aws

用户指南

AWS Migration Hub 重构空间

AWS Migration Hub 重构空间: 用户指南

Table of Contents

什么是 AWS Migration Hub 重构空间？

AWS Migration Hub 重构 Space 目前为预览版，可能会发生变化。

AWS Migration Hub 重构空间是将增量应用程序重构为微服务的起点AWS. 重构空间有助于减少建筑和运营过程中不分化的繁重工作AWS用于增量重构的基础架构。在将应用程序发展为微服务或使用微服务中编写的新功能扩展现有应用程序时，您可以使用 Refactor Spaces 来帮助降低风险。

Refactor Spaces 环境通过编排简化跨账户联网AWS Transit Gateway、AWS Resource Access Manager，以及 Virtual Private Cloud (VPC)。重构 Spaces 桥梁了跨网络AWS账户允许早期和更新的服务进行通信，同时保持单独的独立性AWS 账户.

重构 Spaces 提供了一个应用程序，用于为增量重构建模型的 Strller Fig 模式。重构 Spaces 应用程序可协调 Amazon API 网关、Network Load Balancer 和基于资源的AWS Identity and Access Management(IAM) 策略，以便您可以透明地将新服务添加到外部 HTTP 终端节点。您还可以以增量方式将流量路由到新服务。这使底层架构更改对应用程序使用者透明。有关 Sirtual Pigration Migration 的更多信息，请参阅。Strller 无花果应用.

主题

您是新用户吗？

如果您是新用户 Regration Space，我们建议您从阅读以下章节着手：

Pricing

所有重构 Spaces 编排的资源（例如，Transit Gateway）都在AWS 账户. 因此，您需要为重构空间的使用量以及与预配置资源相关的任何费用付费。有关更多信息，请参阅 。AWSMigration Hub 定价.

> **Note**
>
> 在其预览期间，重构空间不收取任何费用。

重构 Space 概念

本节介绍了在使用 AWS Migration Hub 重构空间时可以创建和管理的关键组件。

主题

- Environment
- Applications
- Services
- Route

Environment

Refactor Spaces 环境提供了跨多个网络、应用程序和服务的统一视图AWS账户。

重构空间环境包含重构空间应用程序和服务。这是一个由桥接虚拟私有云 (VPC) 组成的多账户网络结构，允许其中的资源通过私有 IP 地址进行交互。该环境提供了跨多个网络、应用程序和服务的统一视图AWS 账户.

这些区域有：环境所有者是在其中创建重构空间环境的帐户。无论创建资源的账户如何，环境所有者都可以跨账户了解环境中创建的应用程序、服务和路由。

Applications

Refactor Spaces 应用程序包含服务和路由，并提供单个外部终端节点以向外部呼叫者公开应用程序。该应用程序为增量应用程序重构提供了一个 Strller Fig 代理。有关 Sirtual Pigration 的信息，请参阅。Strller 无花果应用.

重构 Spaces 应用程序对 Strller Fig 模式进行建模，并协调 Amazon API Gateway、API Gateway VPC 链接、Network Load Balancer 和基于资源的AWS Identity and Access Management(IAM) 策略，以便您可以透明地将新服务添加到应用程序的 HTTP 终端节点。它还会以增量方式将流量从现有应用程序传送到新服务。这使底层体系结构更改对应用程序使用者透明。

Services

重构 Spaces 服务可提供应用程序的业务功能，并可通过独特的终端节点访问 服务终端节点是两种类型之一：HTTP/HTTPS URL 或AWS Lambdafunction.

Route

重构空间路由是将请求转发到服务的代理匹配规则。每个请求都是针对应用程序中配置的一组路由运行的。如果规则匹配，请求将发送到为该规则配置的目标服务。应用程序具有默认路由，如果不匹配任何规则，则将请求转发到默认服务。路由是在应用程序的 Amazon API Gateway 代理上配置的。

重构空间的工作原理

开始使用 AWS Migration Hub 重构空间时，您可以使用一个或多个AWS 账户. 您可以使用单个账户进行测试。但是，一旦您准备好开始重构，我们建议您从以下三个账户入手：

- 现有应用程序的一个账户。
- 一个账户是第一个新的微服务。
- 一个账户充当重构环境所有者，其中重构 Spaces 配置跨账户网络并路由流量。

首先，在被选为环境所有者的帐户中创建一个重构空间环境。然后，您可以使用以下方法与其他两个账户共享环境AWS Resource Access Manager（重构 Spaces 控制台会为您执行此操作）。与另一个账户共享环境后，Refactor Spaces 会自动与其他账户共享它在环境中创建的资源。它通过编排来实现这一点AWS Identity and Access Management(IAM) 基于资源的策略。

重构环境通过协调提供跨账户的统一网络AWS Transit Gateway、AWS Resource Access Manager，以及虚拟私有云 (VPC)。重构环境包含现有应用程序和新的微服务。创建重构环境后，您可以在环境中创建重构空间应用程序。Refactor Spaces 应用程序包含服务和路由，它提供了一个终端节点，以便向外部调用者公开应用程序。

应用程序支持路由到在容器、无服务器计算和具有公共或私有可见性的 Amazon Elastic Compute Cloud (Amazon EC2) 中运行的服务。应用程序中的服务可以有两种终端节点类型之一：VPC 中的 URL（HTTP 和 HTTPS），或者AWS Lambdafunction. 在应用程序包含服务后，您可以添加默认路

由，以将所有流量从应用程序的代理引导到代表现有应用程序的服务。在容器或无服务器计算中突破或添加新功能时，您可以添加新的服务和路由以将流量重定向到新服务。

对于 VPC 中具有 URL 终端节点的服务，重构空间使用 Transit Gateway 自动桥接环境中的所有服务 VPC。这意味着AWS您在服务 VPC 中启动的资源可以直接与添加到环境中的所有其他服务 VPC 通信。您可以使用 VPC 安全组应用其他跨账户路由约束。当创建指向使用 Lambda 终端节点的服务的路由时，重构 Spaces 会协调亚马逊 API 网关的 Lambda 集成以调用该函数AWS 账户.

设置

AWS Migration Hub 重构空间目前为预览版，可能会发生变化。

首次使用 AWS Migration Hub 重构空间前，请完成以下任务：

注册AWS
创建 IAM 用户

注册AWS

在本节中，您将注册 AWS 账户。如果您已有 AWS 账户，请跳过此步骤。

当您注册 Amazon Web Services 时 (AWS)，您的AWS所有账户将自动注册AWS服务，包括 AWS Migration Hub 重构空间。您只需为使用的服务付费。

如果您还没有 AWS 账户，请完成以下步骤创建一个。

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，您将接到一通电话，要求您使用电话键盘输入一个验证码。

创建 IAM 用户

当您创建AWS账户时，您将获得一个单点登录身份，此身份对所有AWS账户中的服务和资源。此身份称作 AWS 账户根用户。登录到AWS Management Console通过使用用于创建账户的电子邮件地址和密码，您将获得对所有AWS您的账户中的资源。

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，请遵循安全最佳实践创建单独的 IAM 用户然后创建AWS Identity and Access Management(IAM) 管理员用户。然后，请安全地锁定根用户凭证，并仅使用这些凭证执行少数账户和服务管理任务。

除了创建管理用户外，您还必须创建非管理 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，管理员账户将继承AWSMigrationHubRefactorSpacesFullAccess访问 AWS Migration Hub 重构空间所需的托管策略。

创建管理员用户

- 在 AWS 账户中创建管理员用户。有关说明，请参阅创建您的第一个 IAM 用户和管理员组中的IAM 用户指南.

创建 IAM 非管理员用户

本节介绍如何授予对非管理用户使用重构空间所需的必需权限。

在使用重构空间之前，请使用AWSMigrationHubRefactorSpacesFullAccess托管策略，然后将向用户授予使用重构空间所需额外权限的策略附加该策略。中介绍了此额外必需的权限策略重构空间所需的额外权限.

