aws

用户指南

Migration Hub 策略建议

Migration Hub 策略建议: 用户指南

Table of Contents

什么是 Migration Hub Strategy Recommendations？

Migration Hub Strategy Recommendations 为可行的应用程序转型路径提供迁移与现代化策略建议，从而帮助您规划迁移与现代化计划。

Strategy Recommendations 可以分析您的服务器清单、运行时系统环境，以及 Microsoft IIS、Java Tomcat 和 Jboss 应用程序的应用程序二进制文件，以生成反模式报告。此外，您可以将源代码配置为允许 Strategy Recommentions 对所有应用程序执行源代码和数据库分析。Strategy Recommendations 将比较此分析与您的业务目标，以及您提供的应用程序和数据库的转换首选项，以推荐：

- 每个应用程序的最有效迁移策略。
- 您可以使用的迁移与现代化工具或服务。
- 要为特定选项解决的应用程序不兼容性和反模式。

Migration Hub Strategy Recommendations 会推荐迁移与现代化策略，以便使用关联的部署、目标、工具和程序更换主机、更换平台和重构。有关主机更换、平台更换和重构的信息，请参阅 AWS Prescriptive Guidance 术语表中的 Migration terms - 7 Rs。

Strategy Recommendations 可能会推荐一些简单的选项，例如，使用 AWS Application Migration Service（AWS MGN）在 Amazon Elastic Compute Cloud（Amazon EC2）上更换主机。更优化的建议可能包括使用 AWS App2Container 将平台更换到容器，或者重构到开源技术，例如 .NET Core 和 PostgreSQL。

您是首次使用 Strategy Recommendations 的客户吗？

如果这是您首次使用 Strategy Recommendations，我们建议您先阅读以下部分：

- Strategy Recommendations 概览
- 设置 Strategy Recommendations
- 开始使用 Strategy Recommendations

Strategy Recommendations 概览

您可以使用 AWS Migration Hub 控制台中的 Migration Hub Strategy Recommendations，开始评测您的服务器和应用程序产品组合。您使用控制台设置和执行评测。评测结束后，您可以使用控制台查看每个服务器和应用程序的评测数据，以及推荐的转换工具。

要接收重构建议和不兼容问题列表，您可以使用 Strategy Recommendations 来评测您的应用程序源代码和数据库。

您还能以 Microsoft Excel 文件下载建议数据。

相关服务

- AWS Migration Hub – 您使用 AWS Migration Hub 控制台来访问 Migration Hub Strategy Recommendations 控制台。它还显示有关您从中收集数据的服务器的信息。
- AWS Application Discovery Service – 在使用 Strategy Recommendations 之前，您在 AWS Migration Hub 控制台中使用 Application Discovery Service 收集关于您的服务器和应用程序的数据。
- AWS Application Migration Service – AWS Application Migration Service 是直接迁移到 AWS 时建议使用的主要迁移服务。
- AWS Database Migration Service – AWS Database Migration Service 是一项 Web 服务，用于将数据从本地、Amazon Relational Database Service（Amazon RDS）数据库实例或 Amazon Elastic Compute Cloud（Amazon EC2）实例上的数据库迁移到 AWS 服务上的数据库。
- AWS App2Container – AWS App2Container（A2C）是一个命令行工具，用于将 .NET 和 Java 应用程序现代化为容器化应用程序。
- Porting Assistant for .NET – 用于.NET 源代码分析。Porting Assistant for .NET 是一款兼容性扫描器，可减少将 Microsoft .NET Framework 应用程序移植到 .NET 内核所需的人工操作。Porting Assistant for .NET 会评测 .NET 应用程序源代码并识别不兼容的 API 和第三方软件包。
- 适用于 Windows Server 的支持终止迁移计划 – 适用于 Windows Server 的支持终止迁移计划（EMP）包括无需任何重构即可在 AWS 上将您的传统应用程序从 Windows Server 2003、2008 和 2008 R2 迁移到受支持的更新版本的工具。
- AWS Schema Conversion Tool – 您可以使用 AWS Schema Conversion Tool（AWS SCT），将现有数据库架构从一个数据库引擎转换为另一个数据库引擎。

- Windows Web Application Migration Assistant – 适用于 AWS Elastic Beanstalk 的 Windows Web Application Migration Assistant 是一款交互式 PowerShell 实用程序，可将 ASP.NET 和 ASP.NET Core 应用程序从本地 IIS Windows 服务器迁移到 Elastic Beanstalk。
- 适用于 Aurora PostgreSQL 的 Babelfish – 适用于 Aurora PostgreSQL 的 Babelfish 是 Amazon Aurora PostgreSQL 兼容版的一项新功能，助力 Aurora 理解为 Microsoft SQL 服务器编写的应用程序发出的命令。

设置 Strategy Recommendations

首次使用 Migration Hub Strategy Recommendations 前，请完成以下任务：

主题

注册获取 AWS 账户

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/signup。
2. 按照屏幕上的说明进行操作。

   在注册时，将接到一通电话，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。作为安全最佳实践，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。

AWS 注册过程完成后会向您发送一封确认电子邮件。在任何时候，您都可以通过转至 https://aws.amazon.com/ 并选择我的账户来查看当前的账户活动并管理您的账户。

创建具有管理访问权限的用户

注册后，请保护您的安全 AWS 账户 AWS 账户根用户 AWS IAM Identity Center，启用并创建管理用户，这样您就不会使用 root 用户执行日常任务。

保护你的 AWS 账户根用户

1. 选择 Root 用户并输入您的 AWS 账户 电子邮件地址，以账户所有者的身份登录。AWS Management Console在下一页上，输入您的密码。

要获取使用根用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的以根用户身份登录。

2. 为您的根用户启用多重身份验证 (MFA)。

   有关说明，请参阅 I A M 用户指南中的为 AWS 账户 根用户启用虚拟 MFA 设备（控制台）。

创建具有管理访问权限的用户

1. 启用 IAM Identity Center

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的启用 AWS IAM Identity Center。

2. 在 IAM Identity Center 中，为用户授予管理访问权限。

   有关使用 IAM Identity Center 目录 作为身份源的教程，请参阅《用户指南》 IAM Identity Center 目录中的使用默认设置配置AWS IAM Identity Center 用户访问权限。

以具有管理访问权限的用户身份登录

- 要使用您的 IAM Identity Center 用户身份登录，请使用您在创建 IAM Identity Center 用户时发送到您的电子邮件地址的登录网址。

  有关使用 IAM Identity Center 用户登录的帮助，请参阅AWS 登录 用户指南中的登录 AWS 访问门户。

将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个权限集，该权限集遵循应用最低权限的最佳做法。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的创建权限集。

2. 将用户分配到一个组，然后为该组分配单点登录访问权限。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的添加组。

Strategy Recommendations 用户和角色

我们建议您为 Strategy Recommendations 创建两个角色：

- 要访问控制台，请创建一个同时附加 AWSMigrationHubFullAccess 和 AWSMigrationHubStrategyConsoleFullAccess 托管策略的角色。
- 要访问 Strategy Recommendations 应用程序数据收集器，请创建一个附加 AWSMigrationHubStrategyCollector 托管策略的角色。

IAM 托管策略定义用户对服务的访问权限级别。 AWS Migration Hub AWSMigrationHubFullAccess托管策略授予对 Migration Hub 控制台的访问权限。有关更多信息，请参阅 Migration Hub Roles and Policies。有关 AWSMigrationHubStrategyConsoleFullAccess 和 AWSMigrationHubStrategyCollector 托管策略的更多信息，请参阅AWS Migration Hub 策略建议的托管策略。

要提供访问权限，请为您的用户、组或角色添加权限：

- 中的用户和群组 AWS IAM Identity Center：

  创建权限集合。按照《AWS IAM Identity Center 用户指南》中创建权限集的说明进行操作。
- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中为第三方身份提供商创建角色（联合身份验证）的说明进行操作。
- IAM 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

开始使用 Strategy Recommendations

本部分介绍如何开始使用 Migration Hub Strategy Recommendations。

主题

Strategy Recommendations 的先决条件

以下是 Migration Hub Strategy Recommendations 的先决使用条件。

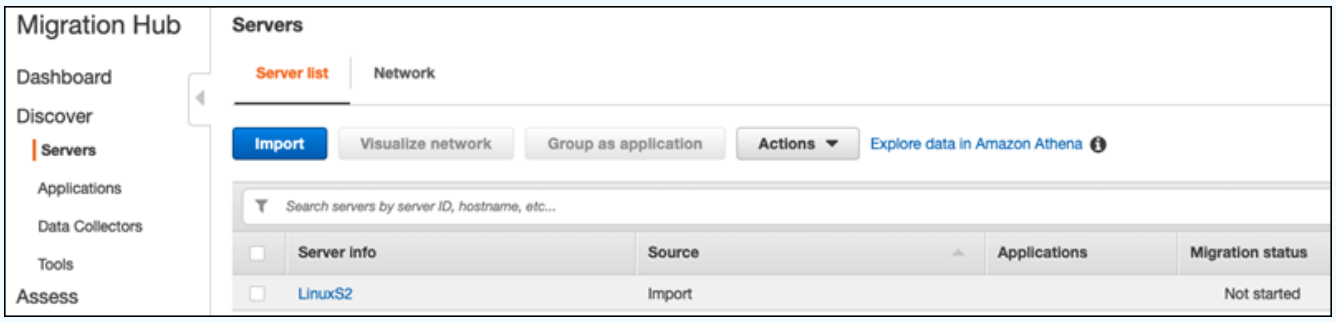
- 您必须有一个或多个 AWS 帐户，并且必须为这些帐户设置用户。有关更多信息，请参阅 设置 Strategy Recommendations。
- Strategy Recommendations 应用程序数据收集器客户端必须能够从服务器远程收集数据。为此，您必须使用一组适用于您的所有 Windows 服务器的凭证，以及一组适用于您的所有 Linux 服务器的凭证。凭证必须具有在您的服务器中创建和删除目录的权限。
- vCenter 中部署的收集器的版本支持 VMware vCenter Server V6.0、V6.5、6.7 或 7.0。

  您还可以使用收集器 AMI 在 Amazon EC2 实例中部署收集器。
- 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
  - Windows

  - Windows Server 2008 R1 SP2、2008 R2 SP1
  - Windows Server 2012 R1、2012 R2
  - Windows Server 2016
  - Windows Server 2019
- 要进行源代码分析，您的存储库 GitHub 和 GitHub 企业存储库必须具有可与 Strategy Recommendations 收集器客户端共享的存储库范围的个人访问令牌。有关使用存储库范围创建个人访问令牌的更多信息，请参阅GitHub文档中的创建个人访问令牌。

  要分析 .NET 存储库以获得 Porting Assistant for .NET 建议，您必须提供通过 Porting Assistant for .NET 移植评测工具设置的 Windows 计算机。有关更多信息，请参阅 Porting Assistant for .NET User Guide 中的 Getting started with Porting Assistant for .NET。
- 要启用 Strategy Recommendations 进行数据库分析，您必须在 AWS Secrets Manager中输入凭证。有关更多信息，请参阅 Strategy Recommendations 数据库分析。
- 在使用策略建议之前 AWS Application Discovery Service ，您必须使用在 AWS Migration Hub 控制台中收集服务器和应用程序的相关数据。您可以使用以下其中一种方法来收集数据。
  - Migration Hub 导入 – 借助 Migration Hub 导入，您可以将关于您的本地服务器和应用程序的信息导入 Migration Hub。有关更多信息，请参阅 Application Discovery Service User Guide 中的 Migration Hub Import。
  - AWS Application Discovery Service 无代理收集器 – 无代理收集器是一款 VMware 设备，用于收集有关 VMware 虚拟机（VM）的信息。有关更多信息，请参阅 Application Discovery Service User Guide 中的 Agentless Collector。
  - AWS A@@ pplicat ion Discovery Agent — Discovery Agent 是安装在本地服务器和虚拟机上的 AWS 软件，用于捕获系统信息和系统间网络连接的详细信息。有关更多信息，请参阅 Application Discovery Service User Guide 中的 AWS Application Discovery Agent。
- Strategy Recommendations 数据收集器 – 如果您的服务器在 VMware vCenter 中托管，并且您提供访问权限，则 Strategy Recommendations 可以自动获取您的服务器清单。Strategy Recommendations 控制台将使用收集的信息来协助评测。

> **Note**
>
> 要验证 Migration Hub 导入是否成功完成，请在 Migration Hub 控制台导航窗格的发现下选择服务器。所有导入的服务器均会列出。



步骤 1：下载 Strategy Recommendations 收集器

Migration Hub 策略建议应用程序数据收集器是一种虚拟设备，您可以在您的本地 VMware 环境中安装它。Strategy Recommendations 应用程序数据收集器还可以作为 Amazon 机器映像（AMI）提供。如果您想使用 AMI 版本的收集器来评估 AWS 应用程序或出于其他原因，则无需下载收集器。您可以跳过本部分并转至在 Amazon EC2 实例中部署 Strategy Recommendations 收集器。

