aws

用户指南

AWS Application Discovery

AWS Application Discovery: 用户指南

Table of Contents

什么是 AWS Application Discovery Service？

AWS Application Discovery Service 通过收集有关本地服务器和数据库的使用情况和配置数据，帮助您规划向 AWS 云的迁移。Application Discovery Service AWS Migration Hub 与 AWS Database Migration Service 舰队顾问集成。Migration Hub 可将您的迁移状态信息聚合到单个控制台中，从而简化您的迁移跟踪。您可以查看发现的服务器，将它们分组为应用程序，然后从您所在地区的 Migration Hub 控制台跟踪每个应用程序的迁移状态。您可以使用 DMS 队列顾问来评估数据库工作负载的迁移选项。

所有发现的数据都存储在您的 AWS Migration Hub 家乡地区。因此，在执行任何发现和迁移活动之前，必须在 Migration Hub 控制台中或使用 CLI 命令设置主区域。您的数据可以导出到微软 Excel 或 AWS 分析工具（例如亚马逊 Athena 和亚马逊）中进行分析。 QuickSight

使用 Application APIs Discovery Service，您可以导出所发现服务器的系统性能和利用率数据。将此数据输入到您的成本模型中，以计算在中运行这些服务器的成本 AWS。此外，您还可以导出有关服务器之间存在的网络连接的数据。该信息可帮助您确定服务器之间的网络依赖关系，并将服务器分组到应用程序中以进行迁移规划。

> **Note**
>
> 在开始发现过程 AWS Migration Hub 之前，必须先设置您的居住区域，因为您的数据将存储在您的家乡区域。有关使用家庭区域的更多信息，请参阅家庭区域。

Application Discovery Service 提供了三种执行发现和收集本地服务器数据的方式：

- 通过您的 vCenter 部署 Application Discovery Service 无代理收集器（无代理收集器）（OVA 文件），可以执行无代理发现。 VMware 配置无代理收集器后，它会识别与 vCenter 关联的虚拟机 (VMs) 和主机。Agentless Collector 收集以下静态配置数据：服务器主机名、IP 地址、MAC 地址、磁盘资源分配、数据库引擎版本和数据库架构。此外，它还收集每个虚拟机和数据库的利用率数据，提供 CPU、RAM 和磁盘 I/O 等指标的平均和峰值利用率。
- 通过在每台服务器 VMs 和物理服务器上部署 AWS 应用程序发现代理（Discovery Agent），可以执行@@ 基于代理的发现。代理安装程序适用于 Windows 和 Linux 操作系统。它收集静态配置数据、详细的时间序列系统性能信息、入站和出站网络连接以及正在运行的进程。
- 基于文件的导入允许您直接将本地环境的详细信息导入到 Migration Hub 中，无需使用无代理收集器或 Discovery Agent，因此您可以直接使用导入的数据进行迁移评估和规划。摄取的数据取决于所提供的数据。

Application Discovery Service 与 AWS 合作伙伴网络 (APN) 合作伙伴提供的应用程序发现解决方案集成。这些第三方解决方案可以帮助您将本地环境的详细信息直接导入到 Migration Hub 中，无需使用任何无代理收集器或发现代理。第三方应用程序发现工具可以查询 AWS Application Discovery Service，也可以使用公共 API 写入应用程序发现服务数据库。通过这种方式，您可以将数据导入到 Migration Hub 来查看它，以便将应用程序与服务器关联并跟踪迁移。

VMware 发现

如果您有在 VMware vCenter 环境中运行的虚拟机 (VMs)，则可以使用无代理收集器收集系统信息，而不必在每台虚拟机上安装代理。相反，您可以将此本地设备加载到vCenter中，并允许它发现其所有主机和。 VMs

无论使用什么操作系统，无代理收集器都会捕获在 vCenter 中运行的每台虚拟机的系统性能信息和资源利用率。但是，它不能 “向内看” 每个虚拟机 VMs，因此无法弄清楚每个虚拟机上正在运行哪些进程，也无法弄清楚存在哪些网络连接。因此，如果您需要这种级别的详细信息并想仔细查看现有 VMs 的一些细节以帮助规划迁移，则可以根据需要安装 Discovery Agent。

此外，对于 VMs 托管在 VMware，您可以同时使用无代理收集器和发现代理来同时执行发现。有关每个发现工具将收集的确切数据类型的详细信息，请参阅使用 VMware vCenter 无代理收集器数据收集模块。

数据库发现

如果您的本地环境中有数据库和分析服务器，则可以使用无代理收集器来发现和清点这些服务器。然后，您可以收集每台数据库服务器的性能指标，而无需在环境中的每台计算机上安装 Agentless Collector。

Agentless Collector 数据库和分析数据收集模块可捕获元数据和性能指标，从而深入了解您的数据基础架构。数据库和分析数据收集模块使用 Microsoft Active Directory 中的 LDAP 来收集有关网络中操作系统、数据库和分析服务器的信息。然后，数据收集模块会定期运行查询，以收集数据库和分析服务器的 CPU、内存和磁盘容量的实际利用率指标。有关收集的指标的详细信息，请参阅数据库和分析模块收集的数据。

在 Agentless Collector 完成从您的环境中收集数据后，您可以使用 AWS DMS 控制台进行进一步分析和规划迁移。例如，要在中选择最佳迁移目标 AWS Cloud，您可以为源数据库生成目标建议。有关更多信息，请参阅 使用数据库和分析数据收集模块。

比较无代理收集器和发现代理

下表简要比较了 Application Discovery Service 支持的数据收集方法。

	无代理收集器	发现代理	Migration Hub 模板	RVTools 出口
Supported server types				
VMware 虚拟机	支持	是	是	是
物理服务器	否	是	是	是
Deployment				
每服务器	否	是	不适用	否
每 vCenter	是	否	不适用	是
同一网络上的每个数据中心	否	否	不适用	否
Collected data				
服务器配置文件（静态配置）数据	支持	是	是	是
来自虚拟机管理程序的服务器利用率指标（CPU、RAM 等）	支持	是	是	否
来自服务器的服务器利用率指标（CPU、RAM 等）	支持	是	是	否

	无代理收集器	发现代理	Migration Hub 模板	RVTools 出口
服务器网络连接（仅限 TCP）	支持	是	否	否
运行的进程	否	是	否	否
收集间隔	-60 分钟	-15 秒	单张快照	单张快照
Server data use cases				
在 Migration Hub 中查看服务器数据	支持	是	仅限个人资料	否
根据服务器配置文件生成 Amazon EC2 推荐	支持	是	是	是
根据使用率数据生成 Amazon EC2 建议	支持	是	是	否
导出最新的利用率快照数据	支持	是	是	否
导出时间序列利用率数据	否	是	否	否
Network data use cases				
Migration Hub 中的可视化	支持	是	否	否
导出到亚马逊 Athena 以供进一步探索	否	是	否	否

	无代理收集器	发现代理	Migration Hub 模板	RVTools 出口
导出到 CSV 文件	否	是	否	否
Database use cases				
数据库服务器配置文件（静态配置）数据	是	否	否	否
支持的数据库引擎	甲骨文、SQL Server、My SQL、Postg reSQL	无	无	无
数据库架构的复杂性和重复性	是	否	否	否
数据库架构对象	是	否	否	否
Platform support				
支持的操作系统	在 c VMware enter v5.5 或更高版本中运行的任何操作系统	任何 Linux 或 Windows 服务器	任何 Linux 或 Windows 服务器	任何 Linux 服务器、Windows 服务器或 VMware v5.5 或更高版本

假设

要使用 Application Discovery Service，需要满足以下条件：

- 你已经注册了 AWS。有关更多信息，请参阅 设置应用程序 Discovery Service。
- 您已经选择了 Migration Hub 的主区域。有关更多信息，请参阅有关主区域的文档。

以下是将要出现的情况：

- Migration Hub 主区域是 Application Discovery Service 存储您的发现和规划数据的唯一区域。

- 发现代理、连接器和导入只能在您选择的 Migration Hub 主区域中使用。
- 有关可以在其中使用 Application Discovery Service 的 AWS 区域列表，请参阅Amazon Web Services 一般参考。

设置应用程序 Discovery Service

在 AWS Application Discovery Service 首次使用之前，请完成以下任务：

注册 Amazon Web Services

创建 IAM 用户

登录 Migration Hub 控制台并选择主区域

注册 Amazon Web Services

如果您没有 AWS 账户，请完成以下步骤来创建一个。

要注册 AWS 账户

1. 打开https://portal.aws.amazon.com/billing/注册。
2. 按照屏幕上的说明操作。

   在注册时，将接到电话或收到短信，要求使用电话键盘输入一个验证码。

   当您注册时 AWS 账户，就会创建AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务 和资源。作为最佳安全实践，请为用户分配管理访问权限，并且只使用根用户来执行需要根用户访问权限的任务。

创建 IAM 用户

创建 AWS 账户时，您将获得一个单一登录身份，该身份可以完全访问该账户中的所有 AWS 服务和资源。此身份称为 AWS 账户根用户。 AWS Management Console 使用创建账户时使用的电子邮件地址和密码登录，即可完全访问账户中的所有 AWS 资源。

强烈建议您不 使用根用户执行日常任务，即使是管理任务。相反，请按照安全最佳实践创建个人 IAM 用户并创建 AWS Identity and Access Management (IAM) 管理员用户。然后请妥善保存根用户凭证，仅用它们执行少数账户和服务管理任务。

除了创建管理用户外，您还需要创建非管理 IAM 用户。以下主题说明如何创建这两种类型的 IAM 用户。

主题

创建 IAM 管理用户

默认情况下，管理员帐户会继承访问 Application Discovery Service 所需的所有策略。

创建管理员用户

- 在您的 AWS 账户中创建管理员用户。有关说明，请参考《IAM 用户指南》中的创建您的第一个 IAM 用户和管理员组。

创建 IAM 非管理员用户

创建非管理型 IAM 用户时，请遵循安全最佳实践 “授予最低权限”，向用户授予最低权限。

使用 IAM 托管策略定义非管理型 IAM 用户对 Application Discovery Service 的访问级别。有关 Application Discovery Service 托管策略的信息，请参见AWS 的托管策略 AWS Application Discovery Service。

创建非管理员 IAM 用户

1. 在中 AWS Management Console，导航到 IAM 控制台。
2. 按照 IAM 用户指南中在您的 AWS 账户中创建 IAM 用户中所述的使用控制台创建用户的说明创建非管理员 IAM 用户。

   按照 IAM 用户指南中的说明进行操作时：

   - 在关于选择访问类型的步骤中，选择编程访问权限。请注意，虽然不建议这样做，但只有当您计划使用相同的 IAM 用户证书访问控制台时，才选择AWS 管理 AWS 控制台访问权限。
   - 在 “设置权限” 页面的步骤中，选择 “将现有策略直接附加到用户” 选项。然后从策略列表中为 Application Discovery Service 选择托管 IAM 策略。有关 Application Discovery Service 托管策略的信息，请参见AWS 的托管策略 AWS Application Discovery Service。
   - 在查看用户的访问密钥（访问密钥 IDs 和私有访问密钥）时，请按照重要说明中的指导进行操作，将用户的新访问密钥 ID 和私有访问密钥保存在安全可靠的地方。

登录 Migration Hub 控制台并选择主区域

你需要在用于的 AWS 账户中选择一个 AWS Migration Hub 居住区域 AWS Application Discovery Service。

选择主区域

1. 使用您的 AWS 账户，登录 AWS Management Console 并打开 Migration Hub 控制台，网址为https://console.aws.amazon.com/migrationhub/。
2. 在 Migration Hub 控制台导航窗格中，选择设置，然后选择主区域。

   您的 Migration Hub 数据存储在您的家乡地区，用于发现、规划和迁移跟踪。有关更多信息，请参阅 Migr ation Hub 主区域。

AWS 应用程序发现代理

AWS 应用程序发现代理（Discovery Agent）是安装在本地服务器上并以发现和迁移为 VMs目标的软件。代理将捕获系统配置、系统性能、运行中的进程以及系统之间网络连接的详细信息。代理支持大多数 Linux 和 Windows 操作系统，您可以将其部署在物理本地服务器、Amazon EC2 实例和虚拟机上。

> **Note**
>
> 在部署 Discovery Agent 之前，必须选择一个 Migr ation Hub 主区域。您必须在您所在的地区注册您的代理人。

Discovery Agent 在您的本地环境中运行，并且需要 root 权限。当你启动 Discovery Agent 时，它会安全地连接到你的家乡并在 Application Discovery Service 中注册。

- 例如，如果`eu-central-1`是您的家乡区域，则它会向 Application Discovery `arsenal-discovery.`*`eu-central-1`*`.amazonaws.com` Service 注册。
- 或者根据需要用您的家乡地区代替除 us-west-2 之外的所有其他区域。
- 如果`us-west-2`是您的家乡区域，则它会向 Application Discovery `arsenal.us-west-2.amazonaws.com` Service 注册。

工作方式

注册后，代理开始为其所在的主机或虚拟机收集数据。代理每隔 15 分钟向 Application Discovery Service 发送一次请求以获取配置信息。

收集的数据包括系统规格、时间序列利用率或性能数据、网络连接和进程数据。您可以使用此信息映射 IT 资产及其网络依赖关系。所有这些数据点都可以帮助您确定在中运行这些服务器的成本 AWS 并规划迁移。

Discovery 代理使用传输层安全 (TLS) 加密将数据安全地传输到 Application Discovery Service。代理配置为在新版本可用时自动进行升级。您可以按需更改此配置设置。

> **Tip**
>
> 在下载并开始安装 Discovery Agent 之前，请务必通读中所有必需的先决条件 发现代理的先决条件

发现代理收集的数据

AWS 应用程序发现代理（Discovery Agent）是安装在本地服务器上的软件，并且 VMs。Discovery Agent 收集系统配置、时序利用率或性能数据、过程数据和传输控制协议 (TCP) 网络连接。本节描述了所收集的数据。

Discovery Agent 收集的数据的表格图例：

- 术语“主机”是指物理服务器或 VM。
- 除非另有说明，否则收集的数据以千字节 (KB) 为度量单位。
- Migration Hub 控制台中的等效数据以兆字节 (MB) 为单位报告。
- 轮询周期间隔约为 15 秒， AWS 每 15 分钟发送一次。
- 以星号 (*) 表示的数据字段仅在代理的 API 导出功能生成的`.csv`文件中可用。

数据字段	描述
agentAssignedProcess身份证 *	代理所发现的进程的进程 ID
agentId	代理的唯一 ID
agentProvidedTime邮票 *	代理人观察的日期和时间 (mm/dd/yyyy hh:mm:ss am/pm)
cmdLine*	在命令行上输入的进程
cpuType	主机中使用的 CPU (中心处理单元) 的类型
destinationIp*	要将数据包发送到的设备的 IP 地址
destinationPort*	要将数据/请求发送到的端口号
系列*	路由协议系列
freeRAM (MB)	可以立即提供给应用程序使用的可用 RAM 和缓存的 RAM（度量单位为 MB）
gateway*	网络的节点地址

数据字段	描述
hostName	在其上收集数据的主机的名称
hypervisor	管理程序的类型
ipAddress	主机的 IP 地址
ipVersion*	IP 版本号
isSystem*	用于指示进程由操作系统拥有的布尔属性
macAddress	主机的 MAC 地址
name*	要为其收集数据的主机的名称、网络、指标等
netMask*	网络主机所属的 IP 地址前缀
osName	主机上的操作系统名称
osVersion	主机上的操作系统版本
path	来自命令行的命令的路径
sourceIp*	正在发送 IP 数据包的设备的 IP 地址
sourcePort*	发出数据/请求的端口号
timestamp*	由代理记录的已报告属性的日期和时间
totalCpuUsagePct	轮询期间主机上的 CPU 使用率的百分比
totalDiskBytesReadPerSecond (Kbps)	所有磁盘每秒读取的总千位数
totalDiskBytesWrittenPerSecond (Kbps)	所有磁盘上每秒写入的总千位数
totalDiskFree大小 (GB)	以 GB 表示的可用磁盘空间
totalDiskReadOpsPerSecond	每秒的读取 I/O 操作总数
totalDiskSize (GB)	以 GB 表示的磁盘的总容量

数据字段	描述
totalDiskWriteOpsPerSecond	每秒的写入 I/O 操作总数
totalNetworkBytesReadPerSecond (Kbps)	每秒读取的字节的总吞吐量
totalNetworkBytesWrittenPerSecond (Kbps)	每秒写入的字节的总吞吐量
totalNumCores	CPU 内的独立处理单元总数
totalNumCpus	中心处理单元的总数
totalNumDisks	主机上的物理硬盘数
totalNumLogical处理器 *	物理内核数乘以每个内核上可运行的线程数的总数
totalNumNetwork卡片	服务器上的网卡总数
totalRAM (MB)	主机上的可用 RAM 的总量
transportProtocol *	所用传输协议的类型

发现代理的先决条件

以下是成功安装 AWS 应用程序发现代理（Discovery Agent）之前必须执行的先决条件和任务。

- 在开始安装 Discovery Agent 之前，必须设置AWS Migration Hub 主区域。
- 如果您已安装 1.x 版本的代理，则在安装最新版本之前，必须先删除此版本。
- 如果安装代理的主机运行的是 Linux，请确认该主机至少支持英特尔 i686 CPU 架构（也称为 P6 微架构）。
- 验证您的操作系统 (OS) 环境受支持：

  Linux

  Amazon Linux 2012.03、2015.03

  Amazon Linux 2（9/25/2018 更新和更高版本）

  Ubuntu 12.04、14.04、16.04、18.04、20.04

  Red Hat Enterprise Linux 5.11、6.10、7.3、7.7、8.1

CentOS 5.11、6.9、7.3

SUSE 11 SP4、12 SP5、15 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

- 如果网络出站连接受限，则需要更新防火墙设置。代理要求通过 TCP 端口 443 访问 `arsenal`。它们不要求打开任何入站端口。

  例如，如果你的家乡区域是`eu-central-1`，你可以使用 `https://arsenal-discovery.eu-central-1.amazonaws.com:443`
- 自动升级需要访问您所在地区的 Amazon S3 才能正常运行。
- 在控制台中创建 AWS Identity and Access Management (IAM) 用户并附加现有的 `AWSApplicationDiscoveryAgentAccess` IAM 托管策略。此策略允许用户代表您执行必要的代理操作。有关托管策略的更多信息，请参阅AWS 的托管策略 AWS Application Discovery Service。
- 检查与网络时间协议 (NTP) 服务器的时间偏移，必要时进行更正。不正确的时间同步会导致代理注册调用失败。

> **Note**
>
> Discovery Agent 具有 32 位代理可执行文件，可在 32 位和 64 位操作系统上运行。拥有单个可执行文件将减少部署所需的安装包数量。此可执行代理适用于 Linux 和 Windows 操作系统。随后的相应安装部分中对此进行了介绍。

安装发现代理

本页介绍如何在 Linux 和微软 Windows 上安装 Discovery 代理。

在 Linux 上安装发现代理

请在 Linux 上完成以下过程。在开始此过程之前，请确保已设置好您的 Migration Hub 主区域。

> **Note**
>
> 如果使用的不是最新 Linux 版本，请参阅旧版 Linux 平台的注意事项。

在您的数据中心安装 AWS 应用程序发现代理

1. 登录基于 Linux 的服务器或 VM，然后创建一个包含代理组件的新目录。
2. 切换到该新目录并通过命令行或控制台下载安装脚本。

   a. 要通过命令行下载，请运行以下命令。

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

   b. 要从 Migration Hub 控制台下载，请执行以下操作：

      i. 登录 AWS Management Console 并打开 Migration Hub 控制台，网址为https://console.aws.amazon.com/migrationhub/。

      ii. 在左侧导航页的 “发现” 下，选择 “工具”。

      iii. 在 “AWS 发现代理” 框中，选择 “下载代理”，然后选择 “下载 Linux 版”。下载将立即开始。

3. 使用下面三个命令验证安装包的加密签名：

   ```
   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
   ```

   代理公有密钥 (discovery.gpg) 指纹为 7638 F24C 6717 F97C 4F1B 3BC0 5133 255E 4DF4 2DA2。

4. 从 tarball 中进行提取，如下所示。

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

5. 要安装代理，请选择以下安装方法之一。

要……	请执行此操作...
安装发现代理	要安装代理，请运行代理安装命令，如以下示例所示。在示例中，*your-home-region* 替换为您所在地区的名称、*aws-access-key-id*访问密钥 ID 和您的私*aws-secret-access-key* 有访问密钥。 `sudo bash install -r your-home-region -k aws-access-key-id -s aws-secret-access-key` 默认情况下，代理会在更新可用时自动下载并应用更新。 建议使用此默认配置。 但是，如果您不希望代理自动下载和应用更新，请在运行代理安装命令时添加`-u false`参数。
（可选）安装 Discovery Agent 并配置不透明的代理	要配置不透明的代理，请在代理安装命令中添加以下参数： • -e 代理密码。 • -f 代理服务器端口号。 • -g 代理方案。 • -i 代理用户名。 以下是使用非透明代理参数执行代理安装命令的示例。

要……	请执行此操作...
	`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` 如果您的代理不需要身份验证，则省略-e和-i参数。 如果您的代理使用 https HTTP，则安装命令使用指定http-g参数值。

6. 如果网络出站连接受限，则需要更新防火墙设置。代理要求通过 TCP 端口 443 访问 arsenal。它们不要求打开任何入站端口。

   例如，如果你的家乡区域是eu-central-1，你可以使用 https://arsenal-discovery.*eu-central-1*.amazonaws.com:443

旧版 Linux 平台的注意事项

某些旧 Linux 平台 (如 SUSE 10、CentOS 5 和 RHEL 5) 已终止使用或者仅享受最低限度的支持。这些平台可能会受到 out-of-date密码套件的影响，这些套件会阻止代理更新脚本下载安装包。

Curl

应用程序发现代理需要与 AWS 服务器curl进行安全通信。某些旧版 curl 不能与现代 Web 服务安全通信。

要对所有操作使用 Application Discovery 代理附带的 curl 版本，请使用 -c true 参数运行安装脚本。

证书颁发机构服务包

较旧的 Linux 系统可能有 out-of-date证书颁发机构 (CA) 捆绑包，这对于安全的互联网通信至关重要。

要对所有操作使用 Application Discovery 代理附带的 CA 服务包，请使用 -b true 参数运行安装脚本。

这些安装脚本选项可以一起使用。在以下示例命令中，两个脚本参数都传递给安装脚本：

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

在微软 Windows 上安装发现代理

完成以下步骤，在微软 Windows 上安装代理。在开始此过程之前，请确保已设置好您的 Migration Hub 主区域。

在您的数据中心安装 AWS 应用程序发现代理

1. 下载 Windows 代理安装程序，但不要双击以在 Windows 中运行该安装程序。

   > **Important**
   >
   > 不要双击在 Windows 中运行安装程序，因为它将无法安装。代理安装仅通过命令提示符运行。(如果您已双击此安装程序，则必须先转到添加/删除程序 并卸载代理，然后才能继续执行剩下的安装步骤。)
   > 如果 Windows 代理安装程序在主机上未检测到任何版本的 Visual C++ x86 运行时，它会在安装代理软件之前自动安装 Visual C++ x86 2015—2019 运行时。

2. 以管理员身份打开命令提示符窗口并导航到您保存安装程序包的位置。
3. 要安装代理，请选择以下安装方法之一。

要……	请执行此操作...
安装发现代理	要安装代理，请运行代理安装命令，如以下示例所示。在示例中，*your-home-region* 替换为您所在地区的名称、*aws-access-key-id*访问密钥 ID 和您的私*aws-secret-access-key* 有访问密钥。 或者，您可以通过指定 INSTALLOCATION 参数的文件夹路径*C:\install-location* 来设置代理安装位置。例如，INSTALLLOCATION=" *C:\install-location* "。

要.....	请执行此操作...
	生成的文件夹层次结构将是 [安装位置路径]\AWS Discovery。默认情况下，安装位置为Program Files文件夹。 或者LOGANDCONFIGLOCATION ，您可以使用覆盖代理日志文件夹和配置文件的默认目录 (ProgramData)。生成的文件夹层次结构为[*LOGANDCONFIGLOCATION path*]\AWS Discovery 。 `.\AWSDiscoveryAgentInstaller.exe REGION=" your-home-region " KEY_ID="aws-access-key-id " KEY_SECRET=" aws-secret-access-key " /quiet` 默认情况下，代理会在更新可用时自动下载并应用更新。 建议使用此默认配置。 但是，如果您不希望代理自动下载和应用更新，请在运行代理安装命令时加入以下参数：AUTO_UPDATE=false **Warning** 禁用自动升级将阻止安装最新的安全修补程序。

要.....	请执行此操作...
（可选）安装 Discovery Agent 并配置不透明的代理	要配置不透明的代理，请在代理安装命令中添加以下公共属性： • PROXY_HOS T-代理主机的名称 • PROXY_SCHEME — 代理方案 • PROXY_PORT-代理端口号 • PROXY_USER-代理用户名 • PROXY_PASSWORD-代理用户密码 以下是使用非透明代理属性的代理安装命令的示例。 `.\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` 如果您的代理不需要身份验证，则省略PROXY_USER 和PROXY_PASSWORD 属性。安装命令使用的示例https。如果您的代理使用 HTTP，请http为该PROXY_SCHEME 值指定。

4. 如果您的网络出站连接受到限制，则必须更新防火墙设置。代理要求通过 TCP 端口 443 访问 arsenal。它们不要求打开任何入站端口。

   例如，如果你的主区域是eu-central-1，你可以使用以下内容：https://arsenal-discovery.*eu-central-1*.amazonaws.com:443

Package 签名和自动升级

对于 Windows Server 2008 及更高版本，亚马逊使用 SHA256 证书对 Application Discovery Service 代理安装包进行加密签名。对于 Windows Server 2008 上带有 SHA2签名的自动更新 SP2，请确保主机安装了支持签名身份验证的修补程序。 SHA2 微软最新的支持修补程序有助于支持 Windows Server 2008 SP2 上的 SHA2 身份验证。

> **Note**
>
> 微软不再公开提供 SHA256 支持 Windows 2003 的修补程序。如果您的 Windows 2003 主机上尚未安装这些修复程序，则需要手动升级。

手动执行升级

1. 下载 Windows 代理更新程序。
2. 以管理员身份打开命令提示符。
3. 导航到保存更新程序的位置。
4. 运行以下命令。

```
AWSDiscoveryAgentUpdater.exe /Q
```

管理发现代理进程

本页介绍如何在 Linux 和微软 Windows 上管理发现代理。

在 Linux 上管理发现代理进程

您可以使用`systemd`、`Upstart`或`System V init`工具在系统级别管理 Discovery Agent 的行为。以下选项卡中列出了每个工具中支持的任务所对应的命令。

systemd

用于 Application Discovery Agent 的管理命令

Task	命令
验证代理是否正在运行	`sudo systemctl status aws-discovery-daemon.service`
启动代理	`sudo systemctl start aws-discovery-daemon.service`
停止代理	`sudo systemctl stop aws-discovery-daemon.service`
重新启动代理	`sudo systemctl restart aws-discovery-daemon.service`

Upstart

应用程序发现代理的管理命令

Task	命令
验证代理是否正在运行	`sudo initctl status aws-discovery-daemon`
启动代理	`sudo initctl start aws-discovery-daemon`
停止代理	`sudo initctl stop aws-discovery-daemon`
重新启动代理	`sudo initctl restart aws-discovery-daemon`

System V init

应用程序发现代理的管理命令

Task	命令
验证代理是否正在运行	`sudo /etc/init.d/aws-discovery-daemon status`
启动代理	`sudo /etc/init.d/aws-discovery-daemon start`
停止代理	`sudo /etc/init.d/aws-discovery-daemon stop`
重新启动代理	`sudo /etc/init.d/aws-discovery-daemon restart`