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

创建非管理员 IAM 用户以与重构 Spaces 一起使用

1. InAWS Management Console，导航到 IAM 控制台。
2. 按照中所述使用控制台创建用户的说明创建非管理员 IAM 用户在您的中创建 IAM 用户AWS帐户中的IAM 用户指南.

   按照中的说明执行IAM 用户指南：

   - 在关于选择访问类型的步骤中，同时选择两者程序化访问和AWS管理控制台访问.
   - 当踏上关于设置权限页面中，选择以下选项直接将现有策略附加到用户. 然后，选择托管 IAM 策略awsmGigation HubbreFactor 空间完全访问.
   - 在执行关于查看用户访问密钥 (访问密钥 ID 和秘密访问密钥) 的步骤时，请遵循重要提示注意如何将用户的新访问密钥 ID 和秘密访问密钥保存在安全的地方。

3. 创建用户后，请按照中所述为用户嵌入内联策略的说明向用户添加额外所需的权限策略添加 IAM 身份权限中的IAM 用户指南. 中介绍了此额外必需的权限策略重构空间所需的额外权限.

入门使用重构空格

AWS Migration Hub 重构 Spaces 目前为预览版，可能会发生变化。

此部分介绍如何开始 AWS Migration Hub 重构空间。

主题

Prerequisites

以下是使用 AWS Migate Hub 重构空间的先决条件。

- 您必须有一个或多个AWS 账户, 和AWS Identity and Access Management(IAM) 用户为这些账户设置。有关更多信息，请参阅设置。
- 将其中一个 IAM 用户账户指定为重构空间环境所有者账户。

以下步骤介绍了如何在 Migration Hub 控制台中使用 AWS Migigration Hub 重构空间。

第 1 步：创建环境

此步骤介绍了如何创建作为重构空间的一部分的环境入门向导。您还可以通过选择创建环境环境下应用程序重构在 “重构空格” 导航窗格中。

重构环境简化了多账户使用案例，以加快应用程序重构的速度。在您创建环境时，我们会协调AWS Transit Gateway、虚拟私有云 (VPC)AWS Resource Access Manager在您的账户中。

创建环境后，您可以与其他人共享环境AWS 账户中的组织单元 (OU)AWS Organizations，或者整个AWS组织。通过与其他人共享环境AWS 账户，除非您使用 IAM 限制访问权限，否则这些账户中的用户可以在环境中创建应用程序、服务和路由。

创建 环境

1. 使用AWS您在其中创建的账户设置，登录到AWS Management Console然后打开 Migration Hub 控制台https://console.aws.amazon.com/migrationhub/.
2. 在 Migate Migration Hub 控制台导航窗格中，选择重构空格.
3. 选择开始使用。
4. Select创建一个重构环境，开始逐步实现多个微服务的现代化AWS账户.
5. 选择开始。
6. 为环境输入名称。
7. （可选）添加环境描述。
8. 重构 Spaces 使用服务相关角色来连接到AWS 服务代表您编排它们。在您首次使用 Reactor Spaces 时，将创建具有正确权限的服务相关角色。有关 service-linked role 服务相关角色的更多信息，请参阅将服务相关角色用于重构 Spaces。
9. 选择下一步要移动到的创建应用程序页.

第 2 步：创建应用程序

此步骤介绍了如何创建应用程序作为重构空间的一部分入门向导。您还可以通过选择创建应用程序创建应用程序下快速操作在 “重构空格” 导航窗格中。

应用程序为应用程序中的服务提供多账户流量路由。对于每个应用程序，我们使用 Amazon API Gateway VPC 链接、Network Load Balancer 和资源策略来编排代理。应用程序是服务和路线的容器。

应用程序的代理需要 VPC。代理的 Network Load Balancer 在 VPC 中启动，并为 VPC 和 Network Load Balancer 配置了 API Gateway VPC 链接。

创建应用程序

1. 在存储库的创建应用程序页面，输入应用程序的名称。
2. UNDU代理 VPC中，选择代理虚拟私有云 (VPC) 或选择创建 VPC.

应用程序的代理需要 VPC。代理的 Network Load Balancer 在 VPC 中启动，并为 VPC 和 Network Load Balancer 配置了 API Gateway VPC 链接。

3. UNDU代理端节点类型选择区域性要么私密.

   代理的终端节点可以是区域性的或私有的。区域 API Gateway 终端节点可以通过公共互联网访问，私有 API Gateway 终端节点只能通过 VPC 访问。

4. 选择下一步要移动到的共享环境页.

第 3 步：共享您的环境

此步骤介绍了如何共享环境作为重构空间的一部分入门向导。您还可以通过选择来共享环境共享环境下快速操作在 “重构空格” 导航窗格中。

环境与其他人共享AWS 账户使用AWS Resource Access Manager(AWS RAM)。受邀账户必须在 12 小时内接受环境共享。否则，必须再次共享环境。如果您在AWS组织，然后你可以启用自动接受股票。AWS RAM支持与其他人共享环境AWS 账户中的组织单元 (OU)AWS Organizations，或者整个AWS组织。

由于环境是应用程序、服务、路由和编排的容器AWS资源，共享环境提供了从受邀账户访问这些资源的一些权限。与其他账户共享后，这些账户中的用户可以在环境中创建应用程序、服务和路由，除非您使用 IAM 限制访问权限。

与另一个环境共享时AWS 账户，重构 Spaces 还共享环境AWS Transit Gateway通过编排与另一个账户AWS RAM.

共享环境

1. 选择以下主体类型之一以与之共享您的环境：

   - AWS 账户
   - 组织-整个AWS组织
   - 组织部门（OU）

   AWS RAM支持与其他人共享环境AWS 账户中的组织单元 (OU)AWS Organizations，或者整个AWS组织。

2. 环境与其他人共享AWS 账户使用AWS Resource Access Manager(AWS RAM)。AWS RAM支持与其他人共享环境AWS 账户中的组织单元 (OU)AWS Organizations，或者整个AWS组织。如果你想与整个环境共享AWS组织或 OU，您必须启用与组织共享AWS RAM在尝试在重构空间中共享之前。
3. 输入AWS 账户的校长，然后选择Add.
4. 选择下一步要移动到的审核页.
5. 查看在先前步骤中输入的信息。
6. 如果一切正常，请选择创建 环境. 如果您想要更改某些内容，请选择上一步.

第 4 步：创建服务

服务提供了应用程序的业务功能。您的现有应用程序由一个或多个服务表示。每个服务都有一个终端节点（HTTP (TTPS) URL 或AWS Lambda函数)。

创建环境后，您可以在环境详细信息页面（以环境名称作为标题的页面）上查看有关环境的信息。环境详细信息页面显示环境的摘要并列出了环境中的应用程序。

以下过程介绍如何从环境详细信息页面开始创建服务。您还可以通过选择创建服务创建服务下快速操作在 “重构空格” 导航窗格中。

从环境详细信息页面创建服务

1. 从应用程序列表中，选择要向其添加服务的应用程序的名称。
2. 在应用程序详细信息页面（以应用程序名称作为标题的页面）上，在服务，选择创建服务.
3. 输入新服务的名称。
4. （可选）输入服务的描述。
5. 选择其中一种服务终端节点类型。
6. 如果服务是 VPC 中的 URL 终端节点，请选择 VPC。
   a. 选择要添加到环境网桥的 VPC。
   b. 输入服务 URL 终端节点。

      VPC 终端节点 URL 可以包含可公开解析的 DNS 名称 (http://www.example.com) 或 IP 地址。服务 URL 中不支持私有 DNS 名称，但是您可以使用服务 VPC 中的私有 IP 地址。
   c. （可选）输入运行状况检查终端节点 URL。
7. a. 如果服务是 Lambda 函数，请选择 Lambda。

b. 从您的账户中选择 Lambda 函数。

8. （可选）下将流量路由到此服务，如果要将此服务设置为应用程序的默认路由，请选中相应的复选框。

   在创建服务时，您可以选择将应用程序流量同时路由到服务。如果在其中创建服务的应用程序没有任何路由，则可以将服务设为应用程序的默认路由，以便将所有流量路由到该服务。如果应用程序有现有路由，则可以添加带有指向该服务的路径的路由。

第 5 步：创建路由

本节介绍如何创建路由。

应用程序用于以增量方式将流量从现有应用程序转移到新服务。您也可以在不触及现有应用程序的情况下使用它来启动新功能。

如果选定的应用程序没有任何路由，则新路由将成为应用程序的默认路由，并将所有流量路由到所选服务。如果应用程序有现有路由，则该路由的范围限定为路径和动词组合。

> **Note**
>
> 创建路由后立即处于活动状态，流量将从默认路由或现有父路由重定向。

要创建路由

在应用程序详细信息页面（以应用程序名称作为标题的页面）上，在路由，选择创建路由.

