de origen debe estar configurada AWS Migration Hub antes de iniciar el proceso de descubrimiento, ya que sus datos se almacenarán en su región de origen. Para obtener más información sobre cómo trabajar con una región local, consulte Región local.

Application Discovery Service ofrece tres formas de realizar el descubrimiento y la recopilación de datos sobre los servidores locales:

- La detección sin agente se puede realizar mediante la implementación del Application Discovery Service Agentless Collector (archivo OVA) (archivo OVA) a través de su vCenter. VMware Una vez configurado Agentless Collector, identifica las máquinas virtuales (VMs) y los hosts asociados a vCenter. Agentless Collector recopila los siguientes datos de configuración estática: nombres de host de los servidores, direcciones IP, direcciones MAC, asignaciones de recursos de disco,

versiones del motor de base 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 (Discovery Agent) en cada uno de sus servidores VMs y en los 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.
- La importación basada en archivos le permite importar detalles de su entorno local directamente a Migration Hub sin usar Agentless Collector o Discovery Agent, de modo que puede realizar la evaluación y la planificación de la migración directamente a partir de los datos importados. Los datos ingeridos dependen de los datos proporcionados.

Application Discovery Service se integra con las soluciones de descubrimiento de aplicaciones de los AWS socios de Partner Network (APN). Estas soluciones de terceros pueden ayudarlo a importar detalles sobre su entorno local directamente a Migration Hub, sin usar ningún recopilador o agente de descubrimiento sin agente. Las herramientas de descubrimiento de aplicaciones de terceros pueden consultar 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.

VMware Descubrimiento

Si tiene máquinas virtuales (VMs) que se ejecutan en el entorno VMware vCenter, puede usar el recopilador sin agente para recopilar información del sistema sin tener que instalar un agente en cada máquina virtual. En su lugar, carga este dispositivo local en vCenter y permite que descubra todos sus hosts y. VMs

Agentless Collector captura la información sobre el rendimiento del sistema y la utilización de los recursos de cada máquina virtual que se ejecute en vCenter, independientemente del sistema operativo que se utilice. Sin embargo, no puede «analizar» cada uno de ellos y VMs, por lo tanto, no puede determinar 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 detenidamente algunos de los VMs que ya tiene para planificar la migración, puede instalar el Discovery Agent según sea necesario.

Además, si VMs está alojado en VMware, puede utilizar tanto el recopilador sin agente como el Discovery Agent para realizar la detección de forma simultánea. Para obtener más información sobre los tipos exactos de datos que recopilará cada herramienta de descubrimiento, consulte. Uso del módulo de VMware recopilación de datos vCenter Agentless Collector

Detección de base de datos

Si tiene servidores de bases de datos y análisis en su entorno local, puede usar el recopilador sin agente para detectar 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 ordenador de su entorno.

El módulo de recopilación de datos analíticos y de bases de datos 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, la base de datos y los servidores de análisis de la red. A continuación, el módulo de recopilación de datos ejecuta consultas periódicamente para recopilar las métricas de uso reales de la CPU, la memoria y la capacidad del disco para las bases de datos y los servidores de análisis. Para obtener más información sobre las métricas recopiladas, consulteDatos recopilados por la base de datos y el módulo de análisis.

Una vez que Agentless Collector complete la recopilación de datos de su entorno, podrá utilizar la AWS DMS consola para realizar análisis adicionales y planificar la migración. Por ejemplo, para elegir un objetivo de migración óptimo en el Nube de AWS, puede generar recomendaciones de objetivos para sus bases de datos de origen. Para obtener más información, consulte Uso del 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 los métodos de recopilación de datos que admite Application Discovery Service.

	Recopilador sin agente	Agente de descubrimiento	Plantilla Migration Hub	RVTools exportar
Supported server types				

	Recopilador sin agente	Agente de descubrimiento	Plantilla Migration Hub	RVTools exportar
VMware máquina virtual	Sí	Sí	Sí	Sí
Servidor físico	No	Sí	Sí	Sí
Deployment				
Por servidor	No	Sí	N/A	No
Por vCenter	Sí	No	N/A	Sí
Por centro de datos en la misma red	No	No	N/A	No
Collected data				
Datos del perfil del servidor (configuración estática)	Sí	Sí	Sí	Sí
Métricas de uso del servidor del hipervisor (CPU, RAM, etc.)	Sí	Sí	Sí	No
Métricas de utilización del servidor (CPU, RAM, etc.)	Sí	Sí	Sí	No
Conexiones de red del servidor (solo TCP)	Sí	Sí	No	No

	Recopilador sin agente	Agente de descubrimiento	Plantilla Migration Hub	RVTools exportar
Procesos en ejecución	No	Sí	No	No
Intervalo de recopilación	-60 minutos	-15 segundos	Instantánea única	Instantánea única
Server data use cases				
Ver los datos del servidor en Migration Hub	Sí	Sí	Solo perfil	No
Genera una EC2 recomendación de Amazon basada en el perfil del servidor	Sí	Sí	Sí	Sí
Genera EC2 recomendaciones de Amazon en función de los datos de uso	Sí	Sí	Sí	No
Exportación de los datos instantáneos de uso más recientes	Sí	Sí	Sí	No
Exportación de datos de utilización de series temporales	No	Sí	No	No

	Recopilador sin agente	Agente de descubrimiento	Plantilla Migration Hub	RVTools exportar
Network data use cases				
Visualización en Migration Hub	Sí	Sí	No	No
Exporte a Amazon Athena para una mayor exploración	No	Sí	No	No
Exportar a un archivo CSV	No	Sí	No	No
Database use cases				
Datos del perfil del servidor de base de datos (configuración estática)	Sí	No	No	No
Motores de bases de datos compatibles	Oracle, SQL Server, MySQL, PostgreSQL	Ninguno	Ninguna	Ninguno
Complejidad y duplicados del esquema de la base de datos	Sí	No	No	No
Objetos del esquema de la base	Sí	No	No	No
Platform support				

	Recopilador sin agente	Agente de descubrimiento	Plantilla Migration Hub	RVTools exportar
Sistemas operativos compatibles	Cualquier sistema operativo que se ejecute en VMware Center v5.5 o versiones más recientes	Cualquier servidor Linux o Windows	Cualquier servidor Linux o Windows	Cualquier servidor Linux, servidor Windows o VMware versión 5.5 o posterior

Supuestos

Para utilizar Application Discovery Service, se supone 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 relativa a 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 detección, 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:

Inscribirse en Amazon Web Services

Crear usuarios de IAM

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

Inscribirse en Amazon Web Services

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

Para suscribirse a una Cuenta de AWS

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

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

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

Crear usuarios de IAM

Cuando creas una AWS cuenta, obtienes 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 fehacientemente 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

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 las 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, consulteAWS 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, consulteAWS políticas gestionadas para AWS Application Discovery Service.
- Cuando desee ver las claves de acceso del usuario (clave de acceso IDs 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 una 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 locales y que está VMs 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, EC2 instancias de Amazon 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 bien, sustituye tu región de origen por todas las demás regiones, excepto us-west-2, según sea necesario.
- Si `us-west-2` es su región de origen, se registra `arsenal.us-west-2.amazonaws.com` en Application Discovery Service.

Funcionamiento

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

Datos recopilados por Discovery Agent

AWS Application Discovery Agent (Discovery Agent) es un software que se instala en servidores locales y VMs. 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
agentAssignedProcessID: *	ID de los procesos detectados por el agente
agentId	ID único del agente
agentProvidedTimeSello *	Fecha y hora de la observación del agente (mm/dd/yyyy hh:mm:ss am/pm)

Campo de datos	Descripción
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 aplicacio nes, 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
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

Campo de datos	Descripción
osVersion	Versión del sistema operativo en el host
path	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
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

Campo de datos	Descripción
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
totalNumLogicalProcesadores *	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

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, 15 SP5 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`, utilizaría `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.

Instalación de Discovery Agent

En esta página se explica cómo instalar Discovery Agent en Linux y Microsoft Windows.

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 Consideraciones sobre 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-region.amazonaws.com/aws-discovery-agent.region/linux/latest/aws-discovery-agent.tar.gz
   ```

   b. Para realizar la descarga desde la consola de Migration Hub, haga lo siguiente:

      i. Inicie sesión en la consola de Migration Hub AWS Management Console y ábrala en https://console.aws.amazon.com/migrationhub/.

      ii. En la página de navegación de la izquierda, en Discover, selecciona Herramientas.

      iii. En el cuadro AWS Discovery Agent, selecciona Descargar agentes y, a continuación, selecciona Descargar para Linux. La descarga comienza inmediatamente.

3. Verifique la firma criptográfica del paquete de instalación con estos tres comandos:

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

```
curl -o ./discovery.gpg https://s3.region.amazonaws.com/aws-discovery-agent.region/
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	Para instalar el agente, ejecute el comando agent install como se muestra en el siguiente ejemplo. En el ejemplo, *your-home-region* sustitúyalo por el nombre de la región de origen, *aws-access-key-id* por el identificador de la clave de acceso y *aws-secret-access-key* por la clave de acceso secreta. `sudo bash install -r your-home-region -k aws-access-key-id -s aws-secret-access-key` De forma predeterminada, los agentes descargan y aplican automáticamente las actualizaciones a medida que están disponibl es.

Para…	Haga lo siguiente...
	Le recomendamos que utilice esta configuración predeterminada. Sin embargo, si no desea que los agentes descarguen y apliquen las actualizaciones automáticamente, incluya el `-u false` parámetro al ejecutar el comando agent install.
(Opcional) Instale Discovery Agent y configure un proxy no transparente	Para configurar un proxy no transparente, añada los siguientes parámetros al comando agent install: • -e La contraseña del proxy. • -f El número de puerto del proxy. • -g El esquema de proxy. • -i El nombre de usuario del proxy. A continuación, se muestra un ejemplo del comando agent install que utiliza parámetros de proxy no transparentes. `sudo bash install -r your-home-region -k aws-access-key-id -s aws-secret-access-key -d myproxy.mycompany.com -e mypassword -f proxy-port-number -g https -i myusername` Si el proxy no requiere autenticación, omita los `-i` parámetros `-e` y. El comando install de ejemplo usa`https`, si tu proxy usa HTTP, especificar `http` el valor del `-g` parámetro.

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 tu región de origen es`eu-central-1`, usarías `https://arsenal-discovery.`*`eu-central-1`*`.amazonaws.com:443`

Consideraciones sobre 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
```

Instalación de Discovery Agent en Microsoft Windows

Complete el siguiente procedimiento para instalar un agente en Microsoft 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 agent install como se muestra en el siguiente ejemplo. En el ejemplo, *your-home-region* sustitúyalo por el nombre de la región de origen, *aws-access-key-id* por el ID de la clave de acceso y *aws-secret-access-key* por la clave de acceso secreta. Si lo desea, puede establecer la ubicación de instalación del agente especificando la ruta de la carpeta *C:\install-locatio*

Para…	Haga lo siguiente...
	n para el parámetro INSTALLLOCATION. Por ejemplo, `INSTALLLOCATION="` *C:\install-location* `"`. La jerarquía de carpetas resultante será [ruta INSTALLLOCATION]\AWS Discovery. De forma predeterminada, la ubicación de instalación es la `Program Files` carpeta. 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[*LOGANDCONFIGLOCATION path*]`\AWS Discovery` . `.\AWSDiscoveryAgentInstaller.exe REGION="` *your-home-region* `" KEY_ID="`*aws-access-key-id* `" KEY_SECRET="` *aws-secret-access-key* `" /quiet` De forma predeterminada, los agentes descargan y aplican automáticamente las actualizaciones a medida que están disponibles. Le recomendamos que utilice esta configuración predeterminada. Sin embargo, si no desea que los agentes descarguen y apliquen las actualizaciones automáticamente, incluya el siguiente parámetro al ejecutar el comando agent install: `AUTO_UPDATE=false`

Para…	Haga lo siguiente...
	Warning La desactivación de las actualizaciones automáticas impedirá que se instalen los parches de seguridad más recientes.

Para…	Haga lo siguiente...
(Opcional) Instale Discovery Agent y configure un proxy no transparente	Para configurar un proxy no transparente, añada las siguientes propiedades públicas al comando agent install: • PROXY_HOST: el nombre del host del proxy • PROXY_SCHEME: el esquema de proxy • PROXY_PORT: el número de puerto del proxy • PROXY_USER: el nombre de usuario del proxy • PROXY_PASSWORD: la contraseña del usuario proxy A continuación, se muestra un ejemplo del comando de instalación del agente que utiliza las propiedades del proxy no transparentes. `.\AWSDiscoveryAgentInstaller.exe REGION=" your-home-region " KEY_ID="aws-access-key-id " KEY_SECRET=" aws-secret-access-key " PROXY_HOST=" myproxy.mycompany.com " PROXY_SCHEME="https" PROXY_PORT=" proxy-port-number " PROXY_USER=" myusername " PROXY_PASSWORD=" mypassword " /quiet` Si el proxy no requiere autenticación, omita las propiedades `PROXY_USER` y `PROXY_PASSWORD`. El ejemplo del comando install usa `https`. Si el proxy usa HTTP, especifique `http` el `PROXY_SCHEME` valor.

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 SHA256 certificado. En el SHA2 caso de las actualizaciones automáticas firmadas en Windows Server 2008 SP2, asegúrese de que los hosts tengan una revisión instalada para admitir la autenticación con firmas. SHA2 La revisión de soporte más reciente de Microsoft ayuda a respaldar SHA2 la autenticación en Windows Server 2008. SP2

> **Note**
>
> Las revisiones de SHA256 soporte 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
```

Administrar el proceso de Discovery Agent

En esta página se explica cómo administrar Discovery Agent en Linux y Microsoft Windows.