在微软 Windows 上管理发现代理进程

您可以通过 Windows 服务器管理器服务控制台在系统级别管理发现代理的行为。下表描述了操作方法。

Task	服务名称	服务状态/操作
验证代理是否正在运行	AWS 发现代理 AWS 探索更新器	已启动
启动代理	AWS 发现代理 AWS 探索更新器	选择开始
停止代理	AWS 发现代理 AWS 探索更新器	选择停止
重新启动代理	AWS 发现代理 AWS 探索更新器	选择重新启动

卸载发现代理

本页介绍如何在 Linux 和微软 Windows 上卸载 Discovery Agent。

在 Linux 上卸载发现代理

本节介绍如何在 Linux 上卸载 Discovery Agent。

如果你使用的是 yum 软件包管理器，请卸载代理

- 如果使用 yum，请使用以下命令卸载代理。

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

如果您使用的是 apt-get 软件包管理器，请卸载代理

- 如果使用 apt-get，请使用以下命令卸载代理。

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

如果您使用的是 zypper 软件包管理器，请卸载代理

- 如果使用 zypper，请使用以下命令卸载代理。

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

在微软 Windows 上卸载发现代理

本节介绍如何在微软 Windows 上卸载 Discovery Agent。

在 Windows 上卸载发现代理

1. 在 Windows 中打开控制面板。
2. 选择程序。
3. 选择程序和功能。
4. 选择 “AWS 发现代理”。

5. 选择卸载。

> **Note**
>
> 如果您选择在卸载代理后重新安装代理，请使用/repair和/norestart选项运行以下命令。
>
> ```
> .\AWSDiscoveryAgentInstaller.exe REGION="your-home-region" KEY_ID="aws-access-key-id" KEY_SECRET="aws-secret-access-key" /quiet /repair /norestart
> ```

使用命令行在 Windows 上卸载发现代理

1. 右键单击 “开始”。
2. 选择 “命令提示符”。
3. 使用以下命令在 Windows 上卸载发现代理。

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

> **Note**
>
> 如果服务器上存在该.exe文件，则可以使用以下命令将代理从服务器上完全卸载。如果使用此命令进行卸载，则在重新安装代理时无需使用/repair和/norestart选项。
>
> ```
> .\AWSDiscoveryAgentInstaller.exe /quiet /uninstall
> ```

启动和停止发现代理数据收集

部署和配置 Discovery Agent 后，如果数据收集停止，则可以重新启动它。您可以按照中的步骤通过控制台启动或停止数据收集在 AWS Migration Hub 控制台中启动和停止数据收集器，也可以通过进行 API 调用 AWS CLI。

安装 AWS CLI 并开始或停止数据收集

1. 如果你还没有这样做，请安装与你的操作系统类型相 AWS CLI 适应的操作系统（Windows 或 Mac/Linux）。有关说明，请参阅《AWS Command Line Interface 用户指南》。
2. 打开命令提示符 (Windows) 或终端 (MAC/Linux)。
   a. 键入 `aws configure` 并按下 Enter。
   b. 输入您的 AWS 访问密钥 ID 和 AWS 私有访问密钥。
   c. 例如，输入您的家乡作为默认区域名称*us-west-2*。（在本例中，我们假设us-west-2这是您的家乡区域。）
   d. 对于默认输出格式，输入 `text`。
3. 要查找要停止或启动数据收集的代理的 ID，请键入以下命令：

```
aws discovery describe-agents
```

4. 要启动代理收集数据，请键入以下命令：

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

要停止代理收集数据，请键入以下命令：

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

对发现代理进行故障排除

本页介绍如何对 Linux 和微软 Windows 上的发现代理进行故障排除。

Linux 上的发现代理疑难解答

如果您在 Linux 上安装或使用 Discovery 代理时遇到问题，请查阅以下有关日志记录和配置的指南。在帮助解决代理或其与 Application Discovery Service 连接的潜在问题时，S AWS upport 经常会请求这些文件。

- 日志文件

  Discovery Agent 的日志文件位于以下目录中。

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

命名日志文件是为了表明它们是由主守护程序、自动升级程序还是安装程序生成的。

- 配置文件

  Discovery Agent 版本 2.0.1617.0 或更高版本的配置文件位于以下目录中。

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

  2.0.1617.0 之前的 Discovery Agent 版本的配置文件位于以下目录中。

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

- 有关如何删除旧版本的 Discovery Agent 的说明，请参阅发现代理的先决条件。

微软 Windows 上的发现代理疑难解答

如果您在 Microsoft Windows 上安装或使用 AWS 应用程序发现代理时遇到问题，请查阅以下有关日志记录和配置的指南。 AWS 支持在帮助解决代理或其与 Application Discovery Service 连接的潜在问题时，通常会请求这些文件。

- 安装日志

  在某些情况下，代理安装命令似乎失败。例如，Windows Services Manager 可能出现一个故障，指示未创建发现服务。在这种情况下，请向该命令添加 /log install.log 以生成详细的安装日志。

- 运行日志

  在 Windows Server 2008 及更高版本中，代理日志文件可在以下目录下找到。

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

  在 Windows Server 2003 上，代理日志文件可在以下目录下找到。

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

命名日志文件是为了表明是由主服务、自动升级还是安装程序生成的。

- 配置文件

  在 Windows Server 2008 及更高版本中，代理配置文件可在以下位置找到。

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

  在 Windows Server 2003 上，代理配置文件可在以下位置找到。

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

- 有关如何删除早期版本的 Discovery Agent 的说明，请参阅发现代理的先决条件。

Applice Discovery Service 无座席活动

Agentless Collector Agentless Cellector Agentless Cellector 是一种本地应用程序，它通过无代理方法收集有关本地环境的信息，包括服务器配置文件信息（例如，操作系统、数量 CPUs、RAM 量）、数据库元数据、利用率指标和有关本地服务器之间网络流量的数据。使用开放虚拟化存档（OVA）文件在您的 vCenter Server 环境中将 Agentless Cellector VMware Agentless Cellector Cellector Cent

无代理收集器采用模块化架构，允许使用多种无代理收集方法。Agentless Collector 提供了用于从数据库 VMware VMs 和分析服务器收集数据的模块。它还提供了一个用于收集本地服务器之间网络流量数据的模块。

Agentless Collector 通过收集有关本地服务器和数据库的使用情况和配置数据以及本地服务器之间的网络流量数据，来支持 AWS Application Discovery Service （Application Discovery Service）的数据收集。

Application Discovery Service 与 AWS Migration Hub该服务集成，该服务可将您的迁移状态信息聚合到单个控制台中，从而简化您的迁移跟踪。您可以查看发现的服务器、获取 Amazon EC2 建议、可视化网络连接、将服务器分组为应用程序，然后从您所在地区的 Migration Hub 控制台跟踪每个应用程序的迁移状态。

无代理收集器数据库和分析数据收集模块与 AWS Database Migration Service ()AWS DMS集成。此集成有助于规划您向的迁移 AWS Cloud。您可以使用数据库和分析数据收集模块来发现环境中的数据库和分析服务器，并生成要迁移到的服务器清单 AWS Cloud。该数据收集模块收集数据库元数据以及 CPU、内存和磁盘容量的实际利用率指标。收集这些指标后，您可以使用 AWS DMS 控制台为源数据库生成目标建议。

无代理收集器的先决条件

以下是使用 Application Discovery Service 无代理收集器（无代理收集器）的先决条件：

- 一个或多个 AWS 账户。
- 设置了 AWS Migration Hub 主区域的 AWS 账户，请参阅登录 Migration Hub 控制台并选择主区域。您的 Migration Hub 数据存储在您的家乡地区，用于发现、规划和迁移跟踪。
- 设置为使用 AWS 托管策略的 AWS 账户 IAM 用户`AWSApplicationDiscoveryAgentlessCollectorAccess`。要使用数据库和分析数据收集模块，此 IAM 用户还必须使用两个客户托管的 IAM 策

略DMSCollectorPolicy和FleetAdvisorS3Policy。有关更多信息，请参阅 部署 Applice Discovery Service 无座席活动。IAM 用户必须在设置了 Migrati AWS on Hub 主区域的账户中创建。

- VMware vCenter Venter Vlice、V6、

> **Note**
>
> 无代理收集器支持所有这些版本的 VMware，但我们目前针对版本 6.7 和 7.0 进行了测试。

- 要安装 VMware vCenter Server，请确保您可以为系统组提供具有读取和查看权限的 vCenter 凭据。
- 无代理收集器需要通过 TCP 端口 443 对多个域进行出站访问。 AWS 有关这些域的列表，请参阅为 AWS 域的出站访问配置防火墙。
- 要使用数据库和分析数据收集模块，请在您设置为 Migration Hub 主区域 AWS 区域 的中创建一个 Amazon S3 存储桶。数据库和分析数据收集模块将库存元数据存储在此 Amazon S3 存储桶中。有关更多信息，请参阅《Amazon S3 用户指南》中的创建存储桶。
- 无代理收集器版本 2 需要 ESXi 6.5 或更高版本。

为 AWS 域的出站访问配置防火墙

如果您的网络出站连接受到限制，则必须更新防火墙设置以允许出站访问无代理收集器所需的 AWS 域。哪些 AWS 域名需要出站访问取决于您的 Migration Hub 主区域是美国西部（俄勒冈）区域、us-west-2 还是其他区域。

如果您的 AWS 账户主区域为 us-west-2，则以下域名需要出站访问：

- `arsenal-discovery.us-west-2.amazonaws.com`— 收集器使用此域来验证其是否配置了所需的 IAM 用户证书。收集器还使用它来发送和存储收集的数据，因为主区域为 us-west-2。
- `migrationhub-config.us-west-2.amazonaws.com`— 收集器使用此域根据提供的 IAM 用户证书来确定收集器将数据发送到哪个主区域。
- `api.ecr-public.us-east-1.amazonaws.com`— 收集器使用此域来发现可用的更新。
- `public.ecr.aws`— 收集器使用此域下载更新。
- dms.*your-migrationhub-home-region*.amazonaws.com— 收集器使用此域连接到 AWS DMS 数据收集器。
- `s3.amazonaws.com`— 收集器使用此域将数据库和分析数据收集模块收集的数据上传到您的 Amazon S3 存储桶。
- `sts.amazonaws.com`— 收集器使用此域来了解收集器配置的帐户。

如果您的 AWS 账户主区域不是，则以下域名需要出站访问权限**us-west-2**：

- `arsenal-discovery.us-west-2.amazonaws.com`— 收集器使用此域来验证其是否配置了所需的 IAM 用户证书。
- `arsenal-discovery.`*`your-migrationhub-home-region`*`.amazonaws.com`— 收集器使用此域来发送和存储收集的数据。
- `migrationhub-config.us-west-2.amazonaws.com`— 收集器使用此域根据提供的 IAM 用户证书来确定收集器应将数据发送到哪个主区域。
- `api.ecr-public.us-east-1.amazonaws.com`— 收集器使用此域来发现可用的更新。
- `public.ecr.aws`— 收集器使用此域下载更新。
- `dms.`*`your-migrationhub-home-region`*`.amazonaws.com`— 收集器使用此域连接到 AWS DMS 数据收集器。
- `s3.amazonaws.com`— 收集器使用此域将数据库和分析数据收集模块收集的数据上传到您的 Amazon S3 存储桶。
- `sts.amazonaws.com`— 收集器使用此域来了解收集器配置的帐户。

在设置 Agentless Collector 时，您可能会收到诸如安装失败 — 请检查您的凭据并重试或AWS 无法联系到之类的错误。请验证网络设置。这些错误可能是由于无代理收集器尝试与其需要出站访问的某个 AWS 域建立 HTTPS 连接失败所致。

如果 AWS 无法建立与的连接，则 Agentless Collector 无法从您的本地环境收集数据。有关如何修复与的连接的信息 AWS，请参阅修复安装过程中无法访问 AWS 的无代理收集器。

部署 Applice Discovery Service 无座席活动

要部署 Application Discovery Service 无代理收集器，您必须先创建 IAM 用户并下载收集器。本页将指导您完成部署收集器所需的步骤。

为无座席活动

要使用无代理收集器，您必须在中使用的 AWS 账户中登录 Migration Hub 控制台并选择主区域创建一个 AWS Identity and Access Management (IAM) 用户。然后，将此 IAM 用户设置为使用以下 AWS 托管策略AWSApplicationDiscoveryAgentlessCollectorAccess。您在创建 IAM 用户时附加此 IAM 策略。

要使用数据库和分析数据收集模块，请创建两个客户托管 IAM 策略。这些策略允许访问您的 Amazon S3 存储桶和 AWS DMS API。有关更多信息，请参阅 IAM 用户指南中的创建客户托管策略。

- 使用以下 JSON 代码创建**DMSCollectorPolicy**策略。

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

- 使用以下 JSON 代码创建**FleetAdvisorS3Policy**策略。

```
{
    "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/*"
            ]
        }
    ]
}
```

在上面的示例中，将*bucket_name*替换为在先决条件步骤中创建的 Amazon S3 存储桶的名称。

我们建议您创建一个非管理性的 IAM 用户以与 Agentless Collector 配合使用。创建非管理型 IAM 用户时，请遵循安全最佳实践 “授予最低权限”，向用户授予最低权限。

创建非管理员 IAM 用户以与无代理收集器配合使用

1. 在中 AWS Management Console，使用您用于设置主区域的 AWS 账户，导航到 IAM 控制台登录 Migration Hub 控制台并选择主区域。
2. 按照 IAM 用户指南中在您的 AWS 账户中创建 IAM 用户中所述的使用控制台创建用户的说明创建非管理员 IAM 用户。

   按照 IAM 用户指南中的说明进行操作时：

   - 在关于选择访问类型的步骤中，选择编程访问权限。请注意，虽然不建议这样做，但只有当您计划使用相同的 IAM 用户证书访问控制台时，才选择AWS 管理 AWS 控制台访问权限。
   - 在 “设置权限” 页面的步骤中，选择 “将现有策略直接附加到用户” 选项。然后从策略列表中选择`AWSApplicationDiscoveryAgentlessCollectorAccess` AWS 托管策略。

     接下来，选择`DMSCollectorPolicy`和`FleetAdvisorS3Policy`客户托管的 IAM 策略。
   - 在查看用户的访问密钥（访问密钥 IDs 和私有访问密钥）时，请遵循重要说明中的指导，将用户的新访问密钥 ID 和私有访问密钥保存在安全可靠的地方。您需要使用这些访问密钥配置无座席活动。

     轮换访问密钥是一种 AWS 安全最佳实践。有关轮换密钥的信息，请参阅《IAM 用户指南》中的对于需要长期凭证的使用场景定期轮换访问密钥。

下载无代理收集器

要设置 Application Discovery Service 无代理收集器（无代理收集器），必须下载并部署无代理收集器开放虚拟化存档 (OVA) 文件。Agentless Cellector 是一种虚拟设备，您可以在本地环境 VMware 中安装它。此步骤介绍如何下载收集器 OVA 文件，下一步介绍如何部署该文件。

下载收集器 OVA 文件并验证其校验和

1. 以 VMware 管理员身份登录 vCenter，然后切换到您想要下载Agentless Cellector OVA 文件的目录。
2. 从以下 URL 下载 OVA 文件：

   无代理收集器 OVA
3. 根据您在系统环境中使用的哈希算法，下载MD5或SHA256以获取包含校验和值的文件。使用下载的值来验证在上一步中下载的`ApplicationDiscoveryServiceAgentlessCollector`文件。

4. 根据您的 Linux 变体，运行相应版本的 MD5 SHA256 命令或命令来验证`ApplicationDiscoveryServiceAgentlessCollector.ova`文件的加密签名是否与您下载的相应 MD5/SHA256 文件中的值相匹配。

```
$ md5sum ApplicationDiscoveryServiceAgentlessCollector.ova
```

```
$ sha256sum ApplicationDiscoveryServiceAgentlessCollector.ova
```

部署无座席活动

Application Discovery Service Cellector（Agentless Cellector）是一种虚拟设备，您可以在本地环境中安装它。 VMware 本部分介绍如何部署在 VMware 环境中下载的开放虚拟化存档（OVA）文件。

无代理收集器虚拟机规格

Agentless Collector version 2

- 操作系统 — 亚马逊 Linux 2023
- 内存-16 GB
- 中央处理器 — 4 个内核
- VMware 要求 — 请参阅在上运行 AL2 023 VMware 的主机要求 VMware

Agentless Collector version 1

- 操作系统 — 亚马逊 Linux 2
- 内存-16 GB
- 中央处理器 — 4 个内核

以下过程将引导您完成在您的 VMware 环境中部署 Agentless Collector OVA 文件。

部署无代理收集器

1. 以管理员身份登录 vCenter。 VMware
2. 使用以下任一方式安装 OVA 文件：
   - 使用用户界面：选择文件，选择部署 OVF 模板，选择您在上一节中下载的收集器 OVA 文件，然后完成向导。确保服务器管理仪表板中的代理设置配置正确。

- 使用命令行：要从命令行安装收集器 OVA 文件，请下载并使用 VMware 开放虚拟化格式工具 (ovftool)。要下载 ovftool，请从 OVF 工具文档页面中选择一个版本。

  以下是使用 ovftool 命令行工具安装收集器 OVA 文件的示例。

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

  以下内容描述了示例中的***replaceable***值

  - 该名称是要用于无座席活动 VM 的名称。
  - 数据存储是 vCenter 中数据存储的名称。
  - OVA 文件名是下载的收集器 OVA 文件的名称。
  - 用户名/密码是您的 vCenter 凭据。
  - vcenterurl 是你的 vCenter 的网址。
  - vi 路径是通往 VMware ESXi 主机的路径。

3. 在 vCenter 中找到已部署的无代理收集器。右键单击 VM，然后选择 “开机”、“开机”。
4. 几分钟后，收集器的 IP 地址将显示在 vCenter 中显示出来。您使用此 IP 地址连接收集器。

访问无代理收集器控制台

以下过程介绍了如何访问 Application Discovery Celles Cellector（Agentless Collector）控制台。

访问无代理收集器控制台

1. 打开 Web 浏览器，然后在地址栏中键入以下 URL：**https://***<ip_address>***/**，其中*<ip_address>*是收集器的 IP 地址部署无座席活动。
2. 首次访问 A gentless Collector 时，请选择 “开始”。之后，系统将要求您登录。

如果你是第一次访问无代理 Collector 控制台，那么接下来你将访问。配置无座席活动否则，接下来你会看到无代理收集器仪表板。

配置无座席活动

Application Discovery Service 无代理收集器（无代理收集器）是一款基于亚马逊 Linux 2 的虚拟机 (VM)。以下部分介绍如何在无代理收集器控制台的 “配置无代理收集器” 页面上配置收集器虚拟机。

在 “配置无代理收集器” 页面上配置收集器虚拟机

1. 在收集器名称中，输入收集器名称以进行识别。名称可以包含空格，但不能包含特殊字符。
2. 在 “数据同步” 下，输入 IAM 用户 AWS 账户的 AWS 访问密钥和密钥，以指定为接收收集器发现的数据的目标账户。有关 IAM 用户要求的信息，请参阅部署 Applice Discovery Service 无座席活动。

   a. 对于AWS 访问密钥，请输入您指定为目标 AWS 账户的账户 IAM 用户的访问密钥。

   b. 对于AWS 密钥，请输入您指定为目标 AWS 账户的 IAM 用户账户的密钥。

   c. （可选）如果您的网络需要使用代理才能访问 AWS，请输入代理主机、代理端口，以及通过现有代理服务器进行身份验证所需的凭据（可选）。
3. 在无代理收集器密码下，设置用于对无代理收集器的访问进行身份验证的密码。

   - 密码区分大小写
   - 密码长度必须在 8 到 64 个字符之间
   - 密码必须包含下列四种类别中每种类别的至少一个字符：
     - 小写字母 (a-z)
     - 大写字母 (A-Z)
     - 数字 (0-9)
     - 非字母数字字符 (@$! #%*？ &)
   - 密码不能包含以下特殊字符：@$! #%*？ &

   a. 对于无代理收集器密码，请输入用于验证对收集器的访问权限的密码。

   b. 要重新输入无代理收集器密码，为了进行验证，请再次输入该密码。
4. 在 “其他设置” 下，阅读许可协议。如果您同意接受，请选中该复选框。
5. 要启用无代理收集器的自动更新，请在 “其他设置” 下，选择 “自动更新无代理收集器”。如果您未选中此复选框，则需要手动更新 Agentless Collector。手动更新 Application Discovery Service 无代理收集器
6. 选择 “保存配置”。

以下主题介绍收集器配置可选任务。

可选配置任务

- （可选）为无代理收集器虚拟机配置静态 IP 地址
- （可选）将无代理收集器虚拟机重置为使用 DHCP
- （可选）配置 Kerberos 身份验证协议

（可选）为无代理收集器虚拟机配置静态 IP 地址

以下步骤介绍如何为 Application Discovery Service 无代理收集器（无代理收集器）虚拟机配置静态 IP 地址。首次安装时，收集器虚拟机配置为使用动态主机配置协议（DHCP）。

> **Note**
>
> 无代理收集器支持。 IPv4它不支持 IPv6。

Agentless Collector version 2

为收集器 VM 配置静态 IP 地址

1. 从 VMware vCenter 收集以下网络信息：
   - 静态 IP 地址-子网中未签名的 IP 地址。例如，192.168.1.138。
   - CIDR 网络掩码 — 要获取 CIDR 网络掩码，请检查托管收集器虚拟机的 vCent VMware er 主机的 IP 地址设置。例如，/24。
   - 默认网关-要获取默认网关，请检查托管收集器虚拟机的 VMware vCenter 主机的 IP 地址设置。例如，192.168.1.1。
   - 主 DNS-要获取主 DNS，请检查托管收集器虚拟机的 VMware vCenter 主机的 IP 地址设置。例如，192.168.1.1。
   - （可选）辅助 DNS
   - （可选）本地域名-这允许收集器在不使用域名的情况下访问 vCenter 主机 URL。
2. 打开收集器的 VM 控制台并**ec2-user**使用密码登录**collector**，如以下示例所示。

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

3. 在远程终端终端输入以下命令可以禁用网络接口。

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

4. 使用以下步骤更新接口配置。

   a. 使用以下命令在 vi 编辑器中打开 10-cloud-init-ens 192.network。

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

   b. 使用您在收集网络信息步骤中收集的信息更新这些值，如以下示例所示。

   ```
   [Match]
   Name=ens192

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

5. 使用以下步骤更新域名系统 (DNS)。

   a. 使用以下命令在 vi 中打开`resolv.conf`文件。

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

   b. 使用以下命令更新 vi 中的`resolv.conf`文件。

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

   以下示例显示了一个编辑过的`resolv.conf`文件。

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

6. 通过输入以下命令启用网络接口。

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

7. 重启虚拟机，如以下示例所示。

```
sudo reboot
```

8. 使用以下步骤验证您的网络设置。

   a. 输入以下命令，检查 IP 地址配置是否正确。

```
ifconfig
ip addr show
```

   b. 输入以下命令，检查网关是否已正确添加。

```
route -n
```

   该输出应类似于以下示例。

```
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. 输入以下命令验证您是否可以 ping ping 公共 URL。

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

   d. 确认您可以 ping vCenter IP 地址或主机名，如以下示例所示。

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

Agentless Collector version 1

为收集器 VM 配置静态 IP 地址

1. 从 VMware vCenter 收集以下网络信息：
   - 静态 IP 地址-子网中未签名的 IP 地址。例如，192.168.1.138。
   - 网络掩码-要获取网络掩码，请检查托管收集器虚拟机的 VMware vCenter 主机的 IP 地址设置。例如，255.255.255.0。
   - 默认网关-要获取默认网关，请检查托管收集器虚拟机的 VMware vCenter 主机的 IP 地址设置。例如，192.168.1.1。
   - 主 DNS-要获取主 DNS，请检查托管收集器虚拟机的 VMware vCenter 主机的 IP 地址设置。例如，192.168.1.1。
   - （可选）辅助 DNS
   - （可选）本地域名-这允许收集器在不使用域名的情况下访问 vCenter 主机 URL。
2. 打开收集器的 VM 控制台并**ec2-user**使用密码登录**collector**，如以下示例所示。

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

3. 在远程终端终端输入以下命令可以禁用网络接口。

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

4. 使用以下步骤更新接口 eth0 配置。

   a. 使用以下命令在 vi 编辑器中打开 ifcfg-eth0。

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

   b. 使用您在收集网络信息步骤中收集的信息更新接口值，如以下示例所示。

```
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. 使用以下步骤更新域名系统 (DNS)。

   a. 使用以下命令在 vi 中打开`resolv.conf`文件。

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

   b. 使用以下命令更新 vi 中的`resolv.conf`文件。

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

   以下示例显示了一个编辑过的`resolv.conf`文件。

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

6. 通过输入以下命令启用网络接口。

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

7. 重启虚拟机，如以下示例所示。

   ```
   sudo reboot
   ```

8. 使用以下步骤验证您的网络设置。

   a. 输入以下命令，检查 IP 地址配置是否正确。

   ```
   ifconfig
   ip addr show
   ```

   b. 输入以下命令，检查网关是否已正确添加。

   ```
   route -n
   ```

该输出应类似于以下示例。

```
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. 输入以下命令验证您是否可以 ping ping 公共 URL。

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

d. 确认您可以 ping vCenter IP 地址或主机名，如以下示例所示。

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

（可选）将无代理收集器虚拟机重置为使用 DHCP

以下步骤介绍了如何重新配置Agentless Collector VM 以使用 DHCP。

Agentless Collector version 2

将收集器虚拟机配置为使用 DHCP

1. 通过在远程终端中运行以下命令禁用网络接口。

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

2. 使用以下步骤更新接口配置。

a. 使用以下命令在 vi 编辑器中打开该`10-cloud-init-ens192.network`文件。

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

b. 更新值，如以下示例所示。

```
[Match]
Name=ens192
```

```
[Network]
DHCP=yes

[DHCP]
ClientIdentifier=mac
```

3. 通过输入以下命令重置 DNS 设置。

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

4. 通过输入以下命令启用网络接口。

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

5. 重新启动收集器虚拟机，如以下示例所示。

```
sudo reboot
```

Agentless Collector version 1

将收集器虚拟机配置为使用 DHCP

1. 通过在远程终端中运行以下命令禁用网络接口。

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

2. 使用以下步骤更新网络配置。

   a. 使用以下命令在 vi 编辑器中打开该`ifcfg-eth0` 文件。

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

   b. 更新`ifcfg-eth0` 文件中的值，如以下示例所示。

   ```
   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. 通过输入以下命令重置 DNS 设置。

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

4. 通过输入以下命令启用网络接口。

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

5. 重新启动收集器虚拟机，如以下示例所示。

```
sudo reboot
```

（可选）配置 Kerberos 身份验证协议

如果您的操作系统服务器支持 Kerberos 身份验证协议，则可以使用此协议连接到您的服务器。为此，您必须配置 Application Diservice Agentless Collector VM。

以下步骤介绍了如何在 Application Discovery Service Agentless Cellector VM 上配置 Agentless Cellector

在收集器虚拟机上配置 Kerberos 身份验证协议

1. 打开收集器的 VM 控制台并**ec2-user**使用密码登录**collector**，如以下示例所示。

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

2. 打开/etc文件夹中的krb5.conf配置文件。为此，您可以使用以下代码示例。

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

3. 使用以下信息更新krb5.conf配置文件。

```
[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
```

保存文件，退出文本编辑器。

4. 重新启动收集器虚拟机，如以下示例所示。