1. 为路由选择服务。
2. 选择 Create route (创建路由)。

AWS Migration Hub 的安全性重构空间

AWS Migration Hub 重构空间目前为预览版，可能会发生变化。

AWS 的云安全性的优先级最高。作为 AWS 客户，您将从专为满足大多数安全敏感型企业的要求而打造的数据中心和网络架构中受益。

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 云中运行 AWS 服务的基础设施。AWS 还向您提供可安全使用的服务。作为AWS合规性计划的一部分，第三方审计人员将定期测试和验证安全性的有效性。要了解适用于重构空间的合规性计划，请参阅AWS合规性计划范围内的服务.
- 云中的安全性 - 您的责任由您使用的 AWS 服务决定。您还需要对其它因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

该文档帮助您了解如何在使用 AWS Migration Hub 重构空间时应用责任共担模式。它说明了如何配置 ReGactor Spaces 以实现您的安全性和合规性目标。您还将了解如何使用其他AWS帮助您监控和保护您的 ReGactor Spaces 资源的服务。

目录

AWS Migration Hub 中的数据保护重构空间

这些区域有：AWS 责任共担模式适用于 AWS Migration Hub 重构空间中的数据保护。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。此内容包括您所使用的 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AWS责任共担模式和 GDPR 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS Identity and Access Management (IAM) 设置单独的用户账户。这仅向每个用户授予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您的数据：

- 对每个账户使用 Multi-Factor Authentication (MFA)。
- 使用 SSL/TLS 与AWS资源进行通信。建议使用 TLS 1.2 或更高版本。
- 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 中的个人数据。
- 如果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（例如您客户的电子邮件地址）放入标签或自由格式字段（例如名称字段）。这包括使用重构空间或其他时AWS使用控制台、API、AWS CLI，或者AWS开发工具包。您在用于名称的标签或自由格式字段中输入的任何数据都可能会用于计费或诊断日志。当您向外部服务器提供 URL 时，强烈建议您不要在 URL 中包含凭证信息来验证您对该服务器的请求。

静态加密

重构 Spaces 将所有静态数据加密。

传输中加密

重构 Spaces 网际通信支持所有组件和客户端之间的 TLS 1.2 加密。

AWS Migration Hub 的 Identity and Access Management 重构空间

AWS Identity and Access Management (IAM) 是一种 AWS 服务，可以帮助管理员安全地控制对 AWS 资源的访问。IAM 管理员控制谁可以是身份验证（已登录）和授权（有权限）可以使用重构空间资源。IAM 是一个可以免费使用的 AWS 服务。

主题

- AWSAWS Migration Hub 的托管策略重构空间
- AWS Migration Hub 的基于身份的策略示例
- 疑难解答 AWS Migration Hub 重构 Spaces 身份和访问权
- 将服务相关角色用于重构 Spaces

Audience

如何使用AWS Identity and Access Management(IAM) 因您在重构空间中执行的操作而异。

服务用户— 如果您使用 Rigration Spaces 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。当您使用更多重构空间功能来完成工作时，您可能需要其他权限。了解如何管理访问权限可帮助您向管理员请求适合的权限。如果您无法访问重构空间中的一项功能，请参阅。疑难解答 AWS Migration Hub 重构 Spaces 身份和访问权.

服务管理员— 如果您在公司负责重构空间资源，则您可能具有的完全访问权限。您有责任确定您的员工应访问哪些 Rigration Spaces 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 与重构空间搭配使用的更多信息，请参阅AWS Migration Hub 重构空间如何与 IAM 配合使用.

IAM 管理员— 如果您是 IAM 管理员，您可能希望了解有关您可以如何编写策略以管理对 Rigration Spaces 的访问权限的详细信息。要查看您可在 IAM 中使用的基于身份的 Rigration Spaces 示例策略，请参阅。AWS Migration Hub 的基于身份的策略示例.

使用身份进行身份验证

身份验证是您使用身份凭证登录 AWS 的方法。有关使用AWS Management Console登录的更多信息，请参阅 IAM 用户指南中的以 IAM 用户或根用户身份登录AWS Management Console。

您必须作为AWS 账户根用户、IAM 用户或代入 IAM 角色以进行身份验证（登录到AWS）。您还可以使用公司的单一登录身份验证方法，甚至使用 Google 或 Facebook 登录。在这些情况下，您的管理员以前使用 IAM 角色设置了联合身份验证。在您使用来自其它公司的凭证访问 AWS 时，您间接地代入了角色。

要直接登录到AWS Management Console，请将密码与根用户电子邮件地址或 IAM 用户名一起使用。您可以使用根用户或 IAM 用户访问密钥以编程方式访问 AWS。AWS 提供了 SDK 和命令行工具，可使用您的凭证对您的请求进行加密签名。如果您不使用 AWS 工具，则必须自行对请求签名。使用 Signature Version 4（用于对入站 API 请求进行验证的协议）完成此操作。有关验证请求的更多信息，请参阅《AWS 一般参考》中的 Signature Version 4 签名流程。

无论使用何种身份验证方法，您可能还需要提供其它安全信息。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《IAM 用户指南》中的在 AWS 中使用多重身份验证 (MFA)。

AWS 账户根用户

当您首次创建AWS 账户时，最初使用的是一个对账户中所有AWS服务和资源有完全访问权限的单点登录身份。此身份称为AWS 账户根用户，使用您创建账户时所用的电子邮件地址和密码登录，即可获得该身份。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，请遵循仅使用根用户创建您的第一个 IAM 用户的最佳实践。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。

IAM 用户和组

IAM 用户是AWS 账户内对某个人员或应用程序具有特定权限的一个身份。IAM 用户可能具有长期凭证，例如用户名和密码或一组访问密钥。要了解如何生成访问密钥，请参阅 IAM 用户指南 中的管理 IAM 用户的访问密钥。为 IAM 用户生成访问密钥时，请确保查看并安全保存密钥对。您以后无法找回秘密访问密钥，而是必须生成新的访问密钥对。

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 用户指南中的何时创建 IAM 用户（而不是角色）。

IAM 角色

IAM 角色是AWS 账户中具有特定权限的身份。它类似于 IAM 用户，但与特定人员不关联。您可以通过切换角色，在 AWS Management Console 中暂时代入 IAM 角色。您可以调用 AWS CLI 或 AWS API 操作或使用自定义 URL 以代入角色。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：

- 临时 IAM 用户权限 – IAM 用户可以代入 IAM 角色，以暂时获得不同的权限以执行特定的任务。
- 联合身份用户访问 – 您可以不创建 IAM 用户，而是使用来自 AWS Directory Service、您的企业用户目录或 Web 身份提供商的现有身份。这些用户称为联合身份用户。在通过身份提供商请求访问权