本部分介绍如何下载收集器开放虚拟化存档（OVA）文件，借助该文件您可以在 VMware 环境中将收集器部署为虚拟机（VM）。

下载收集器 OVA 文件

1. 使用你在中创建的 AWS 账户设置 Strategy Recommendations，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，选择策略。
3. 在 Migration Hub Strategy Recommendations 页面上，选择下载数据收集器。
4. 或者，如果您想导入应用程序数据，您可以选择下载导入模板。有关导入用户的更多信息，请参阅将数据导入 Strategy Recommendations。
5. 单击获得建议按钮并选择同意，允许 Migration Hub 在您的账户中创建服务相关角色（SLR）。首次设置 Strategy Recommendations 时，您必须创建 SLR。有关更多信息，请参阅 使用 Strategy Recommendations 的服务相关角色。

步骤 2：部署 Strategy Recommendations 收集器

本部分介绍如何部署 Strategy Recommendations 应用程序数据收集器。应用程序数据收集器是一种无代理数据收集器，用于识别服务器上正在运行的应用程序、执行源代码分析并分析您的数据库。

有以下两种方法可部署收集器：

- 在 VMware vCenter Server 中作为虚拟机（VM）进行部署。有关更多信息，请参阅 在 vCenter 中部署 Strategy Recommendations 收集器。
- 如果您有要评估的 AWS 应用程序，则可以使用策略建议收集器 Amazon 系统映像 (AMI)。有关更多信息，请参阅 在 Amazon EC2 实例中部署 Strategy Recommendations 收集器。

在 vCenter 中部署 Strategy Recommendations 收集器

Migration Hub 策略建议应用程序数据收集器是一种虚拟设备，您可以在您的本地 VMware 环境中安装它。本部分介绍如何在 VMware 环境中将收集器开放虚拟化存档（OVA）文件部署为虚拟机（VM）。

以下步骤介绍如何在您的 VMware vCenter Server 环境中部署 Strategy Recommendations 收集器。

在 vCenter 中部署收集器

1. 以 VMware 管理员身份登录 vCenter。
2. 部署您在步骤 1 中下载的 OVA 文件。OVA 文件包括收集器和可用于访问 Strategy Recommendations API 的 CLI。

   您还可以通过以下链接下载 OVA 文件：

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

我们建议虚拟机满足以下规格。

Strategy Recommendations 收集器虚拟机规格

- RAM – 最低 8GB
- CPU – 至少 4 个

> **Note**
>
> 为确保您使用的是包含所有新功能和错误修复的最新版本收集器，请在部署收集器 OVA 文件后升级收集器。有关如何升级的说明，请参阅升级 Strategy Recommendations 收集器。

在 Amazon EC2 实例中部署 Strategy Recommendations 收集器

如果您有想要评估的 AWS 应用程序，则可以使用策略建议应用程序数据收集器 Amazon Machine Image (AMI)。

以下步骤介绍如何从收集器 AMI 启动 Amazon EC2 实例。

部署收集器 Amazon EC2 实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在屏幕顶部的导航栏中，会显示当前 区域 [例如，美国东部（俄亥俄）]。从 Strategy Recommendations 使用的区域中选择适合您需求的区域。有关这些区域的列表，请参阅 AWS 一般参考 中的 Strategy Recommendations endpoints。
3. 在导航窗格中，在映像下选择 AMI。
4. 从我拥有的下拉列表中选择公有映像。
5. 选择搜索栏并从菜单中选择 AMI 名称。
6. 输入名称 AWSMHubApplicationDataCollector。
7. 要确保 AMI 来自安全来源，请验证账户所有者是否为 703163444405。
8. 要从此 AMI 启动实例，请选择该实例，然后选择 Launch。有关使用控制台启动实例的更多信息，请参阅 Amazon EC2 用户指南中的从 AMI 启动实例。

   我们建议 Amazon EC2 实例满足以下规格。

   Strategy Recommendations 收集器 Amazon EC2 实例规格

   - RAM – 最低 8GB
   - CPU – 至少 4 个

Strategy Recommendations AMI 文件包括收集器和可用于访问 Strategy Recommendations API 的 CLI。

> **Note**
>
> 为确保您使用的是包含所有新功能和错误修复的最新版本收集器，请在将 Strategy Recommendations 收集器部署为 Amazon EC2 实例后升级收集器。有关如何升级的说明，请参阅升级 Strategy Recommendations 收集器。

步骤 3：登录 Strategy Recommendations 收集器

本部分介绍如何登录已部署的 Migration Hub Strategy Recommendations 应用程序数据收集器。收集器的登录方式取决于您的部署方式。

- 登录在基于 vCenter 的环境中部署的收集器
- 登录作为 Amazon EC2 实例部署的收集器

登录在基于 vCenter 的环境中部署的收集器

登录在基于 vCenter 的环境中部署的 Strategy Recommendations 收集器

1. 使用以下命令通过 SSH 客户端连接到收集器。

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

2. 当系统提示输入密码时，请输入默认密码 aq1@WSde3。首次登录时，您必须更改密码。

登录作为 Amazon EC2 实例部署的收集器

登录作为 Amazon EC2 实例部署的 Strategy Recommendations 收集器

- 使用以下命令通过 SSH 客户端连接到收集器。

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

Keyname.pem 是您从收集器 AMI 启动 Amazon EC2 实例时生成的私钥。

步骤 4：设置 Strategy Recommendations 收集器

本部分介绍如何使用命令行 `collector setup` 命令来配置 Migration Hub Strategy Recommendations 应用程序数据收集器。这些配置在本地存储。

要使用 `collector setup` 命令，您必须先使用以下 `docker exec` 命令在收集器 Docker 容器中创建 Bash Shell 会话。

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

`collector setup` 命令会连续运行以下所有命令，但您可以单独运行这些命令：

- `collector setup --aws-configurations` – 设置 AWS 配置。
- `collector setup --vcenter-configurations` – 设置 vCenter 配置。

> **Note**
>
> 仅当收集器在 vCenter 上托管时，vCenter 配置设置才可用。但是，您可以使用 `collector setup --vcenter-configurations` 命令强制设置 vCenter 配置。

- `collector setup --remote-server-configurations` – 设置远程服务器配置。
- `collector setup --version-control-configurations` – 设置版本控制配置。

同时设置所有收集器配置

1. 输入以下命令。

```
collector setup
```

2. 按照设置 AWS 配置中所述，输入 AWS 配置的信息。
3. 按照设置 vCenter 配置中所述，输入 vCenter 配置的信息。
4. 按照设置远程服务器配置中所述，输入远程服务器配置的信息。
5. 按照设置版本控制配置。中所述，输入版权控制配置的信息。
6. 按照为数据收集准备您的远程 Windows 和 Linux 服务器中的说明，为收集器数据收集准备您的 Windows 和 Linux 服务器。

设置 AWS 配置

在使用 `collector setup` 命令或 `collector setup --aws-configurations` 命令时设置 AWS 配置。

1. 对于您是否已设置 IAM 权限...问题，输入 Y，表示“是”。按照Strategy Recommendations 用户和角色中的步骤，当您使用 `AWSMigrationHubStrategyCollector` 托管策略创建用户以访问收集器时，您可以设置这些权限。
2. 按照Strategy Recommendations 用户和角色中的步骤，通过 AWS 输入您的访问密钥和私有密钥，该账户拥有您用于访问收集器的已创建用户。

3. 输入区域，例如 us-west-2。从 Strategy Recommendations 使用的区域中选择适合您需求的区域。有关这些区域的列表，请参阅 AWS 一般参考 中的 Strategy Recommendations endpoints。
4. 对于是否将收集器相关指标上传到迁移中心策略服务？问题，输入 Y，表示“是”。指标信息有助于 AWS 为您提供适当的支持。
5. 对于是否将收集器相关日志上传到迁移中心策略服务？问题，输入 Y，表示“是”。日志信息有助于 AWS 为您提供适当的支持。

以下示例展示了什么会显示，包括 AWS 配置的示例条目。

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

设置 vCenter 配置

在使用 collector setup 命令或 collector setup --vcenter-configurations 命令时设置 vCenter 配置：

1. 如果您想使用 VMware vCenter 进行身份验证，对于是否要使用 VMware vCenter 凭证进行身份验证问题，输入 Y，表示“是”。

> **Note**
>
> 在使用 VMware vCenter 凭证进行身份验证时，您必须在目标服务器上安装 VMware 工具。

输入主机 URL，可以是 vCenter IP 地址或 URL。然后，输入 VMware vCenter 的用户名和密码。

2. 如果您想配置 Windows 服务器，对于您是否有 VMware vCenter 托管的 Windows 计算机问题，输入 Y，表示“是”。

   输入 Windows 的用户名和密码。

   > **Note**
   >
   > 如果您的 Windows Remote Server 属于 Active Directory 域，则在使用 CLI 提供远程服务器配置时，您必须以 *domain-name**username* 形式输入用户名。例如，如果您的域名是 exampledomain，您的用户名是 Administrator，那么您在 CLI 中输入的用户名是 exampledomain\Administrator。

3. 如果您想配置 Linux 服务器，则对于是否使用 VMware vCenter 设置 Linux 问题，输入 Y，表示“是”。

   输入 Linux 的用户名和密码。

4. 如果您想为 vCenter 以外的服务器设置远程服务器凭证，则对于是否想使用 NTLM（适用于 Windows）和 SSH/Cert（适用于 Linux）为 vCenter 以外的服务器设置凭证问题，输入 Y，表示“是”。

5. 如果 vCenter 之外托管的 Windows 计算机的凭证与配置 vCenter Windows 计算机的凭证时提供的凭证相同，则对于是否要使用 vCenter 设置期间的相同 Windows 凭证问题，请输入 Y，表示“是”。否则，输入 N，表示“否”。

   如果您回答 Y，表示“是”，则系统会提问您以下问题。

   a. 对于您是否同意，在首次与 Windows 服务器交互时，收集器接受并在本地存储服务器证书？问题，请输入 Y，表示“是”。

   b. 如果您想配置 SSH 身份验证，则对于输入您的选项问题，请输入 1。

如果您选择使用 SSH 身份验证，您必须将生成的密钥凭证复制到 Linux 服务器。有关更多信息，请参阅[在 Linux 服务器上设置基于密钥的身份验证]。

以下示例展示了什么会显示，包括 VMware vCenter 配置的示例条目。

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

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

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

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

Username for Windows (Domain\User): username
Password for Windows: password
Reenter password for Windows: password
Successfully stored windows credentials...
You can verify your setup for vCenter windows machines is correct with "collector diag-
check"
Do you have Linux machines managed by VMWare vCenter? [Y/N]: y
Username for Linux: username
Password for Linux: password
Reenter password for Linux: password
Successfully stored linux credentials...
You can verify your setup for vCenter linux machines is correct with "collector diag-
check"
Would you like to setup credentials for servers not managed by vCenter using NTLM for
 windows and SSH/Cert based for Linux? [Y/N]: y
Setting up target server for remote execution:
Would you like to setup credentials for servers not managed by vCenter using NLTM for
 Windows [Y/N]: y
```

```
Would you like to use the same Windows credentials used during vCenter setup? [Y/N]: y
Are you okay with collector accepting and locally storing server certificates on your
 behalf during first interaction with windows servers? These certificates will be used
 by collector for secure communication with windows servers [Y/N]: y
Successfully stored windows server credentials...
Please note that all windows server certificates are stored in directory /opt/amazon/
application-data-collector/remote-auth/windows/certs