```
sudo reboot
```

使用无代理收集器网络数据收集模块

网络数据收集模块使您能够发现本地数据中心内服务器之间的依赖关系。这些网络数据提供了应用程序在服务器之间的通信方式的可见性，从而加快了您的迁移计划。

网络数据收集模块连接到 VMware vCenter 模块识别的服务器，并分析这些服务器的源 IP 到目标 IP/端口的流量。

主题

- 设置网络数据收集模块
- 网络数据收集尝试
- 网络数据收集模块中的服务器状态

设置网络数据收集模块

网络数据收集模块收集来自 VMware vCenter 模块的服务器清单的网络数据。因此，要使用网络数据收集模块，请先设置 VMware vCenter 模块。有关说明，请按照以下主题中的指导进行操作：

1. the section called “部署收集器”
2. the section called “访问收集器控制台”
3. the section called “配置收集器”
4. the section called “使用 VMware 数据收集模块”

设置网络数据收集模块

1. 在 Agentless Collector 仪表板的 “网络数据收集” 部分，选择 “查看网络连接”。
2. 在 “网络连接” 页面上，选择 “编辑收集器”。
3. 在凭据部分，输入至少一组凭据。您最多可以输入 10 组凭据。该模块首次尝试为服务器收集数据时，它会尝试所有凭据，直到找到一组有效的凭据；然后，它会保存该集并在随后的尝试中再次使用它。有关设置凭据的信息，请参阅the section called “设置 凭证”。
4. 在数据收集首选项部分，要在服务器重新启动时自动开始收集数据，请选择自动开始数据收集。
5. 如果您尚未设置 WinRM 证书，请选择 “禁用 W inRM 证书检查”。
6. 选择保存。
7. 每隔 15 秒在服务器上收集一次。要查看给定服务器的收集尝试的详细信息，请在 “服务器” 表中选中该服务器左侧的复选框。

设置 凭证

网络数据收集模块使用 WinRM 从 Windows 服务器收集数据。它使用 SNMPv2 和收集 SNMPv3 来自 Linux 服务器的数据。

WinRM 凭证：

- 指定具有以下内容的 Windows 帐户的用户名和密码：
  - 对`\root\standardcimv2`命名空间的读取权限
  - `MSFT_NetTCPConnection`课堂的读取权限
  - 远程 WMI 访问

- 我们建议您创建一个所需权限最少的专用服务帐户。
- 避免使用域管理员或本地管理员帐户。
- 必须在收集器和目标服务器之间打开端口 5986 (HTTPS)。
- 避免禁用 WinRM 证书检查。有关设置 WinRM 证书的信息，请参见。the section called “解决配置 WinRM 证书时的自签名认证问题”

SNMPv2 凭证：

- 提供一个可以访问 1.3.6.1.2.1.6.13.* OID 的只读社区字符串
- SNMPv3 更可取， SNMPv2 因为中的安全性有所提高 SNMPv3
- 收集器和目标服务器之间必须打开端口 161/UDP
- 使用复杂的非默认社区字符串
- 避免使用诸如 “公共” 或 “私有” 之类的常见字符串
- 像对待密码一样对待社区字符串

SNMPv3 凭证

- 提供具有只读权限的username/password and auth/privacy详细信息，该权限可以访问 1.3.6.1.2.1.6.13.* OID。
- 收集器和目标服务器之间必须打开端口 161/UDP
- 同时启用身份验证和隐私
- 使用强身份验证协议（优先使用 SHA MD5）
- 使用强加密协议（AES 优先于 DES）
- 使用复杂的密码进行身份验证和隐私
- 使用唯一的用户名（避免使用常用名）

凭据管理的一般最佳实践

- 安全地存储凭证
- 定期轮换所有证书
- 使用密码管理器或安全保管库
- 监控凭证使用情况

- 遵循最低权限原则，只授予所需的最低必要权限

网络数据收集尝试

发现新服务器后，收集器会尝试为每个 IP 地址配置的每个凭据。收集器找到有效凭证后，仅使用该凭证。连续两次失败后，收集器会尝试在 30 分钟、2 小时、8 小时和 24 小时后收集服务器的网络数据。在 6 次尝试失败后，收集器继续每天尝试一次所有已配置的凭证。要解决此问题，请编辑当前凭据或通过选择 “编辑收集器” 来添加其他凭据，或者对正在监视的目标服务器进行更改。

网络数据收集模块中的服务器状态

下表说明了收集状态值。

状态	含义
收集或收集	上次尝试收集网络连接已成功。
出错或出错	由于网络或权限问题，上次尝试收集网络连接失败。要了解更多信息，请选中出现错误的服务器左侧的复选框。
Skipped	未提供有效凭据的服务器。更新或配置其他服务器凭据。
无数据	服务器的数据收集尚未开始。要开始收集数据，请选择启动收集器。
待处理	已开始收集，但尚未尝试收集。等待几分钟，然后刷新列表。

使用 VMware vCenter 无代理收集器数据收集模块块

本节介绍了 Application Discovery Service 无代理收集器（无代理收集器） VMware vCenter 数据收集模块，该模块用于从中收集服务器清单、配置文件和利用率数据。 VMware VMs

主题

- 为 vCenter 设置无代理收集器数据收集模块 VMware

- 查看 VMware 数据收集详情
- 控制 vCenter 数据收集的范围
- 无代理收集器 vCenter VMware 数据收集模块收集的数据

为 vCenter 设置无代理收集器数据收集模块 VMware

本节介绍如何设置无代理收集器 vCent VMware er 数据收集模块，以从中收集服务器清单、配置文件和利用率数据。 VMware VMs

> **Note**
>
> 在开始 vCenter 安装之前，请确保您可以为系统组提供已设置读取和查看权限的 vCenter 凭据。

设置 VMware vCenter 数据收集模块

1. 在 “无代理收集器” 仪表板页面上，在 “数据收集” 下，选择 “vCent erVMware ” 部分的 “设置”。
2. 在设置 VMware vCenter 数据收集页面上，执行以下操作：
   a. 在 vCenter 凭据下：
      i. 对于 vCenter URL/IP，请输入您的 vC VMware enter 服务器主机的 IP 地址。
      ii. 在 vCenter 用户名中，输入收集器用来与 vCenter 通信的本地或域用户的姓名。对于域用户，请使用 domain\username 或 username@domain 形式。
      iii. 对于 vCenter Password (vCenter 密码)，请输入本地或域用户密码。
   b. 在 “数据收集偏好设置” 下：
      - 要在成功设置后立即自动开始收集数据，请选择 “自动开始数据收集”。
   c. 选择 Set up (设置)。

接下来，您将看到VMware 数据收集详细信息页面，下一个主题将对此进行介绍。

查看 VMware 数据收集详情

VMware 数据收集详细信息页面显示有关您在中设置的 vCenter 的详细信息。为 vCenter 设置无代理收集器数据收集模块 VMware

在 “已发现的 vCenter 服务器” 下，列出了您设置的 vCenter，其中包含有关 vCenter 的以下信息：

- vCenter 服务器的 IP 地址。
- vCenter 中的服务器数量。
- 数据收集的状态。
- 距离上次更新还有多长时间。

选择移除 vCenter 服务器以移除显示的 vCenter 服务器，然后返回到设置 vCenter VMware 数据收集页面。

如果您没有选择自动开始数据收集，则可以使用此页面上的 “开始数据收集” 按钮开始数据收集。数据收集开始后，开始按钮变为停止数据收集。

如果 “收集状态” 列显示正在收集，则表示数据收集已开始。

您可以在 AWS Migration Hub 控制台中查看收集的数据。如果您正在为 VMware vCenter 服务器清单收集数据，则可以在开启数据收集大约 15 分钟后访问控制台中显示的数据。

如果您的互联网访问未被阻止，则可以选择此页面上的 “在 Migration Hub 中查看服务器” 来打开 Migration Hub 控制台。无论您是否选择此按钮，有关如何访问 Migration Hub 控制台的信息，请参阅查看您收集的数据。

以下是根据迁移规划活动建议的数据收集时间长度的指导方针：

- TCO（总拥有成本）-2 到 4 周
- 迁移计划-2 到 6 周

控制 vCenter 数据收集的范围

vCenter 用户需要每个 ESX 主机或虚拟机的只读权限才能使用 Application Discovery Service 进行清点。使用权限设置，您可以控制数据收集中包含 VMs 哪些主机和主机。您可以允许清点当前 vCenter VMs 下的所有主机，也可以根据需要授予权限。 case-by-case

> **Note**
>
> 作为最佳安全实践，我们建议不要向 Application Discovery Service 的 vCenter 用户授予额外的、不需要的权限。

以下过程介绍从最粗粒度到最细粒度排序的配置方案。这些步骤适用于 vSphere Client v6.7.0.2。其他版本的客户端的操作步骤可能会有所不同，具体取决于您使用的 vSphere 客户机版本。

发现有关所有 ESX 主机和当前 vCenter VMs 下的数据

1. 在 VMware vSphere 客户端中，选择 vCen ter，然后选择主机和集群或和模板。VMs
2. 选择数据中心资源，然后选择 “权限”。
3. 选择 vCenter 用户，然后选择要添加、编辑或移除用户角色的符号。
4. 从 “角色” 菜单中选择 “只读”。
5. 选择 “传播给孩子”，然后选择 “确定”。

发现特定 ESX 主机及其所有 子对象的相关数据

1. 在 VMware vSphere 客户端中，选择 vCen ter，然后选择主机和集群或和模板。VMs
2. 依次选择 Related Objects、Hosts。
3. 打开主机名的上下文 (单击右键) 菜单，然后依次选择 All vCenter Actions、Add Permission。
4. 在 Add Permission 下，将 vCenter 用户添加到主机。对于 Assigned Role，选择 Read-only。
5. 选择 Propagate to children，然后选择 OK。

发现有关特定 ESX 主机或子虚拟机的数据

1. 在 VMware vSphere 客户端中，选择 vCen ter，然后选择主机和集群或和模板。VMs
2. 选择 Related Objects。
3. 选择主机（显示 vCenter 已知的 ESX 主机的列表）或虚拟机（显示所有 ESX 主 VMs 机的列表）。
4. 打开主机名或 VM 名称的上下文 (单击右键) 菜单，然后依次选择 All vCenter Actions、Add Permission。
5. 在 Add Permission 下，将 vCenter 用户添加到主机或虚拟机。对于 Assigned Role，选择 Read-only。
6. 选择确定。

> **Note**
>
> 如果您选择 “传播给子代”，则仍然可以根据需要从 ESX 主机 VMs 上移除只读权限。 case-by-case此选项对应用于其他 ESX 主机的继承权限没有影响。 VMs

无代理收集器 vCenter VMware 数据收集模块收集的数据

以下信息描述了 Application Discovery Service 无代理收集器（无代理收集器）vCenter VMware 数据收集模块收集的数据。有关设置数据收集的信息，请参见为 vCenter 设置无代理收集器数据收集模块 VMware 。

无代理收集器 vCenter VMware 收集数据的表格图例：

- 除非另有说明，否则收集的数据以千字节 (KB) 为度量单位。
- Migration Hub 控制台中的等效数据以兆字节 (MB) 为单位报告。
- 以星号 (*) 表示的数据字段仅在 Application Discovery Service API 导出功能生成的.csv 文件中可用。

  无代理收集器支持使用 CLI AWS 导出数据。要使用 AWS CLI 导出收集的数据，请按照 App lication Discovery Service 用户指南中 “导出收集的数据” 页面上导出所有服务器的系统性能数据下所述的说明进行操作。
- 轮询期的间隔大约为 60 分钟。
- 用双星号 (**) 表示的数据字段当前返回一个 null 值。

数据字段	描述
applicationConfigurationId*	虚拟机所在的迁移应用程序的 ID。
avgCpuUsagePct	轮询期间CPU使用率的平均百分比。
avgDiskBytesReadPerSecond	轮询期间从磁盘读取的平均字节数。
avgDiskBytesWrittenPerSecond	轮询期间写入磁盘的平均字节数。
avgDiskReadOpsPerSecond**	每秒读取 I/O 操作的平均次数为空。
avgDiskWriteOpsPerSecond**	每秒写入 I/O 操作的平均次数。

数据字段	描述
avgFreeRAM	平均可用内存，以 MB 表示。
avgNetworkBytesReadPerSecond	每秒读取字节的平均吞吐量。
avgNetworkBytesWrittenPerSecond	每秒写入字节的平均吞吐量。
计算机制造商	ESXi 主机报告的供应商。
计算机模型	ESXi 主机报告的计算机型号。
configId	Application Discovery Service 为发现的虚拟机分配的 ID。
configType	发现的资源类型。
connectorId	虚拟设备的 ID。
cpuType	虚拟机的 vCPU，主机的实际模型。
datacenterId	vCenter 的 ID。
hostId*	虚拟机主机的 ID。
hostName	运行虚拟化软件的主机的名称。
hypervisor	虚拟机管理程序的类型。
id	服务器的 ID。
lastModifiedTime邮票 *	数据导出前数据收集的最新日期和时间。
macAddress	虚拟机的 MAC 地址。
manufacturer	虚拟化软件的制造商。
maxCpuUsagePct	轮询期间 CPU 使用率的最大百分比。
maxDiskBytesReadPerSecond	轮询期间从磁盘读取的最大字节数。
maxDiskBytesWrittenPerSecond	轮询期间写入磁盘的最大字节数。

数据字段	描述
maxDiskReadOpsPerSecond**	每秒读取 I/O 操作的最大数量。
maxDiskWriteOpsPerSecond**	每秒写入 I/O 操作的最大数量。
maxNetworkBytesReadPerSecond	每秒读取字节的最大吞吐量。
maxNetworkBytesWrittenPerSecond	每秒写入字节的最大吞吐量。
memoryReservation*	限制以避免在虚拟机上过度使用内存。
moRefId	vCenter 托管对象的唯一引用 ID。
name*	虚拟机或网络的名称（用户指定）。
numCores	分配给虚拟机的 CPU 内核数。
numCpus	ESXi 主机上的 CPU 插槽数量。
numDisks**	虚拟机上的磁盘数量。
numNetworkCards**	虚拟机上的网卡数量。
osName	虚拟机上的操作系统名称。
osVersion	虚拟机上的操作系统版本。
portGroupId*	VLAN 成员端口组的 ID。
portGroupName*	VLAN 成员端口组的名称。
powerState*	权力状态。
serverId	Application Discovery Service 为发现的虚拟机分配了 ID。
smBiosId*	系统管理 BIOS 的 ID/版本。
state*	虚拟设备的状态。
toolsStatus	VMware 工具的运行状态

数据字段	描述
totalDiskFree大小	可用磁盘空间，以 MB 表示。适用于 vCenter Server 7.0 及更高版本。
totalDiskSize	磁盘的总容量，以 MB 表示。
totalRAM	虚拟机上可用的 RAM 总量（以 MB 为单位）。
type	主机类型。
vCenterId	虚拟机的唯一 ID 号。
vCenterName*	vCenter 主机的名称。
virtualSwitchName*	虚拟交换机的名称。
vmFolderPath	虚拟机文件的目录路径。
vmName	虚拟机的名称。

使用数据库和分析数据收集模块

本节介绍如何设置、配置和使用数据库和分析数据收集模块。您可以使用此数据收集模块连接到数据环境，并从本地数据库和分析服务器收集元数据和性能指标。有关可通过此模块收集的指标的信息，请参阅由 Agentless Collector 数据库和分析数据收集模块收集的数据。

> **Important**
>
> 终止支持通知：2026 年 5 月 20 日， AWS 将终止对 AWS Database Migration Service Fleet Advisor 的支持。2026 年 5 月 20 日之后，您将无法再访问 AWS DMS 舰队顾问控制台或 AWS DMS 舰队顾问资源。有关更多信息，请参阅 AWS DMS Fleet Advisor 终止支持。

简而言之，在使用数据库和分析数据收集模块时，您需要执行以下步骤。

1. 完成必备步骤，配置您的 IAM 用户，然后创建 AWS DMS 数据收集器。
2. 配置数据转发以确保您的数据收集模块可以将收集的元数据和性能指标发送到 AWS。

3. 添加您的 LDAP 服务器并使用它们发现数据环境中的操作系统服务器。或者，也可以手动添加操作系统服务器或使用使用 VMware 数据收集模块。
4. 配置操作系统服务器的连接凭据，然后使用它们来发现数据库服务器。
5. 配置数据库和分析服务器的连接凭据，然后运行数据收集。有关更多信息，请参阅 数据库和分析数据收集。
6. 在 AWS DMS 控制台中查看收集的数据，并使用这些数据生成迁移到控制台的目标建议 AWS Cloud。有关更多信息，请参阅 数据库和分析数据收集。

主题

支持的操作系统、数据库和分析服务器

无代理收集器中的数据库和分析数据收集模块支持 Microsoft Active Directory LDAP 服务器。

此数据收集模块支持以下操作系统服务器。

- Amazon Linux 2
- CentOS Linux 版本 6 及更高版本
- Debian 版本 10 及更高版本
- 红帽企业 Linux 版本 7 及更高版本
- SUSE Linux Enterprise Server 版本
- Ubuntu 版本 16.01 及更高版本
- Windows Server 2012 及更高
- Windows XP 及更高版本

此外，数据库和分析数据收集模块支持以下数据库服务器。

- Microsoft SQL Server 版本 2012 直至版本 2019
- MySQL 版本 5.6 直至版本 8
- Oracle 版本 11g 第 2 版直至 12c、19c 和 21c
- PostgreSQL 版本 9.6 直至版本 13

创建 AWS DMS 数据收集器

您的数据库和分析数据收集模块使用 AWS DMS 数据收集器与 AWS DMS 控制台进行交互。您可以在 AWS DMS 控制台中查看收集的数据，也可以使用它来确定大小合适的 AWS 目标引擎。有关更多信息，请参阅使用 AWS DMS Fleet Advisor 目标推荐功能。

在创建 AWS DMS 数据收集器之前，请创建一个 IAM 角色，您的 AWS DMS 数据收集器使用该角色来访问您的 Amazon S3 存储桶。您在中完成先决条件时创建了此 Amazon S3 存储桶无代理收集器的先决条件。

为 AWS DMS 数据收集器创建 IAM 角色以访问 Amazon S3

1. 登录到 AWS Management Console 并在上打开 IAM 控制台https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择角色，然后选择创建角色。
3. 在选择可信实体页面中，在可信实体类型下选择 AWS 服务。对于其他 AWS 服务的用例，请选择 DMS。
4. 选中 DMS 复选框，然后选择下一步。
5. 在添加权限页面上，选择您之前创建的 FleetAdvisorS3 Policy。选择下一步。
6. 在命名、检查并创建页面上，在角色名称中输入 **FleetAdvisorS3Role**，然后选择创建角色。
7. 打开您创建的角色，然后选择信任关系选项卡。选择编辑信任策略。
8. 在编辑信任策略页面上，将以下 JSON 粘贴到编辑器中，替换现有代码。

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

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

9. 选择更新策略。

现在，在 AWS DMS 控制台中创建一个数据收集器。

创建 AWS DMS 数据收集器

1. 登录 AWS Management Console 并在 https://console.aws.amazon.com/dms/v2/上打开 AWS DMS 控制台。
2. 选择您设置为 Migration Hub 主区域的。 AWS 区域 有关更多信息，请参阅 登录 Migration Hub 并选择主区域。
3. 在导航窗格中，在发现下选择数据收集器。数据收集器页面将打开。
4. 选择创建数据收集器。创建数据收集器页面将打开。
5. 在常规配置部分的名称中，输入数据收集器的名称。
6. 在连接部分中，选择浏览 S3。从列表中选择您之前创建的 Amazon S3 桶。
7. 对于 IAM 角色`FleetAdvisorS3Role`，请选择您之前创建的角色。
8. 选择创建数据收集器。

配置数据转发

创建所需 AWS 资源后，配置从数据库和分析数据收集模块到收集 AWS DMS 器的数据转发。

配置数据转发

1. 打开无代理收集器控制台。有关更多信息，请参阅 访问收集器控制台。
2. 选择 “查看数据库和分析收集器”。
3. 在 “控制面板” 页面上，选择 “数据转发” 部分的 “配置数据转发”。
4. 对于 AWS 区域IAM 访问密钥 ID 和 IAM 私有访问密钥，您的无代理收集器使用您之前配置的值。有关更多信息，请参阅登录 Migration Hub 并选择主区域和部署收集器。
5. 对于 C onnected DMS 数据收集器，请选择您在 AWS DMS 控制台中创建的数据收集器。
6. 选择保存。

配置数据转发后，请查看 “控制面板” 页面上的数据转发部分。确保您的数据库和分析数据收集模块显示为
“
已
连接” 以访问 DMS 和 “访问 S3”。

添加您的 LDAP 和操作系统服务器

数据库和分析数据收集模块使用 Microsoft Active Directory 中的 LDAP 来收集有关网络中操作系统、数据库和分析服务器的信息。轻型目录访问协议（LDAP）是一种开放标准应用程序协议。您可以使用此协议通过 IP 网络访问和维护分布式目录信息服务。

您可以将现有 LDAP 服务器添加到数据库和分析数据收集模块中，以自动发现网络中的操作系统服务器。如果您未使用 LDAP，则可以手动添加操作系统服务器。

将 LDAP 服务器添加到数据库和分析数据收集模块

1. 打开无代理收集器控制台。有关更多信息，请参阅 访问收集器控制台。
2. 选择 “查看数据库和分析收集器”，然后在导航窗格的 “发现” 下选择 LDAP 服务器。
3. 选择添加 LDAP 服务器。添加 LDAP 服务器页面打开。
4. 对于主机名，输入 LDAP 服务器的主机名。
5. 对于端口，输入 LDAP 请求所使用的端口号。
6. 对于用户名，输入用于连接 LDAP 服务器的用户名。
7. 在 “密码” 中，输入用于连接到 LDAP 服务器的密码。
8. （可选）选择 “验证连接”，确保正确添加了 LDAP 服务器凭据。或者，您可以稍后从 LDAP 服务器页面上的列表中验证您的 LDAP 服务器连接凭证。
9. 选择添加 LDAP 服务器。
10. 在 LDAP 服务器页面上，从列表中选择您的 LDAP 服务器，然后选择发现操作系统服务器。

> **Important**
>
> 对于操作系统发现，数据收集模块需要域服务器凭证，才能使用 LDAP 协议运行请求。

数据库和分析数据收集模块连接到您的 LDAP 服务器并发现您的操作系统服务器。数据收集模块完成操作系统服务器发现后，您可以通过选择 View OS 服务器来查看搜索到的操作系统服务器列表。

或者，您可以手动添加操作系统服务器或从逗号分隔值（CSV）文件导入服务器列表。此外，您还可以使用 VMware vCenter 无代理收集器数据收集模块来发现您的操作系统服务器。有关更多信息，请参阅 使用 VMware 数据收集模块。

将操作系统服务器添加到数据库和分析数据收集模块

1. 在数据库和分析收集器页面上，在导航窗格的 Discovery 下选择操作系统服务器。
2. 选择 “添加操作系统服务器”。将打开 “添加操作系统服务器” 页面。
3. 提供您的操作系统服务器凭据。

   a. 对于操作系统类型，请选择服务器的操作系统。

   b. 对于主机名/ IP，输入操作系统服务器的主机名或 IP 地址。

   c. 对于端口，输入用于远程查询的端口号。

   d. 对于身份验证类型，选择您的操作系统服务器使用的身份验证类型。

   e. 对于用户名，输入用于连接到操作系统服务器的用户名。

   f. 对于 Pass word (密码)，输入用于连接到操作系统服务器的密码。

   g. 选择 “验证”，确保您正确添加了操作系统服务器凭据。
4. （可选）从 CSV 文件添加多个操作系统服务器。

   a. 从 CSV 中选择批量导入操作系统服务器。

   b. 选择 “下载模板” 以保存包含您可以自定义的模板的 CSV 文件。

   c. 根据模板将操作系统服务器的连接凭据输入到文件中。以下示例说明了如何在 CSV 文件中提供操作系统服务器连接凭证。

   ```
   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
   ```

   为所有操作系统服务器添加凭据后，保存 CSV 文件。

   d. 选择 “浏览”，然后选择您的 CSV 文件。
5. 选择 “添加操作系统服务器”。
6. 为所有 OS 服务器添加凭据后，选择您的 OS 服务器并选择 Discover 数据库服务器。

探索您的数据库服务器

本节将指导您完成配置操作系统和数据库服务器必须采取的步骤。然后，您将发现自己的服务器并可以选择手动添加数据库或分析服务器。

对于数据库发现，必须为源数据库创建具有数据收集模块所需最低权限的用户。有关更多信息，请参阅用户指南中的为 AWS DMS Fleet Advisor 创建数据库AWS DMS用户。

配置设置

要发现以前添加的操作系统服务器上运行的数据库，数据收集模块需要访问操作系统和数据库服务器。本页概述了您需要采取的步骤，以确保您的数据库可以通过您在连接设置中指定的端口进行访问。您还需要在数据库服务器上打开远程身份验证，并为数据收集模块提供权限。

在 Linux 上配置设置

完成以下过程以在 Linux 上配置发现数据库服务器的设置。

配置 Linux 以发现数据库服务器

1. 提供对`ss`和`netstat`命令的 sudo 访问权限。

   以下代码示例授予 sudo 对`ss`和`netstat`命令的访问权限。

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

   在前面的示例中，将替换*username*为操作系统服务器连接凭证中指定的 Linux 用户名。

   前面的示例使用了`ss`和`netstat`命令的`/usr/bin/`路径。在您的环境中，此路径可能有所不同。要确定`ss`和`netstat`命令的路径，请运行`which ss`和`which netstat`命令。
2. 配置您的 Linux 服务器以允许运行远程 SSH 脚本并允许互联网控制消息协议（ICMP）流量。

在微软 Windows 上配置设置

完成以下过程以在 Microsoft Windows 上配置发现数据库服务器的设置。

将微软 Windows 配置为发现数据库服务器

1. 提供具以下权限的凭证：运行 Windows Management Languagion（WMI）和 WMI（WQL）查询并读取注册表。
2. 将您在操作系统服务器连接凭据中指定的 Windows 用户添加到以下组：分布式 COM 用户、性能日志用户、性能监视器用户和事件日志读取器。为此，请使用以下代码示例。

```
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
```

   在上述示例中，将替换*username*为操作系统服务器连接凭证中指定的 Windows 用户名。

3. 授予您在操作系统服务器连接凭据中指定的 Windows 用户所需的权限。
   - 在 “Windows 管理和工具属性” 中，选择 “本地启动” 和 “远程激活”。
   - 对于 WMI Control，选择、、和WMI命名空间的 “执行方法”、“启用帐户” **CIMV2**、**DEFAULT** “远程启用” 和 “读取安全” 权限。StandartCimv2
   - 对于 WMI 插件，请运行，winrm configsddl default然后选择 “读取并执行”。
4. 使用以下代码示例配置您的 Windows 主机。

```
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
```

探索数据库服务器

完成以下一组任务以在控制台上发现和添加数据库服务器。

开始发现您的数据库服务器

1. 在数据库和分析收集器页面上，在导航窗格的 Discovery 下选择操作系统服务器。
2. 选择包含您的数据库和分析服务器的操作系统服务器，然后在 “操作” 菜单上选择 “验证连接”。
3. 对于连接状态为 “失败” 的服务器，请编辑连接凭据。

   a. 选择一台或多台具有相同凭据的服务器，然后在 “操作” 菜单上选择 “编辑”。将打开 “编辑操作系统服务器” 页面。

   b. 对于端口，输入用于远程查询的端口号。

   c. 对于身份验证类型，选择您的操作系统服务器使用的身份验证类型。

   d. 对于用户名，输入用于连接到操作系统服务器的用户名。

   e. 对于 Pass word (密码)，输入用于连接到操作系统服务器的密码。

   f. 选择 “验证连接”，确保正确更新了操作系统服务器凭据。接下来，选择 保存。
4. 更新所有操作系统服务器的凭据后，选择您的操作系统服务器并选择发现数据库服务器。

数据库和分析数据收集模块连接到您的操作系统服务器并发现支持的数据库和分析服务器。数据收集模块完成发现后，您可以通过选择 “查看数据库服务器” 来查看已发现的数据库和分析服务器的列表。

或者，您可以手动将数据库和分析服务器添加到清单中。此外，您还可以从 CSV 文件中导入服务器列表。如果您已将所有数据库和分析服务器添加到清单中，则可跳过此步骤。

手动添加数据库或分析服务器

1. 在数据库和分析收集器页面上，选择导航窗格中的数据收集。
2. 选择 “添加数据库服务器”。将打开 “添加数据库服务器” 页面。
3. 提供您的数据库服务器凭据。

   a. 对于数据库引擎，请选择服务器的数据库引擎。有关更多信息，请参阅 支持的操作系统、数据库和分析服务器。

   b. 对于主机名/ IP，输入数据库或分析服务器的主机名或 IP 地址。

   c. 在 “端口” 中，输入服务器运行的端口。

   d. 对于身份验证类型，选择您的数据库或分析服务器使用的身份验证类型。

e. 对于用户名，输入用于连接到服务器的用户名。

f. 对于 Pass word (密码)，输入用于连接到服务器的密码。

g. 选择 “验证” 以确保正确添加了数据库或分析服务器凭据。

4. （可选）从 CSV 文件添加多台服务器。

a. 从 CSV 中选择批量导入数据库服务器。

b. 选择 “下载模板” 以保存包含您可以自定义的模板的 CSV 文件。

c. 根据模板将数据库和分析服务器的连接凭据输入到文件中。以下示例说明了如何在 CSV 文件中提供数据库或分析服务器连接凭证。