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	`sudo systemctl status aws-discovery-daemon.service`
Iniciar un agente	`sudo systemctl start aws-discovery-daemon.service`
Detener un agente	`sudo systemctl stop aws-discovery-daemon.service`
Reiniciar un agente	`sudo systemctl restart aws-discovery-daemon.service`

Upstart

Comandos de administración del Application Discovery Agent

Tarea	Comando
Verificar que se está ejecutando un agente	`sudo initctl status aws-discovery-daemon`
Iniciar un agente	`sudo initctl start aws-discovery-daemon`
Detener un agente	`sudo initctl stop aws-discovery-daemon`
Reiniciar un agente	`sudo initctl restart aws-discovery-daemon`

System V init

Comandos de administración para el Application Discovery Agent

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

Administre el proceso de Discovery Agent en Microsoft Windows

Puede administrar el comportamiento del Discovery Agent a nivel del sistema a través de 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	Iniciada
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).

Tarea	Nombre del servicio	Estado/acción del servicio
Reiniciar un agente	AWS Agente de descubrimiento AWS Discovery Updater	Elija Restart (Reiniciar).

Desinstalar Discovery Agent

En esta página se explica cómo desinstalar Discovery Agent en Linux y Microsoft Windows.

Desinstalar 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
```

Desinstalar Discovery Agent en Microsoft Windows

En esta sección se describe cómo desinstalar Discovery Agent en Microsoft Windows.

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
```

> **Note**
>
> Si el `.exe` archivo está presente en el servidor, puede desinstalar completamente el agente del servidor mediante el siguiente comando. Si usa este comando para desinstalar, no necesitará usar las `/norestart` opciones `/repair` y cuando vuelva a instalar el agente.
>
> ```
> .\AWSDiscoveryAgentInstaller.exe /quiet /uninstall
> ```

Iniciar y 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 siguiendo los pasos que se Iniciar y detener los recopiladores de datos en la AWS Migration Hub consola indican o realizando llamadas a la API a través de AWS CLI.

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. Introduzca su región de origen como nombre de región predeterminado, por ejemplo*us-west-2*. (Suponemos que `us-west-2` es su región de origen en este ejemplo).
   d. Especifique `text` para el formato de salida predeterminado.
3. Para encontrar el ID del agente para el que desea detener o iniciar la recopilación de datos, 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>
```

Solución de problemas del agente Discovery

Esta página trata sobre la solución de problemas del Discovery Agent en Linux y Microsoft Windows.

Solución de problemas de Discovery Agent en Linux

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

Solución de problemas de Discovery Agent en Microsoft Windows

Si tiene problemas al instalar o utilizar el AWS Application Discovery Agent en Microsoft 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, consulteRequisitos previos para Discovery Agent.

Recopilador sin agente de Application Discovery Service

Application Discovery Service Agentless Collector (Agentless Collector) es una aplicación local que recopila información sobre su entorno local mediante métodos sin agente, incluida la información del perfil del servidor (por ejemplo, el sistema operativo, el número o la cantidad de RAM), los metadatos de la base de datos CPUs, las métricas de uso y los datos sobre el tráfico de red entre los servidores locales. El recopilador sin agente se instala como una máquina virtual (VM) en el entorno de VMware vCenter Server mediante un archivo Open Virtualization Archive (OVA).

Agentless Collector tiene una arquitectura modular que permite el uso de varios métodos de recopilación sin agente. Agentless Collector proporciona módulos para la recopilación de datos desde VMware VMs y desde servidores de bases de datos y análisis. También proporciona un módulo para recopilar datos sobre el tráfico de red entre los servidores locales.

Agentless Collector admite la recopilación de datos para AWS Application Discovery Service (Application Discovery Service) mediante la recopilación de datos de uso y configuración sobre sus servidores y bases de datos locales, así como datos sobre el tráfico de red entre sus servidores locales.

Application Discovery Service está integrado con un servicio que simplifica el seguimiento de la migración AWS Migration Hub, ya que agrega la información del estado de la migración en una sola consola. Puede ver los servidores detectados, obtener EC2 recomendaciones de Amazon, 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 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.

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, consulteInicia 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` `FleetAdvisorS3Policy` Para obtener más información, consulte Implementación de Application Discovery Service 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 credenciales de vCenter con los permisos de lectura y visualización establecidos para el grupo de sistema.
- 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 Crear un bucket en la Guía del usuario de Amazon S3.
- La versión 2 de Agentless Collector requiere una versión ESXi 6.5 o posterior.

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 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`— 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.
- `sts.amazonaws.com`— El recopilador usa este dominio para saber con qué cuenta se configuró el recopilador.

Los siguientes dominios requieren acceso saliente si la región de origen de la 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.
- `sts.amazonaws.com`— El recopilador usa este dominio para saber con qué cuenta se configuró el recopilador.

Al configurar Agentless Collector, es posible que reciba errores como, por ejemplo, un error en la configuración: compruebe sus credenciales e inténtelo de nuevo o AWS no se puede 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 a AWS, consulte. Reparación: no se puede acceder AWS a Agentless Collector durante la configuración

Implementación de Application Discovery Service Agentless Collector

Para implementar Application Discovery Service Agentless Collector, primero debe crear un usuario de IAM y descargar el recopilador. En esta página, se explican los pasos a seguir para implementar un recopilador.

Cree un usuario de IAM para Agentless Collector

Para usar Agentless Collector, en la AWS cuenta en la que utilizóInicia 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

gestionada. 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": "*"
    }]
}
```

- Use 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 estés viendo las claves de acceso del usuario (clave de acceso IDs y claves de acceso secretas), sigue 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. Necesitarás introducir estas claves de accesoConfiguración del 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.

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 el entorno local. VMware 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 VMware administrador y vaya 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. Según el algoritmo de hash que utilice en el entorno de su sistema, descargue el MD5o SHA256para 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. Según la versión de Linux que utilice, ejecute el MD5 comando o SHA256 comando correspondiente a la versión para comprobar que la firma criptográfica del `ApplicationDiscoveryServiceAgentlessCollector.ova` archivo coincide con el valor del SHA256 archivo MD5/correspondiente que descargó.

   ```
   $ md5sum ApplicationDiscoveryServiceAgentlessCollector.ova
   ```

   ```
   $ sha256sum ApplicationDiscoveryServiceAgentlessCollector.ova
   ```

Implemente Agentless Collector

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

Especificaciones de la máquina virtual Agentless Collector

Agentless Collector version 2

- Sistema operativo — Amazon Linux 2023
- RAM: 16 GB
- CPU: 4 núcleos
- VMware requisitos: consulte los requisitos del VMware host para ejecutar AL2 023 en VMware

Agentless Collector version 1

- 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 VMware entorno.

Para implementar Agentless Collector

1. Inicie sesión en vCenter como administrador. VMware
2. Utilice una de las siguientes formas de 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. Asegúrese de que la configuración del proxy en el panel de administración del servidor esté configurada correctamente.
    - Utilice la línea de comandos: para instalar el archivo OVA del recopilador desde la línea de comandos, descargue y utilice la herramienta de formato VMware abierto de virtualización (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 ***replaceable*** valores 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. Después de unos minutos, la dirección IP del recopilador aparece en vCenter. Esta dirección IP se utiliza para conectarse al recopilador.

Acceder 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. Implemente Agentless Collector
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. Configuración del recopilador sin agente De lo contrario, verás a continuación. El panel de control de Agentless Collector

Configuración del 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. Implementación de Application Discovery Service 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 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 Application Discovery Service 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. IPv4 No es compatible. IPv6

Agentless Collector version 2

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 CIDR: para obtener la máscara de red CIDR, compruebe la configuración de la dirección IP del host VMware vCenter que aloja la máquina virtual recopiladora. Por ejemplo, /24.
   - Puerta de enlace predeterminada: para obtener la puerta de enlace predeterminada, compruebe la configuración de la dirección IP del host VMware vCenter que aloja la máquina virtual recopiladora. Por ejemplo, 192.168.1.1.
   - DNS principal: para obtener el DNS principal, compruebe 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 ip link set ens192 down
   ```

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

   a. Abra 10- cloud-init-ens 192.network en el editor vi mediante el siguiente comando.

```
sudo vi /etc/systemd/network/10-cloud-init-ens192.network
```

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

```
[Match]
Name=ens192

[Network]
DHCP=no
Address=static-ip-value/CIDR-netmask
Gateway=gateway-value
DNS=dnsserver-value
```

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 dnsserver-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 ip link set ens192 up
```

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
```

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
```

Agentless Collector version 1

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: para obtener la máscara de red, compruebe 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: para obtener la puerta de enlace predeterminada, compruebe la configuración de la dirección IP del host VMware vCenter que aloja la máquina virtual recopiladora. Por ejemplo, 192.168.1.1.
- DNS principal: para obtener el DNS principal, compruebe 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 dnsserver-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
```

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

Los siguientes pasos describen cómo volver a configurar la máquina virtual Collector sin agente para usar DHCP.

Agentless Collector version 2

Para configurar la máquina virtual recopiladora para que utilice DHCP

1. Deshabilite la interfaz de red ejecutando el siguiente comando en el terminal remoto.

```
sudo ip link set ens192 down
```

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

a. Abra el `10-cloud-init-ens192.network` archivo en el editor vi mediante el siguiente comando.

```
sudo vi /etc/systemd/network/10-cloud-init-ens192.network
```

b. Actualice los valores como se muestra en el siguiente ejemplo.

```
[Match]
Name=ens192

[Network]
DHCP=yes

[DHCP]
ClientIdentifier=mac
```

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

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

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

```
sudo ip link set ens192 up
```

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

```
sudo reboot
```

Agentless Collector version 1

Para configurar la máquina virtual del recopilador para que utilice DHCP

1. Deshabilite la interfaz de red ejecutando el siguiente comando en el terminal remoto.

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

2. Actualice la configuración de 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. Active la interfaz de red introduciendo 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 usar 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 recopilador como se muestra en el siguiente ejemplo.