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

SSH key pair path: /opt/amazon/application-data-collector/remote-auth/linux/keys/
id_rsa_assessment
Please add the public key "id_rsa_assessment.pub" to the "$HOME/.ssh/authorized_keys"
 file in your remote machines.
You can verify your setup for remote linux machines is correct with "collector diag-
check
```

设置远程服务器配置

在使用 `collector setup` 命令或 `collector setup --remote-server-configurations` 命令时设置远程服务器配置：

1. 如果您想配置 Windows 服务器，则对于您是否想使用 NLTM（适用于 Windows）为非 vCenter 托管的服务器设置凭证问题，请输入 Y，表示“是”。

   输入 WinRM 的用户名和密码。

> **Note**
>
> 如果您的 Windows Remote Server 属于 Active Directory 域，则在使用 CLI 提供远程服务器配置时，您必须以 *domain-name**username* 形式输入用户名。例如，如果您的域名是 exampledomain，您的用户名是 Administrator，那么您在 CLI 中输入的用户名是 exampledomain\Administrator。

对于您是否同意，在首次与 Windows 服务器交互时，收集器接受并在本地存储服务器证书？问题，请输入 Y，表示“是”。Windows Server 证书存储在 `/opt/amazon/application-data-collector/remote-auth/windows/certs` 目录中。

您必须将生成的服务器凭证复制到您的 Windows 服务器。有关更多信息，请参阅在 Windows 服务器上设置远程服务器配置。

2. 如果您想配置 Linux 服务器，则对于是否使用 SSH 或 Cert 设置 Linux 问题，输入 Y，表示“是”。
3. 如果您想配置基于 SSH 密钥的身份验证，则对于输入您的选项问题，请输入 1。

   如果您选择使用 SSH 身份验证，您必须将生成的密钥凭证复制到 Linux 服务器。有关更多信息，请参阅在 Linux 服务器上设置基于密钥的身份验证。
4. 如果您想配置基于证书的身份验证，则对于输入您的选项问题，请输入 2。

   有关设置基于证书的身份验证的信息，请参阅在 Linux 服务器上设置基于证书的身份验证。

以下示例展示了什么会显示，包括远程服务器配置的示例条目。

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

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

Username for WinRM (Domain\User): username
Password for WinRM: password
Reenter password for WinRM: password
```

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

Please note the IP address of the collector and run the script specified in the user
 documentation on all the windows servers in your inventory
Would you like to setup credentials for servers not managed by vCenter using SSH/Cert
 based for Linux? [Y/N]: Y
Choose one of the following options for remote authentication:
1. SSH based authentication
2. Certificate based authentication
Enter your options [1-2]: 1
User name for remote server: username
Generating SSH key on this machine...
SSH key pair path: /opt/amazon/application-data-collector/remote-auth/linux/keys/
id_rsa_assessment
Please add the public key "id_rsa_assessment.pub" to the "$HOME/.ssh/authorized_keys"
 file in your remote machines.
Your Linux remote server configurations are saved successfully.
```

设置版本控制配置。

在使用 `collector setup` 命令或 `collector setup --version-control-configurations` 命令时设置版本控制配置：

1. 对于是否设置源代码分析？问题，请输入 Y，表示“是”。
2. 如果您想配置 Git 服务器端点，则对于输入您的选项问题，请输入 1。

   对于 GIT 服务器端点：，请输入 github.com。
3. 如果您想配置 GitHub Enterprise Server，则对于输入您的选项问题，请输入 2。

   输入不带 https://的企业端点，如下所示：GIT 服务器端点：*git-enterprise-endpoint*
4. 输入您的 Git ###和个人访问##。
5. 如果您想分析 C# 代码，则对于您是否有任何需要在 Windows 计算机上分析的 csharp 存储库问题，请输入 Y，表示“是”。

> **Note**
>
> 要分析 .NET 存储库以获得 Porting Assistant for .NET 建议，您必须提供通过 Porting Assistant for .NET 移植评测工具设置的 Windows 计算机。有关更多信息，请参阅 Porting Assistant for .NET User Guide 中的 Getting started with Porting Assistant for .NET。

6. 对于您是否想在这台计算机上重用现有的 Windows 凭证？问题。如果用于 C# 源代码分析的 Windows 计算机使用的凭证与之前在设置 `--remote-server-configurations` 或 `--vcenter-configurations` 时提供的凭证相同，请输入 Y，表示“是”。

   如果您想输入新的凭证，请输入 N，表示“否”。

7. 要使用 VMWare vCenter Windows Machine 凭证，则对于为 Windows 凭证选择以下其中一个选项，请选择 1。

8. 输入 Windows 计算机的 IP 地址。

以下示例展示了什么会显示，包括版本控制配置的示例条目。

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

为数据收集准备您的远程 Windows 和 Linux 服务器

> **Note**
>
> 如果您使用 vCenter 凭证设置 Strategy Recommendations 应用程序数据收集器，则无需执行此步骤。

设置远程服务器配置后，如果您使用的是 `collector setup command` 或 `collector setup --remote-server-configurations` 命令，您必须准备您的远程服务器，以便 Strategy Recommendations 应用程序数据收集器可以从中收集数据。

> **Note**
>
> 您必须确保，服务器可以通过它们的私有 IP 地址访问。有关如何通过 AWS 上的虚拟私有云（VPC）设置远程运行环境的进一步说明，请参阅 Amazon Virtual Private Cloud User Guide。

要准备您的远程 Linux 服务器，请参阅准备远程 Linux 服务器。

要准备您的远程 Windows 服务器，请参阅在 Windows 服务器上设置远程服务器配置。

准备远程 Linux 服务器

在 Linux 服务器上设置基于密钥的身份验证

如果您在进行远程服务器配置时选择为 Linux 设置基于 SSH 密钥的身份验证，您必须按照以下步骤在服务器上设置基于密钥的身份验证，以便 Strategy Recommendations 应用程序数据收集器可以收集数据。

在 Linux 服务器上设置基于密钥的身份验证

1. 从容器中的以下文件夹中复制通过名称 id_rsa_assessment.pub 生成的公钥：

   /opt/amazon/application-data-collector/remote-auth/linux/keys。
2. 将复制的公钥附加到所有远程计算机的 `$HOME/.ssh/authorized_keys` 文件中。如果没有可用的文件，请使用 `touch` 或 `vim` 命令创建文件。
3. 确保远程服务器上主文件夹的权限级别为 `755` 或更低。如果是 `777`，那就行不通了。您可以使用 `chmod` 命令来限制权限。

在 Linux 服务器上设置基于证书的身份验证

如果您在进行远程服务器配置时选择为 Linux 设置基于证书的身份验证，您必须按照以下步骤操作，以便 Strategy Recommendations 应用程序数据收集器可以收集数据。

如果您已经为应用程序服务器设置了证书颁发机构（CA），我们建议您使用此选项。

在 Linux 服务器上设置基于证书的身份验证

1. 复制适用于所有远程服务器的用户名。
2. 将收集器的公钥复制到 CA。

   收集器的公钥可以在以下位置找到：

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

   该公钥必须添加到您的 CA 才能生成证书。
3. 将上一步中生成的证书复制到收集器中的以下位置：

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

   证书的名称必须是 id_rsa_assessment-cert.pub。
4. 在设置期间提供证书文件名。

在 Windows 服务器上设置远程服务器配置

如果您在收集器设置中进行远程服务器配置时选择设置 Windows，您必须按照以下步骤操作，以便 Strategy Recommendations 可以收集数据。

> 要了解关于远程服务器上执行的 PowerShell 脚本的更多信息，请阅读此说明。
>
> 该脚本启用 PowerShell 远程功能，禁用除协商之外的所有身份验证方法。这适用于 Windows NT LAN Manager（NTLM）并将“AllowUnencrypted”WSMan 协议设置为 False，以确保新创建的侦听器仅接受加密流量。它使用 Microsoft 提供的脚本 `New-SelfSignedCertificateEx.ps1`，创建自签名证书。
> 任何具有 HTTP 侦听器的 WSMan 实例都将与现有的 HTTPS 侦听器一起删除。然后，它会创建新的 HTTPS 侦听器。它还会为 TCP 端口 5986 创建入站防火墙规则。最后，WinRM 服务将重新启动。

在 Windows 2008 服务器上通过远程连接设置数据收集

1. 使用以下命令来查看您的服务器上安装的 PowerShell 版本。

```
$PSVersionTable
```

2. 如果 PowerShell 版本不是 5.1，请按照 Microsoft 文档中安装并配置 WMF 5.1 的说明下载并安装 WMF 5.1。
3. 在新的 PowerShell 窗口中使用以下命令，确保安装 PowerShell 5.1。

```
$PSVersionTable
```

4. 按照下一组步骤进行操作，这些步骤介绍如何在 Windows 2012 及更高版本上通过远程连接来设置数据收集。

在 Windows 2012 及更新的服务器上通过远程连接设置数据收集

1. 从以下 URL 下载设置脚本：

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

2. 从以下 URL 下载 `New-SelfSignedCertificateEx.ps1`，然后将脚本粘贴到您下载 `WinRMSetup.ps1` 的同一个文件夹中：

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

3. 要完成设置，请在所有应用程序服务器上运行下载的 PowerShell 脚本。

```
.\WinRMSetup.ps1
```

> **Note**
>
> 如果 Windows Remote Server 上未正确设置 Windows Remote Management（WinRM），则从该服务器收集数据的尝试将失败。如果发生这种情况，您必须从容器上的以下位置删除与该服务器对应的证书：
> /opt/amazon/application-data-collector/remote-auth/windows/certs/***ads-server-id***.cer
> 删除证书后，请等待数据收集进程重试。

验证是否已为数据收集设置您的收集器和服务器

验证是否已使用以下命令为数据收集正确设置您的收集器和服务器。