```
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,
```

为所有数据库和分析服务器添加凭据后，保存 CSV 文件。

d. 选择 “浏览”，然后选择您的 CSV 文件。

5. 选择 “添加数据库服务器”。

6. 为所有 OS 服务器添加凭据后，选择您的 OS 服务器并选择 Discover 数据库服务器。

将所有数据库和分析服务器添加到数据收集模块后，将其添加到清单中。数据库和分析数据收集模块可以从清单连接到服务器并收集元数据和性能指标。

将您的数据库和分析服务器添加到清单中

1. 在数据库和分析收集器页面上，在导航窗格的 Discovery 下选择数据库服务器。

2. 选择要为其收集元数据和性能指标的数据库和分析服务器。

3. 选择 “添加到库存”。

将所有数据库和分析服务器添加到清单后，就可以开始收集元数据和性能指标了。有关更多信息，请参阅 数据库和分析数据收集。

由 Agentless Collector 数据库和分析数据收集模块收集的数据

Application Discovery Service 无代理收集器（无代理收集器）数据库和分析数据收集模块从您的数据环境中收集以下指标。有关设置数据收集的信息，请参见使用数据库和分析数据收集模块。

当您使用数据库和分析数据收集模块收集元数据和数据库容量时，它会捕获以下指标。

- 操作系统服务器上的可用内存
- 操作系统服务器上的可用存储
- 数据库版本和发行版
- 您的操作系统服务器 CPUs 上的数量
- 架构的数量
- 已存储程序的数量
- 表的数量
- 触发器的数量
- 视图的数量
- 架构结构

在 AWS DMS 控制台中启动架构分析后，您的数据收集模块将分析并显示以下指标。

- 数据库支持日期
- 代码行数
- 架构复杂性
- 架构的相似性

当您使用数据库和分析数据收集模块收集元数据、数据库容量和资源利用率时，它会捕获以下指标。

- 数据库服务器上的 I/O 吞吐量
- 数据库服务器上每秒进行输入/输出操作的次数（IOPS）
- 您的操作系统服务器使用的数量 CPUs
- 操作系统服务器上的内存使用情况

- 操作系统服务器上的存储使用情况

您可以使用数据库和分析数据收集模块从 Oracle 和 SQL Server 数据库收集元数据、容量和利用率指标。同时，对于 PostgreSQL 和 MySQL 数据库，数据收集模块只能收集元数据。

查看您收集的数据

> **Important**
>
> 终止支持通知：2026 年 5 月 20 日， AWS 将终止对 AWS Database Migration Service Fleet Advisor 的支持。2026 年 5 月 20 日之后，您将无法再访问 AWS DMS 舰队顾问控制台或 AWS DMS 舰队顾问资源。有关更多信息，请参阅 AWS DMS Fleet Advisor 终止支持。

您可以按照中的步骤查看 Application Discovery Service 无代理收集器（无代理收集器）在 Migration Hub 控制台中收集的数据。在 AWS Migration Hub 控制台中查看服务器

您还可以通过执行以下步骤在 AWS DMS 控制台中查看为数据库和分析服务器收集的指标。

在 AWS DMS 控制台中查看数据库和分析数据收集模块发现的数据

1. 登录 AWS Management Console 并在 https://console.aws.amazon.com/dms/v2/上打开 AWS DMS 控制台。
2. 在 “发现” 下选择 “库存”。将打开清单页面。
3. 选择分析清单以确定数据库架构属性，例如相似性和复杂性。
4. 选择 “架构” 选项卡以查看分析结果。

您可以使用 AWS DMS 控制台识别重复的架构，确定迁移的复杂性，并导出清单信息以供将来分析。有关更多信息，请参阅在 F AWS DMS leet Advisor 中使用库存进行分析。

访问无代理收集器

本节介绍如何使用 Application Discovery Service 无代理收集器（无代理收集器）。

主题

- 无代理收集器仪表板

- 编辑无代理收集器设置
- 编辑 VMware vCenter 凭证

无代理收集器仪表板

在 Application Discovery Service 无代理收集器（无代理收集器）仪表板页面上，您可以查看收集器的状态并选择数据收集方法，如以下主题所述。

主题

- 收集器状态
- 数据收集

收集器状态

收集器状态为您提供有关收集器的状态信息。收集器名称、收集器与 AWS 的连接状态、Migration Hub 主区域和版本。

如果您遇到 AWS 连接问题，则可能需要编辑无代理收集器的配置设置。

要编辑收集器配置设置，请选择编辑收集器设置并按照中所述的说明进行操作编辑无代理收集器设置。

数据收集

在 “数据收集” 下，您可以选择数据收集方法。Application Discovery Service 无代理收集器（无代理收集器）目前支持从数据库 VMware VMs 和分析服务器收集数据。未来的模块将支持从其他虚拟化平台收集数据和操作系统级收集。

主题

- VMware vCenter 数据收集
- 数据库和分析数据收集

VMware vCenter 数据收集

要从中收集服务器清单、配置文件和利用率数据 VMware VMs，请设置与 vCenter 服务器的连接。要设置连接，请在 VMware vCenter 部分选择设置，然后按照中所述的说明进行操作。使用 VMware vCenter 无代理收集器数据收集模块

设置 vCenter 数据收集后，您可以从控制面板执行以下操作：

- 查看数据收集状态
- 启动数据收集
- 停止数据收集

> **Note**
>
> 在仪表板页面上，设置 vCenter 数据收集后，vCent VMwareer 部分的设置按钮将替换为数据收集状态信息、停止数据收集按钮以及查看和编辑按钮。

数据库和分析数据收集

您可以在以下两种模式下运行数据库和分析数据收集模块。

元数据和数据库容量

数据收集模块从您的数据库和分析服务器收集架构、版本、版本、CPU、内存和磁盘容量等信息。您可以使用收集到的这些信息在 AWS DMS 控制台中计算目标建议。如果您的源数据库配置过剩或配置不足，则目标建议也会被过度配置或配置不足。

这是默认模式。

元数据、数据库容量和资源利用率

除了元数据和数据库容量信息外，数据收集模块还收集数据库和分析服务器的 CPU、内存和磁盘容量的实际利用率指标。此模式提供的目标建议比默认模式更准确，因为建议基于实际的数据库工作负载。在此模式下，数据收集模块每分钟收集一次性能指标。

开始从数据库和分析服务器收集元数据和性能指标

1. 在数据库和分析收集器页面上，选择导航窗格中的数据收集。
2. 从数据库清单列表中，选择要为其收集元数据和性能指标的数据库和分析服务器。
3. 选择 “运行数据收集”。将打开 “数据收集类型” 对话框。
4. 选择如何收集数据进行分析。

   如果选择元数据、数据库容量和资源利用率选项，请设置数据收集周期。您可以在接下来的 7 天内收集数据，也可以设置自定义范围（1-60 天）。

5. 选择 “运行数据收集”。数据收集页面打开。
6. 选择 “集合运行状况” 选项卡以查看数据收集的状态。

完成数据收集后，您的数据收集模块会将收集的数据上传到您的 Amazon S3 存储桶。然后，您可以按中所述查看收集到的数据查看您收集的数据。

编辑无代理收集器设置

您在首次设置 Application Discovery Service 无代理收集器（无代理收集器）时配置了收集器，如中所述。配置无座席活动以下过程介绍如何编辑无代理收集器配置设置。

编辑收集器配置设置

- 在 “无代理收集器” 控制面板上选择 “编辑收集器设置” 按钮。

  在编辑收集器设置页面上，执行以下操作：

  a. 在收集器名称中，输入用于标识收集器的名称。名称可以包含空格，但不能包含特殊字符。
  b. 在发现数据的目标 AWS 帐户下，输入该 AWS 帐户的 AWS 访问密钥和密钥，以指定为接收收集器发现的数据的目标帐户。有关 IAM 用户要求的信息，请参阅部署 Applice Discovery Service 无座席活动。

     i. 对于AWS 访问密钥，请输入您指定为目标 AWS 账户的账户 IAM 用户的访问密钥。
     ii. 对于AWS 密钥，请输入您指定为目标 AWS 账户的 IAM 用户账户的密钥。
  c. 在 “无代理收集器密码” 下，更改用于对无代理收集器的访问进行身份验证的密码。

     i. 对于无代理收集器密码，请输入用于验证对无代理收集器的访问权限的密码。
     ii. 要重新输入 Agentless Collector 密码，请再次输入密码进行验证。
  d. 选择 “保存配置”。

接下来，你会看到无代理收集器仪表板。

编辑 VMware vCenter 凭证

要从中收集服务器清单、配置文件和利用率数据 VMware VMs，请设置与 vCenter 服务器的连接。有关设置 VMware vCenter 连接的信息，请参阅。使用 VMware vCenter 无代理收集器数据收集模块

本节介绍如何编辑 vCenter 凭据。

> **Note**
>
> 在编辑 vCenter 凭据之前，请确保您可以为系统组提供已设置读取和查看权限的 vCenter 凭据。

编辑 VMware vCenter 凭据

在该查看 VMware 数据收集详情页面上，选择编辑 vCenter 服务器。

- 在编辑 vCenter 页面上，执行以下操作：
  a. 在 vCenter 凭据下：
     i. 对于 vCenter URL/IP，请输入您的 vC VMware enter 服务器主机的 IP 地址。
     ii. 对于 vCenter Username (vCenter 用户名)，请输入连接器用来与 vCenter 通信的本地用户或域用户的名称。对于域用户，请使用 domain\username 或 username@domain 形式。
     iii. 对于 vCenter Password (vCenter 密码)，请输入本地或域用户密码。
  b. 选择保存。

手动更新 Application Discovery Service 无代理收集器

配置 Application Discovery Service 无代理收集器（无代理收集器）时，可以选择启用自动更新，如中所述。配置无座席活动如果您未启用自动更新，则需要手动更新 Agentless Collector。

以下过程介绍如何手动更新无代理收集器。

手动更新无代理收集器

1. 获取最新的无代理收集器开放虚拟化档案 (OVA) 文件。
2. （可选）我们建议您在部署最新的无代理收集器 OVA 文件之前删除以前的无代理收集器 OVA 文件。
3. 按照中的步骤操作部署无座席活动。

前面的过程仅更新无代理收集器。您有责任使操作系统保持最新状态。

更新您的 Amazon EC2 实例

1. 从 v VMware Center 获取无代理收集器的 IP 地址。
2. 打开收集器的 VM 控制台并**ec2-user**使用密码登录**collector**，如以下示例所示。

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

3. 按照 Amazon Linux 2 用户指南中在您的 AL2 实例上更新实例软件中的说明进行操作。

内核实时补丁

Agentless Collector version 2

无代理收集器版本 2 虚拟机使用亚马逊 Linux 2023，如中所述。部署无座席活动

要启用和使用适用于 Amazon Linux 2023 的实时补丁，请参阅《亚马逊用户指南》中的 AL2 023 上的 “内核实时补丁”。 EC2

Agentless Collector version 1

无代理收集器版本 1 虚拟机使用 Amazon Linux 2，如中所述。部署无座席活动

要启用和使用 Amazon Linux 2 的实时补丁，请参阅亚马逊 EC2 用户指南 AL2中的内核实时补丁。

从 Agentless Collector 版本 1 升级到版本 2

1. 使用最新映像安装新的无代理收集器 OVA。
2. 设置凭证。
3. 删除旧的虚拟设备。

对无代理收集器进行故障排除

本节包含的主题可以帮助您解决 Application Discovery Service 无代理收集器（无代理收集器）的已知问题。

主题

- 正在修复 Unable to retrieve manifest or certificate file error

正在修复 Unable to retrieve manifest or certificate file error

如果您在尝试通过 vC VMware enter 用户界面中的 Amazon S3 网址部署 OVA 时收到此错误，请确保您的 vCenter 服务器满足以下要求：

- VMware vCenter Server 版本 8.0 更新 1 或更高版本
- VMware vCenter Server 7.0 更新 3q（ISO 版本 23788036）或更高版本

解决配置 WinRM 证书时的自签名认证问题

如果启用 WinRM 证书检查，则可能需要将自签名证书颁发机构导入无代理收集器。

导入自签名证书颁发机构

1. 在 vCent VMware er 中打开收集器的 VM Web 控制台，然后`ec2-user`使用密码登录`collector`，如下例所示。

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

2. 确保用于签署 WinRM 证书的每个自签名 CA 证书都在目录下。`/etc/pki/ca-trust/source/anchors`例如：

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

3. 要安装新证书，请运行以下命令。

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

4. 运行以下命令重新启动无代理收集器

```
sudo shutdown -r now
```

5. （可选）要验证证书是否已成功导入，可以运行以下命令。

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

修复安装过程中无法访问 AWS 的无代理收集器

无代理收集器需要通过 TCP 端口 443 对多个域进行出站访问。 AWS 在控制台中配置 Agentless Collector 时，可能会收到以下错误消息。

> 无法到达 AWS
>
> AWS 无法到达。请验证网络设置。

出现此错误的原因是 Agentless Collector 尝试与该收集器在设置过程中需要与之通信的 AWS 域建立 HTTPS 连接失败。如果无法建立连接，则无代理收集器配置将失败。

将连接修复到 AWS

1. 请咨询您的 IT 管理员，了解贵公司的防火墙是否阻止了通过端口 443 向任何需要出站访问的 AWS 域名的出站流量。哪些 AWS 域名需要出站访问取决于您的主区域是美国西部（俄勒冈）区域、us-west-2 还是其他区域。

   如果您的 AWS 账户主区域为 us-west-2，则以下域名需要出站访问：

   - `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

如果您的 AWS 账户主区域不是，则以下域名需要出站访问权限**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

如果您的防火墙阻止了对 Agentless Collector 需要与之通信的 AWS 域的出站访问，请在 “收集器配置” 下的 “数据同步” 部分中配置代理主机。

2. 如果更新防火墙不能解决连接问题，请使用以下步骤确保收集器虚拟机具有与上一步中列出的域的出站网络连接。

   a. 从 v VMware Center 获取无代理收集器的 IP 地址。

   b. 打开收集器的 VM Web 控制台并**ec2-user**使用密码登录**collector**，如以下示例所示。

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

   c. 通过在端口 443 上运行 telnet 来测试与所列域的连接，如以下示例所示。

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

3. 如果 telnet 无法解析域，请尝试按照适用于 Amazon Linux 2 的说明配置静态 DNS 服务器。
4. 如果错误仍然存在，要获得更多支持，请参阅就无代理 AWS 收集器问题联系 Support。

修复连接到代理主机时的自签名认证问题

如果通过 HTTPS 与可选提供的代理进行通信，并且该代理具有自签名证书，则可能需要提供证书。

1. 从 v VMware Center 获取无代理收集器的 IP 地址。
2. 打开收集器的 VM Web 控制台并ec2-user使用密码登录collector，如以下示例所示。

```
username: ec2-user
```

```
password: collector
```

3. 将与安全代理关联的证书正文（包括-----BEGIN CERTIFICATE-----和-----END CERTIFICATE-----）粘贴到以下文件中：

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

4. 要安装新证书，请运行以下命令：

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

5. 通过运行以下命令重新启动无代理收集器：

```
sudo shutdown -r now
```

寻找不健康的收藏家

每个收集器的状态信息可在 AWS Migration Hub （Migration Hub）控制台的数据收集器页面上找到。您可以通过查找任何状态为 “需要关注” 的收藏家来识别有问题的收藏家。

以下过程介绍如何访问无代理收集器控制台以识别运行状况问题。

访问无代理收集器控制台

1. 使用您的 AWS 账户，登录 AWS Management Console 并打开 Migration Hub 控制台，网址为https://console.aws.amazon.com/migrationhub/。
2. 在 Migration Hub 控制台导航窗格的 “发现” 下，选择 “数据收集器”。
3. 在 “无代理收集器” 选项卡中，记下状态为 “需要注意” 的每个连接器的 IP 地址。
4. 要打开无代理收集器控制台，请打开 Web 浏览器。然后在地址栏中键入以下 URL: **https://** *<ip_address>***/**，其中 ip_addres s 是运行状况不佳的收集器的 IP 地址。
5. 选择 “登录”，然后输入无代理收集器密码，该密码是在中配置收集器时设置的。配置无座席活动
6. 在 “无代理收集器” 控制板页面上，在 “数据收集” 下，选择 vCent er VMware 部分的 “查看和编辑”。
7. 按照中的说明编辑 VMware vCenter 凭证更正 URL 和凭证。

更正运行状况问题后，收集器将重新建立与 vCenter Server 的连接，并且收集器的状态将更改为 “正在收集” 状态。如果问题仍然存在，请参阅就无代理 AWS 收集器问题联系 Support。

收集器运行状况不佳的最常见原因是 IP 地址和凭据问题。 修复 IP 地址问题并修复 vCenter 凭据问题可以帮助您解决这些问题并将收集器恢复到正常状态。

修复 IP 地址问题

如果收集器安装期间提供的 vCenter 端点格式错误、无效，或者 vCenter 服务器当前已关闭且无法访问，则收集器可能会进入不健康状态。在这种情况下，您将收到一条连接错误消息。

以下过程可以帮助您解决 IP 地址问题。

修复收集器 IP 地址问题

1. 从 v VMware Center 获取无代理收集器的 IP 地址。
2. 打开 Web 浏览器打开无代理收集器控制台，然后在地址栏中键入以下 URL：**`https://`***`<ip_address>`***`/`**，其中 ip_addr ess 是收集器来自的 IP 地址。部署无座席活动
3. 选择 “登录”，然后输入无代理收集器密码，该密码是在中配置收集器时设置的。配置无座席活动
4. 在 “无代理收集器” 控制板页面上，在 “数据收集” 下，选择 vCent er VMware 部分的 “查看和编辑”。
5. 在VMware 数据收集详细信息页面的 “已发现的 vCenter 服务器” 下，记下 vCenter 列中的 IP 地址。
6. 使用单独的命令行工具（如`ping`或）`traceroute`，验证关联的 vCenter 服务器是否处于活动状态，并且可以从收集器虚拟机访问 IP。
   - 如果 IP 地址不正确且 vCenter 服务处于活动状态，请在收集器控制台中更新 IP 地址，然后选择下一步。
   - 如果 IP 地址正确但 vCenter 服务器处于非活动状态，请将其激活。
   - 如果 IP 地址正确且 vCenter 服务器处于活动状态，请检查它是否因防火墙问题而阻止入口网络连接。如果是，请更新您的防火墙设置以允许来自收集器虚拟机的传入连接。

修复 vCenter 凭据问题

如果配置收集器时提供的 vCenter 用户凭据无效，或者没有 vCenter 读取和查看帐户权限，则收集器可能会进入不健康状态。

如果您遇到与 vCenter 凭据相关的问题，请检查并确保已为系统组设置了 vCenter 读取和查看权限。

有关编辑 vCenter 凭据的信息，请参阅。编辑 VMware vCenter 凭证

修复数据库和分析数据收集模块中的数据转发问题

Agentless Collector 中的数据库和分析数据收集模块的主页显示了访问 DMS 和访问 S3 的连接状态。如果您看到 “无法访问 DMS” 和 “访问 S3”，请配置数据转发。有关更多信息，请参阅 配置数据转发。

如果您在配置数据转发后遇到此问题，请检查以确保您的数据收集模块可以访问互联网。然后，请确保您已将DMSCollector策略和 FleetAdvisorS3Policy 策略添加到您的 IAM 用户。有关更多信息，请参阅 部署 Applice Discovery Service 无座席活动。

如果您的数据收集模块无法连接 AWS，请提供对以下域的出站访问权限。

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

修复数据库和分析数据收集模块中的连接问题

Agentless Collector 中的数据库和分析数据收集模块连接到您的 LDAP 服务器，以发现数据环境中的操作系统服务器。然后，数据收集模块连接到您的操作系统服务器以发现数据库和分析服务器。数据收集模块从这些数据库服务器收集容量和性能指标。如果您的数据收集模块无法连接到这些服务器，请验证您是否可以连接到您的服务器。

在以下示例中，用您的*replaceable*值替换值。

- 要验证是否可以连接到 LDAP 服务器，请安装该ldap-util软件包。为此，请运行以下命令。

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

  然后运行以下命令。

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

- 要验证是否可以连接到 Linux 操作系统服务器，请使用以下命令。

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

  在 Windows 中以管理员身份运行前面的示例。

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

在 Linux 中运行前面的示例。

- 要验证是否可以连接到 Windows 操作系统服务器，请使用以下命令。

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

在 Windows 中以管理员身份运行前面的示例。

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

在 Linux 中运行前面的示例。

- 要验证是否可以连接到 SQL Server 数据库，请使用以下命令。

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

- 要验证是否可以连接到 MySQL 数据库，请使用以下命令。

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

- 要验证是否可以连接到 Oracle 数据库，请使用以下命令。

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

- 要验证您是否可以连接到 PostgreSQL 数据库，请使用以下命令。

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

如果您无法连接到数据库和分析服务器，请确保提供所需的权限。有关更多信息，请参阅 探索您的数据库服务器。

支持独立 ESX 主机

无代理收集器不支持独立的 ESX 主机。ESX 主机必须是 vCenter Server 实例的一部分。

就无代理 AWS 收集器问题联系 Support

如果您在使用 Application Discovery Service 无代理收集器（无代理收集器）时遇到问题并需要帮助，请联系AWS 支持部门。我们将与您联系，并可能要求您发送收集器日志。

获取无代理收集器日志

1. 从 v VMware Center 获取无代理收集器的 IP 地址。
2. 打开收集器的 VM Web 控制台并**ec2-user**使用密码登录**collector**，如以下示例所示。

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

3. 使用以下命令导航到日志文件夹。

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

4. 使用以下命令压缩日志文件。

```
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. 从无代理收集器 VM 中复制日志文件。

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

6. 将`tar.gz`文件交给 E AWS nterprise Support。

将数据导入 Migration Hub

AWS Migration Hub （ Migration Hub ）导入允许您直接将本地环境的详细信息导入到 Migration Hub 中，而无需使用 Application Discovery Service 无代理收集器（ 无代理收集器 ）或 AWS 应用程序发现代理（ Discovery Agent ），因此您可以直接从导入的数据中执行迁移评估和规划。您还可以将设备作为应用程序来分组，并跟踪其迁移状态。

本页介绍完成导入请求的步骤。首先，使用以下两个选项之一来准备本地服务器数据。

- 使用常见的第三方工具生成包含本地服务器数据的文件。
- 下载我们的逗号分隔值 (CSV) 导入模板，并使用您的本地服务器数据填充该模板。

使用前面描述的两种方法之一创建本地数据文件后，您可以使用 Migration Hub 控制台或其中一种将文件上传到 Migration Hub AWS SDKs。 AWS CLI有关这两个选项的更多信息，请参阅the section called “支持的导入格式”。

您可以提交多个导入请求。各个请求按顺序处理。您可以随时通过控制台或导入检查导入请求的状态 APIs。

导入请求完成后，您可以查看各个导入记录的详细信息。直接从 Migration Hub 控制台中查看利用率数据、标签和应用程序映射。如果在导入过程中遇到错误，您可以查看成功和失败的记录计数以及每个失败的记录的错误详情。

处理错误：系统提供了一个链接，可将错误日志和失败记录文件以 CSV 格式下载到压缩归档中。纠正错误后，使用这些文件重新提交您的导入请求。

限制适用于导入的记录数、导入的服务器数和您可以保留的已删除记录数。有关更多信息，请参阅 AWS Application Discovery Service 配额。

支持的导入格式

Migration Hub 支持以下导入格式。

- RVTools
- Migration Hub 导入模板

RVTools

Migration Hub 支持通过导入 VMware vSphere 的导出。 RVTools保存来自的数据时 RVTools，首先选择 “全部导出到 csv” 选项或 “全部导出到 Excel” 选项，然后压缩文件夹，然后将 ZIP 文件导入 Migration Hub 中。ZIP 中需要以下文件：VinFO、vNetwork、vCPU、vMemory、vDisk、vPartition、vSource、vTools、vHost、vNIC、vsc_vmk。

Migration Hub 导入模板

Migration Hub 导入允许您从任何来源导入数据。提供的数据必须采用 CSV 文件支持的格式，且数据仅包含支持的字段，同时支持的字段使用支持的范围。

下表中导入字段名称旁边的星号 (*) 表示该字段为必填字段。您的导入文件的每个记录都必须至少填充一个或多个这样的必填字段，以便唯一地标识服务器或应用程序。否则，不含任何必填字段的记录将无法导入。

下表中导入文件名旁边的尖号 (^) 表示如果提供了 serverID，则该名称为只读。

> **Note**
>
> 如果你正在使用任何一个 VMware。 MoRefId 或 VMWare。 VCenter同上，要识别一条记录，必须将两个字段放在同一条记录中。

导入字段名称	描述	示例
ExternalId*^	允许您唯一标识每个记录的自定义标识符。例如，ExternalId可以是数据中心内服务器的清单 ID。	Inventory Id 1 Server 2 CMBD Id 3
SMBios我^	系统管理 BIOS (SMBIOS) ID。	
IPAddress*^	逗号分隔的服务器 IP 地址列表，用引号引起来。	192.0.0.2 "10.12.31.233, 10.12.32.11"

导入字段名称	描述	示例
MACAddress*^	逗号分隔的服务器 MAC 地址列表，用引号引起来。	00:1B:44:11:3A:B7 "00-15-E9-2B-99-3C, 00-14-22-01-23-45"
HostName*^	服务器的主机名。建议对该值使用完全限定的域名 (FQDN)。	ip-1-2-3-4 localhost.domain
VMware.MoRefId*^	托管对象的引用 ID。必须提供 VMware. VCenter同上。	
VMware。 VCenter身份证*^	虚拟机的唯一标识符。必须提供 VMware. MoRefId。	
CPU。 NumberOfProcessors^	的数量 CPUs。	4
CPU。 NumberOfCores^	物理内核的总数。	8
CPU。 NumberOfLogicalCores^	服务器中可以同时 CPUs在所有线程上运行的线程总数。有些 CPUs 支持在单个 CPU 内核上同时运行多个线程。在这种情况下，此数量将大于物理（或虚拟）内核的数量。	16
os.name^	操作系统的名称。	Linux Windows.Hat
os.version^	操作系统的版本。	16.04.3 NT 6.2.8
VMware.VMName^	虚拟机的名称。	Corp1

导入字段名称	描述	示例
公羊。 TotalSizeInMB^	服务器上可用 RAM 的总量，以 MB 为单位。	64 128
公羊。 UsedSizeInmb.avg^	服务器上的平均 RAM 用量，以 MB 为单位。	64 128
公羊。 UsedSizeInmb.max^	服务器上可用的最大 RAM 用量，以 MB 为单位。	64 128
CPU。 UsagePct.Avg^	发现工具收集数据时的平均 CPU 使用率。	45 23.9
CPU。 UsagePct.Max^	发现工具收集数据时的最大 CPU 使用率。	55.34 24
DiskReadsPerSecond Inkb.avg^	每秒平均磁盘读取数 (KB)。	1159 84506
DiskWritesPerSecondInkb.avg^	每秒平均磁盘写入数 (KB)。	199 6197
DiskReadsPerSecond Inkb.max^	每秒最大磁盘读取数 (KB)。	37892 869962
DiskWritesPerSecon dInkb.max^	每秒最大磁盘写入数 (KB)。	18436 1808
DiskReadsOpsPerSec ond.Avg^	每秒平均磁盘读取操作数。	45 28