```
sudo reboot
```

Uso del módulo de recopilación de datos de red Agentless Collector

El módulo de recopilación de datos de red le permite descubrir las dependencias entre los servidores de su centro de datos local. Estos datos de red aceleran la planificación de la migración al proporcionar visibilidad sobre la forma en que las aplicaciones se comunican entre los servidores.

El módulo de recopilación de datos de red se conecta a los servidores que identifica el módulo VMware vCenter y analiza el tráfico de IP o puerto de origen a IP de destino de esos servidores.

Temas

Configuración del módulo de recopilación de datos de red

El módulo de recopilación de datos de red recopila datos de red para el inventario de servidores que proviene del módulo VMware vCenter. Por lo tanto, para usar el módulo de recopilación de datos de red, primero configure el módulo VMware vCenter. Para obtener instrucciones, siga las instrucciones de los temas siguientes:

1. the section called “Implementación de un recopilador”
2. the section called “Acceder a la consola del recopilador”
3. the section called “Configuración del recopilador”
4. the section called “Uso del módulo de recopilación de datos VMware ”

Para configurar el módulo de recopilación de datos de red

1. En el panel de control de Agentless Collector, en la sección Recopilación de datos de red, seleccione Ver conexiones de red.
2. En la página Conexiones de red, seleccione Editar recopilador.
3. En la sección de credenciales, introduzca al menos un conjunto de credenciales. Puede introducir hasta 10 conjuntos de credenciales. La primera vez que el módulo intenta recopilar datos para un servidor, prueba todas las credenciales hasta encontrar un conjunto de

credenciales que funcione; a continuación, guarda ese conjunto y lo vuelve a utilizar en los intentos posteriores. Para obtener información sobre la configuración de las credenciales, consultethe section called “Configuración de las credenciales de ”.

4. En la sección Preferencias de recopilación de datos, para empezar a recopilar datos automáticamente cuando se reinicie un servidor, seleccione Iniciar la recopilación de datos automáticamente.
5. Si no ha configurado los certificados WinRM, seleccione Desactivar las comprobaciones de certificados WinRM.
6. Seleccione Guardar.
7. La recopilación se realiza en los servidores cada 15 segundos. Para ver los detalles de los intentos de recopilación de un servidor determinado, seleccione la casilla de verificación situada a la izquierda del servidor en la tabla Servidores.

Configuración de las credenciales de

El módulo de recopilación de datos de red utiliza WinRM para recopilar datos de los servidores Windows. Utiliza SNMPv2 y SNMPv3 recopila datos de los servidores Linux.

Credenciales de WinRM:

- Especifique el nombre de usuario y la contraseña de una cuenta de Windows que tenga lo siguiente:
  - Acceso de lectura al `\root\standardcimv2` espacio de nombres
  - Permisos de lectura para la clase `MSFT_NetTCPConnection`
  - Acceso remoto a WMI
- Le recomendamos que cree una cuenta de servicio dedicada con los permisos mínimos necesarios.
- Evite utilizar cuentas de administrador de dominio o de administrador local.
- El puerto 5986 (HTTPS) debe estar abierto entre los servidores recopiladores y de destino.
- Evite deshabilitar la comprobación del certificado WinRM. Para obtener información sobre la configuración de los certificados WinRM, consulte. the section called “Solución de problemas de certificación autofirmada al configurar los certificados WinRM”

SNMPv2 credenciales:

- Proporcione una cadena de comunidad de solo lectura que pueda acceder al OID 1.3.6.1.2.1.6.13.*
- SNMPv3 es preferible a SNMPv2 ello debido a la mejora de la seguridad en SNMPv3
- El puerto 161/UDP debe estar abierto entre los servidores recopiladores y de destino
- Utilice cadenas de comunidad complejas y no predeterminadas
- Evita cadenas comunes como «pública» o «privada»
- Trate las cadenas comunitarias como contraseñas

SNMPv3 credenciales

- Proporcione username/password and auth/privacy detalles con un permiso de solo lectura que permita acceder al OID 1.3.6.1.2.1.6.13.*.
- El puerto 161/UDP debe estar abierto entre los servidores recopiladores y de destino
- Habilite tanto la autenticación como la privacidad
- Utilice protocolos de autenticación sólidos (se prefiere el SHA en lugar de MD5)
- Utilice protocolos de cifrado seguros (se prefiere el AES en lugar del DES)
- Utilice contraseñas complejas tanto para la autenticación como para la privacidad
- Usa nombres de usuario únicos (evita los nombres comunes)

Mejores prácticas generales para la administración de credenciales

- Almacene las credenciales de forma segura
- Cambie todas las credenciales con regularidad
- Utilice administradores de contraseñas o bóvedas seguras
- Supervise el uso de credenciales
- Siga el principio del mínimo privilegio y conceda únicamente los permisos mínimos necesarios

Intentos de recopilación de datos de red

Cuando se descubre un servidor nuevo, el recopilador prueba cada credencial configurada para cada dirección IP. Una vez que el recopilador encuentra una credencial válida, solo la usa. Tras dos errores consecutivos, el recopilador intenta recopilar los datos de red de un servidor después de 30 minutos, 2 horas, 8 horas y, después, 24 horas. Tras seis intentos fallidos, el recopilador sigue

probando todas las credenciales configuradas una vez al día. Para resolver el problema, edite las credenciales actuales o añada otras adicionales seleccionando Editar recopilador, o bien realice cambios en el servidor de destino que se está supervisando.

Estado del servidor en el módulo de recopilación de datos de red

En la siguiente tabla se explican los valores del estado de la recopilación.

Estado	Significado
Recolectando o recolectando	El último intento de recopilación de conexiones de red se realizó correctamente.
Error o error	El último intento de recopilación de conexione s de red falló debido a un problema de red o de permisos. Para obtener información adicional , active la casilla de verificación situada a la izquierda del servidor que tiene el error.
Omitido	Servidores para los que no se proporcionaron credenciales válidas. Actualice o configure credenciales de servidor adicionales.
Sin datos	No se ha iniciado la recopilación de datos para el servidor. Para empezar a recopilar datos, seleccione Iniciar recopilador.
Pendiente	Se ha iniciado la recopilación, pero no se ha realizado ningún intento de recopilac ión. Espere unos minutos y, a continuación, actualice la lista.

Uso del módulo de VMware recopilación de datos vCenter Agentless Collector

En esta sección se describe el módulo de recopilación de datos de VMware vCenter de Application Discovery Service Agentless Collector (Agentless Collector), que se utiliza para recopilar datos de inventario, perfil y uso del servidor de su empresa. VMware VMs

Temas

Configuración del módulo de recopilación de datos Agentless Collector para vCenter VMware

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 uso del servidor de su. VMware VMs

> **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 de sistema.

Para configurar el módulo de recopilación de datos VMware de vCenter

1. En la página del panel de control de Agentless Collector, en Recopilación de datos, elija Configurar en la sección vCenterVMware .
2. En la página Configurar la recopilación de datos de VMware vCenter, realice lo siguiente:

    a. En las credenciales de vCenter:

i. En el caso de la URL/IP de vCenter, introduzca la dirección IP del host de VMware vCenter Server.

ii. En 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, selecciona Iniciar la recopilación de datos automáticamente.

c. Elija Set up (Configurar).

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

Ver VMware los detalles de la recopilación de datos

La página de detalles de la recopilación de VMware datos muestra detalles sobre el vCenter en el que ha configurado. Configuración del módulo de recopilación de datos Agentless Collector para vCenter VMware

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

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

Seleccione Eliminar servidor vCenter para eliminar el servidor vCenter mostrado y volver a la página Configurar la recopilación de datos de vCenter VMware .

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, significa que se ha iniciado la recopilación de datos.

Puede ver los datos recopilados en la AWS Migration Hub consola. Si recopila datos para un inventario de VMware vCenter Server, 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, consulteVisualización de los datos recopilados.

Las siguientes son las pautas sobre la duración recomendada de la recopilación de datos en función de 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

Control del alcance de la recopilación de datos de vCenter

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

> **Note**
>
> Como práctica recomendada de seguridad, recomendamos no conceder permisos adicionales e innecesarios al usuario de vCenter de Application Discovery Service.

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 en función de la versión del cliente de vSphere que utilice.

Para descubrir datos sobre todos los hosts ESX y VMs en el vCenter actual

1. En el cliente de VMware vSphere, elija vCenter y, a continuación, elija Hosts and Clusters o and Templates. VMs
2. Elija un recurso de centro de datos y, a continuación, elija Permisos.
3. Elija el usuario de vCenter y, a continuación, elija el símbolo para añadir, editar o eliminar un rol de usuario.
4. Seleccione Solo lectura en el menú Función.
5. Elija Propagar a los 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 and Templates. VMs
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 and Templates. VMs
2. Elija Related Objects.
3. Elija hosts (que muestra una lista de los hosts ESX conocidos por vCenter) o máquinas virtuales (que muestra una lista VMs de 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.

> **Note**
>
> Si eligió Propagar a niños, aún puede eliminar el permiso de solo lectura de los hosts ESX y de forma periódica. VMs case-by-case Esta opción no afecta a los permisos heredados que se aplican a otros hosts ESX y. VMs

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 de vCenter VMware Application Discovery Service Agentless Collector (Agentless Collector). Para obtener información sobre cómo configurar la recopilación de datos, consulte. Configuración del módulo de recopilación de datos Agentless Collector para vCenter VMware

Leyenda de la tabla para los datos recopilados por VMware vCenter de 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.
avgCpuUsagePct	Porcentaje medio de uso de la CPU durante el período de sondeo.

Campo de datos	Descripción
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 ESXi anfitrión.
Modelo de ordenador	Modelo de computadora reportado por el ESXi anfitrión.
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.
datacenterId	ID del vCenter.
hostId*	ID del host de la máquina virtual.

Campo de datos	Descripción
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.
maxCpuUsagePct	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.
memoryReservation*	Límite para evitar un consumo excesivo de memoria en la máquina virtual.

Campo de datos	Descripción
moRefId	ID de referencia único de vCenter Managed Object.
name*	Nombre de la máquina virtual o la red (especifi cado por el usuario).
numCores	Número de núcleos de CPU asignados a la máquina virtual.
numCpus	Número de sockets de CPU en el ESXi host.
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.
state*	Estado del dispositivo virtual.
toolsStatus	Estado operativo de las VMware herramientas

Campo de datos	Descripción
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.

Uso del 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, consulteDatos recopilados por la base de datos Agentless Collector y el módulo de recopilación de datos analíticos.

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 su usuario de IAM y cree el recopilador de AWS DMS 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. Agregue sus servidores LDAP 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. Uso del módulo de recopilación de datos 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

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

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

- Amazon Linux 2

- Centos Linux versión 6 y superior
- Debian versión 10 y superior
- Red Hat Enterprise Linux versión 7 y superior
- SUSE Linux 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 superior hasta 2019
- MySQL versión 5.6 y hasta la 8
- Oracle versión 11g, versión 2 y versiones posteriores hasta 12c, 19c y 21c
- PostgreSQL versión 9.6 y hasta 13

Crear el recopilador AWS DMS de datos

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 motor de AWS destino del tamaño correcto. 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 rol de IAM 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 enRequisitos previos para Agentless Collector.

Para crear una función de IAM para que su recopilador AWS DMS de datos acceda a Amazon S3

1. Inicie sesión en la consola de IAM AWS Management Console y ábrala en. https://console.aws.amazon.com/iam/
2. En el panel de navegación, selecciona Funciones y, a continuación, selecciona Crear función.
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 casilla de verificación DMS 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, pega el siguiente JSON en el editor y reemplaza 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 el rol de IAM, elija el `FleetAdvisorS3Role` que haya creado anteriormente.
8. Elija Crear recopilador de datos.

Configuración del 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 Acceder 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. Región de AWSEn el caso de la clave de acceso de IAM y la clave de acceso secreta de IAM, 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 Implementación de un recopilador.
5. Para el recopilador de datos de Connected DMS, elija el recopilador de datos que creó en la consola. AWS DMS
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

Conne

for Access to DMS y Access to S3.

Añadir sus servidores LDAP y OS

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, 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 usar este protocolo para acceder a los servicios de información de directorio distribuidos y mantenerlos a través de su red IP.

Puede añadir un servidor LDAP 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 usa LDAP, puede agregar los servidores del sistema operativo manualmente.

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

1. Abra la consola Agentless Collector. Para obtener más información, consulte Acceder a la consola del recopilador.
2. Seleccione Ver recopilador de bases de datos y análisis y, a continuación, elija servidores LDAP en Discovery en el panel de navegación.
3. Seleccione Añadir servidor LDAP. Se abre la página Agregar servidor LDAP.
4. En Nombre de host, introduzca el nombre de host de su servidor LDAP.
5. En Puerto, introduzca el número de puerto que se utiliza para las solicitudes de LDAP.
6. En Nombre de usuario, introduzca el nombre de usuario que utiliza para conectarse al servidor LDAP.
7. En Contraseña, introduzca la contraseña que utiliza para conectarse al servidor LDAP.
8. (Opcional) Elija Verificar conexión para asegurarse de que ha agregado las credenciales del servidor LDAP correctamente. Como alternativa, puede comprobar las credenciales de conexión del servidor LDAP más adelante, en la lista de la página de servidores LDAP.
9. Seleccione Añadir servidor LDAP.
10. En la página de servidores LDAP, seleccione su servidor LDAP 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 protocolo LDAP.

El módulo de recopilación de datos analíticos y de bases de datos se conecta al servidor LDAP y detecta 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 seleccionando los servidores de View OS.

Como alternativa, puede agregar los servidores del sistema operativo manualmente o importar la lista de servidores desde un archivo de valores separados por comas (CSV). Además, puede utilizar el módulo de recopilación de datos VMware vCenter Agentless Collector para detectar los servidores del sistema operativo. Para obtener más información, consulte Uso del módulo de recopilación de datos 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 archivo CSV.
    a. Seleccione Importación masiva de servidores de SO desde CSV.
    b. Selecciona Descargar plantilla para guardar un archivo CSV que incluye una plantilla que puedes 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 archivo CSV.

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

d. Selecciona Examinar y, a continuación, selecciona tu archivo CSV.

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.

Descubriendo sus servidores de bases de datos

En esta sección se explican los pasos que debe seguir para configurar el sistema operativo y los servidores de bases de datos. A continuación, descubrirá sus servidores y tendrá la opción de añadir una base de datos o un servidor de análisis manualmente.

Para descubrir las bases de datos, debe crear 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.

Configuración y configuración

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. En esta página se describen los pasos que debe seguir para asegurarse de que se puede acceder a la base de datos en el puerto que especificó en la configuración de conexión. También activará la autenticación remota en el servidor de la base de datos y proporcionará permisos al módulo de recopilación de datos.

Configure, configure en Linux

Complete el siguiente procedimiento para configurar y detectar servidores de bases de datos en Linux.

Para configurar Linux para que detecte servidores de bases de datos

1. Proporcione acceso 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 scripts SSH remotos y permitir el tráfico del Protocolo de mensajes de control de Internet (ICMP).

Configurar configurar en Microsoft Windows

Complete el siguiente procedimiento para configurar y detectar servidores de bases de datos en Microsoft Windows.

Para configurar Microsoft Windows para que detecte servidores de bases de datos

1. Proporcione credenciales con permisos para ejecutar consultas del Instrumento de administración de Windows (WMI) y del lenguaje de consultas de WMI (WQL) y leer el registro.
2. Agregue el usuario de Windows que especificó en las credenciales de conexión al servidor del sistema operativo a los siguientes grupos: usuarios de COM 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.
   - Para el control de WMI, elija los permisos Ejecutar métodos, Habilitar cuenta, Habilitar remotamente y Leer seguridad para los espacios de `DEFAULT` nombres `CIMV2StandartCimv2`, y`WMI`.
   - Para el complemento WMI, 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 ICPM 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 Negosiate auth usage
winrm set winrm/config/service '@{AllowUnencrypted="true"}' # Allow unencrypted
 connection
```

Descubriendo un servidor de base de datos

Complete el siguiente conjunto de tareas para detectar y agregar servidores de bases de datos a la consola.

Para iniciar la detección de los 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 con el estado de conectividad 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 de forma manual. Además, puede importar la lista de servidores desde un archivo CSV. 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. Para el 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 archivo CSV.

   a. Seleccione Importación masiva de servidores de bases de datos desde CSV.

   b. Selecciona Descargar plantilla para guardar un archivo CSV que incluye una plantilla que puedes 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 archivo CSV.

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

d. Selecciona Examinar y, a continuación, selecciona tu archivo CSV.

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.

Después de 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.