```
collector diag-check
```

此命令对您的服务器配置执行一系列诊断检查，并提供失败检查的输入。

当您在 -a 模式下使用该命令时，您会在检查完成后在 DiagnosticCheckResult.txt 文件中获得输出。

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

您可以使用该服务器的 IP 地址对单台服务器的服务器配置执行诊断检查。

以下示例显示了成功设置的输出。

Linux 服务器

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

Windows 服务器

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

以下示例展示了远程服务器凭证不正确时显示的错误消息。

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

步骤 5：使用 Migration Hub 控制台中的 Strategy Recommendations 获得建议

本部分介绍如何使用 Migration Hub 控制台中的 Strategy Recommendations 首次获得迁移建议。

获得推荐

1. 使用您在 设置 Strategy Recommendations 中创建的 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，选择策略。
3. 在 Migration Hub Strategy Recommendations 页面上，选择获得建议。

4. 如果您同意允许 Migration Hub 在您的账户中创建服务相关角色（SLR），请选择同意。有关 SLR 的更多信息，请参阅使用 Strategy Recommendations 的服务相关角色。
5. 配置数据来源
   a. 在配置数据来源页面上，您必须从以下选项中选择要分析的服务器的来源：
      i. Strategy Recommendations 应用程序数据收集器 – 您可以使用 Strategy Recommendations 收集器自动检索有关 VMware vCenter 中托管的虚拟机的信息。使用此选项后，您无需执行其他设置。
      ii. 手动导入 – 如果您想独立导入有关服务器和应用程序的数据，您可以使用 Strategy Recommendations 导入模板。导入模板是一个 JSON 文件，在其中您可以填写您的虚拟机的可用信息。
      iii. Application Discovery Service – 您可以使用 Application Discovery Service 来收集有关您的本地应用程序和服务器的信息。在 Migration Hub 控制台的工具部分下，您可以从发现工具下的多个选项中进行选择。例如，您可以选择 Application Discovery Service 无代理收集器、AWS Discovery Agent 或导入（适用于 CSV 文件）。
   b. 服务器表根据您在数据来源部分中的选择列出了所有可用的服务器。
   c. “已注册的应用程序数据收集器”下列出了您设置的应用程序数据收集器。如果您尚未设置任何数据收集器，您可以下载数据收集器，然后对其进行部署。有关更多信息，请参阅 步骤 1：下载 Strategy Recommendations 收集器 和 步骤 2：部署 Strategy Recommendations 收集器。

      > **Note**
      >
      > 要获得策略建议，您必须至少设置一个应用程序数据收集器或执行应用程序数据导入。如果您想在不设置收集器的情况下添加应用程序级数据，您可以使用应用程序数据导入模板。您可以稍后添加其他数据来源。

   d. 如果您选择了手动导入，则在导入详细信息下，选择添加新导入。
   e. 对于导入名称，请输入您的导入的名称。
   f. 对于 S3 桶 URI，请输入要上传到的导入 JSON 文件的 S3 桶 URI。

      > **Important**
      >
      > S3 桶名称必须以前缀 **`migrationhub-strategy`** 开头。

   g. 选择下一步。

6. 指定首选项

   a. 在指定首选项页面上，设置您的业务目标和迁移首选项。Strategy Recommendations 会根据您指定的首选项推荐应用程序和数据库迁移与现代化的最佳策略。您可以稍后更改这些首选项。

   b. 选择下一步。

7. 查看并提交。

   a. 查看您配置的数据来源和迁移首选项。

   b. 如果一切正确，请选择开始数据分析。这将分析您的服务器清单和运行时系统环境，以及您的 Microsoft IIS 和 Java 应用程序的应用程序二进制文件。

> **Note**
>
> 二进制分析的状态不会在控制台中显示。分析完成后，您将看到指向反模式报告的链接，或者一条表明分析不成功的消息。

Strategy Recommendations 建议

本部分介绍如何查看适用于您的迁移组合中服务器和应用程序的 Strategy Recommendations 迁移与现代化建议。

主题

在 Strategy Recommendations 中查看策略建议

本节介绍如何使用 AWS Migration Hub 控制台中的策略建议来查看迁移策略建议。

查看策略建议

1. 使用你在中创建的 AWS 账户设置 Strategy Recommendations，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，选择策略，然后选择建议。
3. 在建议页面上，您可以查看和导出适用于您的产品组合的摘要建议以及详细的迁移“R”策略建议。您还可以查看迁移与现代化工具和目标，以及服务器和应用程序组件的反模式。

   反模式是在您的产品组合中发现的一系列已知问题，这些问题按严重性分类。高严重性反模式代表需要解决的不兼容问题，中等严重性反模式代表警告，低严重性反模式代表信息问题。有关“R”策略的信息，请参见 AWS Prescriptive Guidance 术语表中的 Migration terms - 7 Rs。

   - 如果您的数据中心发生变化或者您更新了您的首选项，我们建议您重新分析数据。要重新分析您的数据以获得新的建议，请选择重新分析数据。

     在重新分析流程完成之前，您的建议数据结果可能混合了之前的数据和新数据。

     要下载包含建议的报告文件，请选择导出建议。
4. 在应用程序组件选项卡上，您可以查看针对您的迁移产品组合中应用程序组件的建议。有关更多信息，请参阅 Strategy Recommendations 应用程序组件建议。

5. 在服务器选项卡上，您可以查看适用于您的迁移产品组合中服务器的建议。有关更多信息，请参阅 Strategy Recommendations 服务器建议。
6. 在首选项选项卡上，您可以编辑您在步骤 5：获得建议中指定的首选项。有关如何编辑首选项的信息，请参阅Strategy Recommendations 首选项。

Strategy Recommendations 应用程序组件建议

本部分介绍如何使用 Migration Hub 控制台中的 Strategy Recommendations 来查看和分析适用于应用程序组件的迁移策略建议。

主题

- 在 Strategy Recommendations 中使用应用程序组件
- Strategy Recommendations 源代码分析
- Strategy Recommendations 数据库分析
- Strategy Recommendations 二进制分析

在 Strategy Recommendations 中使用应用程序组件

本部分介绍如何使用 Migration Hub 控制台中的 Migration Hub Strategy Recommendations 来查看并配置迁移与现代化策略建议。

主题

- 查看应用程序组件建议
- 为应用程序组件配置源代码分析
- 为应用程序组件配置数据库分析

查看应用程序组件建议

本部分介绍如何使用 Migration Hub 控制台中的 Strategy Recommendations 来查看适用于应用程序组件的迁移策略建议。

查看适用于应用程序组件的建议详细信息

1. 使用你在中创建的 AWS 账户设置 Strategy Recommendations，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，选择策略，然后选择建议。
3. 在建议页面上，选择应用程序组件选项卡。

   a. 应用程序组件摘要下面概述了您在服务器产品组合中运行的各种类型的应用程序组件。

   b. 在应用程序组件下，您可以查看组件名称、组件类型和迁移“R”策略建议。您还可以查看迁移目的地，以及用于服务器产品组合中运行的各种应用程序组件的迁移与现代化工具。有关“R”策略的信息，请参见 AWS Prescriptive Guidance 术语表中的 Migration terms - 7 Rs。

4. 要查看应用程序组件的详细信息，请选择一个应用程序组件，然后选择查看详细信息。
5. 在应用程序组件详细信息页面（以组件名称为标题的页面）的建议摘要下面，您可以查看适用于应用程序组件的建议。您还可以查看已识别的反模式。反模式是在您的产品组合中发现的一系列已知问题，这些问题按严重性分类。
6. 选择策略选项选项卡，查看针对应用程序组件的迁移建议。您可以选择其他策略，然后选择设为首选，从而覆盖推荐的策略。
7. 根据您正在查看的应用程序组件的类型，有源配置或数据库配置选项卡。有关源配置的信息，请参阅为应用程序组件配置源代码分析。有关数据库配置的信息，请参阅为应用程序组件配置数据库分析。

为应用程序组件配置源代码分析

本部分介绍如何使用 Migration Hub 控制台中的 Strategy Recommendations 为应用程序组件配置源代码分析。

为应用程序组件配置源代码分析

1. 在 Migration Hub 控制台导航窗格中，选择策略，然后选择建议。
2. 在建议页面上，选择应用程序组件选项卡。
3. 从应用程序组件下面的组件列表中，选择组件类型为 java、dotnetframework 或 IIS 的应用程序组件，然后选择查看详细信息。
4. 在应用程序组件详细信息页面（以组件名称为标题的页面）上，选择源代码配置选项卡。
5. 在源代码配置详细信息下，选择分析源代码。
6. 在分析源代码页面上，提供用于存储应用程序组件源代码的存储库名称、分支名称和项目名称（如果适用）。选择要使用的 GitHub 源代码版本控制类型，然后选择 Analyz e。

   分析完成后，您可以在应用程序组件详细信息页面上查看更新的建议。

有关源代码分析的更多信息，请参阅Strategy Recommendations 源代码分析。

为应用程序组件配置数据库分析

本部分介绍如何使用 Migration Hub 控制台中的 Strategy Recommendations 为应用程序组件配置数据库分析。

为应用程序组件配置数据库分析

1. 在 Migration Hub 控制台导航窗格中，选择策略，然后选择建议。
2. 在建议页面上，选择应用程序组件选项卡。
3. 从应用程序组件下的组件列表中，选择组件类型为 SQLServer 的应用程序组件，然后选择查看详细信息。
4. 在应用程序组件详细信息页面（以组件名称为标题的页面）上，选择数据库配置选项卡。
5. 在数据库配置详细信息下，选择分析数据库详细信息。
6. 从您在 AWS Secrets Manager 中创建的下拉菜单中选择一个用于数据库凭证的密钥名称，然后选择分析。

   分析完成后，您可以在应用程序组件详细信息页面上查看更新的建议。

有关数据库分析和设置密钥名称的更多信息，请参阅Strategy Recommendations 数据库分析。

Strategy Recommendations 源代码分析

Migration Hub Strategy Recommendations 会自动识别您的产品组合中的应用程序，并为其创建应用程序组件。例如，如果您的产品组合中有一个 Java 应用程序，该应用程序会被识别为组件类型为 java 的应用程序组件。

Strategy Recommendations 会分析应用程序组件的源代码（如果您进行了这样的配置）。有关如何为源代码分析配置应用程序组件的信息，请参见为应用程序组件配置源代码分析。

Strategy Recommendations 会对 Java 和 C# 编程语言执行源代码分析。

有关使用 Strategy Recommendations 源代码分析的先决条件的信息，请参阅Strategy Recommendations 的先决条件。

Strategy Recommendations 数据库分析

Strategy Recommendations 会自动识别您的产品组合中的数据库服务器，并为其创建应用程序组件。例如，如果您的产品组合中有一个 SQL Server 数据库，该数据库会被识别为应用程序组件 sqlservr.exe。

策略建议使用 AWS 架构转换工具（Schema Conversion Tool）分析已确定的 SQL Server 应用程序组件 sqlservr.exe 中的各个数据库。策略建议还指出了将数据库迁移到数据库中的不兼容之处，例如兼容亚马逊 Aurora MySQL 的版本、兼容亚马逊 Aurora PostgreSQL 的版本、适用于 MySQL 的亚马逊 RDS 和适用于 PostgreSQL 的亚马逊 RDS AWS 和 PostgreSQL 版的亚马逊 RDS。

目前，Strategy Recommendations 数据库分析仅适用于 SQL Server。

要配置 Strategy Recommendations 以分析您的数据库，您必须提供凭证，以便 Strategy Recommendations 应用程序数据收集器连接到您的数据库。为此，请在 AWS 账户的 Secrets Manager 中创建一个 AWS 密钥。

有关您提供的凭证的权限信息，请参阅AWS Schema Conversion Tool 凭据所需的权限。有关如何使用凭证创建密钥的信息，请参阅 在 Secrets Manager 中为数据库凭证创建密钥。

设置凭据和密钥后，可以在数据库服务器上配置 AWS Schema Conversion Tool 分析。有关更多信息，请参阅 为应用程序组件配置数据库分析。

为应用程序组件配置数据库分析后，将计划一个 AWS Schema Conversion Tool 清单任务。此任务完成后，您将看到系统为该数据库服务器上的每个单独数据库创建新的应用程序组件。例如，如果您的 SQL Server 有两个数据库（exampledbs1 和 exampledbs2），则为每个数据库分别创建名为 exampledbs1 和 exampledbs2 的应用程序组件。

如果您想在将每个已识别的数据库迁移到 AWS 数据库时看到反模式，请按照为应用程序组件配置数据库分析中的步骤为每个数据库设置分析。

AWS Schema Conversion Tool 凭据所需的权限

您向 S AWS ecrets Manager 提供的登录凭据只需要`VIEW SERVER STATE`和`VIEW ANY DEFINITION`权限。您还可以使用 https://gitlab.aws.dev/dmaf-pub/dmaf/-/blob/master/create_mssql_ro_user.sql 上提供的脚本创建新登录。

在创建 SQL Server 登录时，您可以提供所需的任意登录名和密码。

在 Secrets Manager 中为数据库凭证创建密钥

凭据准备就绪，可供策略建议应用程序数据收集器连接到数据库后，按照以下过程所述在 AWS 账户的 Secr AWS ets Manager 中创建一个密钥。

在你的 AWS 账户中使用 Secr AWS ets Manager 创建密钥

1. 使用你在中创建的 AWS 账户设置 Strategy Recommendations，登录 AWS Management Console 并打开 S AWS ecrets Manager 控制台，网址为 https://console.aws.amazon.com/secretsmanager/。
2. 选择 存储新密钥。
3. 选择其他类型的密钥作为密钥类型。
4. 在键值对下面，输入以下信息。

   username - *your-username*

   然后，选择 + 添加行，输入以下信息。

   password - *your-password*
5. 选择下一步。
6. 输入密钥名称，作为带前缀 migrationhub-strategy- 的任意字符串。例如，migrationhub-strategy-one。

   > **Note**
   >
   > 在安全的位置存储您的密钥名称，以备后用。
7. 选择下一步，然后再次选择下一步。
8. 选择 Store (存储)。

在 Strategy Recommendations 中设置数据库分析时，您可以使用您为数据库凭证创建的密钥。

Strategy Recommendations 二进制分析

Migration Hub Strategy Recommendations 会自动识别您的产品组合中的应用程序，以及属于这些应用程序的应用程序组件。例如，如果您的产品组合中有一个 Java 应用程序，Strategy Recommendations 会将其识别为组件类型为 java 的应用程序组件。您无需配置源代码的访问权限，Strategy Recommendations 可以通过检查 Windows 上的 IIS 应用程序 DLL 或 Linux 上的应用

程序 JAR 文件来执行二进制分析，并提供反模式报告或不兼容问题报告。反模式报告是 Strategy Recommendations 在您的产品组合中发现的已知问题列表，按严重性分类。不兼容问题报告包含反模式的子集，即 API 兼容性、Nuget Package 和 Porting Action。

Strategy Recommendations 会对 Windows IIS 和 Java Tomcat 及 Jboss 应用程序执行分析。如果您有 IIS 应用程序，则默认情况下，Strategy Recommendations 会生成不兼容问题报告；您必须配置源代码访问权限，才能接收完整的反模式报告。如果您有 Java 应用程序，则默认情况下，Strategy Recommendations 会生成完整的反模式报告。

不兼容问题或反模式报告会在分析完成后显示。如果分析不成功，您可以尝试通过提供源代码访问权限来运行源代码分析（如设置版本控制配置。中所述）。

Strategy Recommendations 服务器建议

本部分介绍如何使用 Migration Hub 控制台中的 Migration Hub Strategy Recommendations 来查看针对您的迁移产品组合中的服务器的迁移策略建议。

查看服务器建议

1. 使用你在中创建的 AWS 账户设置 Strategy Recommendations，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，选择策略，然后选择建议。
3. 在建议页面上，选择服务器选项卡。

    a. 在服务器摘要下，您可以概览您在产品组合中运行的各种类型的服务器。

    b. 在服务器下，您可以查看服务器和操作系统详细信息以及迁移“R”策略建议。您还可以根据建议查看迁移目的地，以及服务器上识别的反模式数量。有关“R”策略的信息，请参见 AWS Prescriptive Guidance 术语表中的 Migration terms - 7 Rs。
4. 要查看某个服务器的深入建议详细信息，请从列表中选择该服务器，然后选择查看详细信息。您可以查看为服务器收集的元数据，以及针对服务器的深入分析和建议，这些都基于服务器上运行的应用程序组件。
5. 在服务器详细信息页面（以服务器名称为标题的页面）上，在建议摘要下，您可以概览针对服务器的策略建议。您还可以查看已识别的反模式。反模式是在您的产品组合中发现的一系列已知问题，这些问题按严重性分类。
6. 选择策略选项选项卡，查看针对服务器的迁移建议。您可以选择其他策略，然后选择设为首选，从而覆盖推荐的策略。
7. 选择应用程序组件选项卡，查看与服务器关联的应用程序组件列表。

8. 要查看应用程序组件的详细信息，请从列表中选择组件，然后选择查看详细信息。有关应用程序组件的更多信息，请参阅使用应用程序组件。

Strategy Recommendations 首选项

本部分介绍如何在 Migration Hub 控制台中查看和编辑 Migration Hub Strategy Recommendations 首选项。

在首次设置 Strategy Recommendations 时，您可以选择建议首选项（如步骤 5：获得建议中所述）。您可以编辑这些首选项。

编辑建议首选项

1. 使用你在中创建的 AWS 账户设置 Strategy Recommendations，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，选择策略，然后选择建议。
3. 在建议页面上，选择首选项选项卡。
4. 在优先业务目标下，您可以拖放业务目标，以重新排列这些目标。
5. 选择您所需的应用程序首选项和数据库首选项，然后选择保存更改。

如果您更改首选项，系统会显示横幅，提醒您选择重新分析数据。

Strategy Recommendations 数据来源

本部分介绍 Strategy Recommendations 使用的数据来源。

主题

查看 Strategy Recommendations 数据来源

本节介绍如何在中查看策略建议数据源 AWS Management Console。

查看数据来源

1. 使用你在中创建的 AWS 账户设置 Strategy Recommendations，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，选择策略，然后选择数据来源。
3. 在收集器选项卡上，您可以查看您设置的 Strategy Recommendations 应用程序数据收集器。有关收集器的更多信息，请参阅Strategy Recommendations 应用程序数据收集器。
4. 在导入选项卡上，您可以导入数据并查看您的数据导入。有关更多信息，请参阅 将数据导入 Strategy Recommendations。
5. 在工具选项卡上，您可以下载收集器和应用程序导入数据模板。

Strategy Recommendations 应用程序数据收集器

本部分介绍如何使用 Strategy Recommendations 应用程序数据收集器。

有关下载和设置应用程序数据收集器的信息，请参阅步骤 1：下载 Strategy Recommendations 收集器。

主题

Strategy Recommendations 收集器收集的数据

本部分介绍 Migration Hub Strategy Recommendations 应用程序数据收集器收集的数据类型。应用程序数据收集器是一种无代理数据收集器，用于识别服务器上正在运行的应用程序、执行源代码分析并分析您的数据库。

数据字段	描述
操作系统类型	Windows 或 Linux
操作系统版本	操作系统的特定版本。例如，Windows Server 2003、RHEL 5.2。
操作系统架构	32 位或 64 位操作系统
是否是服务器虚拟机	服务器是虚拟机或物理机。
虚拟化软件	例如，vCenter、Hyper-V。
位置	例如，Amazon Elastic Compute Cloud 控制台（Amazon EC2）或本地。
是否是双启动	允许启动进入多个操作系统
固件类型	BIOS、UEFI
启动加载程序	GRUB、GRUB 2
分区表类型	MBR、GPT
CPU 速度	CPU 速度以 GHz 为单位。例如，2.4 GHz。
Windows OS data	
Windows 版本	标准版、数据中心版、企业版
.NET 框架版本	安装的 .NET 框架的版本。
.NET Core 版本	安装的 .NET Core 的版本。
Linux data	

数据字段	描述
Linux 操作系统发行版	RHEL、CentOS、SUSE 等。
内核版本	uname -r 输出，例如 `4.9.217-0.1.ac.205.84.332.metal1.x86_64`
For each disk volume	
文件系统类型	FAT32、NTFS、ReFS、ext4、jfs 等。
磁盘卷大小	磁盘大小总计
磁盘卷可用空间	可用磁盘空间
虚拟磁盘映像格式	vmdk、vhd、vhdx
磁盘类型（Windows）	基本、动态
Application level data	
应用程序名称	正在运行的进程的名称。例如，SQLServr.exe、MSdtsservr.exe 等。
应用程序类型	IIS、JBoss、Tomcat 等。
编程语言和版本	C#、Java
JDK 版本	安装的 JDK 的版本。
源代码是否可用	如果您提供源代码存储库，则表示源代码可用。
应用程序位大小	16 位、32 位、64 位
Windows	
应用程序使用的 .NET 框架版本	在运行时为应用程序加载的 .NET 框架 DLL 的版本。
.NET Core 版本	在运行时为应用程序加载的 .NET Core DLL 的版本。

数据字段	描述
使用 WPF 框架？	确定基于 .NET 的应用程序是否是一种 WPF 应用程序。
使用 WCF 框架？	确定基于 .NET 的应用程序是否是一种 WCF 应用程序。
ASP.NET 版本	ASP.NET 的版本。
IIS 版本	Windows 计算机上安装的 IIS 服务器的版本。
应用程序操作系统驱动程序位大小	32 位、64 位
Windows 注册表使用情况	查询计算机的注册表项，查找数据库版本、Java 版本、.NET 版本等信息。
应用程序使用的所有 DLL	获取 Windows 进程在运行时加载的所有 DLL 的列表。
PowerShell 版本	检查计算机上安装的 PowerShell 版本，该版本应为 5.1 或更高版本。
Linux	
应用程序框架类型	Tomcat、Spring Boot、jBoss、 WebLogic WebSphere
应用程序框架版本	应用程序框架的版本。
Database	
数据库类型	MS SQL、Oracle、MySQL 等。
数据库版本	数据库的版本。