导入字段名称	描述	示例
DiskWritesOpsPerSecond.Avg^	每秒平均磁盘写入操作数。	8 3
DiskReadsOpsPerSecond.Max^	每秒最大磁盘读取操作数。	1083 176
DiskWritesOpsPerSecond.Max^	每秒最大磁盘写入操作数。	535 71
NetworkReadsPerSecondInkb.avg^	每秒平均网络读取操作数 (KB)。	45 28
NetworkWritesPerSecondInkb.avg^	每秒平均网络写入操作数 (KB)。	8 3
NetworkReadsPerSecondInkb.max^	每秒最大网络读取操作数 (KB)。	1083 176
NetworkWritesPerSecondInkb.max^	每秒最大网络写入操作数 (KB)。	535 71
应用程序	逗号分隔的包括此服务器的应用程序列表，用引号引起来。该值可以包括现有应用程序和/或导入时创建的新应用程序。	Application1 "Application2, Application3"
ApplicationWave	这台服务器的迁移浪潮。	

导入字段名称	描述	示例
标签^	逗号分隔的格式为 name:value 的标签列表。 **Important** 请勿将敏感信息（如个人数据）存储在标签中。	"zone:1, critical:yes" "zone:3, critical:no, zone:1"
ServerId	在 Migration Hub 服务器列表中显示的服务器标识符。	`d-server-01kk9i6yw waxmp`

即便并非导入模板中定义的所有字段都填充了数据，您也可以导入数据，只要每个记录至少填充了一个必填字段即可。通过使用外部或内部匹配键来跨多个导入请求管理重复项。如果您填充自己的匹配键 `External ID`，则此字段用于唯一地标识和导入记录。如果未指定匹配键，则导入将使用内部生成的匹配键，该键由导入模板的某些列派生而来。有关此匹配的更多信息，请参阅匹配已发现的服务器和应用程序的逻辑。

Note

Migration Hub 导入不支持导入模板中定义的字段之外的任何字段。提供的任何自定义字段将被忽略，不会导入。

设置导入权限

在导入数据之前，请确保您的 IAM 用户拥有必要的 Amazon S3 权限，可以将您的导入文件上传 (`s3:PutObject`) 到 Amazon S3 并读取对象 (`s3:GetObject`)。您还必须通过创建 IAM 策略并将其附加到在您的 AWS 账户中执行导入的 IAM 用户来建立编程访问权限（用于 AWS CLI）或控制台访问权限。

Console Permissions

使用以下过程编辑将使用控制台在您的 AWS 账户中提出导入请求的 IAM 用户的权限策略。

编辑用户的已附加托管策略

1. 登录 AWS Management Console 并打开 IAM 控制台，网址为https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择 Users（用户）。
3. 请选择要更改其权限策略的用户的名称。
4. 选择权限选项卡，选择添加权限。
5. 选择直接附加现有策略，然后选择创建策略。

   a. 在打开的创建策略页面上，选择 JSON，然后粘贴以下策略。记住将您的存储桶名称替换成 IAM 用户将导入文件上传到其中的存储桶的实际名称。

```
{
  "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. 选择查看策略。

c. 为您的策略提供一个新名称和描述（可选），然后检查策略摘要。

d. 选择创建策略。

6. 返回将在您的 AWS 账户中提出导入请求的用户的授予权限 IAM 控制台页面。
7. 刷新策略表，搜索您刚才创建的策略的名称。
8. 选择 Next: Review（下一步：审核）。
9. 选择 Add permissions (添加权限)。

现在，您已将策略添加到 IAM 用户，就可以开始导入过程了。

AWS CLI Permissions

使用以下过程创建必要的托管策略，以授予 IAM 用户使用提出导入数据请求的权限 AWS CLI。

创建和附加托管策略

1. 使用`aws iam create-policy` AWS CLI 命令创建具有以下权限的 IAM 策略。记住将您的存储桶名称替换成 IAM 用户将导入文件上传到其中的存储桶的实际名称。

```
{
  "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/*"]
    }
  ]
}
```

有关使用此命令的更多信息，请参阅《命令参考》中的 create-AWS CLI p ol icy。

2. 使用`aws iam create-policy` AWS CLI 命令创建具有以下权限的其他 IAM 策略。

```
{
    "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. 使用`aws iam attach-user-policy` AWS CLI 命令将您在前两个步骤中创建的策略附加到将使用在您的 AWS 账户中执行导入请求的 IAM 用户 AWS CLI。有关使用此命令的更多信息，请参阅《AWS CLI 命令参考》attach-user-policy中的。

现在，您已将策略添加到 IAM 用户，就可以开始导入过程了。

请记住，当 IAM 用户将对象上传到您指定的 Amazon S3 存储桶时，他们必须保留对象的默认权限设置，这样用户才能读取该对象。

将您的导入文件上传到 Amazon S3

接下来，您必须将 CSV 格式的导入文件上传到 Amazon S3，这样才能将其导入。在开始之前，您应该有一个 Amazon S3 存储桶，用于存放您提前创建和/或选择的导入文件。

Console S3 Upload

将您的导入文件上传到 Amazon S3

1. 登录 AWS Management Console 并打开 Amazon S3 控制台，网址为https://console.aws.amazon.com/s3/。
2. 在 Bucket name 列表中，选择要将对象上传到的存储桶的名称。
3. 选择上传。
4. 在 Upload 对话框中，选择 Add files 以选择要上传的文件。
5. 选择要上传的文件，然后选择打开。
6. 选择上传。
7. 上传完文件后，从您的存储桶控制面板选择您的数据文件对象的名称。
8. 从对象详细信息页面的 Overview (概述) 选项卡上，复制 Object URL (对象 URL)。在创建导入请求时，需要这个 URL。
9. 转到 Migration Hub 控制台中的 “导入” 页面，如中所述导入数据。然后，将对象 URL 粘贴到 Amazon S3 对象网址字段中。

AWS CLI S3 Upload

将您的导入文件上传到 Amazon S3

1. 打开终端窗口，导航到保存导入文件的目录。
2. 输入以下命令：

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

3. 这将返回以下结果：

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

4. 复制返回的完整 Amazon S3 对象路径。在创建导入请求时，您将需要这个。

导入数据

从 Migration Hub 控制台下载导入模板并使用现有本地服务器数据填充模板后，就可以开始将数据导入到 Migration Hub 了。以下说明描述了两种实现此目的的方法，要么使用控制台，要么通过进行 API 调用 AWS CLI。

Console Import

在 Migration Hub 控制台的 “工具” 页面上开始导入数据。

启动数据导入

1. 在导航窗格中的 Discover (发现) 下，选择 Tools (工具)。
2. 如果您还没有填写导入模板，可以通过选择 Import (导入) 框中的 import template (导入模板) 下载该模板。打开下载的模板，用您的现有本地服务器数据填充它。你也可以从我们的 Amazon S3 存储桶下载导入模板，网址https://s3.us-west-2.amazonaws.com/templates-7cffcf56-bd96-4b1c-b45b-a5b42f282e46/为 import_template.csv
3. 要打开 “导入” 页面，请在 “导入” 框中选择 “导入”。
4. 在 “导入名称” 下，指定导入的名称。
5. 填写 Amazon S3 对象网址字段。要执行此步骤，您需要将导入数据文件上传到 Amazon S3。有关更多信息，请参阅 将您的导入文件上传到 Amazon S3。
6. 选择右下方的 Import (导入)。这将打开 Import (导入) 页面，在该页面中，您可以查看您的导入及其在表中列出的状态。

按照上述过程启动您的数据导入后，Imports (导入) 页面将显示每个导入请求的详细信息，包括进度状态、完成时间、成功或失败记录的数量以及下载这些记录的功能。从该屏幕中，您还可以导航至 Servers (服务器) 页面，在 Discover (发现) 下查看实际导入的数据。

在 Servers (服务器) 页面上，您可以看到所有被发现的服务器（设备）的列表以及导入名称。当您通过选择 “名称” 列中列出的导入名称从 “导入（导入历史记录）” 页面导航时，您将被带到 “服务器” 页面，在该页面中将根据所选导入的数据集应用筛选器。然后，您只能看到属于该特定导入的数据。

归档为 .zip 格式，其中包含两个文件：`errors-file` 和 `failed-entries-file`。errors 文件包含与来自导入失败的数据文件的每个失败行关联的错误消息列表及关联列名称。您可以使用该文件快速确定问题所在位置。失败的条目文件包含失败的各行和所有提供的列。您可以在该文件中执行 errors 文件中指出的更改，然后再次导入更正了信息的文件。

AWS CLI Import

要从开始数据导入过程 AWS CLI， AWS CLI 必须先在您的环境中安装。有关更多信息，请参阅《AWS Command Line Interface 用户指南》中的安装 AWS 命令行界面。

> **Note**
>
> 如果您尚未填写导入模板，则可以在此处从我们的 Amazon S3 存储桶下载导入模板：https://s3.us-west-2.amazonaws.com/templates-7cffcf56-bd96-4b1c-b45b-a5b42f282e46/import_template.csv

启动数据导入

1. 打开一个终端窗口，键入以下命令：

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

2. 这将创建您的导入任务，并返回以下状态信息：

```
{
    "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"
    }
}
```

追踪您的 Migration Hub 导入请求

您可以使用控制台或其中一个来跟踪 Migration Hub 导入请求的状态 AWS SDKs。 AWS CLI

Console Tracking

在 Migration Hub 控制台的 “导入” 控制面板中，你会发现以下元素。

- 名称-导入请求的名称。
- 导入 ID-导入请求的唯一 ID。
- 导入时间-创建导入请求的日期和时间。
- 导入状态-导入请求的状态。它可以是以下值之一：
  - 导入-此数据文件当前正在导入中。
  - 已@@ 导入-已成功导入整个数据文件。
  - 导入时出错-数据文件中的一条或多条记录导入失败。要解决失败的记录问题，请针对您的导入任务选择 Download failed records (下载失败的记录)，纠正失败条目 csv 文件中的错误，然后再次导入。
  - 导入失败-数据文件中没有导入的记录。要解决失败的记录问题，请针对您的导入任务选择 Download failed records (下载失败的记录)，纠正失败条目 csv 文件中的错误，然后再次导入。
- 导入的记录-特定数据文件中成功导入的记录数。
- 失败的记录-特定数据文件中未导入的记录数。

CLI Tracking

您可以使用`aws discovery describe-import-tasks` AWS CLI 命令跟踪导入任务的状态。

1. 打开一个终端窗口，键入以下命令：

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

2. 这将以 JSON 格式返回您的所有导入任务的列表，并列出导入状态和其他相关信息。（可选）您可以筛选结果以返回导入任务的子集。

在跟踪导入任务时，您可能会发现返回的 `serverImportFailure` 值大于零。如果发生这种情况，则说明您的导入文件中包含一个或多个无法导入的条目。要解决这一问题，可下载您的失败记录归档，检查其中的文件，然后用修改后的 failed-entries.csv 文件再次请求导入。

创建导入任务后，您可以执行其他操作来帮助管理和跟踪您的数据迁移。例如，您可以针对特定请求下载失败记录归档。有关使用失败的记录归档来解决导入问题的信息，请参阅排除导入失败记录的问题。

查看和浏览已发现的数据

Application Discovery Service 无代理收集器（无代理收集器）和 AWS Discovery Agent（Discovery Agent）都根据平均利用率和峰值利用率提供系统性能数据。您可以使用收集到的系统性能数据来计算总体拥有成本 (TCO)。Discovery Agent 会收集更详细的数据，包括系统性能信息、入站和出站网络连接以及服务器上运行的进程的时间序列数据。您可以使用此数据了解服务器之间的网络依赖关系并将相关服务器分组为应用程序以进行迁移规划。

在本节中，您将找到有关如何查看和使用无代理收集器和发现代理从控制台和发现代理发现的数据的说明。 AWS CLI

主题

使用 Migration Hub 控制台查看收集的数据

对于 Application Discovery Service 无代理收集器（无代理收集器）和 AWS Discovery Agent（Discovery Agent），在数据收集过程开始后，您可以使用控制台查看他们收集的有关您的服务器和的数据。 VMs数据收集开始大约 15 分钟后，数据会显示在控制台中。您还可以使用 API 调用导出收集的数据，从而以 CSV 格式查看这些数据 AWS CLI。

要在控制台中查看已发现的服务器的收集数据，请按照中的步骤操作在 AWS Migration Hub 控制台中查看服务器。要了解有关使用控制台查看、排序和标记无代理收集器或 Discovery Agent 发现的服务器的更多信息，请参阅。使用 AWS Migration Hub 控制台发现数据

无代理收集器数据库和分析数据收集模块将收集的数据上传到 Amazon S3 存储桶。您可以在 AWS DMS 控制台中查看该存储桶中的数据。要查看已发现的数据库和分析服务器的收集数据，请按照中的步骤操作查看您收集的数据。

匹配已发现的服务器和应用程序的逻辑

AWS Application Discovery Service （Application Discovery Service）具有内置的匹配逻辑，可以识别它发现的服务器何时与现有条目匹配。当该逻辑发现一个匹配项时，它会用新值更新已存在的被发现服务器的信息。

此匹配逻辑可以处理来自多个来源的重复服务器，包括 AWS Migration Hub （Migration Hub）导入、Application Discovery Service 无代理收集器（无代理收集器）、 AWS 应用程序发现代理

（Discovery Agent）和其他迁移工具。有关 Migration Hub 导入的更多信息，请参阅 Migrat ion Hub 导入。

在执行服务器发现时，每个条目与之前导入的记录进行交叉检查，以确保导入的服务器尚不存在。如果未找到匹配项，则会创建一个新记录，并为新记录分配一个新的唯一服务器标识符。如果找到匹配项，仍会创建一个新条目，但会为新条目分配与现有服务器相同的唯一服务器标识符。在 Migration Hub 控制台中查看此服务器时，只能找到该服务器的一个唯一条目。

与此条目关联的服务器属性被合并，以显示来自先前可用记录和新导入记录的属性值。如果一个给定服务器属性具有来自多个来源的多个值，例如使用导入和使用 Discovery Agent 发现的给定服务器有关联的两个不同的 `Total RAM` 值，则在该服务器的匹配记录中，将显示最近更新的值。

匹配字段

当使用发现工具时，使用以下字段来匹配服务器。

- ExternalId— 这是用于匹配服务器的主要字段。如果此字段中的值与其他条目`ExternalId`中的值相同，则无论其他字段是否匹配，Application Discovery Service 都会匹配这两个条目。
- IPAddress
- HostName
- MacAddress
- VMware。 MoRefId和VMware。 vCenterId— 这两个值必须与另一个条目中的相应字段相同，Application Discovery Service 才能执行匹配。

探索亚马逊 Athena 中的数据

Amazon Athena 中的数据探索允许您在一个地方分析 Discovery Agent 从发现的所有本地服务器中收集的数据。从 Migration Hub 控制台（或使用 StartContinousExport API）启用 Amazon Athena 中的数据探索并开启代理数据收集功能后，代理收集的数据将定期自动存储在您的 S3 存储桶中。有关更多信息，请参阅 探索亚马逊 Athena 中的数据。

Amazon Athena 中的数据探索允许您在一个地方分析发现代理从发现的所有本地服务器收集的数据。从 Migration Hub 控制台（或使用 StartContinousExport API）启用 Amazon Athena 中的数据探索并开启代理数据收集功能后，代理收集的数据将定期自动存储在您的 S3 存储桶中。

然后，您可以访问 Amazon Athena 运行预定义的查询，以分析每台服务器的时间序列系统性能、每台服务器上运行的进程类型以及不同服务器之间的网络依赖关系。此外，您还可以使用 Amazon Athena

编写自己的自定义查询，上传其他现有数据源，例如配置管理数据库 (CMDB) 导出，并将发现的服务器与实际业务应用程序关联起来。您还可以将 Athena 数据库与 A QuickSight mazon 集成，以可视化查询输出并执行其他分析。

本节中的主题描述了在 Athena 中使用数据来评估和规划将本地环境迁移到的方式。 AWS

在 Amazon Athena 中开启数据探索

使用 Migration Hub 控制台或从 API 调用开启持续导出，即可在 Amazon Athena 中进行数据探索。AWS CLI您必须先开启数据探索功能，然后才能在 Amazon Athena 中查看并开始探索已发现的数据。

开启 “连续导出” 后，您的账户将自动使用服务相关角色`AWSServiceRoleForApplicationDiscoveryServiceContinuousExport`。有关此服务相关角色的更多信息，请参阅Application Discovery Service 的服务相关角色权限。

以下说明说明如何使用控制台和 Amazon Athena 开启数据探索功能。 AWS CLI

Turn on with the console

在 Migration Hub 控制台的 “数据收集器” 页面上选择 “开始数据收集”，或者在 Migration Hub 控制台的数据收集器页面上单击 “在 Amazon Athena 中进行数据探索” 的切换开关时，隐式开启持续导出，即可启用 Amazon Athena 中的数据探索。

通过控制台在 Amazon Athena 中开启数据探索

1. 在导航窗格中，选择 Data Collectors (数据收集器)。
2. 选择 Agents (代理) 选项卡。
3. 选择 “开始数据收集”，或者如果您已经开启了数据收集，请单击 “Amazon Athena 中的数据探索” 开关。
4. 在上一步生成的对话框中，单击同意关联成本的复选框并选择 Continue (继续) 或 Enable (启用)。

> **Note**
>
> 您的代理现在以 “持续导出” 模式运行，这将使您能够在 Amazon Athena 中查看和处理发现的数据。首次启用此功能时，您的数据最多可能需要 30 分钟才能显示在 Amazon Athena 中。

Enable with the AWS CLI

Amazon Athena 中的数据探索功能是通过来自 API 调用明确开启的 “持续导出”。 AWS CLI为此，AWS CLI 必须先在您的环境中安装。

要在 Amazon Athena 中安装 AWS CLI 并开启数据探索

1. 安装 AWS CLI 适用于您的操作系统（Linux、macOS 或 Windows）的。有关说明，请参阅AWS Command Line Interface 用户指南。
2. 打开命令提示符 (Windows) 或终端 (Linux 或 macOS)。
   a. 键入 `aws configure` 并按下 Enter。
   b. 输入您的 AWS 访问密钥 ID 和 AWS 私有访问密钥。
   c. 对于默认区域名称，输入 `us-west-2`。
   d. 对于默认输出格式，输入 `text`。
3. 键入以下命令：

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

> **Note**
>
> 您的代理现在以 “持续导出” 模式运行，这将使您能够在 Amazon Athena 中查看和处理发现的数据。首次启用此功能时，您的数据最多可能需要 30 分钟才能显示在 Amazon Athena 中。

直接在 Amazon Athena 中浏览数据

在 Amazon Athena 中开启数据探索后，您可以直接在 Athena 中查询数据，开始探索和处理代理发现的详细当前数据。您可以使用这些数据生成电子表格，运行成本分析，将查询移植到可视化程序以便以示意图方式呈现网络依赖关系等等。

以下说明说明了如何直接在 Athena 控制台中浏览代理数据。如果您在 Athena 中没有任何数据，或者尚未在 Amazon Athena 中启用数据探索，则系统会显示一个对话框提示您在 Amazon Athena 中启用数据探索，如中所述。在 Amazon Athena 中开启数据探索

直接在 Athena 中浏览代理发现的数据

1. 在 AWS Migration Hub 控制台中，选择导航窗格中的服务器。
2. 要打开亚马逊 Athena 控制台，请选择 “在亚马逊 Athena 中浏览数据”。
3. 在 Query Editor (查询编辑器) 页面上，在 Database (数据库) 下的导航窗格中，确保选择了 application_discovery_service_database。

   > **Note**
   >
   > 在 Tables (表) 下，以下各表表示按代理分组的数据集。
   >
   > - os_info_agent
   > - network_interface_agent
   > - sys_performance_agent
   > - processes_agent
   > - inbound_connection_agent
   > - outbound_connection_agent
   > - id_mapping_agent

4. 通过在 Athena 查询编辑器中编写和运行 SQL 查询，在 Amazon Athena 控制台中查询数据。例如，您可以使用以下查询来查看发现的所有服务器 IP 地址。

   ```
   SELECT * FROM network_interface_agent;
   ```

   有关更多示例查询，请参阅在 Amazon Athena 中使用预定义查询。

可视化亚马逊 Athena 数据

为了可视化您的数据，可以将查询移植到亚马逊等可视化程序 QuickSight 或其他开源可视化工具，例如Cytoscape、yEd或Gelphi。使用这些工具来渲染网络图、摘要图表和其他图形表示。使用此方法时，您可以通过可视化程序连接到 Athena，这样它就可以访问您收集的数据作为生成可视化的来源。

使用可视化您的亚马逊 Athena 数据 QuickSight

1. 登录亚马逊 QuickSight。
2. 选择 Connect to another data source or upload a file (连接到其他数据源或上传文件)。

3. 选择 Athena。将显示 “新建 Athena 数据源” 对话框。
4. 在 Data source name (数据源名称) 字段中输入名称。
5. 选择创建数据来源。
6. 在 “选择您的gents-servers-os表” 对话框中选择 A 表，然后选择选择。
7. 在 Finish dataset creation (完成数据集创建) 对话框中，依次选择 Import to SPICE for quicker analytics (导入到 SPICE 以进行快速分析) 和 Visualize (可视化)。

   将呈现您的可视化结果。

在 Amazon Athena 中使用预定义查询

本节包含一组预定义的查询，这些查询可执行典型的使用案例，如 TCO 分析和网络可视化。您可以按原样使用这些查询，或根据自己的需求对其进行修改。

使用预定义的查询

1. 在 AWS Migration Hub 控制台中，选择导航窗格中的服务器。
2. 要打开亚马逊 Athena 控制台，请选择 “在亚马逊 Athena 中浏览数据”。
3. 在 Query Editor (查询编辑器) 页面上，在 Database (数据库) 下的导航窗格中，确保选择了 application_discovery_service_database。
4. 在查询编辑器中选择加号 (+) 以创建新查询的选项卡。
5. 从 预定义查询中复制其中一个查询。
6. 将查询粘贴到刚创建的新查询选项卡的查询窗格中。
7. 选择 Run Query (运行查询)。

预定义查询

选择标题以查看有关此查询的信息。

获取服务器的 IP 地址和主机名

该视图帮助程序函数检索给定服务器的 IP 地址和主机名。您可以在其他查询中使用此视图。有关如何创建视图的信息，请参阅 Amazon Athena 用户指南中的创建视图。

```
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");
```

识别有或没有代理的服务器

此查询可以帮助您执行数据验证。如果您在网络中的多台服务器上部署了代理，则可以使用此查询来了解在网络中是否存在其他没有部署代理的服务器。在此查询中，我们检查入站和出站网络流量，并且只筛选私有 IP 地址的流量。即以 192、10 或 172 开头的 IP 地址。

```
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.%'));
```

分析带有代理的服务器的系统性能数据

您可以使用此查询来分析安装了代理的本地服务器的系统性能和使用率模式数据。此查询结合 system_performance_agent 表与 os_info_agent 表来标识每个服务器的主机名。此查询为其上正在运行代理的所有服务器返回时间序列利用率数据（以 15 分钟为间隔）。

```
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;
```

根据端口号和进程详细信息跟踪服务器之间的出站通信

此查询获取每个服务的出站流量的详细信息，以及端口号和进程详细信息。

在运行查询之前，如果尚未执行此操作，则必须创建 iana_service_ports_import 表，其中包含从 IANA 下载的 IANA 端口注册表数据库。有关如何创建此表的信息，请参阅 创建 IANA 港口注册表导入表。

创建 iana_service_ports_import 表后，创建两个用于跟踪出站流量的视图帮助程序函数。有关如何创建视图的信息，请参阅 Amazon Athena 用户指南中的创建视图。

创建出站跟踪帮助程序函数

1. 从 https://console.aws.amazon.com/athena/ 打开 Athena 控制台。
2. 使用以下列出所有不同出站目标 IP 地址的辅助函数创建valid_outbound_ips_helper视图。

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

3. 使用以下帮助程序函数创建 outbound_query_helper 视图，该函数确定出站流量的通信频率。

```
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. 在创建 iana_service_ports_import 表和两个帮助程序函数之后，您可以运行以下查询来获取每个服务的出站流量的详细信息，以及端口号和进程详细信息。

```
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
```

根据端口号和进程详细信息跟踪服务器之间的入站通信

此查询获取有关每个服务的入站流量的信息，以及端口号和进程详细信息。

在运行此查询之前，如果尚未执行此操作，则必须创建 `iana_service_ports_import` 表，其中包含从 IANA 下载的 IANA 端口注册表数据库。有关如何创建此表的信息，请参阅 创建 IANA 港口注册表导入表。

创建 `iana_service_ports_import` 表后，创建两个用于跟踪入站流量的视图帮助程序函数。有关如何创建视图的信息，请参阅 Amazon Athena 用户指南中的创建视图。

创建导入跟踪帮助程序函数

1. 从 https://console.aws.amazon.com/athena/ 打开 Athena 控制台。
2. 使用以下帮助程序函数创建 `valid_inbound_ips_helper` 视图，该函数列出了所有不同的入站源 IP 地址。

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

3. 使用以下帮助程序函数创建 `inbound_query_helper` 视图，该函数确定入站流量的通信频率。

```
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. 在创建 iana_service_ports_import 表和两个帮助程序函数之后，您可以运行以下查询来获取每个服务的入站流量的详细信息，以及端口号和进程详细信息。

```
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
```

通过端口号识别正在运行的软件

此查询基于端口号识别正在运行的软件。

在运行此查询之前，如果尚未执行此操作，则必须创建 iana_service_ports_import 表，其中包含从 IANA 下载的 IANA 端口注册表数据库。有关如何创建此表的信息，请参阅 创建 IANA 港口注册表导入表。

运行以下查询，以基于端口号识别正在运行的软件。

```
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;
```

创建 IANA 港口注册表导入表

某些预定义的查询需要一个名为 iana_service_ports_import 的表，该表包含从 Internet 号码分配机构 (IANA) 下载的信息。

创建 iana_service_ports_import 表

1. 从 iana.org 上的服务名称和传输协议端口号注册表下载 I AN A 端口注册表数据库 CSV 文件。
2. 将文件上传到 Amazon S3。有关更多信息，请参阅如何将文件和文件夹上传至 S3 存储桶？

3. 在 Athena 中创建一个名为的新表。iana_service_ports_import有关说明，请参阅 Amazon Athen a 用户指南中的创建表。在以下示例中，您需要将 my_bucket_name 替换为在上一步中将 CSV 文件上传到的 S3 存储桶的名称。

```
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");
```

使用 AWS Migration Hub 控制台发现数据

AWS Application Discovery Service （Application Discovery Service）与 AWS Migration Hub （Migration Hub）集成，客户可以在 Migration Hub 中查看和管理其数据收集器、服务器和应用程序。当您使用 Application Discovery Service 控制台时，您将被重定向到 Migration Hub 控制台。使用 Migration Hub 控制台无需您进行任何额外的步骤或设置。

在本节中，您可以了解如何使用控制台管理和监控 Application Discovery Service 无代理收集器（无代理收集器）和 AWS 应用程序发现代理（Discovery Agent）。

主题

在 AWS Migration Hub 控制台仪表板中查看数据

要查看主控制面板，请从 AWS Migration Hub （Migr at ion Hub）控制台导航窗格中选择 “控制面板”。在 Migration Hub 主仪表板中，您可以查看有关服务器、应用程序和数据收集器的高级统计信息，例如 Application Discovery Service 无代理收集器（无代理收集器）和 AWS 应用程序发现代理（发现代理）。

主控制面板将从中心位置的 Discover (发现) 和 Migrate (迁移) 控制面板中收集数据。它包含四个状态和信息窗格以及一系列用于快速访问的链接。利用窗格，您可以查看最近更新的应用程序的摘要状态。您还可以快速访问您的任一应用程序，获得处于不同状态的应用程序的概览，并随着时间推移跟踪迁移进度。