限时，AWS 将为联合身份用户分配角色。有关联合身份用户的更多信息，请参阅 IAM 用户指南 中的联合身份用户和角色。

- 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（可信委托人）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 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 – 某些 AWS 服务使用其它 AWS 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委托人的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 委托人权限 – 当您使用 IAM 用户或角色在 AWS 中执行操作时，您将被视为委托人。策略向委托人授予权限。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触发另一个操作。在这种情况下，您必须具有执行这两个操作的权限。要查看某个操作是否需要策略中的其他相关操作，请参阅。AWS Migration Hub 的操作、资源和条件键中的服务授权参考.
  - 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担任的 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 – 服务相关角色是与 AWS 服务关联的一种服务角色。服务可以代入代表您执行操作的角色。服务相关角色显示在您的 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。
- 在 Amazon 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凭证。这优先于在 EC2 实例中存储访问密钥。要将 AWS 角色分配给 EC2 实例并使其对该实例的所有应用程序可用，您可以创建一个附加到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

您将创建策略并将其附加到 IAM 身份或AWS资源，以便控制AWS中的访问。策略是AWS中的对象；在与标识或资源相关联时，策略定义它们的权限。您可以通过 root 用户或 IAM 用户身份登录，也可以代入 IAM 角色。随后，当您提出请求时，AWS会评估相关的基于身份或基于资源的策略。策略中的权限确定是允许还是拒绝请求。大多数策略在 AWS 中存储为 JSON 文档。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内容。也就是说，哪个委托人可以对什么资源执行操作，以及在什么条件下执行。

每个 IAM 实体（用户或角色）最初没有任何权限。换言之，预设情况下，用户什么都不能做，甚至不能更改他们自己的密码。要为用户授予执行某些操作的权限，管理员必须将权限策略附加到用户。或者，管理员可以将用户添加到具有预期权限的组中。当管理员为某个组授予访问权限时，该组内的全部用户都会获得这些访问权限。

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。具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 用户指南中的创建 IAM 策略。

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。托管式策略是可以附加到AWS 账户中的多个用户、组和角色的独立策略。托管式策略包括 AWS 托管式策略和客户托管式策略。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，策略定义指定委托人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委托人。委托人可以包括账户、用户、角色、联合身份用户或 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来自 IAM 的 AWS 托管式策略。

访问控制列表 (ACL)

访问控制列表 (ACL) 控制哪些委托人（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、AWS WAF 和 Amazon VPC 是支持 ACL 的服务示例。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) 概览。

其它策略类型

AWS 支持额外的、不太常用的策略类型。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功能，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的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 是指定中的组织或组织单位 (OU) 的最大权限的 JSON 策略。AWS Organizations.AWS Organizations是用于分组和集中管理多个服务AWS 账户你的企业拥有的。如果在组织内启用了所有功能，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中实体的权限，包括每个 AWS 账户 根用户。有关 Organizations 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 – 会话策略是当您以编程方式为角色或联合身份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 AWS 如何确定在涉及多种策略类型时是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

AWS Migration Hub 重构空间如何与 IAM 配合使用

在使用 IAM 管理对重构空间的访问之前，请了解哪些 IAM 功能可与重构空间搭配使用。

您可以与 AWS Migration Hub 一起使用的 IAM 功能重构空间

IAM 功能	重构空间支持
基于身份的策略	是
基于资源的策略	是
策略操作	是

IAM 功能	重构空间支持
策略资源	是
策略条件键	是
ACL	否
ABAC（策略中的标签）	部分
临时凭证	是
委托人权限	是
服务角色	否
服务相关角色	是

要了解如何使用重构空间和其他方式的概述AWS服务适用于大多数 IAM 功能，请参阅AWS使用 IAM 的服务中的IAM 用户指南.

适用于的基于身份的策略重构空间

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委托人，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。

适用于的基于身份的策略示例

要查看重构 Space 基于身份的策略的示例，请参阅。AWS Migration Hub 的基于身份的策略示例.

重构 Space 中的基于资源的策略

支持基于资源的策略。	是

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，策略定义指定委托人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委托人。委托人可以包括账户、用户、角色、联合身份用户或 AWS 服务。

要启用跨账户访问，您可以将整个账户或其它账户中的 IAM 实体指定为基于资源的策略中的委托人。将跨账户委托人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的AWS 账户中时，则信任账户中的 IAM 管理员还必须授予委托人实体（用户或角色）对资源的访问权限。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委托人授予访问权限，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。

重构空间的策略操作

支持策略操作	是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。也就是说，哪个委托人 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相关操作的权限。

要查看 “重构空间” 操作的列表，请参阅。AWS Migration Hub 定义的操作中的服务授权参考.

重构空间中的策略操作在操作前使用以下前缀：

```
refactor-spaces
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
      "refactor-spaces:action1",
      "refactor-spaces:action2"
         ]
```

要查看重构 Space 基于身份的策略的示例，请参阅。AWS Migration Hub 的基于身份的策略示例.