从 Strategy Recommendations 中删除您的数据

要从 Strategy Recommendations 中删除您的所有数据，请联系 AWS Support 并请求删除全部数据。

升级 Strategy Recommendations 收集器

Migration Hub Strategy Recommendations 应用程序数据收集器会自动升级。如果需要，您可以按照以下步骤手动升级收集器。

升级 Strategy Recommendations 收集器

1. 使用以下命令通过 SSH 客户端连接到收集器虚拟机。

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

2. 更改为收集器虚拟机中的升级目录，如以下示例所示。

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

3. 使用以下命令运行升级脚本。

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

将数据导入 Strategy Recommendations

作为应用程序数据收集器的替代方法，您可以导入关于迁移与现代化建议针对的应用程序和服务器的信息。

当您导入数据时，建议不像您使用数据收集器时那样深入。例如，您不能对导入的数据使用源代码分析。

本部分介绍如何使用应用程序导入模板将数据导入 Migration Hub 控制台中的 Strategy Recommendations。

导入数据

1. 使用你在中创建的 AWS 账户设置 Strategy Recommendations，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，选择策略，然后选择数据来源。
3. 选择导入选项卡。
4. 选择下载导入模板，下载应用程序导入模板。
5. 填写模板并将其上传到 Amazon S3 桶。确保桶的名称以前缀 `migrationhub-strategy` 开头。

6. 返回到导入选项卡，然后选择导入。
7. 输入导入的名称，输入已填写的数据模板的 Amazon S3 对象 URI，然后选择开始导入。

Strategy Recommendations 导入模板

您下载的导入模板是一个 .json 文件，如以下示例所示。

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

为帮助您填写导入模板，下表列出了数据字段的有效值。

下表列出了服务器的必填字段。

名称	描述	类型	必需	有效值
ResourceId	资源的唯一 ID	String	是	任何唯一字符串
ResourceName	资源的名称	String	是	任何字符串
ResourceType	要导入的资源的类型	String	是	"Server", "Process"
OSDistribution	Windows、Windows Server、Ubuntu	String	是	Windows："Windows PC" , "Windows Server" Linux："Ubuntu", "RHEL", "Amazon Linux", "DEBIAN", "SLES", "CENT_OS" , "ORACLE_LINUX", "FEDORA", "KALI"
OSType	操作系统的类型	String	是	"Windows", "Linux"
OSVersion	内核版本	String	是	请参阅 HTML 版本的文档。
CPUArchitecture	CPU 架构	String	否	"32bit", "64bit"
IpAddress	服务器的 IP 地址	数组	否	格式为 xxx.xxx.xxx.xxx
MacAddresses	与服务器关联的 Mac 地址	数组	否	格式为 xx:xx:xx:xx:xx:xx
Hostname	主机的名称	String	否	任何字符串

下表列出了进程的必填字段。

名称	描述	类型	必需	有效值
ResourceId	资源的唯一 ID	String	是	任何唯一字符串
ResourceName	资源的名称	String	是	任何字符串
ResourceType	要导入的资源的类型	String	是	"Server", "Process"
AssociatedServer身份证	正在运行该进程的服务器 ID 的列表。	String	是	ResourceId 来自您定义ResourceType的 “”: “服务器”。
ApplicationType	应用程序的类型	String	是	“Tomcat”、“JBoss”、“Spring”、“IIS”、“Mongo DB”、“DB2”、“MariaDB”、“MySQL”、“Oracle”、“SqlServer”、“PostgreSqlServer”、“Cassandra”、“IBM”、“Oracle”、“Java Generic” WebSphere WebLogic
ApplicationVersion	应用程序的版本	String	是	"IIS 1.0", "IIS 2.0", "IIS 3.0", "IIS 4.0", "IIS 5.0", "IIS 5.1", "IIS 6.0", "IIS 7.0", "IIS 7.5", "IIS 8.0", "IIS 8.5", "IIS 10.0"
ProgrammingLanguage	应用程序的编程语言	String	否	"Java", "CSharp"
DotNetFrameworkVersion	.NET 框架的版本（如果应用程序基于 .NET 框架）	String	否	“DotnetFramework 1.0”、“1.DotnetFramework 0 SP1”、“1.0 SP2”、“1.0 SP3”、“DotnetFramework 1.1 SP1”、“DotnetFramework 1.1

名称	描述	类型	必需	有效值
				SP1”、“2. DotnetFramework 0 SP1”、“DotnetFramework2.0 SP1” DotnetFramework 、“3. DotnetFramework 0 SP1”、“3.0 SP1”、“3.0 SP2”、“DotnetFramework 3.5 SP1”、“4. DotnetFramework 0”、“4.5.1”、“4.5.1”、“4. DotnetFramework 5.2”、“DotnetFramework 4.6”、“4.6”、“DotnetFramework4.6”、“4.6”、“4.6”、“DotnetFramework 4.6”、“4.6” 6.1 DotnetFramework 英寸、“DotnetFramework 4.6.2”、“4.7”、“DotnetFramework 4.7.1”、“4.7.2”、“4.8” DotnetFramework DotnetFramework DotnetFramework DotnetFramework DotnetFramework DotnetFramework DotnetFramework DotnetFramework
DotNetCoreVersion	.NET Core 的版本（如果应用程序基于 .NET Core）	String	否	".NET Core 1.0", ".NET Core 1.1", ".NET Core 2.0", ".NET Core 2.1", ".NET Core 2.2", ".NET Core 3.0", ".NET Core 3.1"
JdkVersion	JDK 的版本（如果应用程序使用 JDK）	String	否	"JDK1.0", "JDK2.0", "JDK3.0", …, "JDK11.0"

名称	描述	类型	必需	有效值
DatabaseType	数据库的类型	String	否	"SQLServer", "Oracle", "Sybase", "Mongo DB", "Maria DB", "Apache Cassandra", "MySQL", "IBM DB2", "PostgreSQLServer"
DatabaseEdition	数据库的版本	String	否	
DatabaseVersion	数据库的版本	String	否	请参阅 HTML 版本的文档。

从 Strategy Recommendations 中删除您的数据

要从 Migration Hub Strategy Recommendations 中删除您的所有数据，请联系 AWS Support。

Migration Hub Strategy Recommendations 的安全性

AWS 十分重视云安全性。为了满足对安全性最敏感的组织的需求，我们打造了具有超高安全性的数据中心和网络架构。作为 AWS 的客户，您也可以从这些数据中心和网络架构受益。

安全性是 AWS 和您的共同责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云的安全性 – AWS 负责保护在 AWS Cloud 中运行 AWS 服务的基础设施。AWS 还向您提供可安全使用的服务。第三方审核员定期测试和验证我们的安全性的有效性，作为 AWS Compliance Programs 的一部分。要了解适用于 Migration Hub Strategy Recommendations 的合规性计划，请参阅按合规性计划提供的范围内 AWS 服务。
- 云中的安全性——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，包括数据的敏感性、公司的要求以及适用的法律法规。

此文档将帮助您了解如何在使用 Strategy Recommendations 时应用责任共担模型。以下主题说明如何配置 Strategy Recommendations 以实现您的安全性和合规性目标。您还会了解如何使用其他 AWS 服务以帮助您监控和保护 Strategy Recommendations 资源。

主题

Migration Hub Strategy Recommendations 中的数据保护

AWS 责任共担模式适用于 Migration Hub Strategy Recommendations 中的数据保护。如该模式中所述，AWS 负责保护运行所有 AWS Cloud 的全球基础设施。您负责维护对托管在此基础设施上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS 安全性博客 上的博客文章 AWS Shared Responsibility Model and GDPR。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置单个用户。这样，每个用户只获得履行其工作职责所需的权限。我们还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证 (MFA)。

- 使用 SSL/TLS 与 AWS 资源进行通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用 AWS CloudTrail 设置 API 和用户活动日志记录。
- 使用 AWS 加密解决方案以及 AWS 服务 中的所有默认安全控制。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在通过命令行界面或 API 访问 AWS 时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准 (FIPS) 第 140-2 版》。

我们强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括您使用控制台、API、AWS CLI 或 AWS SDK 处理 Strategy Recommendations 或其他 AWS 服务 时。在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，我们强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

静态加密

Strategy Recommendations 数据库中存储的所有数据都经过加密。

传输中加密

Strategy Recommendations 互联网络通信支持所有组件和客户端之间的 TLS 1.2 加密。

Migration Hub Strategy Recommendations 的身份和访问管理

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 管理员控制谁可以通过身份验证（登录）和授权（拥有权限）使用 Strategy Recommendations 资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

- Migration Hub Strategy Recommendations 如何与 IAM 配合使用
- AWS Migration Hub 策略建议的托管策略
- 针对 Migration Hub Strategy Recommendations 的基于身份的策略示例
- 对 Migration Hub Strategy Recommendations 身份和访问进行故障排除
- 使用 Strategy Recommendations 的服务相关角色
- Migration Hub Strategy Recommendations 和接口 VPC 端点（AWS PrivateLink）

受众

您的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于您在策略建议中所做的工作。

服务用户 – 如果您使用 Strategy Recommendations 服务来完成工作，则您的管理员会为您提供所需的凭证和权限。当您使用更多 Strategy Recommendations 功能来完成工作时，您可能需要额外权限。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 Strategy Recommendations 中的功能，请参阅对 Migration Hub Strategy Recommendations 身份和访问进行故障排除。

服务管理员 – 如果您在公司负责管理 Strategy Recommendations 资源，您可能拥有对 Strategy Recommendations 的完全访问权限。您有责任确定您的服务用户应访问哪些 Strategy Recommendations 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。要了解有关您的公司如何将 IAM 与 Strategy Recommendations 结合使用的更多信息，请参阅Migration Hub Strategy Recommendations 如何与 IAM 配合使用。

IAM 管理员 – 如果您是 IAM 管理员，您可能希望详细了解如何编写策略来管理对 Strategy Recommendations 的访问。要查看可在 IAM 中使用的 Strategy Recommendations 基于身份的策略示例，请参阅针对 Migration Hub Strategy Recommendations 的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，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 用户指南中的签署 AWS API 请求。

无论使用何种身份验证方法，您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》中的在 AWS中使用多重身份验证（MFA）。

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。有关要求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。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 AWS 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity C enter 目录中的用户，或者任何使用 AWS 服务 通过身份源提供的凭据进行访问的用户。 AWS Directory Service当联合身份访问时 AWS 账户，他们将扮演角色，角色提供临时证书。

要集中管理访问权限，我们建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和群组，也可以连接并同步到您自己的身份源中的一组用户和群组，以便在您的所有 AWS 账户 和应用程序中使用。有关 IAM Identity Center 的信息，请参阅《AWS IAM Identity Center 用户指南》中的什么是 IAM Identity Center？

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，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，如果有一些特定的使用场景需要长期凭证以及 IAM 用户，我们建议轮换访问密钥。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使用场景定期轮换访问密钥。

IAM 组是一个用于指定一组 IAM 用户的身份。您不能使用群组的身份登录。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，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

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担任。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》中的何时创建 IAM 用户（而不是角色）。

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。您可以 AWS Management Console 通过切换角色在中临时担任 IAM 角色。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》中的使用 IAM 角色。

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。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的为第三方身份提供商创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为控制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 用户或角色可代入 IAM 角色，以暂时获得针对特定任务的不同权限。
- 跨账户访问——您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问账户中的资源。角色是授予跨账户存取权限的主要方式。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 角色与基于资源的策略有何不同。
- 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，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 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，此操作然后在不同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个操作的权限。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 服务服务可以担任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 EC2 上运行的应用程序 — 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。这优先于在 EC2 实例中存储访问密钥。要向 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建附加到该实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用 IAM 角色还是 IAM 用户，请参阅《IAM 用户指南》中的何时创建 IAM 角色（而不是用户）。

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 策略概述。

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 policy。然后，管理员可以向角色添加 IAM policy，并且用户可以代入角色。

IAM policy 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、用户群组或角色）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 创建 IAM policy。

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、群组或角色中。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。要了解如何在托管式策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管式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 (ACL)

访问控制列表(ACL) 控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 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 ACL 的服务示例。 AWS WAF要了解有关 ACL 的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》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。您可以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 (SCP)-SCP 是 JSON 策略，用于指定组织或组织单位 (OU) 的最大权限。 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。如果您在组织内启用了特征，则可对任意或全部账户应用服务控制策略 (SCP)。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。有关组织和 SCP 的更多信息，请参阅《AWS Organizations 用户指南》中的 SCP 的工作原理。
- 会话策略——会话策略是当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。

Migration Hub Strategy Recommendations 如何与 IAM 配合使用

在使用 IAM 管理对 Strategy Recommendations 的访问之前，了解哪些 IAM 功能可用于 Strategy Recommendations。

您可以与 Migration Hub Strategy Recommendations 结合使用的 IAM 功能

IAM 功能	Strategy Recommendations 支持
基于身份的策略	是
基于资源的策略	否
策略操作	是
策略资源	不支持
策略条件密钥	否
ACL	否
ABAC（策略中的标签）	不支持
临时凭证	是
主体权限	支持
服务角色	否
服务相关角色	支持

要全面了解策略建议和其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中的与 IAM 配合使用的AWS 服务。

针对 Strategy Recommendations 的基于身份的策略

支持基于身份的策略	是

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》中的创建 IAM 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。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

针对 Strategy Recommendations 的基于身份的策略示例

要查看 Strategy Recommendations 基于身份的策略示例，请参阅针对 Migration Hub Strategy Recommendations 的基于身份的策略示例。

Strategy Recommendations 内基于资源的策略

支持基于资源的策略	否

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。

要启用跨账户存取，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同位置时 AWS 账户，可信账户中的 IAM 管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅IAM 用户指南中的 IAM 角色与基于资源的策略有何不同。

针对 Strategy Recommendations 的策略操作

支持策略操作	支持

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。

要查看 Strategy Recommendations 操作列表，请参阅 Service Authorization Reference 中的 Actions Defined by Migration Hub Strategy Recommendations。

Strategy Recommendations 的策略操作在操作前使用以下前缀：