要查看主控制面板，请从 M ig ration Hub 控制台主页左侧的导航窗格中选择 “控制面板”。

在 AWS Migration Hub 控制台中启动和停止数据收集器

Application Discovery Service 无代理收集器（无代理收集器）和 AWS 应用程序发现代理（发现代理）是（Appl AWS Application Discovery Service ication Discovery Service）用来帮助您发现现有基础架构的数据收集工具。以下步骤说明了如何下载和部署这些发现数据收集工具，部署无座席活动以及AWS 应用程序发现代理。

这些数据收集工具将其数据存储在应用程序发现服务的存储库中，提供有关每台服务器及其上运行的进程的详细信息。部署这两个工具中的任何一个后，您都可以从 AWS Migration Hub （Migration Hub）控制台启动、停止和查看收集的数据。

部署 AWS 应用程序发现代理（发现代理）后，您可以在 AWS Migration Hub （Migration Hub）控制台的 “数据收集器” 页面上启动或停止数据收集过程。

启动或停止数据收集工具

1. 使用您的 AWS 账户，登录 AWS Management Console 并打开 Migration Hub 控制台，网址为https://console.aws.amazon.com/migrationhub/。
2. 在 Migration Hub 控制台导航窗格的 “发现” 下，选择 “数据收集器”。
3. 选择 Agents (代理) 选项卡。
4. 选中要启动或停止的收集工具的复选框。
5. 选择 Start data collection (启动数据收集) 或 Stop data collection (停止数据收集)。

在 AWS Migration Hub 控制台中对数据收集器进行排序

如果您部署了许多数据收集器，则可以在控制台的 “数据收集器” 页面上对显示的已部署收集器列表进行排序。您可以通过在搜索栏中应用筛选器来对列表进行排序。您可以搜索和筛选在 Data Collectors (数据收集器) 列表中指定的大多数条件。

下表显示了可用于代理的搜索条件，包括运算符、值和值的定义。

搜索条件	运算符	值：定义
代理 ID	==	从安装了收集工具的预填充列表中选择的任何代理 ID。

搜索条件	运算符	值：定义
主机名	== !=	对于代理，是从在其中安装代理的主机的预填充列表中选择的任何主机名。
收集状态	== !=	已启动：正在收集数据并将其发送到 Application Discovery Service 已计划启动：数据收集已计划启动。数据将在下次 ping 时发送到 Application Discovery Service，状态将更改为 “已启动”。 已停止：未收集数据，也未将数据发送到 Application Discovery Service。 已计划停止：数据收集已计划停止。下次 ping 操作时，数据将停止发送到 Application Discovery Service，状态将更改为 “已停止”。

搜索条件	运算符	值：定义
健康	== !=	运行状况良好：数据收集未开启。工具运行正常。 运行状况不佳：工具处于错误状态。没有在收集或报告数据。 未知：在超过一个小时的时间内未建立连接。 关闭：工具上次由于系统、服务或守护程序关闭而显示了“正在关闭”。如果发生了重启或工具升级，状态将在第一个报告周期更改为另一个状态。 正在运行：数据收集已开启。工具运行正常。
IP 地址	== !=	从在其中安装收集工具的预填充列表中选择的任何 IP 地址。

下表显示了可用于无代理收集器的搜索条件，包括运算符、值和值的定义。

搜索条件	运算符	值：定义
ID	==	从安装了收集工具的预填充列表中选择的任何无代理收集器 ID。
主机名	== !=	对于无代理收集器，指从安装了无代理收集器的预填充的主机列表中选择的任何主机名。

搜索条件	运算符	值：定义
状态	== !=	收集数据：数据收集已开启。工具运行正常。 准备配置-数据收集未开启。工具运行正常。 需要注意— 该工具处于错误状态，需要注意。 未知：在超过一个小时的时间内未建立连接。 关闭：由于系统、服务或守护程序关闭，该工具最后一次通信 “关闭”。如果发生了重启或工具升级，状态将在第一个报告周期更改为另一个状态。
IP 地址	== !=	从在其中安装收集工具的预填充列表中选择的任何 IP 地址。

通过应用搜索筛选条件为数据收集器分类

1. 使用您的 AWS 账户，登录 AWS Management Console 并打开 Migration Hub 控制台，网址为https://console.aws.amazon.com/migrationhub/。
2. 在 Migration Hub 控制台导航窗格的 “发现” 下，选择 “数据收集器”。
3. 选择 “无代理收集器” 或 “代理” 选项卡。
4. 在搜索栏内单击并从列表中选择一个搜索条件。
5. 从下一个列表中选择一个运算符。
6. 从最后一个列表中选择一个值。

在 AWS Migration Hub 控制台中查看服务器

Servers (服务器) 页提供了有关数据收集工具所知的每个服务器实例的系统配置和性能数据。您可以查看服务器信息，使用筛选条件为服务器分类，使用键/值对标记服务器以及导出详细的服务器和系统信息。

您可以获得数据收集工具发现的服务器的常规视图和详细视图。

查看发现的服务器

1. 使用您的 AWS 账户，登录 AWS Management Console 并打开 Migration Hub 控制台，网址为https://console.aws.amazon.com/migrationhub/。
2. 在 Migration Hub 控制台导航窗格的 “发现” 下，选择 “服务器”。发现的服务器将显示在服务器列表中。
3. 要了解某个服务器的更多详细信息，请在 Server info (服务器信息) 列中选择其服务器链接。这样做将显示一个描述服务器的屏幕。

该服务器的详细屏幕将显示系统信息和性能指标。您还可以查找用于导出网络依赖关系和进程信息的按钮。要导出详细的服务器信息，请参阅AWS Migration Hub 用于导出服务器数据。

在 AWS Migration Hub 控制台中对服务器进行排序

要轻松查找特定服务器，请应用搜索筛选条件为收集工具发现的所有服务器分类。您可以根据大量条件进行搜索和筛选。

通过应用搜索筛选条件为服务器分类

1. 使用您的 AWS 账户，登录 AWS Management Console 并打开 Migration Hub 控制台，网址为https://console.aws.amazon.com/migrationhub/。
2. 在 Migration Hub 控制台导航窗格的 “发现” 下，选择 “服务器”。
3. 在搜索栏内单击并从列表中选择一个搜索条件。
4. 从下一个列表中选择一个运算符。
5. 为搜索条件键入一个区分大小写的值，然后按 Enter。
6. 可以通过重复步骤 2 - 4 来应用多个筛选器。

在控制台中标记服务器 AWS Migration Hub

为协助迁移规划和帮助保持井然有序，您可以为每个服务器创建多个标签。标签 是用户定义的键/值对，可存储有关服务器的自定义数据和元数据。您可以在单个操作中标记一台或多台服务器。 AWS Application Discovery Service （ Application Discovery Service ） AWS 标签与标签类似，但这两种类型的标签不能互换使用。

您可以从 Servers (服务器) 主页面为一个或多个服务器添加或删除多个标签。在服务器的详细信息页面上，您只能为所选服务器添加或删除一个或多个标签。您可以在单个操作中执行涉及多个服务器或标签的任何类型的标记任务。您也可以删除标签。

将标签添加到一台或多个服务器

1. 使用您的 AWS 账户，登录 AWS Management Console 并打开 Migration Hub 控制台，网址为https://console.aws.amazon.com/migrationhub/。
2. 在 Migration Hub 控制台导航窗格的 “发现” 下，选择 “服务器”。
3. 在 Server info (服务器信息) 列中，选择要为其添加标签的服务器的服务器链接。要一次将标签添加到多个服务器，请在多个服务器的复选框内单击。
4. 选择 “添加标签”，然后选择 “添加新标签”。
5. 在对话框中，在键字段中键入一个密钥，也可以在 “值” 字段中键入一个值。

   通过选择添加新标签并添加更多信息来添加更多标签。
6. 选择保存。

从一个或多个服务器中删除标签

1. 使用您的 AWS 账户，登录 AWS Management Console 并打开 Migration Hub 控制台，网址为https://console.aws.amazon.com/migrationhub/。
2. 在 Migration Hub 控制台导航窗格的 “发现” 下，选择 “服务器”。
3. 在 Server info (服务器信息) 列中，选择要从中删除标签的服务器的服务器链接。选中多台服务器的复选框可一次从多台服务器上移除标签。
4. 选择 “移除标签”。
5. 选择要删除的每个标签。
6. 选择确认。

AWS Migration Hub 用于导出服务器数据

本主题介绍如何使用 AWS Management Console AWS Command Line Interface、或 API 导出服务器数据。

使用导 AWS Management Console 出所有服务器的服务器数据

1. 登录 AWS Management Console 并打开 Migration Hub 控制台，网址为https://console.aws.amazon.com/migrationhub/。
2. 在左侧导航窗格的 “发现” 下，选择 “服务器”。
3. 选择 “操作”，然后选择 “导出发现数据”。
4. 在屏幕底部的 Exports (导出) 部分，选择 Export server details (导出服务器详细信息)。此操作会生成一个.zip 文件，其中包含下表中描述的.csv 文件。

文件名	描述
{account_id} _Application.csv	每个应用程序的详细信息，包括服务器数量、名称和描述。
{账号_id} _ .csv ApplicationResourceAssociation	服务器和应用程序之间的关系。
{账号_id} _ ImportTemplate	每台服务器的应用程序和标签的摘要。可以修改和重新导入此文件以更新与服务器关联的应用程序。
{账号_id} _ .csv NetworkInterface	每个网络接口的详细信息，包括关联的服务器、地址和交换机。
{account_id} _Server.csv	每台服务器的详细信息，包括操作系统、主机名和虚拟机管理程序。
{账号_id} _ .csv SystemPerformance	每台服务器的详细信息，包括 CPU、内存和存储配置以及性能。
{account_id} _Tags.csv	与服务器关联的每个标签的详细信息。

文件名	描述
{account_id} _ Info.csv VMware	每种 VMware 配置的详细信息，包括 moreF、VMname 和 vCenter。

使用导 AWS Management Console 出特定服务器的代理数据

1. 登录 AWS Management Console 并打开 Migration Hub 控制台，网址为https://console.aws.amazon.com/migrationhub/。
2. 在左侧导航窗格的 “发现” 下，选择 “服务器”。
3. 将光标置于 “服务器” 下的搜索字段中。这将显示一个下拉列表。在该列表中，在 “属性” 下，选择 “源”，然后选择 “=” 运算符，然后选择 “源 = 代理”。
4. 在搜索结果中，选择要为其导出数据的服务器的名称。此操作会将您带到该服务器的详细信息页面。
5. 输入开始时间和结束时间，然后选择 “导出”。导出的.zip 文件包括下表中描述的.csv 文件。

{账号_id} _ .csv destinationProcessConnection	服务器入站连接的详细信息。
{account_id} _networkInterface.csv	每个网络接口的详细信息，包括地址、掩码和名称
{account_id} _osInfo.csv	操作系统的详细信息，包括 CPU 类型、虚拟机管理程序和操作系统名称。
{account_id} _process.csv	服务器上运行的进程的详细信息。
{账号_id} _ .csv sourceProcessConnection	来自服务器的出站连接的详细信息。
{account_id} _systemPerformance.csv	服务器的 CPU、内存和存储配置及性能的详细信息。

使用 AWS Command Line Interface 或 API 导出服务器数据

1. 运行 start-export-task。相应的 API 操作是 StartExportTask
2. 运行 describe-export-tasks。相应的 API 操作是 DescribeExportTasks。

在 AWS Migration Hub 控制台中对服务器进行分组

您的一部分已发现服务器可能需要一起迁移才能保持正常运行。在这种情况下，您可采用逻辑方式定义已发现服务器并将其分组到应用程序中。

在分组过程中，您可以搜索、筛选和添加标签。

将服务器分组到新的或现有的应用程序

1. 使用您的 AWS 账户，登录 AWS Management Console 并打开 Migration Hub 控制台，网址为https://console.aws.amazon.com/migrationhub/。
2. 在 Migration Hub 控制台导航窗格的 “发现” 下，选择 “服务器”。
3. 在服务器列表中，选择要分组到新的或现有的应用程序的每个服务器。

   为了帮助为您的组选择服务器，您可以基于您在服务器列表中指定的任何条件进行搜索和筛选。在搜索栏内单击并从列表中选择一项，从下一个列表中选择一个运算符，然后键入您的条件。
4. 可选：对于每个选定服务器，选择 Add tag (添加标签)，为 Key (键) 键入一个值，然后根据需要为 Value (值) 键入一个值。
5. 选择 Group as application (作为应用程序分组) 以创建您的应用程序，或添加到一个现有应用程序。
6. 在 Group as application (作为应用程序分组) 对话框中，选择 Group as a new application (作为新应用程序分组) 或 Add to an existing application (添加到现有应用程序)。

   a. 如果您选择 Group as a new application (作为新应用程序分组)，请为 Application name (应用程序名称) 键入一个名称。(可选) 您可以为 Application description (应用程序描述) 键入一个描述。

   b. 如果您选择 Add to an existing application (添加到现有应用程序)，请选择要添加到列表的应用程序的名称。
7. 选择保存。

使用 Application Discovery Service API 查询发现的配置项目

配置项目是代理或通过导入在您的数据中心发现的 IT 资产。使用 AWS Application Discovery Service（Application Discovery Service）时，您可以使用 API 来指定筛选器并查询服务器、应用程序、进程和连接资产的特定配置项目。有关 API 的信息，请参阅 App lication Discovery Service API 参考。

以下各节中的表格列出了两个 Application Discovery Service 操作的可用输入筛选器和输出排序选项：

- `DescribeConfigurations`
- `ListConfigurations`

筛选和排序选项按其适用于的资源类型（服务器、应用程序、进程或连接）排列。

> **Important**
>
> `DescribeConfigurations`、`ListConfigurations`和返回的结果`StartExportTask`可能不包含最近的更新。有关更多信息，请参阅 the section called “最终一致性”。

使用 `DescribeConfigurations` 操作

该`DescribeConfigurations`操作会检索配置 IDs列表的属性。所提供的所有资产类型 IDs 必须相同（服务器、应用程序、进程或连接）。输出字段特定于所选的资产类型。例如，服务器配置项的输出包含有关服务器的属性的列表，例如主机名、操作系统和网卡数。有关命令语法的更多信息，请参阅DescribeConfigurations。

`DescribeConfigurations` 操作不支持筛选。

`DescribeConfigurations` 的输出字段

下表按资产类型排列，列出了 `DescribeConfigurations` 操作支持的输出字段。输出中始终包含标记为必填的字段。

服务器资产

字段	强制性
`server.agentId`	

字段	强制性
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	
server.performance.avgCpuUs agePct	
server.performance.avgDiskR eadIOPS	
server.performance.avgDiskR eadsPerSecondInKB	

字段	强制性
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	
server.performance.maxNetworkReadsPerSecondInKB	
server.performance.maxNetworkWritesPerSecondInKB	
server.performance.minFreeRAMInKB	

字段	强制性
server.performance.numCores	
server.performance.numCpus	
server.performance.numDisks	
server.performance.numNetwo rkCards	
server.performance.totalRAMInKB	

进程资产

字段	强制性
process.commandLine	
process.configurationId	x
process.name	
process.path	
process.timeOfCreation	x

应用程序资产

字段	强制性
application.configurationId	x
application.description	
application.lastModifiedTime	x
application.name	x

字段	强制性
application.serverCount	x
application.timeOfCreation	x

使用 ListConfigurations 操作

ListConfigurations 操作根据您在筛选条件中指定的条件检索配置项目的列表。有关命令语法的更多信息，请参阅ListConfigurations。

ListConfigurations 的输出字段

下表按资产类型排列，列出了 ListConfigurations 操作支持的输出字段。输出中始终包含标记为必填的字段。

服务器资产

字段	强制性
server.configurationId	x
server.agentId	
server.hostName	
server.osName	
server.osVersion	
server.timeOfCreation	x
server.type	

进程资产

字段	强制性
process.commandLine	
process.configurationId	x
process.name	
process.path	
process.timeOfCreation	x
server.agentId	
server.configurationId	x

应用程序资产

字段	强制性
application.configurationId	x
application.description	
application.name	x
application.serverCount	x
application.timeOfCreation	x
application.lastModifiedTime	x

连接资产

字段	强制性
connection.destinationIp	x

字段	强制性
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	

支持的 **ListConfigurations** 筛选条件

下表按资产类型排列，列出了 ListConfigurations 操作支持的筛选条件。筛选条件和值所处的关系是由支持的逻辑条件之一定义的键/值关系。您可以对所示过滤条件的输出排序。

服务器资产

筛选条件	支持的条件	支持的值	支持的排序
server.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• 任何有效的服务器配置 ID	无
server.hostName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	• ASC • DESC
server.osName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	• ASC • DESC
server.osVersion	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	• ASC • DESC
server.agentId	• EQUALS • NOT_EQUALS • EQ • NE	• 字符串	无

筛选条件	支持的条件	支持的值	支持的排序
server.connectorId	• EQUALS • NOT_EQUALS • EQ • NE	• 字符串	无
server.type	• EQUALS • NOT_EQUALS • EQ • NE	具有以下值之一的字符串： • EC2 • OTHER • VMWARE_VM • VMWARE_HOST • VMWARE_VM_TEMPLATE	无
server.vmWareInfo.morefId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	无
server.vmWareInfo.vcenterId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	无

筛选条件	支持的条件	支持的值	支持的排序
server.vmWareInfo.hostId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	无
server.networkInterfaceInfo.portGroupId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	无
server.networkInterfaceInfo.portGroupName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	无
server.networkInterfaceInfo.virtualSwitchName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	无

筛选条件	支持的条件	支持的值	支持的排序
server.networkInterfaceInfo.ipAddress	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	无
server.networkInterfaceInfo.macAddress	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	无
server.performance.avgCpuUsagePct	• GE • LE • GT • LT	• 百分比	无
server.performance.totalDiskFreeSizeInKB	• GE • LE • GT • LT	• 双精度	无
server.performance.avgFreeRAMInKB	• GE • LE • GT • LT	• 双精度	无

筛选条件	支持的条件	支持的值	支持的排序
server.tag.value	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	无
server.tag.key	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	无
server.application.name	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	无
server.application.description	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	无

筛选条件	支持的条件	支持的值	支持的排序
server.application.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• 任何有效的应用程序配置 ID	无
server.process.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	无
server.process.name	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	无
server.process.commandLine	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	无

应用程序资产

筛选条件	支持的条件	支持的值	支持的排序
application.configurationId	• EQUALS • NOT_EQUALS • EQ	• ApplicationId	无

筛选条件	支持的条件	支持的值	支持的排序
	• NE		
application.name	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	• ASC • DESC
application.description	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	• ASC • DESC
application.serverCount	不支持筛选。	不支持筛选。	• ASC • DESC
application.timeOfCreation	不支持筛选。	不支持筛选。	• ASC • DESC
application.lastModifiedTime	不支持筛选。	不支持筛选。	• ASC • DESC

筛选条件	支持的条件	支持的值	支持的排序
server.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ServerId	无

进程资产

筛选条件	支持的条件	支持的值	支持的排序
process.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	
process.name	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	• ASC • DESC
process.commandLine	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	• ASC • DESC
server.configurationId	• EQUALS • NOT_EQUALS • EQ	• ServerId	

筛选条件	支持的条件	支持的值	支持的排序
	• NE		
server.hostName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	• ASC • DESC
server.osName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	• ASC • DESC
server.os Version	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	• ASC • DESC
server.agentId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	

连接资产

筛选条件	支持的条件	支持的值	支持的排序
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	• 整数	• ASC • DESC
sourceServer.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ServerId	
sourceServer.hostName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	• ASC • DESC

筛选条件	支持的条件	支持的值	支持的排序
destinationServer.osName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	• ASC • DESC
destinationServer.osVersion	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	• ASC • DESC
destinationServer.agentId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	
sourceProcess.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	

筛选条件	支持的条件	支持的值	支持的排序
sourceProcess.name	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	• ASC • DESC
sourceProcess.commandLine	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	• ASC • DESC
destinationProcess.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	
destinationProcess.name	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	• ASC • DESC

筛选条件	支持的条件	支持的值	支持的排序
`destinationprocess.commandLine`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字符串	• ASC • DESC

AWS Application Discovery Service API 的最终一致性

以下更新操作最终是一致的。读取操作可能无法立即看到更新StartExportTaskDescribeConfigurations、和ListConfigurations。

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

管理最终一致性的建议：

- 当您调用读取操作StartExportTaskDescribeConfigurations、或 ListConfigurations（或其相应的 AWS CLI 命令）时，请使用指数退避算法，以便有足够的时间让先前的任何更新操作在系统中传播。为此，请重复运行读取操作，从两秒钟的等待时间开始，然后逐渐增加到五分钟的等待时间。
- 即使更新操作返回 200-OK 响应，也要增加后续操作之间的等待时间。应用指数回退算法，以几秒钟的等待时间开始，然后逐渐增加达到大约五分钟的等待时间。

AWS Application Discovery Service 使用接口端点进行访问 (AWS PrivateLink)

您可以使用 AWS PrivateLink 在您的 VPC 和之间创建私有连接 AWS Application Discovery Service。您可以像在您的 VPC 中一样访问 Application Discovery Service，无需使用互联网网关、NAT 设备、VPN AWS Direct Connect 连接或连接。您的 VPC 中的实例不需要公有 IP 地址即可访问 Application Discovery Service。

您可以通过创建由 AWS PrivateLink提供支持的接口端点来建立此私有连接。我们将在您为接口端点启用的每个子网中创建一个端点网络接口。这些是请求者管理的网络接口，用作发往 Application Discovery Service 的流量的入口点。

有关更多信息，请参阅《AWS PrivateLink 指南》中的通过 AWS PrivateLink访问 AWS 服务。

Application Discovery 服务的注意事项

在为 Application Discovery Service 设置接口终端节点之前，请查看AWS PrivateLink 指南中的使用接口 VPC 终端节点访问 AWS 服务。

Application Discovery Service 支持两个接口：一个用于调用其所有 API 操作，另一个用于无代理收集器和 AWS 应用程序发现代理发送发现数据。

创建接口端点

您可以使用 Amazon VPC 控制台或 AWS Command Line Interface (AWS CLI) 创建接口端点。有关更多信息，请参阅AWS PrivateLink 指南中的使用接口 VPC 终端节点访问 AWS 服务。

For Application Discovery Service

使用以下服务名称为 Application Discovery Service 创建接口终端节点：

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

如果您为接口终端节点启用私有 DNS，则可以使用其默认区域 DNS 名称向 Application Discovery Service 发出 API 请求。例如，`discovery.us-east-1.amazonaws.com`。

For Agentless Collector and AWS Application Discovery Agent

使用以下服务名称创建接口终端节点：

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

如果您为接口终端节点启用私有 DNS，则可以使用其默认区域 DNS 名称向 Application Discovery Arsenal 发出 API 请求。例如，`arsenal-discovery.us-east-1.amazonaws.com`。

为 VPC 端点创建端点策略

端点策略是一种 IAM 资源，您可以将其附加到接口端点。默认终端节点策略允许通过接口终端节点对 AWS 服务进行完全访问。要控制允许从 VPC 访问 AWS 服务的权限，请将自定义终端节点策略附加到接口终端节点。

端点策略指定以下信息：

- 可执行操作的主体（AWS 账户、IAM 用户和 IAM 角色）。
- 可执行的操作。

有关更多信息，请参阅《AWS PrivateLink 指南》中的使用端点策略控制对服务的访问权限。

示例：VPC 终端节点策略

以下是自定义端点策略的一个示例。将此策略附加到接口端点时，其会向所有资源上的所有主体授予对列出的 操作的访问权限。

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":"*"
      }
   ]
}
```

将 VPC 终端节点用于无代理收集器和 AWS 应用程序发现代理

无代理收集器和 AWS 应用程序发现代理不支持可配置的端点。相反，请使用arsenal-discovery亚马逊 VPC 终端节点的私有 DNS 功能。

- 设置 AWS Direct Connect 路由表，将私有 AWS IP 地址路由到 VPC。例如，目标 = 10.0.0.0/8，目标 = 本地。对于此设置，您至少需要将 arsenal-discovery Amazon VPC 终端节点的私有 IP 地址路由到 VPC。
- 使用 arsenal-discovery Amazon VPC 终端节点私有 DNS 功能，因为无代理收集器不支持可配置的 Arsenal 终端节点。
- 在私有子网中设置 arsenal-discovery Amazon VPC 终端节点，该子网与您要将 AWS Direct Connect 流量路由到的 VPC 相同。
- 使用安全组设置 arsenal-discovery Amazon VPC 终端节点，该组允许来自 VPC 内部的入站流量（例如 10.0.0.0/8）。
- 设置 Amazon Route 53 入站解析器，为arsenal-discovery亚马逊 VPC 终端节点私有 DNS 名称路由 DNS 解析，该名称将解析为 VPC 终端节点的私有 IP。如果您不这样做，收集器将使用本地解析器执行 DNS 解析，并将使用公共 Arsenal 终端节点，流量将不会通过 VPC。
- 如果您禁用了所有公共流量，则自动更新功能将失败。这是因为无代理收集器通过向 Amazon ECR 终端节点发送请求来检索更新。要在不通过公共互联网发送请求的情况下使用自动更新功能，请为 Amazon ECR 服务设置 VPC 终端节点，并为该终端节点启用私有 DNS 功能。

安全性 AWS Application Discovery Service

云安全 AWS 是重中之重。作为 AWS 客户，您可以从专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构中受益。

安全是双方共同承担 AWS 的责任。责任共担模式将其描述为云的 安全性和云中 的安全性：

- 云安全 — AWS 负责保护在 AWS 云中运行 AWS 服务的基础架构。 AWS 还为您提供可以安全使用的服务。作为 AWS 合规性计划的一部分，我们的安全措施的有效性定期由第三方审计员进行测试和验证。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您组织的要求以及适用的法律法规。

要使用 AWS 应用程序发现代理或 Application Discovery Service 无代理收集器，您必须向您的 AWS 帐户提供访问密钥。然后，这些信息将存储在您的本地基础设施中。作为责任共担模式的一部分，您有责任确保对基础设施的访问安全。

本文档将帮助您了解在使用 Application Discovery Service 时如何应用分担责任模型。以下主题向您介绍如何配置 Application Discovery Service 以满足您的安全和合规性目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 Application Discovery Service 资源。

主题

- Identity and Access Management AWS Application Discovery Service
- 记录 Application Discovery Service API AWS CloudTrail

Identity and Access Management AWS Application Discovery Service

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以进行身份验证（登录）和授权（拥有权限）来使用 Application Discovery Service 资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

- 受众
- 使用身份进行身份验证

- 使用策略管理访问
- 如何 AWS Application Discovery Service 与 IAM 配合使用
- AWS 的托管策略 AWS Application Discovery Service
- AWS Application Discovery Service 基于身份的策略示例
- 为 Application Discovery Service 使用服务相关角色
- AWS Application Discovery Service 身份和访问疑难解答

受众

您的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于您在 Application Discovery Service 中所做的工作。

服务用户-如果您使用 Application Discovery Service 服务完成工作，则您的管理员会为您提供所需的凭据和权限。当你使用更多 Application Discovery Service 功能来完成工作时，你可能需要额外的权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 Application Discovery Service 中的某项功能，请参阅AWS Application Discovery Service 身份和访问疑难解答。

服务管理员 — 如果您负责公司的 Application Discovery Service 资源，那么您可能拥有对 Application Discovery Service 的完全访问权限。您的工作是确定您的服务用户应访问哪些 Application Discovery Service 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要详细了解贵公司如何将 IAM 与 Application Discovery Service 配合使用，请参阅如何 AWS Application Discovery Service 与 IAM 配合使用。

IAM 管理员 — 如果您是 IAM 管理员，则可能需要详细了解如何编写策略来管理 Application Discovery Service 的访问权限。要查看您可以在 IAM 中使用的基于身份的 Application Discovery Service 策略示例，请参阅。AWS Application Discovery Service 基于身份的策略示例

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 AWS 账户根用户任 IAM 角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （IAM Identity Center）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的如何登录到您 AWS 账户的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅《IAM 用户指南》中的用于签署 API 请求的AWS 签名版本 4。

无论使用何种身份验证方法，您都可能需要提供其他安全信息。例如， AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《AWS IAM Identity Center 用户指南》中的多重身份验证和《IAM 用户指南》中的 IAM 中的AWS 多重身份验证。

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关需要您以根用户身份登录的任务的完整列表，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

IAM 用户和群组

I AM 用户是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的用例，应在需要时更新访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可以拥有一个名为的群组，IAMAdmins并向该群组授予管理 IAM 资源的权限。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅《IAM 用户指南》中的 IAM 用户的使用案例。

IAM 角色

I AM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。要在中临时担任 IAM 角色 AWS Management Console，您可以从用户切换到 IAM 角色（控制台）。您可以通过调用 AWS CLI 或 AWS API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的代入角色的方法。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问：要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关用于联合身份验证的角色的信息，请参阅《IAM 用户指南》中的针对第三方身份提供商创建角色（联合身份验证）。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的权限集。
- 临时 IAM 用户权限：IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取：您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅 IAM 用户指南中的 IAM 中的跨账户资源访问。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在服务中拨打电话时，该服务通常会在 Amazon 中运行应用程序 EC2 或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两项操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。
  - 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。
  - 服务相关角色-服务相关角色是一种与服务相关联的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 A@@ mazon 上运行的应用程序 EC2 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这比在 EC2 实例中存储访问密钥更可取。要为 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建一个附加到该实例的实例配置文件。实例配置文件包含该角色，并允许在 EC2 实例上运行的程序获得临时证书。有关更多信息，请参阅 IAM 用户指南中的使用 IAM 角色向在 A mazon EC2 实例上运行的应用程序授予权限。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的结构和内容的更多信息，请参阅 IAM 用户指南中的JSON 策略概览。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

IAM 策略定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从 AWS Management Console AWS CLI、或 AWS API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户托管策略定义自定义 IAM 权限。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用 IAM 中的 AWS 托管策略。

访问控制列表 (ACLs)

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。 ACLs 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Amazon S3 和 Amazon VPC 就是支持的服务示例 ACLs。 AWS WAF要了解更多信息 ACLs，请参阅《亚马逊简单存储服务开发者指南》中的访问控制列表 (ACL) 概述。

其他策略类型

AWS 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界：权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅IAM 用户指南中的 IAM 实体的权限边界。
- 服务控制策略 (SCPs)- SCPs 是指定组织或组织单位 (OU) 的最大权限的 JSON 策略 AWS Organizations。 AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果您启用组织中的所有功能，则可以将服务控制策略 (SCPs) 应用于您的任何或所有帐户。SCP 限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关 Organization SCPs s 和的更多信息，请参阅《AWS Organizations 用户指南》中的服务控制策略。
- 资源控制策略 (RCPs) — RCPs 是 JSON 策略，您可以使用它来设置账户中资源的最大可用权限，而无需更新附加到您拥有的每个资源的 IAM 策略。RCP 限制成员账户中资源的权限，并可能影响身份（包括身份）的有效权限 AWS 账户根用户，无论这些身份是否属于您的组织。有关 Organizations 的更多信息 RCPs，包括 AWS 服务 该支持的列表 RCPs，请参阅《AWS Organizations 用户指南》中的资源控制策略 (RCPs)。
- 会话策略：会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 IAM 用户指南中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

如何 AWS Application Discovery Service 与 IAM 配合使用

在使用 IAM 管理对 Application Discovery Service 的访问权限之前，您应该了解哪些可用于 Application Discovery Service 的 IAM 功能。要全面了解 Application Discovery Service 和其他 AWS 服务如何与 IAM 配合使用，请参阅 IAM 用户指南中的与 IAM 配合使用的AWS 服务。

主题

Application Discovery 服务基于身份的策略

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。Application Discovery Service 支持特定的操作、资源和条件键。要了解在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》 中的 IAM JSON 策略元素参考。

操作

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

Application Discovery Service 中的策略操作在操作前使用以下前缀：`discovery:`。策略语句必须包含 `Action` 或 `NotAction` 元素。Application Discovery Service 定义了自己的一组操作，这些操作描述了您可以使用该服务执行的任务。

要在单个语句中指定多项操作，请使用逗号将它们隔开，如下所示：