重构空间的策略资源

支持策略资源	是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。也就是说，哪个委托人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 Resource Name（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": "*"
```

要查看重构 Space 资源类型及其 ARN 的列表，请参阅。AWS Migration Hub 定义的资源中的服务授权参考. 要了解您可以使用哪些操作指定每个资源的 ARN，请参阅。AWS Migration Hub 定义的操作.

要查看重构 Space 基于身份的策略的示例，请参阅。AWS Migration Hub 的基于身份的策略示例.

重构空间的策略条件键

支持策略条件密钥	是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。也就是说，哪个委托人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，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。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，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 AWS 使用逻辑 OR 运算来评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。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支持全局条件键和特定于服务的条件键。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的 AWS 全局条件上下文键。

要查看重构 Space 条件键的列表，请参阅。AWS Migration Hub 的条件键中的服务授权参考. 要了解您可以对哪些操作和资源使用条件键，请参阅。AWS Migration Hub 定义的操作.

要查看重构 Space 基于身份的策略的示例，请参阅。AWS Migration Hub 的基于身份的策略示例.

重构空间中的访问控制列表 (ACL)

支持 ACL	否

访问控制列表 (ACL) 控制哪些委托人（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。

使用重构空间的基于属性的访问控制 (ABAC)

支持 ABAC（策略中的标签）	部分

基于属性的访问控制 (ABAC) 是一种授权策略，该策略基于属性来定义权限。在 AWS 中，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）以及AWS资源。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在委托人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，您需要使用 aws:ResourceTag/*key-name*、aws:RequestTag/*key-name* 或 aws:TagKeys 条件键在策略的条件元素中提供标签信息。

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控制（ABAC）。

将临时凭证与重构空间结合使用

支持临时凭证	是

某些AWS服务在您使用临时凭证登录时无法正常工作。有关更多信息，包括AWS服务与临时凭证配合使用，请参阅《IAM 用户指南》中的使用 IAM 的AWS服务。

如果您不使用用户名和密码而用其它方法登录到AWS Management Console，则使用临时凭证。例如，当您使用贵公司的单点登录（SSO）链接访问AWS时，该过程将自动创建临时凭证。当您以用户身份登录控制台，然后切换角色时，您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 或者 AWS API 创建临时凭证。之后，您可以使用这些临时凭证访问AWS。AWS建议您动态生成临时凭证，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。

重构空间的跨服务主体权限

支持委托人权限	是

当您使用 IAM 用户或角色在AWS中执行操作时，您将被视为委托人。策略向委托人授予权限。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触发另一个操作。在这种情况下，您必须具有执行这两个操作的权限。要查看某个操作是否需要策略中的其他相关操作，请参阅。AWS Migration Hub 的操作、资源和条件键中的服务授权参考.

重构空间的服务角色

支持服务角色	否

服务角色是由一项服务担任、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重构空间功能。仅当重构空间提供了这样做的指导时才编辑服务角色。

适用于重构 Space 的服务相关角色

支持服务相关角色	是

服务相关角色是一种与AWS服务相关的服务角色。服务可以代入代表您执行操作的角色。服务相关角色显示在您的 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。

有关创建或管理服务相关角色的详细信息，请参阅能够与 IAM 搭配使用的AWS服务。在表中查找服务相关角色列中包含 Yes 额表。选择 Yes 链接以查看该服务的服务相关角色文档。

AWSAWS Migration Hub 的托管策略重构空间

要向用户、组和角色添加权限，与自己编写策略相比，使用 AWS 托管策略更简单。创建仅为团队提供所需权限的 IAM 客户托管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托管式策略。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服务负责维护和更新AWS托管式策略。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）。当启动新功能或新操作可用时，服务最有可能会更新AWS托管策略。服务不会从AWS托管策略中删除权限，因此策略更新不会破坏您的现有权限。

AWS托管策略：awsmGigation HubbreFactor 空间完全访问

您可以将 AWSMigrationHubRefactorSpacesFullAccess 策略附加得到 IAM 身份。

这些区域有：AWSMigrationHubRefactorSpacesFullAccess策略授予对 AWS Migration Hub 重构空间、重构空间控制台功能和其他相关功能的完全访问权限AWS服务。

权限细节

这些区域有：AWSMigrationHubRefactorSpacesFullAccess策略包含以下权限。

- refactor-spaces— 允许 IAM 用户账户对重构空间的完全访问权限。
- ec2— 允许 IAM 用户账户执行重构空间使用的 Amazon Elastic Compute Cloud (Amazon EC2) 操作。
- elasticloadbalancing— 允许 IAM 用户账户执行重构空间使用的 Elastic Load Balancing 操作。
- apigateway— 允许 IAM 用户账户执行重构空间使用的 Amazon API Gateway 操作。
- organizations— 允许 IAM 用户账户AWS Organizations重构空间使用的操作。
- cloudformation— 允许 IAM 用户账户执行AWS CloudFormation从控制台创建一键式示例环境的操作。
- iam— 允许为 IAM 用户账户创建服务相关角色，这是使用重构空间的必要条件。

重构空间所需的额外权限

在使用重构空间之前，除了AWSMigrationHubRefactorSpacesFullAccess以下所需的额外权限必须分配给您账户中的 IAM 用户、组或角色。

- 为创建服务相关角色授予权限AWS Transit Gateway.
- 授予将虚拟私有云 (VPC) 附加到所有资源的调用账户的传输网关的权限。
- 为所有资源授予修改 VPC 终端节点服务的权限的权限。
- 授予对所有资源的调用帐户返回带标记或之前标记的资源的权限。
- 授予执行所有操作的权限AWS Resource Access Manager(AWS RAM) 对所有资源的调用帐户的操作。
- 授予执行所有操作的权限AWS Lambda针对所有资源的调用帐户的操作。

您可以通过向 IAM 用户、组或角色添加内联策略来获取这些额外权限。但是，您可以使用以下策略 JSON 创建 IAM 策略，然后将其附加到 IAM 用户、组或角色，而不是使用内联策略。

以下策略授予了能够使用重构空间所需的额外权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "transitgateway.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTransitGatewayVpcAttachment"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyVpcEndpointServicePermissions"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ram:*"
            ],
            "Resource": "*"
        },
        {
```

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

以下是AWSMigrationHubRefactorSpacesFullAccess政策。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RefactorSpaces",
            "Effect": "Allow",
            "Action": [
                "refactor-spaces:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcs",
                "ec2:DescribeTransitGatewayVpcAttachments",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeTags",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeInternetGateways"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "ec2:CreateTransitGateway",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTransitGatewayVpcAttachment"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/refactor-spaces:environment-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTransitGateway",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTransitGatewayVpcAttachment"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/refactor-spaces:environment-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateVpcEndpointServiceConfiguration"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteTransitGateway",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteTransitGatewayVpcAttachment",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DeleteTags"
            ],
```

```
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/refactor-spaces:environment-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteVpcEndpointServiceConfigurations",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/refactor-spaces:application-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:CreateLoadBalancer"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/refactor-spaces:application-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTags",
                "elasticloadbalancing:DescribeTargetHealth",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeListeners"
```

```
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:CreateLoadBalancerListeners",
                "elasticloadbalancing:CreateListener",
                "elasticloadbalancing:DeleteListener",
                "elasticloadbalancing:DeleteTargetGroup"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/refactor-spaces:route-id": [
                        "*"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:DeleteLoadBalancer",
            "Resource": "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-
spaces-nlb-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:CreateListener"
            ],
            "Resource": "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-
spaces-nlb-*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/refactor-spaces:route-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:DeleteListener",
```

```
            "Resource": "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-
nlb-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:DeleteTargetGroup",
                "elasticloadbalancing:RegisterTargets"
            ],
            "Resource": "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-
*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:CreateTargetGroup"
            ],
            "Resource": "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-
*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/refactor-spaces:route-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "apigateway:GET",
                "apigateway:DELETE",
                "apigateway:PATCH",
                "apigateway:POST",
                "apigateway:PUT",
                "apigateway:UpdateRestApiPolicy"
            ],
            "Resource": [
                "arn:aws:apigateway:*::/restapis",
                "arn:aws:apigateway:*::/restapis/*",
                "arn:aws:apigateway:*::/vpclinks",
                "arn:aws:apigateway:*::/vpclinks/*",
                "arn:aws:apigateway:*::/tags",
                "arn:aws:apigateway:*::/tags/*"
            ],
```

```
            "Condition": {
                "Null": {
                    "aws:ResourceTag/refactor-spaces:application-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "apigateway:GET",
            "Resource": [
                "arn:aws:apigateway:*::/vpclinks",
                "arn:aws:apigateway:*::/vpclinks/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "refactor-spaces.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
```

```
                    "iam:AWSServiceName": "elasticloadbalancing.amazonaws.com"
                }
            }
        }
    ]
}
```

重构空间更新为AWS托管策略

查看有关更新的详细信息AWS此服务开始跟踪这些更改以来，适用于重构 Space 的托管策略。要获取有关此页面更改的提示，请订阅 RSS 源（RSS 源）。

更改	描述	日期
awsmGigation HubbreFactor 空间完全访问— 发布时发布了新政策	这些区域有：AWSMigrationHubRefactorSpacesFullAccess 此策略授予对重构空间、重构空间控制台功能和其他相关功能的完全访问权限。AWS服务。	2021 年 11 月 29 日
迁移 HubbreFactor Spaces Spaces 服务角色策略— 发布时发布了新政策	MigrationHubRefactorSpacesServiceRolePolicy 提供对AWSAWS Migration Hub 管理或使用的资源重构空间。AWS Service RoleForMigration Hub 为服务相关角色使用此策略。	2021 年 11 月 29 日
开启了跟踪更改	为其重构 Space 开始跟踪更改AWS托管策略。	2021 年 11 月 29 日

AWS Migration Hub 的基于身份的策略示例

默认情况下，IAM 用户和角色没有创建或修改 Rigration Spaces 资源的权限。它们还无法使用 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，以对所需资源执行操作。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
- 使用重构空间控制台
- 允许用户查看他们自己的权限

策略最佳实践

基于身份的策略非常强大。它们确定某个人是否可以创建、访问或删除您账户中的 Rigration Spaces 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— 要快速开始使用重构空间，请使用AWS为您的员工授予所需的权限的托管策略。这些策略已在您的账户中提供，并由 AWS 维护和更新。有关更多信息，请参阅 IAM 用户指南中的开始使用 AWS 托管式策略中的权限。
- 授予最低权限 – 创建自定义策略时，仅授予执行任务所需的许可。最开始只授予最低权限，然后根据需要授予其它权限。这样做比起一开始就授予过于宽松的权限而后再尝试收紧权限来说更为安全。有关更多信息，请参阅 IAM 用户指南 中的授予最低权限。
- 为敏感操作启用 MFA – 为增强安全性，要求 IAM 用户使用多重身份验证 (MFA) 来访问敏感资源或 API 操作。要了解更多信息，请参阅《IAM 用户指南》中的在 AWS 中使用多重身份验证 (MFA)。
- 使用策略条件来增强安全性 – 在切实可行的范围内，定义基于身份的策略在哪些情况下允许访问资源。例如，您可编写条件来指定请求必须来自允许的 IP 地址范围。您也可以编写条件，以便仅允许指定日期或时间范围内的请求，或者要求使用 SSL 或 MFA。有关更多信息，请参阅 。IAM JSON 策略元素：Condition中的IAM 用户指南.

使用重构空间控制台

要访问 AWS Migration Hub 重构空间控制台，您必须具有一组最低的权限。这些权限必须允许您列出和查看有关您的 Rigration Spaces 资源的详细信息。AWS 账户. 如果您创建的基于身份的策略比所需的最低权限更严格，则无法为具有该策略的实体（IAM 用户或角色）正常运行控制台。

对于只需要调用 AWS CLI 或 AWS API 的用户，无需为其提供最低控制台权限。相反，只允许访问与您尝试执行的 API 操作相匹配的操作。

为确保用户和角色仍可使用 “重构空间” 控制台，还请附加重构空间ConsoleAccess要么ReadOnly AWS对于实体的托管策略。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

该示例说明了您如何创建策略，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完成此操作或者以编程方式使用 AWS CLI 或 AWS API 所需的权限。