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

El módulo de recopilación de datos analíticos y de base de datos de análisis Application Discovery Service Agentless Collector (Agentless Collector) recopila las siguientes métricas de su entorno de datos. Para obtener información sobre cómo configurar la recopilación de datos, consulte. Uso del módulo de recopilación de datos analíticos y de bases de datos

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

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

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

- Fechas de soporte de la base de datos
- Número de líneas de código
- Complejidad de esquema
- Similitud de esquemas

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

- Rendimiento de E/S en los servidores de bases de datos
- Operaciones de entrada/salida por segundo (IOPS) en los servidores de bases de datos
- Número de los CPUs que utilizan los servidores del sistema operativo
- Uso de memoria en los servidores del sistema operativo
- Uso de almacenamiento en los servidores del sistema operativo

Puede utilizar el módulo de recopilación de datos analíticos y de bases de datos para recopilar metadatos, métricas de capacidad y utilización 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.

Visualización de los datos recopilados

Puede ver los datos que su Application Discovery Service Agentless Collector (Agentless Collector) recopiló en la consola de Migration Hub siguiendo los pasos que se indican en. Visualización de los servidores en la consola AWS Migration Hub

También puede ver las métricas recopiladas de los servidores de bases de datos y análisis en la AWS DMS consola siguiendo estos pasos.

Para ver los datos descubiertos por la base de datos y el módulo de recopilación de datos analíticos en la AWS DMS consola

1. Inicie sesión en la AWS DMS consola AWS Management Console y ábrala en la versión https://console.aws.amazon.com/dms/2/.
2. Selecciona 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 utilizar la AWS DMS consola para identificar esquemas duplicados, determinar la complejidad de la migración y exportar la información de inventario para futuros análisis. Para obtener más información, consulte Uso de inventarios para el análisis en AWS DMS Fleet Advisor.

Acceso al recopilador sin agente

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

Temas

El panel de control de Agentless Collector

En la página del panel de control de Application Discovery Service Agentless Collector (Agentless Collector), 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

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

Si tiene problemas de AWS conexión, es posible que deba editar los ajustes de configuración de Agentless Collector.

Para editar los ajustes de configuración del recopilador, seleccione Editar los ajustes 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. Application Discovery Service Agentless Collector (Agentless Collector) admite actualmente la recopilación de datos desde VMware VMs 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

- VMware Recopilación de datos de vCenter
- Recopilación de datos de bases de datos y análisis

VMware Recopilación de datos de vCenter

Para recopilar datos de inventario, perfil y uso de los servidores VMware VMs, configure las conexiones a sus servidores vCenter. Para configurar las conexiones, elija Configurar en la sección VMware vCenter y siga las instrucciones que se describen en. Uso del módulo de VMware recopilación de datos vCenter Agentless Collector

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

- Vea el estado de la recopilación de datos
- Iniciar 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 VMwarevCenter se sustituye por la información del estado de la recopilación de datos, el botón Detener la recopilación de datos y el botón Ver y editar.

Recopilación de datos de bases de datos y análisis

Puede ejecutar la base de datos y el módulo de recopilación de datos analíticos 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 del 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 la base de datos y utilización de recursos

Además de la información sobre los metadatos y 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 de 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 sus servidores de bases de datos y análisis

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

   Si elige la opción de metadatos, capacidad de la base de datos y utilización de recursos, establezca el período de recopilación de datos. Puede recopilar datos durante los próximos 7 días o establecer el intervalo personalizado de 1-60 días.
5. Elija Ejecutar recopilación de datos. Se abre la página de recopilación de datos.
6. Seleccione la pestaña Estado de la recopilación para ver el estado de la recopilación de datos.

Tras completar la recopilación de datos, su 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 enVisualización de los datos recopilados.

Edición de la configuración de Agentless Collector

Configuró el recopilador la primera vez que configuró Application Discovery Service Agentless Collector (Agentless Collector), tal y como se describe en. Configuración del recopilador sin agente El siguiente procedimiento describe cómo editar los ajustes de configuración del recopilador sin agente.

Para editar los ajustes de configuración del recopilador

- Pulse 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 AWS Cuenta de destino para los datos de descubrimiento, introduzca la clave de AWS acceso y la clave secreta de la AWS 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, consulteImplementación de Application Discovery Service Agentless Collector.

     i. 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.

     ii. 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. En Contraseña del recopilador sin agente, cambie la contraseña que se utilizará para autenticar el acceso al recopilador sin agente.

     i. En el caso de la contraseña del recopilador sin agente, introduzca una contraseña para autenticar el acceso al recopilador sin agente.

     ii. Para volver a introducir la contraseña de Agentless Collector, vuelva a introducir la contraseña para verificarla.

  d. Seleccione Guardar configuraciones.

A continuación, verásEl panel de control de Agentless Collector.

Edición de VMware credenciales de vCenter

Para recopilar datos de inventario, perfil y uso de los servidores VMware VMs, configure las conexiones a sus servidores vCenter. Para obtener información sobre la configuración de las conexiones de VMware vCenter, consulte. Uso del módulo de VMware recopilación de datos vCenter 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 de sistema.

Para editar las credenciales de VMware vCenter

En la Ver VMware los detalles de la recopilación de datos página, elija Editar servidores vCenter.

- En la página Editar vCenter, realice lo siguiente:
  a. En las credenciales de vCenter:
     i. En el caso de la URL/IP de vCenter, introduzca la dirección IP del 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 Application Discovery Service Agentless Collector

Al configurar Application Discovery Service Agentless Collector (Agentless Collector), puede optar por habilitar las actualizaciones automáticas como se describe en. Configuración del 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. Siga los pasos que se indican. Implemente Agentless Collector

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

Para actualizar tu EC2 instancia de Amazon

1. Obtenga la dirección IP del recopilador sin agente de VMware vCenter.
2. Abra la consola de máquinas virtuales 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 AL2 instancia en la Guía del usuario de Amazon Linux 2.

Parcheo en vivo del kernel

Agentless Collector version 2

> La máquina virtual Agentless Collector versión 2 utiliza Amazon Linux 2023 tal y como se describe en. Implemente Agentless Collector

Para habilitar y usar Live Patching para Amazon Linux 2023, consulte Kernel Live Patching on AL2 023 en la Guía del usuario de Amazon EC2 .

Agentless Collector version 1

La máquina virtual Agentless Collector versión 1 utiliza Amazon Linux 2, tal y como se describe en. Implemente Agentless Collector

Para habilitar y usar Live Patching para Amazon Linux 2, consulte Kernel Live Patching on AL2 en la Guía del EC2 usuario de Amazon.

Para actualizar de la versión 1 de Agentless Collector a la versión 2

1. Instale una nueva OVA de Agentless Collector con la imagen más reciente.
2. Configurar las credenciales.
3. Elimine el antiguo dispositivo virtual.

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

- ¿Arreglando Unable to retrieve manifest or certificate file error
- Solución de problemas de certificación autofirmada al configurar los certificados WinRM
- Reparación: no se puede acceder AWS a Agentless Collector durante la configuración
- 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

- Cómo ponerse en contacto con AWS Support por problemas con Agentless Collector

¿Arreglando `Unable to retrieve manifest or certificate file error`

Si recibe este error al intentar implementar la OVA desde la URL de Amazon S3 en la interfaz de usuario de VMware vCenter, asegúrese de que el servidor vCenter cumpla los siguientes requisitos:

- VMware vCenter Server versión 8.0, actualización 1 o posterior
- VMware vCenter Server 7.0 Update 3q (compilación ISO 23788036) o posterior

Solución de problemas de certificación autofirmada al configurar los certificados WinRM

Si habilita las comprobaciones de certificados de WinRM, es posible que deba importar una entidad de certificación autofirmada al recopilador sin agente.

Para importar una entidad emisora de certificados autofirmada

1. Abra la consola web de máquinas virtuales del recopilador en VMware vCenter e inicie sesión `ec2-user` con la contraseña, `collector` como se muestra en el siguiente ejemplo.

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

2. Asegúrese de que todos los certificados de CA autofirmados que se utilizan para firmar los certificados WinRM estén en el directorio. `/etc/pki/ca-trust/source/anchors` Por ejemplo:

   ```
   /etc/pki/ca-trust/source/anchors/https-winrm-ca-1.pem
   ```

3. Para instalar los nuevos certificados, ejecute el siguiente comando.

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

4. Reinicie el recopilador sin agente ejecutando el siguiente comando

   ```
   sudo shutdown -r now
   ```

5. (Opcional) Para comprobar que los certificados se han importado correctamente, puede ejecutar el siguiente comando.

```
sudo trust list --filter=ca-anchors | less
```

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

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

> No se pudo acceder 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 web de máquinas virtuales 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, consulteCómo ponerse en contacto 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 web de máquinas virtuales 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. Configuración del 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 vCenterVMware .
7. Siga las instrucciones Edición de VMware credenciales de 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. Cómo ponerse en contacto 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 IPy 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. Implemente Agentless Collector
3. Seleccione Iniciar sesión y, a continuación, introduzca la contraseña del recopilador sin agente, que se configuró cuando se configuró el recopilador en. Configuración del 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 vCenterVMware .
5. En la página de detalles de la recopilación de VMware datos, en Servidores vCenter detectados, anote la dirección IP en la columna vCenter.
6. Con una herramienta de línea de comandos independiente, como `ping` `otraceroute`, 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 VMware credenciales de 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 Configuración del 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 DMSCollectorpolíticas Policy y FleetAdvisorS3Policy a su usuario de IAM. Para obtener más información, consulte Implementación de Application Discovery Service 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 *`replaceable`* los valores por los suyos.

- 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 Descubriendo 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.

Cómo ponerse en contacto 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 web de máquinas virtuales 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.

Importación de datos a Migration Hub

AWS Migration Hub La importación (Migration Hub) le permite importar detalles de su entorno local directamente a Migration Hub sin utilizar el Application Discovery Service Agentless Collector (Agentless Collector) o el AWS Application Discovery Agent (Discovery Agent), de modo que puede realizar la evaluación y la planificación de la migración directamente desde los datos importados. También puede agrupar los dispositivos como aplicaciones y realizar un seguimiento de su estado de migración.

En esta página se describen los pasos para completar una solicitud de importación. En primer lugar, utilice una de las dos opciones siguientes para preparar los datos del servidor local.

- Utilice las herramientas habituales de terceros para generar un archivo que contenga los datos del servidor local.
- Descarga nuestra plantilla de importación de valores separados por comas (CSV) y rellénala con los datos de tu servidor local.

Después de usar uno de los dos métodos descritos anteriormente para crear el archivo de datos local, cargue el archivo en Migration Hub mediante la consola de Migration Hub o uno de los AWS SDKs. AWS CLI Para obtener más información sobre las dos opciones, consultethe section called “Formatos de importación compatibles”.

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 mediante la importación APIs.

Una vez completada una solicitud de importación, puede ver los detalles de los registros importados individuales. Vea los datos de uso, las etiquetas y las asignaciones de aplicaciones directamente desde la consola de 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.

Tratamiento 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 AWS Application Discovery Service Cuotas.

Formatos de importación compatibles

Migration Hub admite los siguientes formatos de importación.

- RVTools
- Plantilla de importación de Migration Hub

RVTools

Migration Hub admite la importación de exportaciones de VMware vSphere mediante. RVTools Al guardar datos de RVTools, primero selecciona la opción Exportar todo a csv, comprime la carpeta e importa el archivo ZIP a Migration Hub. CSVs Se requiere lo siguiente en el ZIP: vInfo, vNetwork, vCPU, vMemory, vDisk, vPartition, vSource, vTools, vHost, vNIC, vSC_VMK.

Plantilla de importación de Migration Hub

La importación de Migration Hub le permite importar datos de cualquier fuente. 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 al nombre de un 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 rellenados 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.

Un signo de intercalación (^) junto al nombre de un campo de importación en la siguiente tabla indica que es de solo lectura si se proporciona un ServerID.

> **Note**
>
> Si está utilizando alguno de los dos. 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, ExternalIdpuede ser el identificador de inventario del servidor de su centro de datos.	ID de inventario 1 Servidor 2 ID de CMBD 3
SMBiosIdentificación^	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 "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. Debe estar provisto de un VMware. VCenterCarné.	
VMware. VCenterIdentificación*^	Identificador único de la máquina virtual. Debe estar provisto de un. VMware MoRefId.	

Nombre del campo de importación	Descripción	Ejemplos
TAZA. NumberOfProcessors^	El número de CPUs.	4
TAZA. NumberOfCores^	El número total de núcleos físicos.	8
TAZA. NumberOfLogicalCores^	El número total de subprocesos que se pueden ejecutar simultáneamente CPUs en todos los componentes de un servidor. Algunos CPUs admiten varios subprocesos para que se ejecuten simultáneamente en un único núcleo de CPU. En esos casos, este número será mayor que el número de núcleos físicos (o virtuales).	16
Nombre del sistema operativo^	Nombre del sistema operativo.	Linux Windows.Hat
Sistema operativo^	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

Nombre del campo de importación	Descripción	Ejemplos
RAM. UsedSizeInMB. Max^	La cantidad máxima de RAM utilizada disponible en el servidor, en MB.	64 128
TAZA. UsagePct.Promedio ^	Utilización de CPU media cuando la herramienta de detección estaba recolectando datos.	45 23.9
TAZA. UsagePct.Máx^	Utilización de CPU máxima cuando la herramienta de detección estaba recolectando datos.	55.34 24
DiskReadsPerSecondInkB.Avg^	Número medio de lecturas de disco por segundo, en KB.	1159 84506
DiskWritesPerSecondInkB.Avg^	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.Promedio ^	El número medio de operaciones de lectura en disco por segundo.	45 28
DiskWritesOpsPerSecond.Promedio ^	Número medio de operaciones de escritura en disco por segundo.	8 3

Nombre del campo de importación	Descripción	Ejemplos
DiskReadsOpsPerSecond.Máx^	Número máximo de operaciones de lectura en disco por segundo.	1083 176
DiskWritesOpsPerSecond.Máx^	Número máximo de operaciones de escritura en disco por segundo.	535 71
NetworkReadsPerSecondInkB.Avg^	Número medio de operaciones de lectura de red por segundo, en KB.	45 28
NetworkWritesPerSecondInkB.Avg^	Número medio de operaciones de escritura de red por segundo, en KB.	8 3
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"
ApplicationWave	La ola de migración de este servidor.	