```
"Action": [
      "discovery:action1",
      "discovery:action2"
```

您也可以使用通配符（*）指定多个操作。例如，要指定以单词 Describe 开头的所有操作，包括以下操作：

```
"Action": "discovery:Describe*"
```

要查看 Application Discovery Service 操作列表，请参阅 IAM 用户指南 AWS Application Discovery Service中定义的操作。

资源

Application Discovery Service 不支持 ARNs 在策略中指定资源。要分开访问权限，请分别创建和使用 AWS 账户。

条件键

Application Discovery Service 不提供任何特定于服务的条件密钥，但它确实支持使用某些全局条件密钥。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

示例

要查看 Application Discovery Service 基于身份的策略的示例，请参阅。AWS Application Discovery Service 基于身份的策略示例

基于资源的应用程序 Discovery Service 策略

Application Discovery Service 不支持基于资源的策略。

基于 Application Discovery Service 标签

Application Discovery Service 不支持标记资源或根据标签控制访问权限。

Application Discovery Servic

I AM 角色是您的 AWS 账户中具有特定权限的实体。

在 Application Discovery Service 中使用

Application Discovery Service 不支持使用临时证书。

服务相关角色

服务相关角色允许 AWS 服务访问其他服务中的资源以代表您完成操作。服务相关角色显示在 IAM 账户中，并归该服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

Application Discovery Service 支持服务相关角色。有关创建或管理 Application Discovery Service 服务相关角色的详细信息，请参阅为 Application Discovery Service 使用服务相关角色。

服务角色

此功能允许服务代表您担任服务角色。此角色允许服务访问其他服务中的资源以代表您完成操作。服务角色显示在 IAM 账户中，并归该账户所有。这意味着，IAM 管理员可以更改该角色的权限。但是，这样做可能会中断服务的功能。

Application Discovery 服务支持服务角色。

AWS 的托管策略 AWS Application Discovery Service

要向用户、群组和角色添加权限，使用 AWS 托管策略比自己编写策略要容易得多。创建仅为团队提供所需权限的 IAM 客户管理型策略需要时间和专业知识。要快速入门，您可以使用我们的 AWS 托管策略。这些策略涵盖常见使用案例，可在您的 AWS 账户中使用。有关 AWS 托管策略的更多信息，请参阅 IAM 用户指南中的AWS 托管策略。

AWS 服务维护和更新 AWS 托管策略。您无法更改 AWS 托管策略中的权限。服务偶尔会向 AWS 托管式策略添加额外权限以支持新特征。此类更新会影响附加策略的所有身份（用户、组和角色）。当启动新特征或新操作可用时，服务最有可能会更新 AWS 托管式策略。服务不会从 AWS 托管策略中移除权限，因此策略更新不会破坏您的现有权限。

此外，还 AWS 支持跨多个服务的工作职能的托管策略。例如，ReadOnlyAccess AWS 托管策略提供对所有 AWS 服务和资源的只读访问权限。当服务启动一项新功能时， AWS 会为新操作和资源添加只读权限。有关工作职能策略的列表和说明，请参阅 IAM 用户指南中的适用于工作职能的AWS 托管式策略。

AWS 托管策略： AWSApplicationDiscoveryServiceFullAccess

该`AWSApplicationDiscoveryServiceFullAccess`策略授予 IAM 用户账户访问 Application Discovery Service 和 Migration Hub 的权限 APIs。

附加了此策略的 IAM 用户账户可以配置 Application Discovery Service、启动和停止代理、启动和停止无代理发现，以及从 Discovery Ser AWS vice 数据库中查询数据。有关此策略的示例，请参阅[授予对 Application Discovery 服务的完全访问权限]。

AWS 托管策略： AWSApplicationDiscoveryAgentlessCollectorAccess

`AWSApplicationDiscoveryAgentlessCollectorAccess`托管策略授予 Application Discovery Service 无代理收集器（无代理收集器）注册应用程序发现服务并与之通信以及与其他服务通信的权限。 AWS

必须将此策略附加到使用其证书配置无代理收集器的 IAM 用户。

权限详细信息

该策略包含以下权限。

- `arsenal`— 允许收集器在 Application Discovery Service 应用程序中注册。为了能够将收集到的数据发送回去，这是必要的 AWS。
- `ecr-public`— 允许收集器调用亚马逊弹性容器公共注册表（Amazon ECR Public），在那里可以找到收集器的最新更新。
- `mgh`— 允许收集器调用 AWS Migration Hub 以检索用于配置收集器的帐户的主区域。这对于知道收集的数据应发送到哪个区域是必要的。
- `sts`— 允许收集器检索服务承载令牌，以便收集器可以调用 Amazon ECR Public 以获取最新更新。

```
{
    "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 托管策略： AWSApplicationDiscoveryAgentAccess

该AWSApplicationDiscoveryAgentAccess策略授予应用程序发现代理注册和与 Application Discovery Service 通信的权限。

您可以将此策略附加到应用程序发现代理使用其凭据的任何用户。

此策略还授予用户访问 Arsenal 的权限。阿森纳是一项由管理和托管的代理服务 AWS。阿森纳将数据转发到云端的 Application Discovery Service。有关此策略的示例，请参阅向发现代理授予访问权限。

AWS 托管策略： AWSAgentlessDiscoveryService

该AWSAgentlessDiscoveryService策略授予在您的 v AWS Center Serv VMware er 中运行的无代理 Discovery Connector 访问权限，以注册连接器并与之通信并与之共享连接器运行状况指标 Application Discovery Service。

您可将此策略附加到被连接器使用了其凭证的任何用户。

AWS 托管策略： ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

如果您的 IAM 账户已附加AWSApplicationDiscoveryServiceFullAccess政策，ApplicationDiscoveryServiceContinuousExportServiceRolePolicy则当您在 Amazon Athena 中开启数据探索功能时，该账户会自动关联到您的账户。

该策略 AWS Application Discovery Service 允许创建 Amazon Data Firehose 流，以转换 AWS Application Discovery Service 代理收集的数据并将其传输到您 AWS 账户中的 Amazon S3 存储桶。

此外，此策略还创建了一个 AWS Glue Data Catalog 名为 applicati on_discovery_service_database 的新数据库和用于映射代理收集的数据的表架构。有关此策略的示例，请参阅 授予代理数据收集权限。

AWS 托管策略： AWSDiscoveryContinuousExportFirehosePolicy

该AWSDiscoveryContinuousExportFirehosePolicy政策是在 Amazon Athena 中使用数据探索功能所必需的。它允许 Amazon Data Firehose 将从 Application Discovery Service 收集的数据写入亚马逊 S3。有关使用此策略的信息，请参阅创建 AWSApplicationDiscoveryServiceFirehose 角色。有关此策略的示例，请参阅授予数据探索权限。

创建 AWSApplicationDiscoveryServiceFirehose 角色

管理员将托管策略附加到您的 IAM 用户账户。使用AWSDiscoveryContinuousExportFirehosePolicy策略时，管理员必须先创建一个名为 Firehose AWSApplicationDiscoveryServiceFirehose的角色作为可信实体，然后将该AWSDiscoveryContinuousExportFirehosePolicy策略附加到该角色，如以下过程所示。

创建 AWSApplicationDiscoveryServiceFirehose IAM 角色

1. 在 IAM 控制台中，选择导航窗格上的角色。
2. 请选择 Create Role(创建角色)。
3. 选择 Kinesis。
4. 选择 Kinesis Firehose 作为您的使用案例。
5. 选择下一步: 权限。
6. 在 “筛选策略” 下搜索AWSDiscoveryContinuousExportFirehosePolicy。
7. 选中旁边的复选框 AWSDiscoveryContinuousExportFirehosePolicy，然后选择 “下一步：查看”。
8. 输入AWSApplicationDiscoveryServiceFirehose角色名称，然后选择创建角色。

Application Discovery Service 更新 AWS 了托

查看自 Application Discovery Service AWS 托管策略开始跟踪这些更改以来该服务更新的详细信息。要获得有关此页面更改的自动提示，请订阅 的文档历史记录 AWS Application Discovery Service 页面上的 RSS 源。

更改	描述	日期
AWSApplicationDiscoveryAgentlessCollectorAccess— 随着无代理收集器的推出，新政策已推出	Application Discovery Service 添加了新的托管策略，该策略`AWSApplicationDiscoveryAgentlessCollectorAccess` 授予无代理收集器注册应用程序发现服务并与之通信以及与其他 AWS 服务通信的权限。	2022 年 8 月 16 日
Application Discovery Service 开始	Application Discovery Service 开始跟踪其 AWS 托管策略的更改。	2021 年 3 月 1 日

AWS Application Discovery Service 基于身份的策略示例

默认情况下，IAM 用户和角色无权创建或修改 Application Discovery Service 资源。他们也无法使用 AWS Management Console AWS CLI、或 AWS API 执行任务。IAM 管理员必须创建 IAM 策略，以便为用户和角色授予权限以对所需的指定资源执行特定的 API 操作。然后，管理员必须将这些策略附加到需要这些权限的 IAM 用户或组。

要了解如何使用这些示例 JSON 策略文档创建 IAM 基于身份的策略，请参阅《IAM 用户指南》中的 在 JSON 选项卡上创建策略。

主题

- 策略最佳实践
- 授予对 Application Discovery 服务的完全访问权限

- 向发现代理授予访问权限
- 授予代理数据收集权限
- 授予数据探索权限
- 授予使用 Migration Hub 控制台网络图的权限

策略最佳实践

基于身份的策略决定了某人是否可以在您的账户中创建、访问或删除 Application Discovery Service 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的AWS 托管式策略或工作职能的AWS 托管式策略。
- 应用最低权限：在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 AWS CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言（JSON）和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM Access Analyzer 验证策略。
- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的使用 MFA 保护 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实践。

授予对 Application Discovery 服务的完全访问权限

AWSApplicationDiscoveryServiceFullAccess 托管策略授予 IAM 用户账户访问 Application Discovery Service 和 Migration Hub 的权限 APIs。

将此策略附加到其账户的 IAM 用户可以配置 Application Discovery Service、启动和停止代理、启动和停止无代理发现，以及从 Discovery Ser AWS vice 数据库中查询数据。有关此策略的更多信息，请参阅“AWS 的托管策略 AWS Application Discovery Service”。

Example AWSApplicationDiscoveryServiceFullAccess 政策

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "mgh:*",
                "discovery:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "iam:GetRole"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

向发现代理授予访问权限

AWSApplicationDiscoveryAgentAccess 托管策略授予应用程序发现代理注册和与 Application Discovery Service 通信的权限。有关此策略的更多信息，请参阅“AWS 的托管策略 AWS Application Discovery Service”。

将此策略附加到应用程序发现代理使用其凭据的任何用户。

此策略还授予用户访问 Arsenal 的权限。阿森纳是一项由管理和托管的代理服务 AWS。阿森纳将数据转发到云端的 Application Discovery Service。

Example AWSApplicationDiscoveryAgentAccess 政策

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

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

授予代理数据收集权限

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy 托管策略 AWS Application Discovery Service 允许创建 Amazon Data Firehose 流，以转换应用程序发现服务代理收集的数据并将其传输到您 AWS 账户中的 Amazon S3 存储桶。

此外，此策略还会创建一个 AWS Glue 数据目录，其中包含一个名为的新数据库`application_discovery_service_database`和用于映射代理收集的数据的表架构。

有关使用此策略的信息，请参阅AWS 的托管策略 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"
                }
            }
        }
    ]
}
```

授予数据探索权限

该 AWSDiscoveryContinuousExportFirehosePolicy 政策是在 Amazon Athena 中使用数据探索功能所必需的。它允许 Amazon Data Firehose 将从 Application Discovery Service 收集的数据写入亚马逊 S3。有关使用此策略的信息，请参阅创建 AWSApplicationDiscoveryServiceFirehose 角色。

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:*"
            ]
        }
    ]
}
```

授予使用 Migration Hub 控制台网络图的权限

要在创建允许或拒绝访问 Application Discovery Service 或 Migration Hub 的基于身份的策略时授予对 AWS Migration Hub 控制台网络图的访问权限，您可能需要将`discovery:GetNetworkConnectionGraph`操作添加到策略中。

如果策略符合以下两个条件，则必须在新策略中使用`discovery:GetNetworkConnectionGraph`该操作或更新较旧的策略：

- 该策略允许或拒绝访问 Application Discovery Service 或 Migration Hub。
- 该策略使用另一种特定的发现操作来授予访问权限，比如 “`discovery:`*`action-name`*而不是” `discovery:*`。

以下示例说明如何在 IAM 策略中使用`discovery:GetNetworkConnectionGraph`操作。

Example

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

```
            "Effect": "Allow",
            "Action": ["discovery:GetNetworkConnectionGraph"],
            "Resource": "*"
        }
    ]
}
```

有关 Migration Hub 网络图的信息，请参阅在 Migration Hub 中查看网络连接。

为 Application Discovery Service 使用服务相关角色

AWS Application Discovery Service 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种独特的 IAM 角色，直接链接到 Application Discovery Service。服务相关角色由 Application Discovery Service Service 预定义，包括该服务代表您调用其他 AWS 服务所需的所有权限。

服务相关角色使设置 Application Discovery Service 变得更加容易，因为您不必手动添加必要的权限。Application Discovery Service 定义了其服务相关角色的权限，除非另有定义，否则只有应用程序发现服务才能担任其角色。定义的权限包括信任策略和权限策略，以及不能附加到任何其他 IAM 实体的权限策略。

只有在首先删除相关资源后，您才能删除服务相关角色。这可以保护您的 Application Discovery Service 资源，因为您不会无意中删除访问这些资源的权限。

主题

- Application Discovery Service 的服务相关角色权限
- 为 Application Discovery Service 创建服务相关角色
- 删除 Application Discovery Service 的服务相关角色

有关支持服务相关角色的其他服务的信息，请参阅使用 IAM 的AWS 服务并查找服务相关角色列中显示为是的服务。选择是和链接，查看该服务的服务相关角色文档。

Application Discovery Service 的服务相关角色权限

Application Discovery Service 使用名为的 AWS 服务相关角色 AWSServiceRoleForApplicationDiscoveryServiceContinuousExport— 允许访问所使用或管理的 AWS Application Discovery Service服务和资源。

AWSServiceRoleForApplicationDiscoveryServiceContinuousExport 服务相关角色信任以下服务来代入该角色：

- continuousexport.discovery.amazonaws.com

角色权限策略允许 Application Discovery Service 完成以下操作：

glue

  CreateDatabase

  UpdateDatabase

  CreateTable

  UpdateTable

Firehose

  CreateDeliveryStream

  DeleteDeliveryStream

  DescribeDeliveryStream

  PutRecord

  PutRecordBatch

  UpdateDestination

S3

  CreateBucket

  ListBucket

  GetObject

日志

  CreateLogGroup

  CreateLogStream

  PutRetentionPolicy

IAM

  PassRole

这是显示上述操作所适用资源的完整策略：

```
{
    "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"
                }
            }
        }
    ]
}
```

您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的服务相关角色权限。

为 Application Discovery Service 创建服务相关角色

您无需手动创建服务相关角色。当 a) 选择 “开始数据收集” 后确认数据收集器页面显示的对话框中的选项，或者单击标有 “Athena 中的数据探索” 的滑块，或 b) 使用 CLI 调用 API 时，隐式启用 “持续导出” 时， AWSServiceRoleForApplicationDiscoveryServiceContinuousExport 服务相关角色将自动创建。StartContinuousExport AWS

> **Important**
>
> 如果您在其他使用此角色支持的功能的服务中完成某个操作，此服务相关角色可以出现在您的账户中。要了解更多信息，请参阅我的 IAM 账户中的新角色。

通过 Migration Hub 控制台创建服务相关角色

您可以使用 Migration Hub 控制台创建 AWSServiceRoleForApplicationDiscoveryServiceContinuousExport 服务相关角色。

创建服务相关角色（控制台）

1. 在导航窗格中，选择 Data Collectors (数据收集器)。
2. 选择 Agents (代理) 选项卡。
3. 将 “Athena 中的数据浏览” 滑块切换到 “打开” 位置。
4. 在上一步生成的对话框中，单击同意关联成本的复选框并选择 Continue (继续) 或 Enable (启用)。

从中创建服务相关角色 AWS CLI

您可以使用中的 Application Discovery Service 命令 AWS Command Line Interface 来创建 AWSServiceRoleForApplicationDiscoveryServiceContinuousExport服务相关角色。

当您从启动 “连续导出” 时，系统会自动创建此服务相关角色 AWS CLI （ AWS CLI 必须先在您的环境中安装该角色）。

要创建服务相关角色 (CLI)，请从中启动 “持续导出” AWS CLI

1. 安装 AWS CLI 适用于您的操作系统（Linux、macOS 或 Windows）的。有关说明，请参阅《AWS Command Line Interface 用户指南》。
2. 打开命令提示符 (Windows) 或终端 (Linux 或 macOS)。

a. 键入 `aws configure` 并按下 Enter。

b. 输入您的 AWS 访问密钥 ID 和 AWS 私有访问密钥。

c. 对于默认区域名称，输入 `us-west-2`。

d. 对于默认输出格式，输入 `text`。

3. 键入以下命令：

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

您还可以使用 IAM 控制台通过 “发现服务-持续导出” 用例创建服务相关角色。在 IAM CLI 或 IAM API 中，用 `continuousexport.discovery.amazonaws.com` 服务名称创建一个服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的创建服务相关角色。如果您删除了此服务相关角色，可以使用同样的过程再次创建角色。

删除 Application Discovery Service 的服务相关角色

如果不再需要使用某个需要服务相关角色的功能或服务，我们建议您删除该角色。这样就没有未被主动监控或维护的未使用实体。但是，您必须先清除您的服务相关角色，然后才能手动删除它。

清除 服务相关角色

必须先删除服务相关角色使用的所有资源，然后才能使用 IAM 删除该角色。

> **Note**
>
> 如果您尝试删除资源时 Application Discovery Service 正在使用该角色，则删除可能会失败。如果发生这种情况，请等待几分钟后重试。

从 Migration Hub 控制台中删除 AWSServiceRoleForApplicationDiscoveryServiceContinuousExport 服务相关角色使用的 Application Discovery Service 资源

1. 在导航窗格中，选择 Data Collectors (数据收集器)。
2. 选择 Agents (代理) 选项卡。
3. 将 “Athena 中的数据浏览” 滑块切换到 “关闭” 位置。

从中删除 AWSServiceRoleForApplicationDiscoveryServiceContinuousExport 服务相关角色使用的 Application Discovery Service 资源 AWS CLI

1. 安装 AWS CLI 适用于您的操作系统（Linux、macOS 或 Windows）的。有关说明，请参阅《AWS Command Line Interface 用户指南》。
2. 打开命令提示符 (Windows) 或终端 (Linux 或 macOS)。
   a. 键入 `aws configure` 并按下 Enter。
   b. 输入您的 AWS 访问密钥 ID 和 AWS 私有访问密钥。
   c. 对于默认区域名称，输入 `us-west-2`。
   d. 对于默认输出格式，输入 `text`。
3. 键入以下命令：

```
aws discovery stop-continuous-export --export-id <export ID>
```

   - 如果不知道要停止的连续导出的导出 ID，请输入以下命令查看连续导出的 ID：

```
aws discovery describe-continuous-exports
```

4. 输入以下命令，通过验证连续导出的返回状态为 “非活动状态” 来确保其已停止：

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

手动删除服务相关角色

您可以使用 IAM 控制台、IAM CLI 或 IAM API 删除 AWSServiceRoleForApplicationDiscoveryServiceContinuousExport 服务相关角色。如果您不再需要使用需要此服务相关角色的 Discovery Service-持续导出功能，我们建议您删除该角色。这样就没有未被主动监控或维护的未使用实体。有关更多信息，请参见《IAM 用户指南》中的删除服务相关角色。

> **Note**
>
> 必须先清除服务相关角色，然后才能将其删除。请参阅 清除 服务相关角色。

AWS Application Discovery Service 身份和访问疑难解答

使用以下信息来帮助您诊断和修复在使用 Application Discovery Service 和 IAM 时可能遇到的常见问题。

主题

我无权执行 iam：PassRole

如果您收到错误消息，说您无权执行该操作，则必须更新您的策略以允许您将角色传递给 Applicati `iam:PassRole` on Discovery Service。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为的 IAM 用户`marymajor`尝试使用控制台在 Application Discovery Service 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

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

在这种情况下，必须更新 Mary 的策略以允许她执行 `iam:PassRole` 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

记录 Application Discovery Service API AWS CloudTrail

AWS Application Discovery Service 与一项服务集成 AWS CloudTrail，该服务提供用户、角色或服务在 Application Discovery Serv AWS ice 中执行的操作的记录。您可以使用 CloudTrail 记录、持续监控和保留账户活动，以便进行故障排除和审计。 CloudTrail 提供您的 AWS 账户活动的事件历史记录，包括通过 AWS 管理控制台和命令行工具执行的操作。 AWS SDKs

CloudTrail 捕获 Application Discovery Service 的所有 API 调用作为事件。捕获的调用包括来自 Application Discovery Service 控制台的调用和对应用程序发现服务 API 操作的代码调用。

如果您创建了跟踪，则可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括 Application Discovery Service 的事件。如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的 “事件历史记录” 中

查看最新的事件。使用收集的信息 CloudTrail，您可以确定向 Application Discovery Service 发出的请求、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。

要了解更多信息 CloudTrail，请参阅AWS CloudTrail 用户指南。

Application Discovery 服务信息位于 CloudTrail

CloudTrail 在您创建 AWS 账户时已在您的账户上启用。当 Application Discovery Service 中发生活动时，该活动与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在自己的 AWS 账户中查看、搜索和下载最近发生的事件。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

要持续记录您的 AWS 账户中的事件，包括Application Discovery Service的事件，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。默认情况下，当您在控制台中创建跟踪时，该跟踪将应用于所有 AWS 区域。跟踪记录 AWS 分区中所有区域的事件，并将日志文件传送到您指定的 Amazon S3 存储桶。此外，您可以配置其他 AWS 服务，以进一步分析 CloudTrail 日志中收集的事件数据并对其采取行动。有关更多信息，请参阅下列内容：

- 创建跟踪概述
- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail
- 接收来自多个区域的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail 日志文件

Application Discovery Service 的所有操作都由 A CloudTrail pp lication Discovery Service API 参考记录并记录在案。例如，对`CreateTags`、`DescribeTags`、和`GetDiscoverySummary`操作的调用会在 CloudTrail 日志文件中生成条目。

每个事件或日志条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用根证书还是 AWS Identity and Access Management (IAM) 用户凭证发出。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务发出。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

了解应用程序发现服务 Service 日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。事件代表来自任何来源的单个请求，包括有关请求的操作、操作的日期和时间、请求参数等的信息。 CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此它们不会按任何特定的顺序出现。