```
migrationhub-strategy
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

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

要查看 Strategy Recommendations 基于身份的策略示例，请参阅针对 Migration Hub Strategy Recommendations 的基于身份的策略示例。

Strategy Recommendations 的策略资源

支持策略资源	不支持

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。

Resource JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。作为最佳实践，请使用其 Amazon 资源名称 (ARN)指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*"
```

要查看 Strategy Recommendations 的资源类型及其 ARN 的列表，请参阅 Service Authorization Reference 中的 Resources Defined by Migration Hub Strategy Recommendations。要了解您可以在哪些操作中指定每个资源的 ARN，请参阅 Actions Defined by Migration Hub Strategy Recommendations。

要查看 Strategy Recommendations 基于身份的策略示例，请参阅针对 Migration Hub Strategy Recommendations 的基于身份的策略示例。

Strategy Recommendations 的策略条件键

支持特定于服务的策略条件密钥	不支持

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。

在 Condition 元素（或 Condition 块）中，您可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个密钥，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

您也可以在指定条件时使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM 策略元素：变量和标签。

AWS 支持全局条件密钥和特定于服务的条件密钥。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。

要查看 Strategy Recommendations 条件键列表，请参阅 Service Authorization Reference 中的 Condition Keys for Migration Hub Strategy Recommendations。要了解您可以对哪些操作和资源使用条件键，请参阅 Actions Defined by Migration Hub Strategy Recommendations。

要查看 Strategy Recommendations 基于身份的策略示例，请参阅针对 Migration Hub Strategy Recommendations 的基于身份的策略示例。

Strategy Recommendations 中的访问控制列表（ACL）

支持 ACL	否

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

支持 Strategy Recommendations 的基于属性的访问权限控制（ABAC）

支持 ABAC（策略中的标签）	不支持

基于属性的访问权限控制 (ABAC) 是一种授权策略，该策略基于属性来定义权限。在中 AWS，这些属性称为标签。您可以将标签附加到 IAM 实体（用户或角色）和许多 AWS 资源。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件密钥在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件密钥，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件密钥，则该值为部分。

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的什么是 ABAC？。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

对 Strategy Recommendations 使用临时凭证

支持临时凭证	支持

当你使用临时证书登录时，有些 AWS 服务 不起作用。有关更多信息，包括哪些 AWS 服务 适用于临时证书，请参阅 IAM 用户指南中的AWS 服务 与 IAM 配合使用的信息。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的切换到角色（控制台）。

您可以使用 AWS CLI 或 AWS API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 AWS。 AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

Strategy Recommendations 的跨服务主体权限

支持转发访问会话 (FAS)	支持

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，此操作然后在不同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个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

Strategy Recommendations 的服务角色

支持服务角色	否

服务角色是由一项服务代入、代表您执行操作的 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。

> **Warning**
>
> 更改服务角色的权限可能会破坏 Strategy Recommendations 的功能。仅当 Strategy Recommendations 提供相关指导时才编辑服务角色。

Strategy Recommendations 的服务相关角色

支持服务相关角色	支持

服务相关角色是一种与服务相关联的 AWS 服务服务角色。服务可以担任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。

有关创建或管理 Strategy Recommendations 服务相关角色的详细信息，请参阅使用 Strategy Recommendations 的服务相关角色。

AWS Migration Hub 策略建议的托管策略

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 托管策略添加其他权限以支持新功能。此类更新会影响附加策略的所有身份（用户、组和角色）。当推出新功能或有新操作可用时，服务最有可能更新 AWS 托管策略。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： AWSMigrationHubStrategyConsoleFullAccess

您可以将 `AWSMigrationHubStrategyConsoleFullAccess` 策略附加到 IAM 身份。

`AWSMigrationHubStrategyConsoleFullAccess` 策略授予用户通过 AWS Management Console 访问 Strategy Recommendations 服务的完全访问权限。

权限详细信息

该策略包含以下权限。

- discovery – 授予用户在 Application Discovery Service 中获取发现摘要的权限。
- iam – 允许为用户创建服务相关角色，这是使用 Strategy Recommendations 的必要条件。
- migrationhub-strategy – 授予用户对 Strategy Recommendations 的完全访问权限。
- s3 – 允许用户创建 Strategy Recommendations 使用的 S3 桶并从中读取数据。
- secretsmanager – 允许用户在 Secrets Manager 中列出密钥访问权限。

要查看此策略的权限，请参阅AWSMigrationHubStrategyConsoleFullAccess《AWS 托管策略参考指南》。

AWS 托管策略： AWSMigrationHubStrategyCollector

您可以将 AWSMigrationHubStrategyCollector 策略附加到 IAM 身份。

权限详细信息

该策略包含以下权限。

- application-transformation— 授予上传用于应用程序转换操作的日志和指标数据的权限，以及使用移植兼容性评估和建议。
- execute-api – 允许用户访问 Amazon API Gateway，将日志和指标上传到 AWS。
- migrationhub-strategy— 授予用户注册消息、发送消息、上传日志数据以及将指标数据上传到策略建议的权限。
- s3— 授予用户列出存储桶及其位置的权限。用户还被授予写入、检索对象、向其中添加对象、返回访问控制列表 (ACL)、创建、访问、配置加密、修改PublicAccessBlock配置、设置版本控制状态以及创建或替换策略建议使用的 S3 存储桶的生命周期配置的权限。
- secretsmanager – 允许用户访问 Secrets Manager 中由 Strategy Recommendations 使用的密钥。

要查看此策略的权限，请参阅AWSMigrationHubStrategyCollector《AWS 托管策略参考指南》。

AWS 托管策略的策略建议更新

查看自该服务开始跟踪策略建议的 AWS 托管策略变更以来这些更新的详细信息。有关此页面更改的自动提示，请订阅 Strategy Recommendations 文档历史记录页面上的 RSS 源。

更改	描述	日期
AWSMigrationHubStrategyCollector – 对现有策略的更新	此策略已更新，包括 PutLogData 、StartPortingCompatibilityAssessment GetPortingCompatibilityAssessment 、StartPortingRecommendationAssessment 和GetPortingRecommendationAssessment 应用程序转换操作，以允许应用程序转换服务向该服务发送日志和指标。ListBucket 和GetBucketLocation 是为亚马逊简单存储服务 (Amazon S3) Simple Storage Service 添加的，以支持日志和指标上传。添加PutLogData 和PutMetricData 也是为了允许 “策略建议” 收集器向服务的端点发送日志和指标。	2024年4月1日
AWSMigrationHubStrategyCollector – 更新了现有策略	此政策已更新为PutMetricData 和PutLogData 操作。这些操作允许上传应用程序转换操作的日志和指标数据。此更新还增加了条件，确保等aws:ResourceAccoun	2024年2月5日

更改	描述	日期
	t 于使用随附aws:PrincipalAccount 的 Amazon 简单存储服务和 AWS Secrets Manager 操作的权限。	
AWSMigrationHubStrategyCollector – 更新了现有策略	本策略更新了以下 Amazon S3 API – CreateBucket 、PutEncryptionConfiguration 、PutBucketPublicAccessBlock 、PutBucketPolicy 、PutBucketVersioning 和 PutLifecycleConfiguration 。	2023 年 9 月 15 日
AWSMigrationHubStrategyCollector – 更新了现有策略	该政策更新授予源代码分析权限。	2023 年 3 月 8 日
AWSMigrationHubStrategyConsoleFullAccess – 更新了现有策略	此政策已更新为三个 AWS Application Discovery Service API — DescribeConfigurations DescribeTags 、和ListConfigurations 。	2022 年 11 月 10 日
AWSMigrationHubStrategyCollector – 更新了现有策略	此政策已根据UpdateCollectorConfiguration 操作进行了更新。该操作存储您的收集器的配置，便于检索。	2022 年 9 月 7 日

更改	描述	日期
AWSMigrationHubStrategyConsoleFullAccess— 新政策在发布时公布	`AWSMigrationHubStrategyConsoleFullAccess` 授予用户通过 AWS Management Console访问 Strategy Recommendations 服务的完全访问权限。	2021 年 10 月 25 日
AWSMigrationHubStrategyCollector— 新政策在发布时公布	`AWSMigrationHubStrategyCollector` 授予用户对 Strategy Recommendations 的访问权限，以及对服务相关的 S3 桶的读/写访问权限。它还授予 Amazon API Gateway 向其上传日志和指标的权限 AWS，以及 S AWS ecrets Manager 获取凭证的权限。	2021 年 10 月 25 日
AWSMigrationHubStrategyServiceRolePolicy— 新政策在发布时公布	`AWSMigrationHubStrategyServiceRolePolicy` 服务相关角色策略提供对 AWS Migration Hub 和 AWS Application Discovery Service的访问权限。本策略还授予在 Amazon Simple Storage Service（Amazon S3）中存储报告的权限。	2021 年 10 月 25 日
Strategy Recommendations 开始跟踪更改	策略建议已开始跟踪其 AWS 托管策略的变化。	2021 年 10 月 25 日

针对 Migration Hub Strategy Recommendations 的基于身份的策略示例

默认情况下，用户和角色没有创建或修改 Strategy Recommendations 资源的权限。他们也无法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 执行任务。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 policy。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅《IAM 用户指南》中的 创建 IAM 策略。

有关 Strategy Recommendations 定义的操作和资源类型的详细信息，包括每种资源类型的 ARN 格式，请参阅 Service Authorization Reference 中的 Actions, Resources, and Condition Keys for Migration Hub Strategy Recommendations。

主题

- 策略最佳实践
- 使用 Strategy Recommendations 控制台
- 允许用户查看他们自己的权限
- 访问一个 Amazon S3 存储桶

策略最佳实践

基于身份的策略决定某人是否可以在您的账户中创建、访问或删除 Strategy Recommendations 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，请遵循以下准则和建议：

- 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 policy 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 policy 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 AWS 服务的（例如）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 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 IAM policy，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，确保策略符合 IAM policy 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，有助于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 IAM Access Analyzer 策略验证。

- 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。要在调用 API 操作时需要 MFA，请将 MFA 条件添加到策略中。有关更多信息，请参阅《IAM 用户指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html中的配置受 MFA 保护的 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 中的安全最佳实操。

使用 Strategy Recommendations 控制台

要访问 Migration Hub Strategy Recommendations 控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您的 “策略建议” 资源的详细信息 AWS 账户。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

为确保用户和角色仍然可以使用策略建议控制台，还要将策略建议`ConsoleAccess`或`ReadOnly` AWS 托管策略附加到实体。有关更多信息，请参阅《IAM 用户指南》中的为用户添加权限。

允许用户查看他们自己的权限

该示例说明了如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
```

```
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

访问一个 Amazon S3 存储桶

在本示例中，您想向您的 IAM 用户授予 AWS 账户 访问您的 Amazon S3 存储桶的权限。examplebucket您还想要允许该用户添加、更新和删除对象。

除了授予该用户 s3:PutObject、s3:GetObject 和 s3:DeleteObject 权限外，此策略还授予 s3:ListAllMyBuckets、s3:GetBucketLocation 和 s3:ListBucket 权限。这些是控制台所需的其他权限。此外，s3:PutObjectAcl 和 s3:GetObjectAcl 操作需要能够在控制台中复制、剪切和粘贴对象。有关向用户授予权限并使用控制台测试这些权限的演练示例，请参阅 An example walkthrough: Using user policies to control access to your bucket。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"ListBucketsInConsole",
         "Effect":"Allow",
         "Action":[
            "s3:ListAllMyBuckets"
         ],
         "Resource":"arn:aws:s3:::*"
      },
      {
         "Sid":"ViewSpecificBucketInfo",
         "Effect":"Allow",
         "Action":[
```

```
            "s3:ListBucket",
            "s3:GetBucketLocation"
         ],
         "Resource":"arn:aws:s3:::examplebucket"
      },
      {
         "Sid":"ManageBucketContents",
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:GetObject",
            "s3:GetObjectAcl",
            "s3:DeleteObject"
         ],
         "Resource":"arn:aws:s3:::examplebucket/*"
      }
   ]
}
```