```
{
    "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": "*"
        }
    ]
}
```

疑难解答 AWS Migration Hub 重构 Spaces 身份和访问权

可以使用以下信息，以帮助您诊断和修复在使用 Reration Spaces 和 IAM 时可能遇到的常见问题。

主题

我无权在重构空间中执行操作

如果 AWS Management Console 告诉您，您无权执行某个操作，则必须联系您的管理员寻求帮助。您的管理员是指为您提供用户名和密码的那个人。

当 `mateojackson` 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 `refactor-spaces:`*`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:
 refactor-spaces: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 `refactor-spaces:`*`GetWidget`* 操作访问 *`my-example-widget`* 资源。

我无权执行 iam:PassRole

如果您收到错误消息，提示您无权执行 `iam:PassRole` 操作，则必须联系您的管理员寻求帮助。您的管理员是指为您提供用户名和密码的那个人。要求该人员更新您的策略，以便允许您将角色传递给 Rigration Spaces。

有些 AWS 服务允许您将现有角色传递到该服务，而不是创建新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 用户时，会发生以下示例错误。`marymajor`尝试使用控制台在重构空间中执行操作。但是，服务必须具有服务角色所授予的权限才可执行操作。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，Mary 请求她的管理员来更新其策略，以允许她执行 iam:PassRole 操作。

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。如果您这样做，可能会向某人提供对您的账户的永久访问权限。

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 Rigration Space

要允许其他人访问 Reration Space，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 Rigration Spaces 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。

我想要允许人们在我之外AWS 账户访问我的重构空间资源

您可以创建一个角色，以便其它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：

- 要了解重构空间是否支持这些功能，请参阅。AWS Migration Hub 重构空间如何与 IAM 配合使用.
- 要了解如何为您拥有的 AWS 账户 中的资源提供访问权限，请参阅 IAM 用户指南中的为您拥有的另一个 AWS 账户 中的 IAM 用户提供访问权限。
- 要了解如何为第三方AWS 账户提供您的资源的访问权限，请参阅 IAM 用户指南中的为第三方拥有的 AWS 账户提供访问权限。
- 要了解如何通过联合身份验证提供访问权限，请参阅 IAM 用户指南中的为经过外部身份验证的用户（联合身份验证）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。

将服务相关角色用于重构 Spaces

AWS Migration Hub 重构 Spaces 使用AWS Identity and Access Management(IAM)服务相关角色. 服务相关角色是一种与重构空间直接关联的独特类型的 IAM 角色。服务相关角色由 Rateway 预定义，并包含该服务调用其他服务所需的一切权限。AWS服务代表您。

服务相关角色可让您更轻松地设置 Refactor Spaces，因为您不必手动添加必要的权限。只有重构空间可定义其服务相关角色的权限，除非另外定义，否则只有重构空间可以代入该角色。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它 IAM 实体的权限策略。

只有在首先删除相关资源后，才能删除服务相关角色。这将保护您的 Rateway 资源，因为您不会无意中删除对资源的访问权限。

有关支持服务相关角色的其他服务的信息，请参见用于 IAM 的 AWS 服务，查找 Service-Linked Role（服务相关角色）列为 Yes（是）的服务。选择 Yes（是）和链接，查看该服务的服务相关角色文档。

重构空间的服务相关角色权限

服务相关角色使用名为的服务相关角色。AWS 服务迁移 HubbreFactor 空间的角色然后将其与迁移 HubbreFactor Spaces Spaces 服务角色策略IAM 策略 — 提供访问AWSAWS Migration Hub 管理或使用的资源重构空间。

AWS ServiceRoleForMigration HUBREFactSpaces 服务相关角色信任以下服务代入该角色：

- `refactor-spaces.amazonaws.com`

以下是 AWS ServiceRoleForMigration HUBREFactSpaces 的 Amazon 资源名称 (ARN)。