以下示例显示了演示该DescribeTags操作的 CloudTrail 日志条目。

```
{
    "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 ARN 格式

Amazon 资源名称 (ARN) 是一个唯一标识资源的字符串。 AWS AWS 当你想在所有资源中明确指定资源时，需要一个 ARN。 AWS AWS Application Discovery Service 定义了以下内容 ARNs。

- 发现代理：`arn:aws:discovery:region:account:agent/discovery-agent/agentId`
- 无代理收集器：`arn:aws:discovery:region:account:agent/agentless-collector/agentId`
- 迁移评估器收集器：`arn:aws:discovery:region:account:agent/migration-evaluator-collector/agentId`
- 发现连接器：`arn:aws:discovery:region:account:agent/discovery-connector/agentId`

AWS Application Discovery Service 配额

Service Quotas 控制台提供有关 AWS Application Discovery Service 配额的信息。您可以使用“服务限额”控制台查看默认的服务限额或可调整限额请求增加限额。

当前，唯一可以增加的配额是每个账户导入的服务器。

Application Discovery Service 具有以下默认配额：

- 每个账户 1,000 个应用程序。

  如果您达到此配额并想要导入新的应用程序，则可以使用 `DeleteApplications` API 操作删除现有应用程序。有关更多信息，请参阅《App lication Discovery Service API 参考》DeleteApplications中的。
- 每个导入文件的最大文件大小为 10 MB。
- 每个账户导入了 25,000 条服务器记录。
- 每天删除 25,000 条进口记录。
- 每个账户导入 10,000 台服务器（您可以请求增加此配额）。
- 1,000 个活跃代理，他们正在收集数据并将其发送到 Application Discovery Service。
- 10,000 个不活跃的代理，它们正在响应但不收集数据。
- 每个应用程序 400 个服务器。
- 每台服务器 30 个标签。

故障排除 AWS Application Discovery Service

在本部分中，可以找到有关如何修复 AWS Application Discovery Service的常见问题的信息。

主题

通过数据探索停止数据收集

要停止数据探索，您可以关闭 Migration Hub 控制台中发现 > 数据收集器 > 代理选项卡下的切换开关，也可以调用 `StopContinuousExport` API。停止数据收集最多可能需要 30 分钟，在此阶段，控制台上的切换开关和 `DescribeContinuousExport` API 调用会将数据探索状态显示为 “Stop In Progress”。

> **Note**
>
> 如果刷新控制台页面后，切换开关未关闭并且引发错误消息或 `DescribeContinuousExport` API 返回“Stop_Failed”状态，则可通过关闭切换开关或调用 `StopContinuousExport` API 来重试。如果 “数据探索” 仍然显示错误且无法成功停止，请联系 AWS 支持人员。

也可以按照以下步骤所述手动停止数据收集。

选项 1：停止代理数据收集

如果已使用 ADS 代理完成发现并且不再想要在 ADS 数据库存储库中收集更多数据：

1. 从 Migration Hub 控制台中，选择 “发现” > “数据收集器” > “代理” 选项卡。
2. 选择所有正在运行的现有代理并选择 Stop Data Collection (停止数据收集)。

   这将确保代理在 ADS 数据存储库和您的 S3 存储桶中均不会收集新数据。您的现有数据仍可访问。

选项 2：删除数据探索的 Amazon Kinesis Data Streams

如果您想继续通过 ADS 数据存储库中的代理收集数据，但又不想使用数据探索在 Amazon S3 存储桶中收集数据，则可以手动删除数据探索创建的 Amazon Data Firehose 流：

1. 从 AWS 控制台登录 Amazon Kinesis，然后从导航窗格中选择 D ata Firehose。
2. 删除由数据探索功能创建的以下流：
   - `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`

移除通过数据探索收集的数据

移除通过数据探索收集的数据

1. 移除存储在 Amazon S3 中的发现代理数据。

   由 AWS Application Discovery Service (ADS) 收集的数据存储在名为的 S3 存储桶中`aws-application-discover-discovery-service-`*`uniqueid`*。

   > **Note**
   >
   > 在 Amazon Athena 中启用数据浏览功能时，删除 Amazon S3 存储桶或其中的任何对象都会导致错误。它继续向 S3 发送新的发现代理数据。在 Athena 中也将无法再访问已删除的数据。

2. 移除 AWS Glue Data Catalog。

   在 Amazon Athena 中开启数据探索后，它会在您的账户中创建一个 Amazon S3 存储桶，用于存储 ADS 代理定期收集的数据。此外，它还创建了一个 AWS Glue Data Catalog 以允许您从 Amazon Athena 查询存储在 Amazon S3 存储桶中的数据。当您在 Amazon Athena 中关闭数据探索功能时，不会在您的 Amazon S3 存储桶中存储任何新数据，但之前收集的数据将保持不

变。如果您不再需要这些数据，并且想要将您的账户恢复到 Amazon 中开启数据探索之前的状态，Athena。

a. 从 AWS 控制台访问 Amazon S3 并手动删除名为 “aws-application-discover-discovery-service-uniqueid” 的存储桶
b. 您可以通过删除application-discovery-service-database数据库和所有这些表来手动移 AWS 除数据探索 Glue Data Catalog：

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

从中移除您的数据 AWS Application Discovery Service

要从 Application Discovery Service 中删除所有数据，请联系AWS 支持部门并申请删除全部数据。

修复在 Amazon Athena 中探索数据的常见问题

在本节中，您可以找到有关如何解决在 Amazon Athena 中进行数据探索的常见问题的信息。

主题

- 无法在 Amazon Athena 中启动数据探索，因为无法创建服务相关角色和 AWS 所需资源
- 新的代理数据未显示在亚马逊 Athena 中
- 您没有足够的权限访问亚马逊 S3、Amazon Data Firehose 或 AWS Glue

无法在 Amazon Athena 中启动数据探索，因为无法创建服务相关角色和 AWS 所需资源

当你在 Amazon Athena 中开启数据探索功能时，它会在你的账户中创建服务相关角色`AWSServiceRoleForApplicationDiscoveryServiceContinuousExport`，这样它就可以创建 AWS 所需的资源，使代理收集的数据可以在亚马逊雅典娜中访问，包括亚马逊 S3 存储

桶、Amazon Kinesis 流和。 AWS Glue Data Catalog如果您的账户没有适当的权限在 Amazon Athena 中进行数据浏览以创建此角色，则该角色将无法初始化。请参考AWS 的托管策略 AWS Application Discovery Service。

新的代理数据未显示在亚马逊 Athena 中

如果新数据未流入 Athena，则代理启动已超过 30 分钟，且数据探索状态为 “活动”，请查看下面列出的解决方案：

- AWS 发现代理

  确保代理的 Collection (收集) 状态标记为 Started (已启动)，Health (运行状况) 状态标记为 Running (正在运行)。

- Kinesis 角色

  确保您的账户中具有 `AWSApplicationDiscoveryServiceFirehose` 角色。

- Firehose 状态

  确保以下 Firehose 传送流正常运行：

  - `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

  确保`application-discovery-service-database`数据库已在 AWS Glue。确保 AWS Glue中存在以下表：

  - `os_info_agent`
  - `network_interface_agent`
  - `sys_performance_agent`

- `processes_agent`
- `inbound_connection_agent`
- `outbound_connection_agent`
- `id_mapping_agent`

- Amazon S3 存储桶

  确保您的账户`aws-application-discovery-service-`*`uniqueid`*中有一个名为 Amazon S3 存储桶。如果存储桶中的对象已被移动或删除，则它们将无法正确显示在 Athena 中。

- 您的本地服务器

  确保您的服务器正在运行，以便代理收集数据并将数据发送到 AWS Application Discovery Service。

您没有足够的权限访问亚马逊 S3、Amazon Data Firehose 或 AWS Glue

如果您正在使用 AWS Organizations，并且在 Amazon Athena 中初始化数据探索失败，则可能是因为您无权访问亚马逊 S3、Amazon Data Firehose、Athena 或。 AWS Glue

您需要具有管理员权限的 IAM 用户才能授予您访问这些服务的权限。管理员可以使用他们的账户来授予此访问权限。请参阅AWS 的托管策略 AWS Application Discovery Service。

为确保 Amazon Athena 中的数据探索正常运行，请勿修改或删除 AWS 在亚马逊 Athena 中通过数据探索创建的资源，包括 Amazon S3 存储桶、Amazon Data Firehose Streams 和。 AWS Glue Data Catalog如果意外删除或修改了这些资源，请停止并启动数据探究，它将自动再次创建这些资源。如果您删除通过数据探索创建的 Amazon S3 存储桶，则可能会丢失在存储桶中收集的数据。

排除导入失败记录的问题

Migration Hub 导入允许您直接将本地环境的详细信息导入到 Migration Hub 中，无需使用 Discovery Connector 或 Discovery 代理。这让您可以直接根据导入的数据执行迁移评估和规划。您还可以将设备作为应用程序来分组，并跟踪其迁移状态。

在导入数据时，您有可能遇到错误。这些错误通常由于以下原因所致：

- 已达到与导入相关的配额-存在与导入任务相关的配额。如果您提出的导入任务请求超出配额，则该请求将失败并返回错误。有关更多信息，请参阅 AWS Application Discovery Service 配额。

- 在@@ 导入文件中插入了一个额外的逗号 (,) — .CSV 文件中的逗号用于区分一个字段和下一个字段。不支持字段中出现逗号，因为逗号总是用来拆分字段。这会导致一连串格式错误。确保逗号只在字段之间使用，切勿用在导入文件中。
- 字段的值超出了其支持的范围 — 有些字段（例如某些字段）CPU.NumberOfCores必须具有它们支持的值范围。如果超出支持的范围，则记录无法导入。

如果您的导入请求发生错误，要解决错误，可下载您的导入任务的失败记录，然后在失败条目 CSV 文件中纠正错误，并再次导入。

Console

下载失败记录归档

1. 登录并打开 Mig AWS Management Console ration Hub 控制台，网址为https://console.aws.amazon.com/migrationhub。
2. 在左侧导航窗格中，在 Discover (发现) 下，选择 Tools (工具)。
3. 从 Discovery Tools (发现工具) 中，选择 view imports (查看导入)。
4. 从 Imports (导入) 控制面板中，选择关联导入请求与 Failed records (失败的记录) 数量的单选按钮。
5. 从控制面板中表格的上方，选择 Download failed records (下载失败的记录)。这将打开浏览器下载对话框，以下载归档文件。

AWS CLI

下载失败记录归档

1. 打开一个终端窗口，键入以下命令，其中 *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. 从输出中，复制为 errorsAndFailedEntriesZip 返回的值的整个内容，但不复制引号。
3. 打开一个 Web 浏览器，将该内容粘贴到 URL 文本框，并按 ENTER。这将下载压缩为 .zip 格式的失败记录归档。

现在，您已下载了失败记录归档，可以提取其中包含的两个文件并纠正错误。请注意，如果您的错误与基于服务的限制有关，则您需要请求放宽限制，或者删除足够多的相关资源，以使您的账户不超出限制。归档中包含下列文件：

- errors-file.csv — 此文件是您的错误日志，它跟踪每条失败条目的行`ExternalId`、列名和每条失败记录的描述性错误消息。
- failed-entries-file.csv-此文件仅包含原始导入文件中失败的条目。

要更正您遇到的 non-limit-based错误，请使用更正`failed-entries-file.csv`文件中的问题，然后导入该文件。`errors-file.csv`有关导入文件的说明，请参阅导入数据。

的文档历史记录 AWS Application Discovery Service

最新用户指南文档更新：2023 年 5 月 16 日

下表描述了 2019 年 1 月 18 日之后《App lication Discovery Service 用户指南》的重要更改。如需有关文档更新的通知，您可以订阅 RSS 源。

变更	说明	日期
从 Discovery 连接器过渡到无代理收集器	我们建议当前正在使用 Discovery Connector 的客户过渡到新的无代理收集器。从 2025 年 11 月 17 日起， AWS Application Discovery Service 将停止接受来自 Discovery Connectors 的新数据。有关更多信息，请参阅 Discovery 连接器。	2024 年 11 月 12 日
发布了无代理收集器网络数据收集模块	网络数据收集模块使您能够发现本地数据中心内服务器之间的依赖关系。有关更多信息，请参阅使用无代理收集器网络数据收集模块。	2024 年 11 月 8 日
Support 支持用于依赖关系映射的无代理集合	有关更多信息，请参阅使用 VMware vCenter 无代理收集器数据收集模块。	2024 年 10 月 24 日
2023 年发布基于亚马逊 Linux 的无代理收集器第 2 版	有关更多信息，请参阅无代理收集器的先决条件。	2024 年 9 月 26 日
更新了无代理收集器的先决条件	有关更多信息，请参阅无代理收集器的先决条件。	2024 年 9 月 9 日
API 的最终一致性	有关更多信息，请参阅 AWS Application Discovery Service API 中的最终一致性。	2024 年 6 月 20 日

无代理收集器更新	我们已sts.amazonaws.com 添加到需要出站访问的域名列表中。有关更多信息，请参阅为出站访问 AWS 域配置防火墙。	2024 年 6 月 20 日
要分开访问权限，请创建和使用单独的 AWS 账户。	有关更多信息，请参阅 AWS Application Discovery Service 的操作、资源和条件键。	2024 年 4 月 5 日
介绍无代理收集器数据库和分析数据收集模块	数据库和分析数据收集模块是 Application Discovery Service 无代理收集器（无代理收集器）的新模块。您可以使用此数据收集模块连接到您的环境，并从本地数据库和分析服务器收集元数据和性能指标。有关更多信息，请参阅数据库和分析数据收集模块。	2023 年 5 月 16 日
介绍 Application Discovery Service 无代理收集器	Application Discovery Service 无代理收集器（无代理收集器）是一款新的 AWS Application Discovery Service 本地应用程序，它通过无代理方法收集有关本地环境的信息，以帮助您有效地规划向的迁移。 AWS Cloud有关更多信息，请参阅无代理收集器。	2022 年 8 月 16 日

IAM 更新	AWS Identity and Access Management (IAM) `discovery:GetNetworkConnectionGraph` 操作现在可用于在创建基于身份的策略时授予对 AWS Migration Hub 控制台网络图的访问权限。有关更多信息，请参阅授予使用网络图的权限。	2022 年 5 月 24 日
介绍家乡地区	Migration Hub 主区域为您的整个投资组合提供单一的发现和迁移计划信息存储库，以及向多个 AWS 区域迁移的单一视图。	2019 年 11 月 20 日
介绍 Migration Hub 导入功能	Migration Hub 导入允许您将有关本地服务器和应用程序的信息（包括服务器规格和利用率数据）导入到 Migration Hub。您也可以使用该数据跟踪应用程序迁移的状态。有关更多信息，请参阅 Migrati on Hub 导入。	2019 年 1 月 18 日

下表描述了 2019 年 1 月 18 日之前发布的《App lication Discovery Service 用户指南》的文档版本：

更改	描述	日期
新功能	更新了文档以支持在 Amazon Athena 中进行数据探索，并添加了 “故障排除” 章节。	2018 年 8 月 9 日
主要修订	重新编写了使用和输出详细信息；调整了整个文档的结构。	2018 年 5 月 25 日

更改	描述	日期
Discovery Agent 2.0	发布了新的和改进过的 Application Discovery Agent。	2017 年 10 月 19 日
控制台	AWS Management Console 已添加。	2016 年 12 月 19 日
无代理发现	此版本介绍了如何设置和配置无代理发现。	2016 年 7 月 28 日
新增了 Microsoft Windows Server 的详细信息并修复了命令问题	此更新添加了有关 Microsoft Windows Server 的详细信息。它还记录了对各种命令问题的修复。	2016 年 5 月 20 日
初次发布	这是《Application Discovery Service 用户指南》的第一版。	2016 年 5 月 12 日

AWS 词汇表

有关最新 AWS 术语，请参阅《AWS 词汇表 参考资料》中的AWS 词汇表。

探索连接器

> **Important**
>
> 我们建议当前正在使用 Discovery Connector 的客户过渡到新的无代理收集器。从2025年11月17日起， AWS Application Discovery Service 将停止接受来自Discovery Connectors的新数据。

本节介绍如何从 AWS 无代理发现连接器（Discovery Connector）过渡到 Application Discovery Service 无代理收集器（无代理收集器）。

我们建议当前正在使用 Discovery Connector 的客户过渡到新的无代理收集器。

要了解如何开始使用无代理收集器，请参阅。Applice Discovery Service 无座席活动

部署无代理收集器后，可以删除 Discovery Connector 虚拟机。之前收集的所有数据将继续在 AWS Migration Hub （Migration Hub）中提供。

使用 Discovery 连接器收集数据

> **Important**
>
> 我们建议当前正在使用 Discovery Connector 的客户过渡到新的无代理收集器。从2025年11月17日起， AWS Application Discovery Service 将停止接受来自Discovery Connectors的新数据。有关更多信息，请参阅 探索连接器。

发现连接器收集有关您的 vCenter Ser VMware ver 主机的信息，以及。 VMs但是，只有安装了 vCenter Ser VMware ver 工具，才能捕获这些数据。要确保您使用的 AWS 账户具有执行此任务所需的权限，请参阅AWS 的托管策略 AWS Application Discovery Service。

接下来，您可以找到 Discovery Connector 收集的信息清单。

发现连接器收集数据的表格图例：

- 除非另有说明，否则收集的数据以千字节 (KB) 为度量单位。
- Migration Hub 控制台中的等效数据以兆字节 (MB) 为单位报告。

- 以星号 (*) 表示的数据字段仅在连接器的 API 导出功能生成的.csv 文件中可用。
- 轮询期的间隔大约为 60 分钟。
- 用双星号 (**) 表示的数据字段当前返回一个 null 值。

数据字段	描述
applicationConfigurationId*	VM 被分组到的迁移应用程序的 ID
avgCpuUsagePct	轮询期内的 CPU 使用率的平均百分比
avgDiskBytesReadPerSecond	轮询期内从磁盘读取的平均字节数
avgDiskBytesWrittenPerSecond	轮询期内写入到磁盘的平均字节数
avgDiskReadOpsPerSecond**	每秒平均读取 I/O 操作数为 null
avgDiskWriteOpsPerSecond**	每秒平均写入 I/O 操作数
avgFreeRAM	以 MB 表示的平均可用 RAM
avgNetworkBytesReadPerSecond	平均每秒读取的字节数的吞吐量
avgNetworkBytesWrittenPerSecond	平均每秒写入的字节数的吞吐量
configId	Application Discovery Service 为发现的虚拟机分配了
configType	发现的资源的类型
connectorId	Discovery Connector 虚拟设备的 ID
cpuType	虚拟机的 vCPU，主机的实际模型
datacenterId	vCenter 的 ID
hostId*	VM 主机的 ID
hostName	运行虚拟化软件的主机的名称
hypervisor	管理程序的类型

数据字段	描述
id	服务器的 ID
lastModifiedTime邮票 *	数据导出之前的数据收集的最近日期和时间
macAddress	VM 的 MAC 地址
manufacturer	虚拟化软件的制作者
maxCpuUsagePct	轮询期内的 CPU 使用率的最大百分比
maxDiskBytesReadPerSecond	轮询期内从磁盘读取的最大字节数
maxDiskBytesWrittenPerSecond	轮询期内写入到磁盘的最大字节数
maxDiskReadOpsPerSecond**	每秒的最大读取 I/O 操作数
maxDiskWriteOpsPerSecond**	每秒的最大写入 I/O 操作数
maxNetworkBytesReadPerSecond	每秒读取的最大字节数的吞吐量
maxNetworkBytesWrittenPerSecond	每秒写入的最大字节数的吞吐量
memoryReservation*	用于避免 VM 上发生内存超量承诺的限制
moRefId	唯一 vCenter 托管对象引用 ID
name*	VM 或网络的名称 (用户指定)
numCores	CPU 内的独立处理单元的数量
numCpus	VM 上的中心处理单元的数量
numDisks**	VM 上的磁盘数
numNetworkCards**	VM 上的网卡数
osName	VM 上的操作系统名称
osVersion	VM 上的操作系统版本

数据字段	描述
portGroupId*	VLAN 的成员端口的组的 ID
portGroupName*	VLAN 的成员端口的组的名称
powerState*	电源状态
serverId	Application Discovery Service 为发现的虚拟机分配了
smBiosId*	系统管理 BIOS 的 ID/版本
state*	Discovery Connector 虚拟设备的状态
toolsStatus	VMware 工具的运行状态（在 AWS Migration Hub 控制台中对数据收集器进行排序有关完整列表，请参阅。）
totalDiskSize	以 MB 表示的磁盘的总容量
totalRAM	VM 上可用的 RAM 的总量 (MB)
type	主机类型
vCenterId	VM 的唯一 ID 号
vCenterName*	vCenter 主机的名称
virtualSwitchName*	虚拟开关的名称
vmFolderPath	VM 文件的目录路径
vmName	虚拟机的名称

收集发现连接器数据

在您的 VMware 环境中部署和配置 Discovery Connector 后，如果数据收集停止，则可以重新启动数据收集。您可以通过控制台或通过调用 API 来启动或停止数据收集 AWS CLI。以下过程对这两种方法进行了描述。

Using the Migration Hub Console

以下过程显示了如何在 Migration Hub 控制台的 “数据收集器” 页面上启动或停止 Discovery Connector 数据收集过程。

开始或停止数据收集

1. 在导航窗格中，选择 Data Collectors (数据收集器)。
2. 选择 Connectors (连接器) 选项卡。
3. 选中要启动或停止的连接器的复选框。
4. 选择 Start data collection (启动数据收集) 或 Stop data collection (停止数据收集)。

> **Note**
>
> 如果在使用连接器启动数据收集后没有看到清单信息，请确认您是否已向 vCenter Server 注册该连接器。

Using the AWS CLI

要从启动 Discovery Connector 数据收集过程 AWS CLI，AWS CLI 必须先将其安装到您的环境中，然后必须将 CLI 设置为使用所选的 Migration Hub 主区域。

安装 AWS CLI 并开始数据收集

1. 安装 AWS CLI 适用于您的操作系统（Linux、macOS 或 Windows）的。有关说明，请参阅《AWS Command Line Interface 用户指南》。
2. 打开命令提示符 (Windows) 或终端 (Linux 或 macOS)。
   a. 键入 `aws configure` 并按下 Enter。
   b. 输入您的 AWS 访问密钥 ID 和 AWS 私有访问密钥。
   c. 输入您的家乡作为默认区域名称。例如，`us-west-2`。
   d. 对于默认输出格式，输入 `text`。
3. 要查找要为其启动或停止数据收集的连接器的 ID，请键入以下命令以查看该连接器的 ID：

```
aws discovery describe-agents --filters
 condition=EQUALS,name=hostName,values=connector
```

4. 要通过连接器启动数据收集，请键入以下命令：

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

> **Note**
>
> 如果在使用连接器启动数据收集后没有看到清单信息，请确认您是否已向 vCenter Server 注册该连接器。

要停止连接器收集数据，请键入以下命令：

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

对发现连接器进行故障排除

> **Important**
>
> 我们建议当前正在使用 Discovery Connector 的客户过渡到新的无代理收集器。从2025年11月17日起， AWS Application Discovery Service 将停止接受来自Discovery Connectors的新数据。有关更多信息，请参阅 探索连接器。

本节包含的主题可以帮助您解决 Application Discovery Service Discovery Connector 已知问题。

修复安装 AWS 过程中无法访问发现连接器的问题

在控制台中配置 AWS 无代理发现连接器时，您可能会收到以下错误消息：

> **无法到达 AWS**
>
> AWS 无法访问（连接重置）。请验证网络和代理设置。

出现此错误是因为 Discovery Connector 在设置过程中尝试与该连接器需要与之通信的 AWS 域建立 HTTPS 连接失败。如果无法建立连接，则发现连接器配置将失败。

将连接修复到 AWS

1. 请咨询您的 IT 管理员，了解您的公司防火墙是否阻止了通过端口 443 向任何需要出站访问的 AWS 域的出站流量。

   以下 AWS 域需要出站访问权限：

   - 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

   如果您的防火墙阻止了出口流量，请将其解除封锁。更新防火墙后，重新配置连接器。

2. 如果更新防火墙不能解决连接问题，请检查并确保连接器虚拟机具有到所列域的出站网络连接。如果虚拟机具有出站连接，请通过在端口 443 上运行 telnet 来测试与所列域的连接，如下例所示。

   ```
   telnet ec2.amazonaws.com 443
   ```

3. 如果启用了来自虚拟机的出站连接，则必须联系 Su AWS pp ort 以进一步排除故障。

修复不健康的连接器

每个 Discovery Connector 的健康信息都可以在Migration Hub控制台的数据收集器页面中找到。您可以通过查找任何 Health (运行状况) 为 Unhealthy (运行状况不佳) 的连接器来确定有问题的连接器。以下过程概述如何访问连接器控制台以确定运行状况问题。

访问连接器控制台

1. 在网络浏览器中打开 Migration Hub 控制台，然后从左侧导航栏中选择 “数据收集器”。
2. 在 “连接器” 选项卡中，记下每个运行状况为 “不健康” 的连接器的 IP 地址。
3. 在任何可以连接到连接器虚拟机的计算机上打开浏览器，然后输入连接器控制台的 URLhttps://*ip_address_of_connector*，其中ip_address_of_connector是运行状况不佳的连接器的 IP 地址。
4. 输入连接器管理控制台密码，该密码是在配置连接器时设置的。

访问连接器控制台后，可以采取措施解决运行状况不佳的状态。在这里，您可以选择 “查看 vCenter 连接信息”，您将看到一个包含诊断消息的对话框。View Info (查看信息) 链接仅适用于版本 1.0.3.12 或更高版本的连接器。

更正运行状况问题后，连接器将重新建立与 vCenter 服务器的连接，并且连接器的状态将更改为 HEALTHY (运行状况正常) 状态。如果问题仍然存在，请联系 Supp AWS ort。

连接器运行状况不佳的最常见原因是 IP 地址问题和凭证问题。以下部分可以帮助您解决这些问题，并将连接器恢复到正常运行状态。

主题

IP 地址问题

如果在连接器设置过程中提供的 vCenter 终端节点格式错误、无效或 vCenter 服务器当前关闭而无法访问，则连接器可能会进入运行状况不佳的状态。在这种情况下，当你选择 vCenter 连接的 “查看信息” 时，你会看到一个对话框，上面写着 “确认 vCenter 服务器的运行状态，或者选择编辑设置以更新 vCenter 端点”。

以下过程可以帮助您解决 IP 地址问题。

1. 从连接器控制台(`https://ip_address_of_connector`) 中，选择 Edit Settings (编辑设置)。
2. 从左侧导航中，选择 Step 5: Discovery Connector Set Up (步骤 5：发现连接器设置)。
3. 从 Configure vCenter credentials (配置 vCenter 凭证) 中，记下 vCenter Host (vCenter 主机) IP 地址。
4. 使用单独的命令行工具（如`ping`或）`traceroute`，验证关联的 vCenter 服务器是否处于活动状态，并且可以从连接器虚拟机访问 IP。
   - 如果 IP 地址不正确而 vCenter 服务处于活动状态，则在连接器控制台中更新 IP 地址，然后选择 Next (下一步)。
   - 如果 IP 地址正确但 vCenter 服务器处于非活动状态，请将其激活。
   - 如果 IP 地址正确且 vCenter 服务器处于活动状态，请检查它是否因防火墙问题而阻止入口网络连接。如果是，请更新防火墙设置以允许来自连接器 VM 的传入连接。

凭证问题

如果在连接器安装过程中提供的 vCenter 用户凭证无效或没有 vCenter 读取和查看账户权限，则连接器可能会进入运行状况不佳的状态。在这种情况下，当您选择 vCenter 连接的 “查看信息” 时，您将看到一个对话框，上面写着 “选择编辑设置以更新具有读取和查看权限的帐户的 vCenter 用户名和密码”。

以下过程可以帮助您解决凭证问题。作为先决条件，请确保您已创建在 vCenter 服务器上具有读取和查看账户权限的 vCenter 用户。

1. 从连接器控制台(`https://ip_address_of_connector`) 中，选择 Edit Settings (编辑设置)。
2. 从左侧导航中，选择 Step 5: Discovery Connector Set Up (步骤 5：发现连接器设置)。
3. 在 Configure vCenter credentials (配置 vCenter 凭证) 中，通过为具有读取和查看权限的 vCenter 用户提供凭证来更新 vCenter Username (vCenter 用户名)和 vCenter Password (vCenter 密码)。
4. 选择 Next (下一步) 以完成设置。

支持独立 ESX 主机

Discovery Connector 不支持独立的 ESX 主机。ESX 主机必须是 vCenter Server 实例的一部分。

为连接器问题获得更多支持

如果您遇到问题并需要帮助，请联系 Supp AWS ort。我们将与您联系，并可能要求您发送连接器日志。要获取日志，请执行以下操作：

- 重新登录 Ag AWS entless Discovery Connector 控制台，然后选择 “下载日志包”。
- 当日志包下载完后，请按照 AWS 的指示发送它。

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。