对 Migration Hub Strategy Recommendations 身份和访问进行故障排除

以下信息可帮助您诊断和修复在使用 Strategy Recommendations 和 IAM 时可能遇到的常见问题。

主题

- 我没有在 Strategy Recommendations 中执行操作的权限
- 我无权执行 iam：PassRole
- 我想要查看我的访问密钥
- 我是管理员并希望允许其他人访问 Strategy Recommendations
- 我想允许我以外的人 AWS 账户 访问我的策略建议资源

我没有在 Strategy Recommendations 中执行操作的权限

如果 AWS Management Console 告诉您您无权执行某项操作，则必须联系管理员寻求帮助。管理员是指提供用户名和密码的人员。

当 `mateojackson` IAM 用户尝试使用控制台查看有关虚构 *`my-example-widget`* 资源的详细信息，但不拥有虚构 `migrationhub-strategy:`*`GetWidget`* 权限时，会发生以下示例错误。

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

在这种情况下，Mateo 请求他的管理员更新其策略，以允许他使用 `migrationhub-strategy:GetWidget` 操作访问 *my-example-widget* 资源。

我无权执行 iam：PassRole

如果您收到一个错误，表明您无权执行 `iam:PassRole` 操作，则必须更新策略以允许您将角色传递给 Strategy Recommendations。

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 `marymajor` 的 IAM 用户尝试使用控制台在 Strategy Recommendations 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。

我想要查看我的访问密钥

在创建 IAM 用户访问密钥后，您可以随时查看您的访问密钥 ID。但是，您无法再查看您的秘密访问密钥。如果您丢失了私有密钥，则必须创建一个新的访问密钥对。

访问密钥包含两部分：访问密钥 ID（例如 `AKIAIOSFODNN7EXAMPLE`）和秘密访问密钥（例如 `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`）。与用户名和密码一样，您必须同时使用访问密钥 ID 和秘密访问密钥对请求执行身份验证。像对用户名和密码一样，安全地管理访问密钥。

> **Important**
>
> 请不要向第三方提供访问密钥，即便是为了帮助找到您的规范用户 ID 也不行。通过这样做，您可以授予他人永久访问您的权限 AWS 账户。

当您创建访问密钥对时，系统会提示您将访问密钥 ID 和秘密访问密钥保存在一个安全位置。秘密访问密钥仅在您创建它时可用。如果丢失了您的秘密访问密钥，您必须为 IAM 用户添加新的访问密钥。您最多可拥有两个访问密钥。如果您已有两个密钥，则必须删除一个密钥对，然后再创建新的密钥。要查看说明，请参阅 IAM 用户指南中的管理访问密钥。

我是管理员并希望允许其他人访问 Strategy Recommendations

要允许其他人访问 Strategy Recommendations，您必须为需要访问权限的人员或应用程序创建一个 IAM 实体（用户或角色）。它们将使用该实体的凭证访问 AWS。然后，您必须将策略附加到实体，以便在 Strategy Recommendations 中向其授予正确的权限。

要立即开始使用，请参阅《IAM 用户指南》中的创建您的第一个 IAM 委派用户和组。

我想允许我以外的人 AWS 账户 访问我的策略建议资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表（ACL）的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解 Strategy Recommendations 是否支持这些功能，请参阅Migration Hub Strategy Recommendations 如何与 IAM 配合使用。
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（身份联合验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。

使用 Strategy Recommendations 的服务相关角色

Migration Hub 策略建议使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种独特类型的 IAM 角色，它与 Strategy Recommendations 直接相关。服务相关角色由 Strategy Recomments 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。

服务相关角色可让您更轻松地设置 Strategy Recommendations，因为您不必手动添加必要的权限。Strategy Recommendations 定义其服务相关角色的权限，除非另外定义，否则只有 Strategy Recommendations 可以担任该角色。定义的权限包括信任策略和权限策略，而且权限策略不能附加到任何其它 IAM 实体。

有关支持服务相关角色的其他服务的信息，请参阅与 IAM 结合使用的AWS 服务，并查找服务相关角色列中显示为是的服务。选择是，可转到查看该服务的服务相关角色文档的链接。

Strategy Recommendations 的服务相关角色权限

策略建议使用名为AWSServiceRoleForMigrationHubStrategy的服务相关角色并将其与AWSMigrationHubStrategyServiceRolePolicyIAM 策略关联——提供对 AWS Migration Hub 和 AWS Application Discovery Service的访问权限。本策略还授予在 Amazon Simple Storage Service（Amazon S3）中存储报告的权限。

AWSServiceRoleForMigrationHubStrategy 服务相关角色信任以下服务代入该角色：

- `migrationhub-strategy.amazonaws.com`

角色权限策略允许 Strategy Recommendations 完成以下操作。

AWS Application Discovery Service 行动

```
discovery:ListConfigurations

discovery:DescribeConfigurations
```

AWS Migration Hub 行动

```
mgh:GetHomeRegion
```

Amazon S3 操作

```
s3:GetBucketAcl

s3:GetBucketLocation

s3:GetObject

s3:ListAllMyBuckets

s3:ListBucket

s3:PutObject
```

```
s3:PutObjectAcl
```

要查看此策略的权限，请参阅AWSMigrationHubStrategyServiceRolePolicy《AWS 托管策略参考指南》。

要查看此策略的更新历史记录，请参阅AWS 托管策略的策略建议更新。

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 Strategy Recommendations 创建服务相关角色

您无需手动创建服务相关角色。当您同意允许 Migration Hub 在您的账户中创建服务相关角色 (SLR) 时 AWS Management Console，策略建议将为您创建服务相关角色。

如果您删除该服务相关角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。当您同意允许 Migration Hub 在您的账户中创建服务相关角色（SLR）时，Strategy Recommendations 将再次为您创建服务相关角色。

为 Strategy Recommendations 编辑服务相关角色

策略建议不允许您编辑AWSServiceRoleForMigrationHubStrategy服务相关角色。创建服务相关角色后，将无法更改角色名称，因为可能有多个实体引用该角色。但是，您可以使用 Strategy Recommendations 控制台、CLI 或 API 编辑角色的描述。

为 Strategy Recommendations 删除服务相关角色

使用 IAM 手动删除服务相关角色

使用 IAM 控制台 AWS CLI、或 AWS API 删除 AWSServiceRoleForMigrationHubStrategy服务相关角色。有关更多信息，请参见《IAM 用户指南》中的删除服务相关角色。

删除 AWSServiceRoleForMigrationHubStrategySLR 使用的策略建议资源时，您不能有任何正在运行的评估（生成建议的任务）。您也无法运行任何背景评测。如果评测正在运行，则 IAM 控制台中的 SLR 删除会失败。如果 SLR 删除失败，您可以在所有后台任务完成后重新尝试删除。在删除 SLR 之前，您无需清理任何已创建的资源。