Nombre del campo de importación	Descripción	Ejemplos
Etiquetas^	Una lista delimitada por comas de etiquetas con el formato nombre:valor. **Important** No guarde informaci ón confidencial (como datos personales) en etiquetas.	"zone:1, critical:yes" "zone:3, critical:no, zone:1"
ServerId	El identificador del servidor tal y como aparece en la lista de servidores de Migration Hub.	`d-server-01kk9i6yw waxmp`

Puede importar datos aunque no tenga datos rellenados 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 los servidores y aplicaciones descubiertos.

Note

La importación de Migration Hub no admite ningún campo que no sea el definido en la plantilla de importación. Se ignorará cualquier campo personalizado suministrado y no se importará.

Configurar los permisos de importación

Antes de importar los datos, asegúrese de que su usuario de IAM tenga los permisos de Amazon S3 necesarios para cargar (`s3:PutObject`) el archivo de importación en Amazon S3 y leer el objeto (`s3:GetObject`). También debe establecer el acceso programático (para el AWS CLI) o el acceso a la consola, creando una política de IAM y adjuntándola al usuario de IAM que realiza las importaciones en su cuenta. AWS

Console Permissions

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

Para editar las políticas administradas asociadas a un usuario

1. Inicie sesión en la consola de IAM AWS Management Console y ábrala en. https://console.aws.amazon.com/iam/
2. En el panel de navegación, seleccione Usuarios.
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 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 Crear política.

6. Vuelva a la página de la consola de IAM sobre la concesión de permisos para el usuario que realizará las solicitudes de importación en su AWS cuenta.
7. Actualice la tabla de políticas y busque el nombre de la política que acaba de crear.
8. Elija Next: Review (Siguiente: Revisión).
9. Elija Add permissions (Agregar permisos).

Ahora que has añadido la política a tu usuario de IAM, estás listo para iniciar el proceso de importación.

AWS CLI Permissions

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

Para crear y adjuntar las políticas administradas

1. Utilice el `aws iam create-policy` AWS CLI comando 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 sobre el uso de este comando, consulte create-policy en la AWS CLI Referencia de comandos.

2. Utilice el `aws iam create-policy` AWS CLI comando 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. Utilice el `aws iam attach-user-policy` AWS CLI comando para adjuntar las políticas que creó en los dos pasos anteriores al usuario de IAM que realizará las solicitudes de importación en su AWS cuenta mediante el. AWS CLI Para obtener más información sobre el uso de este comando, consulte attach-user-policyla Referencia de AWS CLI comandos.

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

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

Cargar el archivo de importación a Amazon S3

A continuación, debe cargar el archivo de importación con formato CSV en Amazon S3 para poder importarlo. Antes de empezar, debe tener un bucket de Amazon S3 que alojará el archivo de importación creado o elegido con antelación.

Console S3 Upload

Para cargar el archivo de importación a Amazon S3

1. Inicie sesión en la consola de Amazon S3 AWS Management Console y ábrala 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 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 Abrir.
6. Seleccione 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 de la consola de Migration Hub tal y como se describe enImportar datos. A continuación, pegue la URL del objeto en el campo URL del objeto de Amazon S3.

AWS CLI S3 Upload

Para cargar el archivo de importación a Amazon S3

1. Abra una ventana de terminal y navegue hasta el directorio en el que está guardado el archivo de importación.
2. Escriba el siguiente comando:

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

3. Esto devuelve los siguientes resultados:

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

4. Copie la ruta completa del objeto de Amazon S3 que se devolvió. La necesitará cuando cree su solicitud de importación.

Importar datos

Tras descargar la plantilla de importación desde la consola de Migration Hub y rellenarla con los datos del servidor local existente, estará listo para empezar a importar los datos a Migration Hub. En las siguientes instrucciones se describen dos formas de hacerlo, ya sea mediante la consola o realizando llamadas a la API a través de. AWS CLI

Console Import

Inicie la importación de datos en la página Herramientas de 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 desde nuestro bucket de Amazon S3 en https://s3.us-west-2.amazonaws.com/templates-7cffcf56-bd96-4b1c-b45b-a5b42f282e46/import_template.csv
3. Para abrir la página de importación, selecciona Importar en el cuadro de importación.
4. En Nombre de importación, especifique un nombre para la importación.
5. Rellene el campo URL del objeto de Amazon S3. Para realizar este paso, tendrá que cargar el archivo de datos de importación a Amazon S3. Para obtener más información, consulte Cargar el archivo de importación a 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 página Importaciones (historial de importaciones) y seleccionar el nombre de la importación que aparece en la columna Nombre, accederá a la página Servidores, donde se aplicará un filtro en función del conjunto de datos de la importación seleccionada. A continuación, solo verá los datos que pertenezcan a esa importación concreta.

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 iniciar el proceso de importación de datos desde AWS CLI, primero AWS CLI deben estar instalados en su entorno. Para obtener más información, consulte Instalación de la interfaz de línea de AWS comandos en la Guía del AWS Command Line Interface usuario.

> **Note**
>
> Si aún no has rellenado una plantilla de importación, puedes descargarla desde nuestro bucket de Amazon S3 aquí: https://s3.us-west-2.amazonaws.com/templates-7cffcf56-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 sus solicitudes de importación de Migration Hub

Puede realizar un seguimiento del estado de sus solicitudes de importación de Migration Hub mediante la consola o una de las AWS SDKs. AWS CLI

Console Tracking

En el panel de control de importaciones de la consola de Migration Hub, encontrarás 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: 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 valores siguientes:
  - Importación: este archivo de datos se está importando actualmente.
  - Importado: todo el archivo de datos se importó correctamente.
  - Importado con errores: no se pudo importar uno o más 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.
  - Error al 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 importaron correctamente.
- Registros fallidos: el número de registros de un archivo de datos específico que no se importaron.

CLI Tracking

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

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.

Vea y explore los datos descubiertos

Tanto Application Discovery Service Agentless Collector (Agentless Collector) como Discovery Agent (AWS Discovery Agent) proporcionan datos de rendimiento del sistema basados en el uso promedio y máximo. Puede utilizar los datos de rendimiento del sistema recopilados para calcular el coste total de propiedad (TCO) de alto nivel. Los agentes de detección recopilan datos más detallados, incluidos datos de series temporales para obtener información sobre el 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 la consola. AWS CLI

Temas

Vea 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. VMs Los datos aparecen en la consola aproximadamente 15 minutos después de que se inicie la recopilación de datos. También puede ver estos datos en formato CSV exportando los datos recopilados realizando llamadas a la API mediante AWS CLI.

Para ver los datos recopilados sobre los servidores descubiertos en la consola, sigue los pasos que se indicanVisualización de los servidores en la consola AWS Migration Hub. Para obtener más información sobre el uso de la consola para ver, ordenar y etiquetar los servidores descubiertos por sus recopiladores sin agentes o agentes de detección, consulte. Descubrimiento de datos con la AWS Migration Hub consola

El módulo de recopilación de datos analíticos y de base de datos Agentless Collector carga los datos recopilados en el bucket de Amazon S3. Puede ver los datos de este depósito en la consola del DMS. AWS Para ver los datos recopilados sobre los servidores de bases de datos y análisis descubiertos, siga los pasos que se indican a continuación. Visualización de los datos recopilados

Lógica de coincidencia para los servidores y aplicaciones descubiertos

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 varias fuentes, incluidas la importación 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 a otro `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. MoRefIdy VMware. vCenterId — Ambos valores deben ser idénticos a los campos respectivos de otra entrada para que Application Discovery Service realice una coincidencia.

Exploración de datos en Amazon Athena

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

La exploración de datos en Amazon Athena le permite analizar los datos recopilados de todos los servidores locales descubiertos por los agentes de detección en un solo lugar. Una vez que se habilita la exploración de datos en Amazon Athena desde la consola de Migration Hub (o mediante la StartContinousExport API) y se activa la recopilación de datos para los agentes, los datos recopilados por los agentes se almacenan automáticamente en su bucket de S3 a intervalos regulares.

A continuación, puede visitar Amazon Athena para ejecutar consultas predefinidas a fin de analizar el rendimiento del sistema en series temporales para cada servidor, el tipo de procesos que se ejecutan en cada servidor y las dependencias de red entre los distintos servidores. Además, puede escribir sus propias consultas personalizadas con Amazon Athena, cargar fuentes de datos adicionales existentes, 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 las consultas y realizar análisis adicionales.

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

Activar la exploración de datos en Amazon Athena

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

Al activar la exportación continua, su cuenta utiliza automáticamente la función `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` vinculada al

servicio. Para obtener más información sobre este rol vinculado a servicio, consulte Permisos de rol vinculados a servicios para Application Discovery Service.

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

Turn on with the console

La exploración de datos en Amazon Athena se habilita al activar la exportación continua de forma implícita al seleccionar «Iniciar la recopilación de datos» o al hacer clic en el botón denominado «Exploración de datos en Amazon Athena» en la página de recopiladores de datos de la consola de Migration Hub.

Para activar 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 Agentes.
3. Seleccione Iniciar recopilación de datos o, si ya tiene activada la recopilación de datos, haga clic en el botón Exploración de datos en Amazon Athena.
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 funcionan en modo de «exportación continua», lo que le permitirá ver los datos descubiertos y trabajar con ellos en Amazon Athena. La primera vez que se active, 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 mediante una llamada a la API desde. AWS CLI Para ello, primero AWS CLI debe estar instalado en su entorno.

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

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

Exploración de datos directamente en Amazon Athena

Después de activar la exploración de datos en Amazon Athena, puede empezar a explorar y trabajar con los datos actuales detallados descubiertos por 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.

Las siguientes instrucciones explican cómo explorar los datos de sus agentes directamente en la consola de Athena. Si no tiene ningún dato en Athena o no ha activado la exploración de datos en Amazon Athena, aparecerá un cuadro de diálogo en el que se le solicitará que habilite la exploración de datos en Amazon Athena, tal y como se explica en. Activar la exploración de datos en Amazon Athena

Para explorar los datos descubiertos por agentes directamente en Athena

1. En la AWS Migration Hub consola, elija Servidores en el panel de navegación.
2. Para abrir la consola de Amazon Athena, elija 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. Para consultar los datos en la consola de Amazon Athena, escriba y ejecute 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 Uso de consultas predefinidas en Amazon Athena.

Visualización de datos de Amazon Athena

Para visualizar los datos, se puede portar una consulta a un programa de visualización como Amazon QuickSight u otras herramientas de visualización de código abierto como Cytoscape, yEd o Gelphi. 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. Inicia 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. Elige Athena. Aparece el cuadro de diálogo Nueva fuente de datos de Athena.
4. Escriba un nombre en el campo Data source name (Nombre del origen de datos).
5. Elija Crear origen de datos.
6. Seleccione la gents-servers-os tabla A en el cuadro de diálogo Elija su tabla y elija Seleccionar.
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.

Uso de consultas predefinidas en Amazon 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 AWS Migration Hub consola, elija Servidores en el panel de navegación.
2. Para abrir la consola de Amazon Athena, elija 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.

Obtenga las direcciones IP y los nombres de host de 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 CREATE VIEW en la 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");
```

Identifique los 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.%'));
```

Analice los datos de rendimiento del sistema para los 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 los servidores en función del 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 IANA.

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 CREATE VIEW en la Guía del usuario de Amazon Athena.

Para crear funciones de ayuda de seguimiento de salida

1. Abra la consola Athena en https://console.aws.amazon.com/athena/.
2. Cree la `valid_outbound_ips_helper` vista mediante la siguiente función auxiliar, que muestra todas las direcciones IP de destino salientes 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";
```

4. 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 los servidores en función del 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 IANA.

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 CREATE VIEW en la Guía del usuario de Amazon Athena.

Para crear funciones de ayuda de seguimiento de la importación

1. Abra la consola 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
```

Identifique el software en ejecución a partir del número de puerto

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 IANA.