```
arn:aws:iam::111122223333:role/aws-service-role/refactor-spaces.amazonaws.com/
AWSServiceRoleForMigrationHubRefactorSpaces
```

重构空间使用AWS 服务迁移 HubbreFactor 空间的角色执行跨账户更改时的服务相关角色。该角色必须存在于您的账户中才能使用重构空间。如果它不存在，重构空间会在以下 API 调用期间创建它：

- `CreateEnvironment`
- `CreateService`
- `CreateApplication`
- `CreateRoute`

您必须具备创建服务相关角色的 `iam:CreateServiceLinkedRole` 权限。如果服务相关角色在您的账户中不存在并且无法创建，则`Create`通话将失败。在使用重构空间之前，必须在 IAM 控制台中创建服务相关角色，除非您正在使用重构空间控制台。

在更改当前登录账户时，重构 Spaces 不使用服务相关角色。例如，创建应用程序时，重构空间会更新环境中的所有 VPC，以便它们可以与新添加的 VPC 进行通信。如果 VPC 在其他账户中，则重构 Spaces 将使用服务相关角色和`ec2:CreateRoute`在其他账户中更新路由表的权限。

为了进一步扩展创建应用程序示例，在创建应用程序时，Refactor Spaces 会更新中提供的虚拟私有云 (VPC) 中的路由表`CreateApplication`调用。这样，VPC 就可以与环境中的其他 VPC 进行通信。

呼叫者必须有`ec2:CreateRoute`我们用来更新路由表的权限。此权限存在于服务相关角色中，但 Refactor Spaces 不使用调用者账户中的服务相关角色来获取此权限。相反，调用方必须具有`ec2:CreateRoute`权限。否则，调用将会失败。

您不能使用服务相关角色升级您的权限。您的账户必须已经拥有服务相关角色的权限才能对调用帐户进行更改。这些区域有：`AWSMigrationHubRefactorSpacesFullAccess`托管策略以及授予额外所需权限的策略定义了创建重构空间资源所需的所有必要权限。服务相关角色是这些权限的子集，用于特定的跨账户调用。有关 `AWSMigrationHubRefactorSpacesFullAccess` 的更多信息，请参阅 AWS托管策略：awsmGigation HubbreFactor 空间完全访问。

Tags

当重构空间在您的账户中创建资源时，它们将使用适当的重构空间资源 ID 进行标记。例如，从中创建的 Transit Gateway`CreateEnvironment`被标记为`refactor-spaces:environment-id`以环境 ID 作为值的标签。从创建 API Gateway API`CreateApplication`被标记为`refactor-`

spaces:application-id以应用程序 ID 作为值。这些标签允许重构空间管理这些资源。如果编辑或删除标签，重构空间将无法再更新或删除资源。

MigrationHubRefactorSpacesServiceRolePolicy

使用名为 Migration ationHubreFactRolePolicy 的角色权限策略，允许重构空间对指定的资源完成以下操作：

Amazon API Gateway 操作

- apigateway:PUT
- apigateway:POST
- apigateway:GET
- apigateway:PATCH
- apigateway:DELETE

Amazon Elastic Compute Cloud 操作

- ec2:DescribeNetworkInterfaces
- ec2:DescribeRouteTables
- ec2:DescribeSubnets
- ec2:DescribeSecurityGroups
- ec2:DescribeVpcEndpointServiceConfigurations
- ec2:DescribeTransitGatewayVpcAttachments
- ec2:AuthorizeSecurityGroupIngress
- ec2:RevokeSecurityGroupIngress
- ec2:DeleteSecurityGroup
- ec2:DeleteTransitGatewayVpcAttachment
- ec2:CreateRoute
- ec2:DeleteRoute
- ec2:DeleteTags

- `ec2:DeleteVpcEndpointServiceConfigurations`

AWS Resource Access Manager 操作

- `ram:GetResourceShareAssociations`
- `ram:DeleteResourceShare`
- `ram:AssociateResourceShare`
- `ram:DisassociateResourceShare`

Elastic Load Balancing；操作

- `elasticloadbalancing:DescribeTargetHealth`
- `elasticloadbalancing:DescribeListener`
- `elasticloadbalancing:DescribeTargetGroups`
- `elasticloadbalancing:RegisterTargets`
- `elasticloadbalancing:CreateLoadBalancerListeners`
- `elasticloadbalancing:CreateListener`
- `elasticloadbalancing:DeleteListener`
- `elasticloadbalancing:DeleteTargetGroup`
- `elasticloadbalancing:DeleteLoadBalancer`
- `elasticloadbalancing:AddTags`
- `elasticloadbalancing:CreateTargetGroup`

以下是显示上述操作所适用资源的完整策略：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
```

```
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeTransitGatewayVpcAttachments",
                "elasticloadbalancing:DescribeTargetHealth",
                "elasticloadbalancing:DescribeListeners",
                "elasticloadbalancing:DescribeTargetGroups",
                "ram:GetResourceShareAssociations"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteTransitGatewayVpcAttachment",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DeleteTags",
                "ram:DeleteResourceShare",
                "ram:AssociateResourceShare",
                "ram:DisassociateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/refactor-spaces:environment-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteVpcEndpointServiceConfigurations",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/refactor-spaces:application-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:CreateLoadBalancerListeners",
                "elasticloadbalancing:CreateListener",
                "elasticloadbalancing:DeleteListener",
                "elasticloadbalancing:DeleteTargetGroup"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/refactor-spaces:route-id": [
                        "*"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "apigateway:PUT",
                "apigateway:POST",
                "apigateway:GET",
                "apigateway:PATCH",
                "apigateway:DELETE"
            ],
            "Resource": [
                "arn:aws:apigateway:*::/restapis",
                "arn:aws:apigateway:*::/restapis/*",
                "arn:aws:apigateway:*::/vpclinks/*",
                "arn:aws:apigateway:*::/tags",
                "arn:aws:apigateway:*::/tags/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/refactor-spaces:application-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "apigateway:GET",
            "Resource": "arn:aws:apigateway:*::/vpclinks/*"
        },
        {
```

```
            "Effect": "Allow",
            "Action": "elasticloadbalancing:DeleteLoadBalancer",
            "Resource": "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-
spaces-nlb-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:CreateListener"
            ],
            "Resource": "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-
spaces-nlb-*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/refactor-spaces:route-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:DeleteListener",
            "Resource": "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-
nlb-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:DeleteTargetGroup",
                "elasticloadbalancing:RegisterTargets"
            ],
            "Resource": "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-
*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:CreateTargetGroup"
            ],
            "Resource": "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-
*",
            "Condition": {
                "Null": {
```

```
                    "aws:RequestTag/refactor-spaces:route-id": "false"
                }
            }
        }
    ]
}
```

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。

为重构 Spaces 创建服务相关角色

无需手动创建服务相关角色。在中创建重构 Spaces 环境、应用程序、服务或路由资源时AWS Management Console，AWS CLI，或者AWSAPI、Rateway Spaces 将为您创建服务相关角色。有关为重构空间创建服务相关角色的更多信息，请参阅重构空间的服务相关角色权限.

如果删除此服务相关角色，然后需要再次创建，可以使用相同流程在账户中重新创建此角色。当您创建重构 Spaces 环境、应用程序、服务或路由资源时，Refactor Spaces 将再次为您创建服务相关角色。

编辑为重构 Spaces 编辑服务相关角色

服务相关角色不允许您编辑 AWSServiceRoleForMigration HUBREFactSpaces 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。但是可以使用 IAM 编辑角色说明。有关更多信息，请参见《IAM 用户指南》中的编辑服务相关角色。

删除重构 Spaces 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。这样您就没有未被主动监控或维护的未使用实体。但是，您必须先清除服务相关角色的资源，然后才能手动删除它。

> **Note**
>
> 如果在您试图删除资源时重构 Spaces 服务正在使用该角色，则删除操作可能会失败。如果发生这种情况，请等待几分钟后重试。

要删除 AWS ServicerOleformMigation HubreFactSpaces 使用的重构空间资源，请使用重构空间控制台删除资源，或对资源使用删除 API 操作。有关删除 API 操作的更多信息，请参阅重构空间 API 参考.

使用 IAM 手动删除服务相关角色

使用 IAM 控制台，AWS CLI，或者AWS删除 AWS ServiceRoleForMigration HubbreForSpaces 服务相关角色的 API。有关更多信息，请参阅《IAM 用户指南》的删除服务相关角色。

服务相关角色的重构 Spaces 支持的区域

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 区域和终端节点。

AWS Migration Hub 的合规性验证

作为多个项目的一部分，第三方审计员将评估 AWS Migration Hub 的安全性和合规性。AWS合规性计划。其中包括 SOC、PCI、FedRAMP、HIPAA 及其它。

列表AWS特定合规性计划范围内的服务，请参阅合规性计划范围内的 AWS 服务. 有关常规信息，请参阅AWS合规性计划。

您可以使用 AWS Artifact 下载第三方审计报告。有关更多信息，请参阅下载 AWS Artifact 中的报告。

您在使用 ReFration Space 时的合规性责任由您的数据的敏感性、您公司的合规性目标以及适用的法律法规决定。AWS您可以提供以下资源来帮助实现合规性：

- 安全性与合规性 Quick Start 指南 - 这些部署指南讨论了架构注意事项，并提供了在 AWS 上部署基于安全性和合规性的基准环境的步骤。
- 《设计符合 HIPAA 安全性和合规性要求的架构》白皮书 – 此白皮书介绍公司如何使用AWS创建符合 HIPAA 标准的应用程序。
- AWS合规性资源 – 此业务手册和指南集合可能适用于您的行业和位置。
- 《AWS Config 开发人员指南》中的使用规则评估资源 – AWS Config；评估您的资源配置对内部实践、行业指南和法规的遵循情况。
- AWS Security Hub – 此AWS服务提供了AWS中安全状态的全面视图，可帮助您检查是否符合安全行业标准和最佳实践。

使用其他服务

AWS Migration Hub 重构空间目前为预览版，可能会发生变化。

本节介绍其他AWS与重构空间交互的服务。

使用 CloudFormation 创建重构空间资源

AWS Migration Hub 重构空间与AWS CloudFormation，是一项服务，可帮助您对您进行建模和设置AWS这样您只需花较少的时间来创建和管理资源与基础设施。您创建一个模板来描述所有AWS所需的资源（例如环境、应用程序、服务和路由），以及AWS CloudFormation为您预置和配置这些资源。

在您使用时AWS CloudFormation，可重复使用您的模板来不断地重复设置您的 Rreation Space 资源。描述一次您的资源，然后在多个 AWS 账户和区域中反复预置相同的资源。

重构空间和 CloudFormation 模板

要为 Rreation Space 和相关服务设置和配置资源，您必须了解。AWS CloudFormation模板. 模板是 JSON 或 YAML 格式的文本文件。这些模板描述要在 AWS CloudFormation 堆栈中调配的资源。如果您不熟悉 JSON 或 YAML，可以在 AWS CloudFormation Designer 的帮助下开始使用 AWS CloudFormation 模板。有关更多信息，请参阅 AWS CloudFormation 用户指南中的什么是 AWS CloudFormation Designer？。

重构 Spaces 支持在中创建环境、应用程序、服务和路由AWS CloudFormation. 有关更多信息（包括用于环境、应用程序、服务和路由的 JSON 和 YAML 模板示例），请参阅AWS Migration Hub 重构空间中的AWS CloudFormation用户指南.