Strategy Recommendations 服务相关角色的支持区域

Strategy Recommendations 支持在服务可用的所有区域中使用服务相关角色。有关更多信息，请参阅 AWS 区域和端点。

Migration Hub Strategy Recommendations 和接口 VPC 端点（AWS PrivateLink）

您可以创建接口 VPC 端点，从而在 VPC 和 Migration Hub Strategy Recommendations 之间创建私有连接。接口终端节点由 提供支持AWS PrivateLink 借助 AWS PrivateLink，您可以私下访问 Strategy Recommendations API 操作，而无需互联网网关、NAT 设备、VPN 连接或 AWS Direct Connect 连接。VPC 中的实例无需公有 IP 地址即可与 Strategy Recommendations API 操作进行通信。您的 VPC 与 Strategy Recommendations 之间的流量保留在 Amazon 网络内。

每个接口端点均由子网中的一个或多个弹性网络接口表示。

有关更多信息，请参阅 Amazon VPC 用户指南 中的接口 VPC 端点 (AWS PrivateLink)。

Strategy Recommendations VPC 端点的注意事项

请务必先查看《Amazon VPC 用户指南》中的接口端点属性和限制和 AWS PrivateLink 配额，然后再为 Strategy Recommendations 设置接口 VPC 端点。

Strategy Recommendations 支持从 VPC 调用它的所有 API 操作。要使用所有 Strategy Recommendations，您必须创建 VPC 端点。

为 Strategy Recommendations 创建接口 VPC 端点

您可以使用 Amazon VPC 控制台或 AWS Command Line Interface（AWS CLI）为 Strategy Recommendations 创建 VPC 端点。有关更多信息，请参阅 Amazon VPC 用户指南中的创建接口端点

使用以下服务名称为 Strategy Recommendations 创建 VPC 端点：

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

如果为端点使用私有 DNS，您可以使用区域的默认 DNS 名称，向 Strategy Recommendations 发送 API 请求。例如，您可以使用名称 `migrationhub-strategy.us-east-1.amazonaws.com`。

有关更多信息，请参阅 Amazon VPC 用户指南中的通过接口端点访问服务。

为 Strategy Recommendations 创建 VPC 端点策略

您可以为 VPC 端点附加端点策略，控制对 Strategy Recommendations 的访问。该策略指定以下信息：

- 可执行操作的委托人。
- 可执行的操作。
- 可对其执行这些操作的资源。

有关更多信息，请参阅 Amazon VPC 用户指南中的使用 VPC 端点控制对服务的访问。

示例：针对 Strategy Recommendations 操作的 VPC 端点策略

下面是针对 Strategy Recommendations 的端点策略示例。当附加到端点时，此策略会向所有资源上的所有主体授予对列出的 Strategy Recommendations 操作的访问权限。

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

Migration Hub Strategy Recommendations 的合规性验证

要了解是否属于特定合规计划的范围，请参阅AWS 服务 “按合规计划划分的范围” ”，然后选择您感兴趣的合规计划。 AWS 服务 有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。 AWS 提供了以下资源来帮助实现合规性：

- 安全与合规性快速入门指南 — 这些部署指南讨论了架构注意事项，并提供了在这些基础上 AWS 部署以安全性和合规性为重点的基准环境的步骤。
- 在 A@@ mazon Web Services 上构建 HIPAA 安全与合规架构 — 本白皮书描述了各公司如何使用 AWS 来创建符合 HIPAA 资格的应用程序。

> **Note**
>
> 并非所有 AWS 服务 人都符合 HIPAA 资格。有关更多信息，请参阅符合 HIPAA 要求的服务参考。

- AWS 合规资源AWS — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- AWS 客户合规指南 — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践， AWS 服务并将指南映射到跨多个框架（包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO)）的安全控制。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- AWS Security Hub— 这 AWS 服务 提供了您内部安全状态的全面视图 AWS。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 Security Hub 控件参考。
- Amazon GuardDuty — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务检测您的工作负载、容器和数据面临的潜在威胁。 GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。
- AWS Audit Manager— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

使用其他服务

本部分介绍与 Migration Hub Strategy Recommendations 交互的其他 AWS 服务。

主题

使用 AWS CloudTrail 记录 Strategy Recommendations API 调用

Migration Hub Strategy Recommendations 集成了 AWS CloudTrail，后者是一项服务，可以提供 Strategy Recommendations 中用户、角色或 AWS 服务所执行的操作的记录。CloudTrail 将 Strategy Recommendations 的 API 调用作为事件捕获。捕获的调用包括来自 Strategy Recommendations 控制台的调用和对 Strategy Recommendations API 操作的代码调用。

如果您创建跟踪记录，则可以使 CloudTrail 事件持续传送到 Amazon S3 桶（包括 Strategy Recommendations 的事件）。如果您不配置跟踪，则仍可在 CloudTrail 控制台中的 Event history（事件历史记录）中查看最新事件。使用 CloudTrail 收集的信息，您可以确定向 Strategy Recommendations 发出了什么请求、发出请求的 IP 地址、何人发出的请求、请求的发出时间以及其他详细信息。

要了解有关 CloudTrail 的更多信息，请参阅《AWS CloudTrail 用户指南》。

CloudTrail 中的 Strategy Recommendations 信息

在您创建 AWS 账户 时，将在该账户上启用 CloudTrail。当 Strategy Recommendations 中发生活动时，该活动将与事件历史记录中的其他 AWS 服务事件一同记录在 CloudTrail 事件中。您可以在 AWS 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用 CloudTrail 事件历史记录查看事件。

要持续记录 AWS 账户 中的事件（包括 Strategy Recommendations 的事件），请创建跟踪记录。通过跟踪记录，CloudTrail 可将日志文件传送至 Simple Storage Service（Amazon S3）存储桶。预设情况下，在控制台中创建跟踪记录时，此跟踪记录应用于所有AWS 区域。此跟踪记录在 AWS 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Simple Storage Service（Amazon S3）桶。此外，您可以配置其他 AWS 服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取行动。有关更多信息，请参阅下列内容：

- 创建跟踪概览
- CloudTrail 支持的服务和集成

- 为 CloudTrail 配置 Amazon SNS 通知
- 从多个区域接收 CloudTrail 日志文件和从多个账户接收 CloudTrail 日志文件

Strategy Recommendations 支持将以下操作记录为 CloudTrail 日志文件中的事件：

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

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

- 请求是使用根用户凭证还是 AWS Identity and Access Management (IAM) 用户凭证发出的
- 请求是使用角色还是联合身份用户的临时安全凭证发出的
- 请求是否由其它 AWS 服务发出

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

了解 Strategy Recommendations 日志文件条目

跟踪是一种配置，可用于将事件作为日志文件传送到您指定的 Amazon S3 桶。CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

下面的示例显示了一个 CloudTrail 日志条目，该条目说明了 GetServerDetails 操作。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "777777777777",
        "arn": "arn:aws:sts::111122223333:assumed-role/myUserName/...",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "777777777777",
                "arn": "arn:aws:iam::111122223333:role/myUserName",
                "accountId": "111122223333",
                "userName": "myUserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2021-09-20T01:07:16Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2021-09-20T01:07:43Z",
    "eventSource": "migrationhub-strategy.amazonaws.com",
    "eventName": "GetServerDetails",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "",
    "userAgent": "",
    "requestParameters": {
        "serverId": "ads-server-006"
    },
    "responseElements": null,
    "requestID": "07D681279BD94AED",
```

```
    "eventID": "cdc4b7ed-e171-4cef-975a-ad829d4123e8",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Migration Hub Strategy Recommendations 的配额

您的 AWS 账户对于每项 AWS 服务都具有默认配额（以前称为限制）。除非另有说明，否则，每个配额是区域特定的。您可以请求增加某些配额，但其他一些配额无法增加。

要查看 Migration Hub Strategy Recommendations 的配额列表，请参阅 Strategy Recommendations service quotas。

您还可以打开服务限额控制台，以查看 Strategy Recommendations 的配额。在导航窗格中，选择 AWS 服务，然后选择 Migration Hub Strategy Recommendations。

要请求提高配额，请参阅 Service Quotas 用户指南中的请求提高配额。如果配额在 Service Quotas 中尚不可用，请使用提高限制表格。

发布说明

主题

2023 年 11 月 17 日

新功能

- 收藏家 v1.1.47
- 支持.NET 8 应用程序。

2023 年 10 月 12 日

新功能

- 收藏家 v1.1.45

- Support 支持多数据源。

2023 年 4 月 17 日

新功能

- Collector v1.1.22
- 升级脚本增强功能。这需要最新版本的收集器。

2023 年 3 月 17 日

新特征

添加了二进制分析，无需源代码即可提供反模式和不兼容性检测。

2022 年 11 月 7 日

新特征

- 应用程序的应用程序筛选
- 按 AWS Application Discovery Service 标签筛选的服务器

2022 年 9 月 27 日

新特征

- Collector v1.1.12
  - SCT 版本 667
  - EMPAnalyzer 2.2.0.368
- 添加了针对服务器见解的 `diag check` 命令。
- 增加了针对潜在建议的支持。
- 增强了用户界面，用于检查配置和评测状态。

错误修复

- 移植助手转换器和其他修复。

2022 年 6 月 30 日

新特征

- Collector v1.1.11
  - 添加了 VMware API 支持。
  - A2C 在下载二进制文件时请求更改以添加用户标题。
  - 添加了 Linux 主路径、默认 Shell 和所有 Shell 的远程终端。
- A2C v1.17 公有二进制文件
  - 增加了对 Azure DevOps 作为管道部署目标的支持。

2022 年 4 月 18 日

新特征

- Collector v1.1.7
- 增加了从公有 URL 动态下载 A2C 二进制文件的功能。

错误修复

- A2C v1.1.5

2022 年 2 月 25 日

错误修复

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

2022 年 2 月 10 日

错误修复

- SCT v5.6.8

- A2C v1.1.1
  - 添加了针对 Linux tar 命令的检查。
  - 修复了在 Amazon ECR 中检查应用程序映像的问题。
  - 修复了需要移除容器才能进行预验证的问题。
- Collector v1.1.3
  - 修复了远程 32 位计算机的 4xx 错误。
  - 更新了 A2C 错误代码。
  - 验证了 C# 中用于远程计算机源代码分析的 IP 地址。

2022 年 1 月 28 日

新特征

- Collector v1.1.2
- 为源代码分析添加了 Azure DevOps Git 存储库支持。

2022 年 1 月 14 日

新特征

- Collector v1.1.1
- 添加了针对 SQL 数据库的 Babelfish 建议。

2021 年 12 月 21 日

已解决的问题

- Collector v1.1.0
- 恢复了数据库分析。

2021 年 12 月 15 日

已知问题

- Collector v1.0.4
- 目前不支持数据库分析（CVE-2021-44228）。

2021 年 10 月 25 日

新特征

- Collector v1.0.0
- 《Migration Hub Strategy Recommendations 用户指南》的首次发布。

文档和版本历史记录

下表介绍了 Strategy Recommendations 的文档版本。有关更多信息，请参阅 发布说明。

更改	描述	日期
AWS 托管策略更新-更新为 AWSMigrationHubStrategyCollector	更新了AWSMigrationHubStrategyCollector政策，加入了新的`s3application-transformation` 、和`migrationhub-strategy` 操作。	2024年4月1日
AWS 托管策略更新-更新为 AWSMigrationHubStrategyCollector	更新了AWSMigrationHubStrategyCollector政策，加入了新的`application-transformation` 操作。此更新还添加了限制各种操作的条件，其中`aws:ResourceAccount` 必须等于`aws:PrincipalAccount` .	2024年2月5日
新特征	策略建议应用程序数据收集器客户端 v1.1.47 支持.NET 8 应用程序。	2023 年 11 月 17 日
新特征	策略建议应用程序数据收集器客户端 v1.1.45 支持多个数据源。	2023 年 10 月 12 日
AWS 托管策略更新-更新为 AWSMigrationHubStrategyCollector	更新了AWSMigrationHubStrategyCollector政策，加入了新的 Amazon S3 API。	2023 年 9 月 15 日
AWS 托管策略更新-更新为 AWSMigrationHubStrategyCollector	更新了AWSMigrationHubStrategyCollector政策，增加了新的源代码分析器。	2023 年 3 月 8 日

IAM 最佳实践更新	有关更多信息，请参阅 IAM 安全最佳实践。	2023 年 2 月 25 日
AWS 托管策略更新-更新现有策略	M@@ igration Hub 策略建议在现有策略中添加了三个 AWS Application Discovery Service API。	2022 年 11 月 10 日
安全更新	与接口 VPC 端点建立私有连接。	2022 年 3 月 7 日
新特征	为源代码分析添加了 Azure DevOps Git 存储库支持。	2022 年 1 月 28 日
新特征	添加了针对 SQL 数据库的 Babelfish 建议。	2022 年 1 月 14 日
初始版本	《Migration Hub Strategy Recommendations 用户指南》的首次发布。	2021 年 10 月 25 日

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。