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 IANA

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 en la 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");
```

Descubrimiento de datos con la AWS Migration Hub 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 utiliza la consola Application Discovery Service, se le redirige a la consola de Migration Hub. Trabajar con la consola de Migration Hub no requiere ningún paso ni configuración adicionales por tu parte.

En esta sección, encontrará información sobre cómo administrar y monitorear Application Discovery Service Agentless Collector (Agentless Collector) y AWS Application Discovery Agent (Discovery Agent) mediante la consola.

Temas

Visualización de los datos en el panel de control de la consola AWS Migration Hub

Para ver el panel principal, elija Panel en el panel de navegación de la consola AWS Migration Hub (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 Application Discovery Agent (Discovery Agent).

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, selecciona Panel de control en el panel de navegación, que se encuentra en la parte izquierda de la página de inicio de la consola de Migration Hub.

Iniciar y detener los recopiladores de datos en la AWS Migration Hub consola

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) utiliza para ayudarlo a descubrir su infraestructura existente. En los siguientes pasos se explica cómo descargar e implementar estas herramientas de recopilación de datos de descubrimiento, y. Implemente Agentless Collector AWS Agente de descubrimiento de aplicaciones

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

Una vez desplegado el AWS Application Discovery Agent (Discovery Agent), puede iniciar o detener el proceso de recopilación de datos en la página Recopiladores de datos de la consola AWS Migration Hub (Migration Hub).

Para iniciar o detener las herramientas de recopilación de datos

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. Elija la pestaña 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).

Ordenar los recopiladores de datos en la AWS Migration Hub consola

Si ha desplegado muchos recopiladores de datos, puede ordenar la lista de recopiladores desplegados que se muestra en la página de recopiladores de datos de la consola. 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).

La siguiente tabla muestra los criterios de búsqueda que puede utilizar para los agentes, incluidos los operadores, los valores y una definición de los valores.

Criterio de búsqueda	Operador	Valor: definición
ID de agente	==	Cualquier ID de agente seleccionado de la lista rellenada previamente desde la que se instala una herramienta de recopilación.
Hostname	== !=	Para los agentes, cualquier nombre de host seleccionado de la lista de hosts rellenada automáticamente cuando se instala un agente.
Estado de recopilación	== !=	Iniciado: los datos se recopilan y envían a Application Discovery Service Start scheduled (Programado para inicio): se ha programad o el inicio de la recopilación de datos. Los datos se enviarán a Application Discovery Service en el siguiente ping y el estado cambiará a Iniciado.

Criterio de búsqueda	Operador	Valor: definición
		Detenido: los datos no se recopilan ni se envían a Application Discovery Service. Stop scheduled (Programa do para detención): se ha programado la detención de la recopilación de datos. Los datos dejarán de enviarse a Application Discovery Service en el siguiente ping y el estado cambiará a Detenido.

Criterio de búsqueda	Operador	Valor: definición
Estado	== !=	Healthy (Buen estado): la recopilación de datos no está activada. La herramienta funciona con normalidad. Unhealthy (Mal estado): la herramienta se encuentra en un estado de error. No se están recopilando ni registrando datos. Unknown (Desconocido): no se ha establecido una conexión en más de una hora. Shutdown (Apagar): la herramienta comunicó una acción de apagado debido a que se ha apagado un sistema, servicio o daemon. Si se ha producido un reinicio o actualización de la herramienta, el estado cambiará a otro estado en el primer ciclo de notificación. Running (En ejecución): la recopilación de datos está activada. La herramienta funciona con normalidad.
Dirección IP	== !=	Cualquier dirección IP seleccionada de la lista rellenada automáticamente en la que se ha instalado una herramienta de recopilación.

La siguiente tabla muestra los criterios de búsqueda que puede utilizar para los recopiladores sin agente, incluidos los operadores, los valores y una definición de los valores.

Criterio de búsqueda	Operador	Valor: definición
ID	==	Cualquier ID de recopilador sin agente seleccionado de la lista rellenada previamente desde la que se instala una herramienta de recopilación.
Hostname	== !=	En el caso de los recopiladores sin agente, cualquier nombre de host seleccionado de la lista rellenada previamente de hosts en los que está instalado un recopilador sin agente.
Estado	== !=	Recopilación de datos: la recopilación de datos está activada. La herramienta funciona con normalidad. Listo para la configuración: la recopilación de datos no está activada. La herramienta funciona con normalidad. Requiere atención: la herramienta se encuentra en un estado de error y necesita atención. Unknown (Desconocido): no se ha establecido una conexión en más de una hora.

Criterio de búsqueda	Operador	Valor: definición
		Apagar: la última vez que la herramienta comunicó que estaba «apagándose» se debió a un cierre del sistema, servicio o daemon. Si se ha producido un reinicio o actualización de la herramien ta, el estado cambiará a otro estado en el primer ciclo de notificación.
Dirección IP	== !=	Cualquier dirección IP seleccionada de la lista rellenada 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. 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 Data Collectors.
3. Seleccione la pestaña Recolectores sin agente o Agentes.
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.

Visualización de los servidores en la consola AWS Migration Hub

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.

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. 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 Servidores. 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 Se utiliza AWS Migration Hub para exportar los datos del servidor.

Ordenar los servidores en la AWS Migration Hub consola

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. 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 Servidores.
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.

Etiquetar servidores en la consola AWS Migration Hub

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 Las etiquetas (Application Discovery Service) son similares a las AWS 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. 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 Servidores.
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. Elija Agregar etiquetas y, a continuación, elija Agregar nueva etiqueta.
5. En el cuadro de diálogo, escriba una clave en el campo Clave y, si lo desea, un valor en el campo Valor.

   Para añadir más etiquetas, seleccione Añadir nueva etiqueta y añada más información.
6. Seleccione Guardar.

Para eliminar etiquetas de uno o varios servidores

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 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 las etiquetas de más de un servidor a la vez.

4. Selecciona Eliminar etiquetas.
5. Selecciona cada etiqueta que quieras eliminar.
6. Elija Confirmar.

Se utiliza AWS Migration Hub para exportar los datos del servidor

En este tema se explica cómo exportar los datos del servidor mediante la AWS Management Console AWS Command Line Interface, la o la API.

Para utilizarla AWS Management Console para exportar los datos del servidor de todos los servidores

1. Inicie sesión en la consola de Migration Hub AWS Management Console y ábrala en https://console.aws.amazon.com/migrationhub/.
2. En el panel de navegación izquierdo, en Discover, selecciona Servidores.
3. Elija Acciones y, a continuación, seleccione Exportar datos de descubrimiento.
4. En la sección Exports (Exportaciones) situada en la parte inferior de la pantalla, elija Export server details (Exportar detalles del servidor). Esta acción genera un archivo.zip que incluye los archivos.csv que se describen en la siguiente tabla.

Nombre de archivo	Descripción
{account_id} _Application.csv	Detalles de cada aplicación, incluidos el número de servidores, el nombre y la descripción.
{account_id} _ .csv ApplicationResourceAssociation	La relación entre los servidores y las aplicaciones.
{account_id} _ ImportTemplate	El resumen de la aplicación y las etiquetas de cada servidor. Este archivo se puede modificar y volver a importar para actualizar la aplicación asociada al servidor.

Nombre de archivo	Descripción
{account_id} _ .csv NetworkInterface	Detalles de cada interfaz de red, incluidos el servidor, la dirección y el conmutador asociados.
{account_id} _Server.csv	Detalles de cada servidor, incluidos el sistema operativo, el nombre de host y el hipervisor.
{account_id} _ .csv SystemPerformance	Detalles de cada servidor, incluida la configuración de la CPU, la memoria y el almacenamiento, y el rendimiento.
{account_id} _Tags.csv	Detalles de cada etiqueta asociada a un servidor.
{account_id} _ Info.csv VMware	Detalles de cada VMware configuración, incluidos moreF, VMname y vCenter.

Para utilizarlos AWS Management Console para exportar los datos del agente de un servidor específico

1. Inicie sesión en la consola de Migration Hub AWS Management Console y ábrala en https://console.aws.amazon.com/migrationhub/.
2. En el panel de navegación izquierdo, en Discover, selecciona Servidores.
3. Coloque el cursor en el campo de búsqueda, debajo de Servidores. Se muestra una lista desplegable. En esa lista, en Propiedades, elija Fuente, elija el operador = y, a continuación, elija Fuente = Agente.
4. En los resultados de la búsqueda, elija el nombre del servidor para el que desee exportar los datos. Esta acción lo lleva a la página de detalles de ese servidor.
5. Introduzca una hora de inicio y una hora de finalización y, a continuación, seleccione Exportar. El archivo.zip exportado incluye los archivos.csv que se describen en la siguiente tabla.

{account_id} _ .csv destinationProcess Connection	Detalles de las conexiones entrantes al servidor.
{account_id} _networkInterface.csv	Detalles de cada interfaz de red, incluida la dirección, la máscara y el nombre
{account_id} _osInfo.csv	Detalles del sistema operativo, incluidos el tipo de CPU, el hipervisor y el nombre del sistema operativo.
{account_id} _process.csv	Detalles de los procesos que se ejecutan en el servidor.
{account_id} _ .csv sourceProcessConne ction	Detalles de la conexión saliente que se origina en el servidor.
{account_id} _systemPerformance.csv	Detalles de la configuración y el rendimiento de la CPU, la memoria y el almacenamiento del servidor.

Para usar la API AWS Command Line Interface o la API para exportar los datos del servidor

1. Ejecute start-export-task. La operación de API correspondiente es StartExportTask
2. Ejecute describe-export-tasks. La operación de API correspondiente es DescribeExportTasks.

Agrupar los servidores en la consola AWS Migration Hub

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. 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 Servidores.
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, elija Add tag (Añadir etiqueta), escriba un valor para Key (Clave) y, a continuación y de forma opcional, escriba un valor para Value (Valor).
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 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 `DescribeConfigurationsListConfigurations`, y es `StartExportTask` posible que no contengan actualizaciones recientes. Para obtener más información, consulte the section called “Consistencia final”.

Uso de la acción `DescribeConfigurations`

La `DescribeConfigurations` acción recupera los atributos de una lista de configuraciones IDs. Todos los datos proporcionados IDs deben ser para el mismo tipo de activo (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
`server.agentId`	
`server.applications`	
`server.applications.hasMore Values`	
`server.configurationId`	x
`server.cpuType`	
`server.hostName`	
`server.hypervisor`	
`server.networkInterfaceInfo`	
`server.networkInterfaceInfo .hasMoreValues`	
`server.osName`	
`server.osVersion`	
`server.tags`	
`server.tags.hasMoreValues`	
`server.timeOfCreation`	x
`server.type`	

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

Campo	Obligatorio
server.performance.maxNetwo rkReadsPerSecondInKB	
server.performance.maxNetwo rkWritesPerSecondInKB	
server.performance.minFreeR AMInKB	
server.performance.numCores	
server.performance.numCpus	
server.performance.numDisks	
server.performance.numNetwo rkCards	
server.performance.totalRAMInKB	

Procesamiento de recursos

Campo	Obligatorio
process.commandLine	
process.configurationId	x
process.name	
process.path	
process.timeOfCreation	x

Recursos de aplicación

Campo	Obligatorio
application.configurationId	x
application.description	
application.lastModifiedTime	x
application.name	x
application.serverCount	x
application.timeOfCreation	x

Uso de la acción **ListConfigurations**

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
server.configurationId	x
server.agentId	
server.hostName	
server.osName	
server.osVersion	

Campo	Obligatorio
server.timeOfCreation	x
server.type	

Procesamiento de recursos

Campo	Obligatorio
process.commandLine	
process.configurationId	x
process.name	
process.path	
process.timeOfCreation	x
server.agentId	
server.configurationId	x

Recursos de aplicación

Campo	Obligatorio
application.configurationId	x
application.description	
application.name	x
application.serverCount	x
application.timeOfCreation	x
application.lastModifiedTime	x

Recursos de conexión

Campo	Obligatorio
connection.destinationIp	x
connection.destinationPort	x
connection.ipVersion	x
connection.latestTimestamp	x
connection.occurrence	x
connection.sourceIp	x
connection.transportProtocol	
destinationProcess.configurationId	
destinationProcess.name	
destinationServer.configurationId	
destinationServer.hostName	
sourceProcess.configurationId	
sourceProcess.name	
sourceServer.configurationId	
sourceServer.hostName	

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
`server.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• Cualquier ID de configuración de servidor válido	Ninguno
`server.hostName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	• ASC • DESC
`server.osName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	• ASC • DESC
`server.osVersion`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	• ASC • DESC
`server.agentId`	• EQUALS	• Cadena	Ninguno

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
	• NOT_EQUALS • EQ • NE		
`server.connectorId`	• EQUALS • NOT_EQUALS • EQ • NE	• Cadena	Ninguno
`server.type`	• EQUALS • NOT_EQUALS • EQ • NE	Cadena con uno de los siguientes valores: • EC2 • OTHER • VMWARE_VM • VMWARE_HOST • VMWARE_VM_TEMPLATE	Ninguno
`server.vmWareInfo.morefId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	Ninguno

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
`server.vmWareInfo.vcenterId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	Ninguno
`server.vmWareInfo.hostId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	Ninguno
`server.networkInterfaceInfo.portGroupId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	Ninguno
`server.networkInterfaceInfo.portGroupName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	Ninguno

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
`server.networkInterfaceInfo.virtualSwitchName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	Ninguno
`server.networkInterfaceInfo.ipAddress`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	Ninguno
`server.networkInterfaceInfo.macAddress`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	Ninguno
`server.performance.avgCpuUsagePct`	• GE • LE • GT • LT	• Porcentaje	Ninguno
`server.performance.totalDiskFreeSizeInKB`	• GE • LE • GT • LT	• Doble	Ninguno

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
`server.performance.avgFreeRAMInKB`	• GE • LE • GT • LT	• Doble	Ninguno
`server.tag.value`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	Ninguno
`server.tag.key`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	Ninguno
`server.application.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	Ninguno

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
`server.application.description`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	Ninguno
`server.application.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• Cualquier ID de configuración de aplicación válida	Ninguno
`server.process.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	Ninguno
`server.process.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	Ninguno
`server.process.commandLine`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	Ninguno

Recursos de aplicación

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
`application.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ApplicationId	Ninguno
`application.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	• ASC • DESC
`application.description`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	• ASC • DESC
`application.serverCount`	No se admite el filtrado.	No se admite el filtrado.	• ASC • DESC
`application.timeOfCreation`	No se admite el filtrado.	No se admite el filtrado.	• ASC • DESC

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
`application.lastModifiedTime`	No se admite el filtrado.	No se admite el filtrado.	• ASC • DESC
`server.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ServerId	Ninguno

Procesamiento de recursos

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
`process.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	
`process.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	• ASC • DESC
`process.commandLine`	• EQUALS • NOT_EQUALS • EQ • NE	• Cadena	• ASC • DESC

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
	• CONTAINS • NOT_CONTAINS		
`server.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ServerId	
`server.hostName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	• ASC • DESC
`server.osName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	• ASC • DESC
`server.osVersion`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	• ASC • DESC

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
`server.agentId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	

Recursos de conexión

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
`connection.sourceIp`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• IP	• ASC • DESC
`connection.destinationIp`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• IP	• ASC • DESC
`connection.destinationPort`	• EQUALS • NOT_EQUALS • EQ • NE	• Entero	• ASC • DESC

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
`sourceServer.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ServerId	
`sourceServer.hostName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	• ASC • DESC
`destinationServer.osName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	• ASC • DESC
`destinationServer.osVersion`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	• ASC • DESC

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
`destinationServer.agentId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	
`sourceProcess.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	
`sourceProcess.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	• ASC • DESC
`sourceProcess.commandLine`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	• ASC • DESC
`destinationProcess.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	

Filtro	Condiciones admitidas	Valores admitidos	Clasificación admitida
`destinationProcess.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	• ASC • DESC
`destinationprocess.commandLine`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Cadena	• ASC • DESC

Coherencia eventual en la AWS Application Discovery Service API

En última instancia, las siguientes operaciones de actualización son coherentes. Es posible que las actualizaciones no estén visibles inmediatamente en las operaciones de lectura StartExportTaskDescribeConfigurations, y ListConfigurations.

- AssociateConfigurationItemsToApplication
- CreateTags
- DeleteApplications
- DeleteTags
- DescribeBatchDeleteConfigurationTask
- DescribeImportTasks
- DisassociateConfigurationItemsFromApplication
- UpdateApplication

Sugerencias para gestionar la coherencia eventual:

- Cuando invoque las operaciones StartExportTaskde lectura 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. DescribeConfigurations Para ello, ejecute la operación de lectura varias veces, comenzando con un tiempo de espera de dos segundos y aumentando gradualmente hasta cinco minutos de espera.
- 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 retroceso exponencial comenzando con un par de segundos de tiempo de espera y aumente gradualmente hasta unos cinco minutos de tiempo de espera.

Acceso AWS Application Discovery Service mediante un punto final de interfaz (AWS PrivateLink)

Puede usarlo AWS PrivateLink para crear una conexión privada entre su VPC y. AWS Application Discovery Service Puede acceder a Application Discovery Service como si estuviera en su VPC, sin usar una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o AWS Direct Connect una conexión. Las instancias de su VPC no necesitan direcciones IP públicas para acceder a Application Discovery Service.

Esta conexión privada se establece mediante la creación de un punto de conexión de interfaz alimentado por AWS PrivateLink. Creamos una interfaz de red de punto de conexión en cada subred habilitada para el punto de conexión de interfaz. Se trata de interfaces de red administradas por el solicitante que sirven como punto de entrada para el tráfico destinado a Application Discovery Service.

Para obtener más información, consulte Acceso a los Servicios de AWS a través de AWS PrivateLink en la Guía de AWS PrivateLink .

Consideraciones sobre Application Discovery Service

Antes de configurar un punto final de interfaz para Application Discovery Service, consulte Acceder a un AWS servicio mediante un punto final de interfaz de VPC en la AWS PrivateLink Guía.

Application Discovery Service admite dos interfaces: una para realizar llamadas a todas sus acciones de API y otra para que Agentless Collector y AWS Application Discovery Agent envíen datos de descubrimiento.

Creación de un punto de conexión de interfaz

Puede crear un punto de conexión de interfaz mediante la consola de Amazon VPC o la AWS Command Line Interface (AWS CLI). Para obtener más información, consulte Acceder a un AWS servicio mediante un punto final de VPC de interfaz en la AWS PrivateLink Guía.

For Application Discovery Service

- Cree un punto final de interfaz para Application Discovery Service con el siguiente nombre de servicio:

```
com.amazonaws.region.discovery
```

Si habilita el DNS privado para el punto final de la interfaz, puede realizar solicitudes de API a Application Discovery Service con su nombre de DNS regional predeterminado. Por ejemplo, `discovery.us-east-1.amazonaws.com`.

For Agentless Collector and AWS Application Discovery Agent

Cree un punto final de interfaz con el siguiente nombre de servicio:

```
com.amazonaws.region.arsenal-discovery
```

Si habilita el DNS privado para el punto final de la interfaz, puede realizar solicitudes de API a Application Discovery Arsenal utilizando su nombre de DNS regional predeterminado. Por ejemplo, `arsenal-discovery.us-east-1.amazonaws.com`.

Creación de una política de puntos de conexión para el punto de conexión de interfaz

Una política de punto de conexión es un recurso de IAM que puede adjuntar al punto de conexión de su interfaz. La política de punto final predeterminada permite el acceso total a un AWS servicio a través del punto final de la interfaz. Para controlar el acceso permitido a un AWS servicio desde su VPC, adjunte una política de punto final personalizada al punto final de la interfaz.

Una política de punto de conexión especifica la siguiente información:

- Las entidades principales que pueden llevar a cabo acciones (Cuentas de AWS, usuarios de IAM y roles de IAM).
- Las acciones que se pueden realizar.

Para obtener más información, consulte Control del acceso a los servicios con políticas de punto de conexión en la Guía del usuario de AWS PrivateLink .

Ejemplo: políticas de puntos de conexión de VPC

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

Example policy for Application Discovery Service

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "discovery:action-1",
            "discovery:action-2",
            "discovery:action-3"
         ],
         "Resource":"*"
      }
   ]
}
```

Example policy for the Agentless Collector and AWS Application Discovery Agent

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "arsenal:RegisterOnPremisesAgent"
         ],
         "Resource":"*"
      }
   ]
}
```

Uso del punto final de VPC para el recopilador sin agente y el agente de descubrimiento de aplicaciones AWS

El recopilador sin agente y el agente de descubrimiento de AWS aplicaciones no admiten puntos de conexión configurables. En su lugar, utilice la función de DNS privado para el punto de `arsenal-discovery` conexión de Amazon VPC.

- Configure la tabla de AWS Direct Connect enrutamiento para enrutar las direcciones IP privadas de AWS a la VPC. Por ejemplo, destino = 10.0.0.0/8 y objetivo = local. Para esta configuración, necesita al menos enrutar las direcciones IP privadas del punto de enlace de `arsenal-discovery` Amazon VPC a la VPC.
- Utilice la función de DNS privado de punto final de `arsenal-discovery` Amazon VPC porque el recopilador sin agente no admite puntos de enlace de Arsenal configurables.
- Configure el punto de enlace de `arsenal-discovery` Amazon VPC en una subred privada con la misma VPC a la que va a enrutar el tráfico. AWS Direct Connect
- Configure el punto de enlace de `arsenal-discovery` Amazon VPC con un grupo de seguridad que permita el tráfico entrante desde la VPC (por ejemplo, 10.0.0.0/8).
- Configure una resolución de entrada de Amazon Route 53 para enrutar la resolución de DNS para el nombre de DNS privado del punto de enlace de VPC de `arsenal-discovery` Amazon, que se resolverá en la IP privada del punto de enlace de la VPC. Si no lo hace, el recopilador resolverá el DNS mediante la resolución local y utilizará el punto final público de Arsenal, y el tráfico no pasará por la VPC.
- Si tienes todo el tráfico público desactivado, la función de actualización automática fallará. Esto se debe a que el recopilador sin agente recupera las actualizaciones mediante el envío de solicitudes al punto de conexión de Amazon ECR. Para que la función de actualización automática funcione sin enviar solicitudes a través de la Internet pública, configure un punto de enlace de VPC para el servicio Amazon ECR y habilite la función de DNS privado para este punto de enlace.

Seguridad en AWS Application Discovery Service

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

La seguridad es una responsabilidad compartida entre usted 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 AWS los servicios en la AWS nube. AWS también le 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 AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Para utilizar AWS Application Discovery Agent o Application Discovery Service Agentless Collector, debe proporcionar las claves de acceso a su AWS cuenta. A continuación, 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

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

Temas

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 ayudarle a solicitar los permisos correctos al administrador. Si no puede acceder a una función de Application Discovery Service, consulteSolución 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. Luego, debe enviar solicitudes a su gestionador de IAM para cambiar los permisos de

los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con Application Discovery Service, consulte¿Cómo AWS Application Discovery Service funciona con IAM.

Administrador de IAM: si es administrador de IAM, puede que desee obtener más información sobre cómo redactar políticas para administrar el acceso a Application Discovery Service. Para ver ejemplos de políticas basadas en la identidad de Application Discovery Service que puede usar en 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 usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

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

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

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

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

Cuenta de AWS usuario root

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

Usuarios y grupos de IAM

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

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

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

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una persona determinada. Para asumir temporalmente un rol de IAM en el AWS Management Console, puede cambiar de un rol de usuario

a uno de IAM (consola). Puedes asumir un rol llamando a una operación de AWS API AWS CLI o usando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulta Métodos para asumir un rol en la Guía del usuario de IAM.

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

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

obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulta Reenviar sesiones de acceso.

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

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

Administración de acceso mediante políticas

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

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

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

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

Políticas basadas en identidades

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

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

Políticas basadas en recursos

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

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

Listas de control de acceso () ACLs

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

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

Otros tipos de políticas

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

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

del rol y las políticas de la sesión. Los permisos también puedes proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulta Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

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

¿Cómo AWS Application Discovery Service funciona con IAM

Antes de usar IAM para administrar el acceso a Application Discovery Service, debe comprender qué funciones de IAM están disponibles para su uso con Application Discovery Service. Para obtener una visión general de cómo funcionan Application Discovery Service y otros AWS servicios con IAM, consulte AWS Servicios que funcionan con IAM en la Guía del usuario de IAM.

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
- Funciones de IAM de Application Discovery Service

Políticas basadas en la identidad de Application Discovery Service

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. Application Discovery Service admite acciones, recursos y claves de condición específicos. Para obtener información sobre todos los elementos que utiliza en una política JSON, consulte Referencia de los elementos de las políticas JSON de IAM en la Guía del usuario de IAM.

Acciones

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

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

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

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 usuario de IAM.

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 usuario de IAM.

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.

Funciones de IAM de Application Discovery Service

Un rol de IAM 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 a servicios aparecen en la cuenta de IAM y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

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 funciones vinculadas 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 cuenta de IAM y son propiedad de la cuenta. Esto significa que un administrador de IAM 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 gestionada por 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 descripciones de las políticas de funciones de trabajo, consulte Políticas administradas de AWS para funciones de trabajo en la Guía del usuario de IAM.

AWS política gestionada: AWSApplication DiscoveryServiceFullAccess

La `AWSApplicationDiscoveryServiceFullAccess` política otorga a una cuenta de usuario de IAM acceso a Application Discovery Service y a Migration Hub APIs.

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: AWSApplication DiscoveryAgentlessCollectorAccess

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::446372222237: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: AWSApplication DiscoveryAgentAccess

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 Conceder acceso a los agentes de detección.

AWS política gestionada: AWSAgentless DiscoveryService

La `AWSAgentlessDiscoveryService` política otorga al conector de detección AWS sin agente 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 administrada: ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

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: AWSDiscovery ContinuousExportFirehosePolicy

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 Creación del rol de AWSApplicationDiscoveryServiceFirehose . Para obtener un ejemplo de esta política, consulte Otorgar permisos para la exploración de datos.

Creación del rol de 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. Elija 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 documentos para 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, los usuarios y roles de IAM no tienen permiso para crear o modificar los recursos de Application Discovery Service. Tampoco pueden realizar tareas mediante la AWS API AWS Management Console AWS CLI, o. Un administrador de IAM debe crear políticas de IAM que concedan permisos a los usuarios y a los roles para realizar operaciones de la API concretas en los recursos especificados que necesiten. El administrador debe adjuntar esas políticas a los usuarios o grupos de IAM que necesiten esos permisos.

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

Temas

- Prácticas recomendadas relativas a políticas
- Concesión de acceso completo a Application Discovery Service
- Conceder 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 relativas a 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 avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulta las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se puedes llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulta Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utiliza condiciones en las políticas de IAM para restringir aún más el acceso: puedes agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puedes escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulta Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

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

Concesión de acceso completo a Application Discovery Service

La política AWSApplication DiscoveryServiceFullAccess gestionada concede a la cuenta de usuario de IAM acceso a Application Discovery Service y a Migration Hub APIs.

Un usuario de IAM con esta política asociada a su cuenta 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 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": "*"
        }
    ]
}
```