模板示例

以下示例模板创建了一个 Virtual Private Cloud (VPC) 和重构 Spaces 资源。当你选择部署AWS CloudFormation模板来创建演示重构环境入门对话框中，重构空间控制台将部署以下模板。

Example YAML 重构空间模板

```
AWSTemplateFormatVersion: '2010-09-09'
Description: This creates resources in one account.
Resources:
  VPC:
```

```
    Type: AWS::EC2::VPC
    Properties:
      CidrBlock: 10.2.0.0/16
      Tags:
        - Key: Name
          Value: VpcForRefactorSpaces
  PrivateSubnet1:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref VPC
      AvailabilityZone: !Select [ 0, !GetAZs  '' ]
      CidrBlock: 10.2.1.0/24
      MapPublicIpOnLaunch: false
      Tags:
        - Key: Name
          Value: RefactorSpaces Private Subnet (AZ1)
  PrivateSubnet2:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref VPC
      AvailabilityZone: !Select [ 1, !GetAZs  '' ]
      CidrBlock: 10.2.2.0/24
      MapPublicIpOnLaunch: false
      Tags:
        - Key: Name
          Value: RefactorSpaces Private Subnet (AZ2)
  RefactorSpacesTestEnvironment:
    Type: AWS::RefactorSpaces::Environment
    DeletionPolicy: Delete
    Properties:
      Name: EnvWithMultiAccountServices
      NetworkFabricType: TRANSIT_GATEWAY
      Description: "This is a test environment"
  TestApplication:
    Type: AWS::RefactorSpaces::Application
    DeletionPolicy: Delete
    DependsOn:
      - PrivateSubnet1
      - PrivateSubnet2
    Properties:
      Name: proxytest
      EnvironmentIdentifier: !Ref RefactorSpacesTestEnvironment
      VpcId: !Ref VPC
      ProxyType: API_GATEWAY
```

```
      ApiGatewayProxy:
        EndpointType: "REGIONAL"
        StageName: "admintest"
  AdminAccountService:
    Type: AWS::RefactorSpaces::Service
    DeletionPolicy: Delete
    Properties:
      Name: AdminAccountService
      EnvironmentIdentifier: !Ref RefactorSpacesTestEnvironment
      ApplicationIdentifier: !GetAtt TestApplication.ApplicationIdentifier
      EndpointType: URL
      VpcId: !Ref VPC
      UrlEndpoint:
        Url: "http://aws.amazon.com"
  RefactorSpacesDefaultRoute:
    Type: AWS::RefactorSpaces::Route
    Properties:
      RouteType: "DEFAULT"
      EnvironmentIdentifier: !Ref RefactorSpacesTestEnvironment
      ApplicationIdentifier: !GetAtt TestApplication.ApplicationIdentifier
      ServiceIdentifier: !GetAtt AdminAccountService.ServiceIdentifier
  RefactorSpacesURIRoute:
    Type: AWS::RefactorSpaces::Route
    DependsOn: 'RefactorSpacesDefaultRoute'
    Properties:
      RouteType: "URI_PATH"
      EnvironmentIdentifier: !Ref RefactorSpacesTestEnvironment
      ApplicationIdentifier: !GetAtt TestApplication.ApplicationIdentifier
      ServiceIdentifier: !GetAtt AdminAccountService.ServiceIdentifier
      UriPathRoute:
        SourcePath: "/cfn-created-route"
        ActivationState: ACTIVE
        Methods: [ "GET" ]
```

了解有关的更 CloudFormation

要了解有关 AWS CloudFormation 的更多信息，请参阅以下资源：

- AWS CloudFormation
- AWS CloudFormation 用户指南
- AWS CloudFormation API 参考
- AWS CloudFormation 命令行界面用户指南

使用记录重构 Spaces API 调用AWS CloudTrail

AWS Migration Hub 重构空间与AWS CloudTrail，提供用户、角色或用户所采取操作的记录的服务AWS重构空间中的服务。CloudTrail 将重构空间的所有 API 调用作为事件捕获。捕获的调用包含来自重构 Spaces 控制台的调用和对重构 Spaces API 操作的代码调用。如果您创建了一个跟踪，则可以使 CloudTrail 事件持续传送到 Amazon S3 存储桶（包括重构 Space 的事件）。如果您不配置跟踪记录，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，您可以确定向重构 Spaces 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。

重构 CloudTrail 中的空间信息

在您创建 AWS 账户时，将在该账户上启用 CloudTrail。当重构空间中发生活动时，该活动将记录在 CloudTrail 事件中，并与其他事件一同保存在中AWS中的服务事件事件记录. 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。

要持续记录中的事件，请持续记录AWS创建跟踪（包括重构空间的事件）。通过跟踪，CloudTrail 可将日志文件传送至 Amazon S3 存储桶。默认情况下，在控制台中创建跟踪记录时，此跟踪记录应用于所有亚马逊云科技区域。此跟踪在 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 Amazon S3 存储桶。此外，您可以配置其它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
- 从多个账户接收 CloudTrail 日志文件

CloudTrail 记录所有重构空间操作，并记录在重构 Space API 参考. 例如，对 `CreateEnvironment`、`GetEnvironment` 和 `ListEnvironments` 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。

了解重构 Spaces 日志文件条目

跟踪记录是一种配置，可用于将事件作为日志文件传送到您指定的 Amazon S3 存储桶。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。

使用共享重构空间环境AWS RAM

AWS Migration Hub 重构空间与AWS Resource Access Manager(AWS RAM) 以启用资源共享。AWS RAM是一项服务，允许您与其他方式共享一些重构空间资源。AWS 账户或通过AWS Organizations. 利用 AWS RAM，您可通过创建资源共享 来共享您拥有的资源。资源共享指定要共享的资源以及与之共享资源的使用者。消费者可以包括：

- SPACEAWS 账户中的组织内部或外部AWS Organizations
- 中的所有者组织内部的组织单位AWS Organizations
- 中的整个所有者组织AWS Organizations

有关 AWS RAM 的更多信息，请参阅 AWS RAM 用户指南。

有关共享重构空间环境的更多信息，请参阅第 3 步：共享您的环境 .

AWS Migration Hub 的重构空间的配额

AWS Migration Hub 重构 Space 目前为预览版，可能会发生变化。

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 AWS Migigration Hub 重构空间的配额列表，请参阅重构 Spaces 服务配额.

您也可以通过打开Service Quotas 控制台. 在导航窗格中，选择AWS服务然后选择AWS Migration Hub 重构空间.

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。

“重构空间用户指南” 的文档历史记录

AWS Migration Hub 重构空间目前为预览版，可能会发生变化。

下表介绍了重构空间的文档版本。

update-history-change	update-history-description	update-history-date
首次发布	“重构空间用户指南” 的初始版本	2021 年 11 月 29 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。