Conceder acceso a los agentes de detección

La política AWSApplication DiscoveryAgentAccess 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 AWSApplicationDiscoveryAgentAccess Política

```
{
    "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 AWSDiscovery ContinuousExportFirehosePolicy 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 Creación del rol de 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 hacerlo`discovery:*`.

En el siguiente ejemplo, se muestra cómo utilizar la `discovery:GetNetworkConnectionGraph` acción en una política de IAM.

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 funciones vinculadas a servicios para Application Discovery Service

AWS Application Discovery Service utiliza funciones vinculadas al AWS Identity and Access Management servicio (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Application Discovery Service. Application Discovery Service predefine las funciones vinculadas al servicio e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Un rol vinculado a un servicio facilita la configuración de Application Discovery Service porque no es necesario agregar manualmente los permisos necesarios. Application Discovery Service define los permisos de sus funciones vinculadas a servicios y, a menos que se defina lo contrario, solo Application Discovery Service puede asumir sus funciones. 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 es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. Esto protege los recursos de Application Discovery Service porque no puede eliminar inadvertidamente el permiso de acceso a los recursos.

Temas

- Permisos de rol vinculados a servicios para Application Discovery Service
- Creación de un rol vinculado a un servicio para Application Discovery Service
- Eliminar un rol vinculado a un servicio para Application Discovery Service

Para obtener información acerca de otros servicios que son compatibles con 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). Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

Permisos de rol vinculados a servicios para Application Discovery Service

Application Discovery Service utiliza el rol vinculado al servicio denominado AWSServiceRoleForApplicationDiscoveryServiceContinuousExport: Permite el acceso a AWS los servicios y recursos utilizados o administrados por. AWS Application Discovery Service

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

- `continuousexport.discovery.amazonaws.com`

La política de permisos de roles permite a Application Discovery Service realizar las siguientes acciones:

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 función AWSService RoleForApplicationDiscoveryServiceContinuousExport vinculada al servicio se crea automáticamente cuando la exportación continua se activa implícitamente al: a) confirmar las opciones del cuadro de diálogo que se presenta en la página de recopiladores de datos después de seleccionar «Iniciar la recopilación de datos», o hacer clic en el control deslizante denominado «Exploración de datos en Athena», o b) cuando se llama a la API mediante la CLI. StartContinuousExport AWS

> **Important**
>
> Este rol vinculado a servicios 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.

Crear el rol vinculado al servicio desde la consola de Migration Hub

Puede usar la consola de Migration Hub para crear el rol AWSService RoleForApplicationDiscoveryServiceContinuousExport vinculado al servicio.

Para crear la función vinculada al servicio (consola)

1. En el panel de navegación, elija Data Collectors (Recopiladores de datos).
2. Elija la pestaña Agentes.
3. Mueva el control deslizante Exploración de datos en Athena a la posición Activada.
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).

Crear el rol vinculado al servicio a partir del AWS CLI

Puede utilizar los comandos de Application Discovery Service desde el AWS Command Line Interface para crear el rol AWSService RoleForApplicationDiscoveryServiceContinuousExport vinculado al servicio.

Esta función vinculada al servicio se crea automáticamente al iniciar la exportación continua desde el AWS CLI (primero AWS CLI debe instalarse en su entorno).

Para crear el rol vinculado al servicio (CLI) iniciando la exportación continua desde el AWS CLI

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. 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 el caso práctico Discovery Service: Continuous Export. 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 Creación de 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.

Eliminar un rol vinculado a un servicio para Application Discovery Service

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le 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 del rol vinculado al servicio de

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 utiliza el rol al intentar eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos de Application Discovery Service utilizados por el rol AWSService RoleForApplicationDiscoveryServiceContinuousExport vinculado al servicio de la consola de Migration Hub

1. En el panel de navegación, elija Data Collectors (Recopiladores de datos).
2. Elija la pestaña Agentes.
3. Mueva el control deslizante Exploración de datos en Athena a la posición Desactivada.

Para eliminar los recursos de Application Discovery Service utilizados por el rol AWSService RoleForApplicationDiscoveryServiceContinuousExport vinculado al servicio del AWS CLI

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. 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 comprobando que su estado de devolución es «INACTIVO»:

```
aws discovery describe-continuous-export
```

Eliminación manual de un rol vinculado a servicios

Puede eliminar el rol AWSService RoleForApplicationDiscoveryServiceContinuousExport vinculado al servicio mediante la consola de IAM, la CLI de IAM o la API de IAM. Si ya no necesita usar las funciones Discovery Service: Continuous Export que requieren esta función vinculada al servicio, le recomendamos que la elimine. Así no tendrá una entidad no utilizada que no se supervise 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 del rol vinculado al servicio de .

Solución de problemas AWS Application Discovery Service de identidad y acceso

Utilice la siguiente información como ayuda para diagnosticar y solucionar problemas comunes que pueden surgir al trabajar con Application Discovery Service e IAM.

Temas

No estoy autorizado a realizar la 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.

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

El siguiente ejemplo de error se produce cuando un usuario de IAM 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 el AWS administrador. El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

Registro de llamadas a la API Application Discovery Service con AWS CloudTrail

AWS Application Discovery Service está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Application Discovery Service. Se puede utilizar CloudTrail para registrar, supervisar de forma continua y conservar la actividad de la cuenta con fines de solución de problemas y auditoría. CloudTrail proporciona un historial de eventos de la actividad de su AWS cuenta, incluidas las acciones realizadas a través AWS de la consola de administración y las herramientas de línea de comandos. AWS SDKs

CloudTrail captura todas las llamadas a la API de Application Discovery Service como eventos. Las llamadas capturadas incluyen llamadas desde la consola de Application Discovery Service y llamadas de código a las operaciones de la API de Application Discovery Service.

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

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

Información de Application Discovery Service en CloudTrail

CloudTrail está activado en su AWS cuenta al crear la cuenta. Cuando se produce una actividad en Application Discovery Service, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los eventos recientes en su AWS cuenta. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para obtener un registro continuo de los eventos de su AWS cuenta, incluidos los eventos de Application Discovery Service, cree un registro. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando crea una ruta en la consola, la ruta se aplica a todas AWS las regiones. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos que se

recopilan en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

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

Todas las acciones de Application Discovery Service se registran CloudTrail y se documentan en la referencia de la API de Application Discovery Service. Por ejemplo, las llamadas a las `CreateTags` `GetDiscoverySummary` acciones y las llamadas generan entradas en los archivos de CloudTrail registro. `DescribeTags`

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

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

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

Descripción de las entradas del archivo de registro de Application Discovery Service

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

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

```
{
    "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"
}
```

AWS Application Discovery Service Formatos ARN

Un nombre de recurso de Amazon (ARN) es una cadena que identifica un recurso de forma exclusiva. AWS AWS requiere un ARN cuando se quiere especificar un recurso de forma inequívoca en todos los. AWS AWS Application Discovery Service define lo siguiente. ARNs

- Agente de detección: `arn:aws:discovery:region:account:agent/discovery-agent/agentId`
- Coleccionista sin agente: `arn:aws:discovery:region:account:agent/agentless-collector/agentId`
- Recopilador de evaluadores de migración: `arn:aws:discovery:region:account:agent/migration-evaluator-collector/agentId`
- Conector Discovery: `arn:aws:discovery:region:account:agent/discovery-connector/agentId`

AWS Application Discovery Service Cuotas

La consola Service Quotas proporciona información sobre AWS Application Discovery Service las cuotas. Puede utilizar la consola Service Quotas para consultar las cuotas de servicio predeterminadas o para solicitar aumentos de cuota para las cuotas ajustables.

Actualmente, la única cuota que se puede aumentar son los servidores importados por cuenta.

Application Discovery Service tiene las siguientes cuotas predeterminadas:

- 1000 aplicaciones por cuenta.

  Si alcanzas esta cuota y quieres importar nuevas aplicaciones, puedes eliminar las aplicaciones existentes con la acción de la `DeleteApplications` API. Para obtener más información, consulte la referencia DeleteApplicationsde la API de Application Discovery Service.
- Cada archivo de importación puede tener un tamaño máximo 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 un aumento de esta cuota).
- 1000 agentes activos, que recopilan y envían datos a Application Discovery Service.
- 10 000 agentes inactivos, que responden pero 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

Para detener la exploración de datos, puede desactivar el conmutador de la consola de Migration Hub, en la pestaña Discover > Data Collectors > Agents, o invocar la `StopContinuousExport` API. La recopilación de datos puede tardar hasta 30 minutos en detenerse y, durante esta etapa, el interruptor de la consola y la invocación a la `DescribeContinuousExport` API mostrarán el estado de exploración de datos como «Parada en curso».

> **Note**
>
> Si después de actualizar la página de la consola, el conmutador no se desactiva y aparece un mensaje de error, o la API `DescribeContinuousExport` devuelve el estado "Stop_Failed", puede volver a intentarlo desactivando el conmutador o llamando a la API `StopContinuousExport`. 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 completado la detección con agentes de ADS y ya no quiere recopilar datos adicionales en el repositorio de base de datos de ADS:

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).

   De este modo, se asegurará de que los agentes no recopilen nuevos datos en el repositorio de datos de ADS y en su bucket 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 datos de ADS, pero no quiere recopilar datos 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-discover-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 eliminados 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 agentes de ADS 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 la exploración de datos AWS Glue Data Catalog 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 inicia 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 para 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.

- Sus servidores locales

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 usuario de IAM 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 AWS Application Discovery Service Cuotas.

- Se insertó una coma adicional (,) en el archivo de importación. Las comas de los archivos.CSV 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, para resolverlo puede descargar los registros con error para la tarea de importación, resolver los errores en el archivo CSV de entradas con error 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 enhttps://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 texto de URL y pulse `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, usa `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 Importar datos.

Historial de documentos para 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 los cambios importantes en la Guía del usuario de Application Discovery Service después del 18 de enero de 2019. Para obtener notificaciones sobre las actualizaciones de la documentación, puede suscribirse a la fuente RSS.

Cambio	Descripción	Fecha
Transición de Discovery Connector a Agentless Collector	Recomendamos que los clientes que utilizan Discovery Connector actualmente hagan la transición al nuevo recopilador sin agente. A partir del 17 de noviembre de 2025, AWS Application Discovery Service dejarán de aceptar nuevos datos de Discovery Connectors. Para obtener más información, consulte Discovery Connector.	12 de noviembre de 2024
Publicó el módulo de recopilación de datos en red Agentless Collector	El módulo de recopilación de datos de red le permite descubrir las dependencias entre los servidores de su centro de datos local. Para obtener más información, consulte Uso del módulo de recopilación de datos de red Agentless Collector.	8 de noviembre de 2024

Support para la recopilación sin agentes para el mapeo de dependencias	Para obtener más información, consulte Uso del módulo de recopilación de datos de VMware vCenter Agentless Collector.	24 de octubre de 2024
Publicada la versión 2 de Agentless Collector basada en Amazon Linux 2023	Para obtener más información, consulte Requisitos previos para Agentless Collector.	26 de septiembre de 2024
Se actualizaron los requisitos previos de Agentless Collector	Para obtener más información, consulte Requisitos previos de Agentless Collector.	9 de septiembre de 2024
Coherencia eventual en la API	Para obtener más información, consulte Coherencia eventual en la AWS Application Discovery Service API.	20 de junio de 2024
Actualizaciones de Agentless Collector	Hemos añadido dominios `sts.amazonaws.com` a las listas de dominios que requieren acceso saliente. Para obtener más información, consulte Configurar el firewall para el acceso saliente a los dominios de AWS.	20 de junio de 2024
Para separar el acceso, cree y utilice cuentas de AWS independientes.	Para obtener más información, consulte Acciones, recursos y claves de condición de AWS Application Discovery Service.	5 de abril de 2024

Presentamos la base de datos Agentless Collector y el módulo de recopilación de datos analíticos	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 usar 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 a través de métodos sin agente sobre su entorno local para ayudarlo a planificar eficazmente su migración al. Nube de AWSPara obtener más información, consulte Agentless Collector.	16 de agosto de 2022

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 la identidad. 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, consulte Migration Hub Import.	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 facilitar 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	AWS Management Console Se agregó el.	19 de diciembre de 2016
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 Guía del usuario de Application Discovery Service.	12 de mayo de 2016

AWS Glosario

Para obtener la AWS terminología más reciente, consulte el AWS glosario de la Glosario de AWS Referencia.

Conector Discovery

> **Important**
>
> Recomendamos que los clientes que utilizan Discovery Connector actualmente hagan la transición al nuevo recopilador sin agente. A partir del 17 de noviembre de 2025, AWS Application Discovery Service dejarán de aceptar nuevos datos de Discovery Connectors.

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. Recopilador sin agente de Application Discovery Service

Tras implementar 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).

Recopilación de datos con el Discovery Connector

> **Important**
>
> Recomendamos que los clientes que utilizan Discovery Connector actualmente hagan la transición al nuevo recopilador sin agente. A partir del 17 de noviembre de 2025, AWS Application Discovery Service dejarán de aceptar nuevos datos de Discovery Connectors. Para obtener más información, consulte Conector Discovery.

El Discovery Connector recopila información sobre los hosts de VMware vCenter Server y. VMs Sin embargo, solo puede capturar estos datos si las herramientas de VMware vCenter Server están instaladas. Para asegurarse de que la AWS cuenta que está utilizando tiene los permisos necesarios para esta tarea, consulteAWS 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
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

Campo de datos	Descripción
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
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

Campo de datos	Descripción
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 (especifi cado 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
osVersion	Versión del sistema operativo en la máquina virtual
portGroupId*	ID de grupo de puertos miembro de VLAN
portGroupName*	Nombre del grupo de puertos miembro de VLAN

Campo de datos	Descripción
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 VMware las herramientas (consulte Ordenar los recopiladores de datos en la AWS Migration Hub consola para obtener 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
vmFolderPath	Ruta de directorio de los archivos de la máquina virtual
vmName	Nombre de la máquina virtual

Recoja datos de Discovery Connector

Después de implementar y configurar el Discovery Connector en su VMware entorno, puede reiniciar las recopilaciones de datos si se detiene. 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 la recopilación de datos 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

> **Important**
>
> Recomendamos a los clientes que utilizan Discovery Connector actualmente que hagan la transición al nuevo recopilador sin agente. A partir del 17 de noviembre de 2025, AWS Application Discovery Service dejarán de aceptar nuevos datos de Discovery Connectors. Para obtener más información, consulte Conector Discovery.

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. Abre 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 conectorhttps://*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` `otraceroute`, 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 version original de inglés, prevalecerá la version en inglés.