亚马逊云科技

用户指南

Amazon IAM Identity Center

Amazon IAM Identity Center: 用户指南

Amazon Web Services 文档中描述的 Amazon Web Services 服务或功能可能因区域而异。要查看适用于中国区域的差异，请参阅 中国的 Amazon Web Services 服务入门 (PDF)。

Table of Contents

IAM Identity Center 是什么？

Amazon IAM Identity Center 是将您的员工用户连接到 Kiro 和 Amazon Quick 等 Amazon 托管应用程序以及其他 Amazon 资源的 Amazon 解决方案。您可以连接现有身份提供者，同步目录中的用户和组，或者直接在 IAM Identity Center 中创建和管理用户。然后，您可以将 IAM Identity Center 用于以下一个或两个用途：

- 用户对应用程序的访问权限
- 用户访问权限 Amazon Web Services 账户

已经在使用 IAM 进行访问了 Amazon Web Services 账户吗？

您无需对当前 Amazon Web Services 账户 的工作流程进行任何更改即可使用 IAM Identity Center 访问 Amazon 托管应用程序。如果您使用与 IAM 的联合身份验证进行 Amazon Web Services 账户 访问，则您的用户可以继续以与往常相同的方式进行访问 Amazon Web Services 账户 ，并且您可以继续使用现有的工作流程来管理该访问权限。

为何使用 IAM Identity Center？

IAM Identity Center 通过以下关键功能简化并简化了员工用户对应用程序或 Amazon Web Services 账户两者的访问。

与 Amazon 托管应用程序集成

Amazon 托管应用程序，例如 Kiro，并 Amazon Redshift 与 IAM 身份中心集成。IAM Identity Center 为 Amazon 托管应用程序提供了用户和群组的通用视图。

跨应用程序的可信身份传播

通过可信身份传播，诸如 Amazon Quick 之类的托 Amazon 管应用程序可以安全地与其他 Amazon 托管应用程序（例如）共享用户的身份， Amazon Redshift 并根据用户的身份授权访问 Amazon 资源。您可以更轻松地审计用户活动，因为 CloudTrail 事件是根据用户和用户启动的操作记录的。这可让您更轻松地用户的访问记录。有关支持的用例的信息，包括 end-to-end配置指南，请参阅可信身份传播应用场景。

一站式为多个 Amazon Web Services 账户分配权限

借助多账户权限，IAM Identity Center 提供了集中向多个 Amazon Web Services 账户中的用户组分配权限的平台。您可以根据常见的工作职能创建权限，或定义满足您安全需求的自定义权限。然

后，您可以将这些权限分配给员工用户，以控制他们对特定的访问权限 Amazon Web Services 账户。

此可选功能仅适用于 IAM Identity Center 的组织实例。

一个联合身份验证点可简化对 Amazon的用户访问权限

通过提供一个联合点，IAM Identity Center 减少了使用多个 Amazon 托管应用程序所需的管理工作和 Amazon Web Services 账户。通过 IAM Identity Center，您只需进行一次联合身份验证，并且在使用 SAML 2.0 身份提供者时只需管理一个证书。IAM Identity Center 为 Amazon 托管应用程序提供用户和群组的通用视图，用于可信身份传播用例，或者当用户与其他人共享 Amazon 资源访问权限时。

有关如何配置常用身份提供者来使用 IAM Identity Center 的信息，请参阅 IAM Identity Center 身份源教程。当前没有身份提供者，可直接在 IAM Identity Center 目录中创建和管理用户。

两种实例类型

IAM Identity Center 支持两种类型的实例：组织实例和账户实例。使用组织实例是最佳做法。它是唯一允许您管理访问权限的实例， Amazon Web Services 账户 建议将其用于应用程序的所有生产用途。组织实例部署在 Amazon Organizations 管理账户中，可让您通过单点管理用户访问权限 Amazon。

账户实例绑定 Amazon Web Services 账户 到启用它们的。仅使用 IAM Identity Center 的账户实例来支持特定 Amazon 托管应用程序的隔离部署。有关更多信息，请参阅 IAM Identity Center 的组织和账户实例。

便于用户访问的 Web 门户

Amazon Web Services 访问门户是一个用户友好的门户网站，可让您的用户无缝访问他们分配的所有应用程序 Amazon Web Services 账户，或两者兼而有之。

多区域访问 Amazon Web Services 账户 和应用程序

当您将您的 IAM Identity Center 实例复制到其他区域时，您的员工可以通过所有启用的区域访问分配给 Amazon Web Services 账户 他们的应用程序和应用程序，并且他们可以在每个启用的区域中部署 Amazon 托管应用程序。

开始使用 IAM Identity Center

以下概述如何开始使用 IAM Identity Center。

1. 启用 IAM Identity Center

   当您启用 IAM Identity Center时，您需要在两种类型的 IAM Identity Center 实例之间进行选择。这些类型是：组织实例（推荐）和账户实例。要了解这些实例类型的不同功能，请参阅 IAM Identity Center 的组织和账户实例。

   > **Note**
   >
   > 启用 IAM Identity Center 后，您可以通过以下任一方式登录并打开 IAM Identity Center 控制台：
   >
   > - 组织实例- Amazon 使用管理账户中具有管理权限的证书登录。
   > - 账户实例-在启用 IAM Identity Center 的 Amazon Web Services 账户 位置 Amazon 使用具有管理权限的证书登录。

2. 将您的身份源连接到 IAM Identity Center

   在 IAM Identity Center 控制台中，确认您要使用的身份源。有关身份源，请参阅如下内容：

   - 外部身份提供者 - 如果您有现有的身份提供者来管理工作用户，可以将其连接到 IAM Identity Center。有关如何配置常用身份提供者来使用 IAM Identity Center 的更多信息，请参阅 IAM Identity Center 身份源教程。
   - Active Directory - 如果您使用 Active Directory 管理工作用户，可以将其连接到 IAM Identity Center。有关更多信息，请参阅 使用 Active Directory 作为身份源。
   - IAM Identity Center - 或者，您可以直接在 IAM Identity Center 中创建和管理用户和组。

   > **Note**
   >
   > 目前，您必须使用外部身份提供商作为身份来源，才能利用您的 IAM Identity Center 的多区域设置。有关此设置的好处的更多信息，请参阅跨多个 IAM 身份中心使用 Amazon Web Services 区域。

3. 设置用户访问权限 Amazon Web Services 账户 （仅限组织实例）

如果您使用的是 IAM Identity Center 的组织实例，则可以向用户或群组分配访问权限 Amazon Web Services 账户，使用权限集向您的用户授予对 Amazon Web Services 账户 和资源的访问权限。

4. 设置用户对应用程序的访问权限

   使用 IAM Identity Center，您可以授予用户对两种类型应用程序的访问权限：

   a. Amazon 托管应用程序

      - 您可以将 IAM 身份中心与 Amazon Q Business 和 Amazon Redshi Amazon CLI ft 等 Amazon 托管应用程序一起使用。有关更多信息，请参阅Amazon 托管应用程序和将 Amazon CLI 与 IAM 身份中心集成。

   b. 客户托管的应用程序

      - 您可将以下任一类型的客户管理型应用程序与 IAM Identity Center 集成：
        - IAM Identity Center 目录中列出的应用程序
        - 您的自定义应用程序
      - 配置应用程序后，您可以分配用户对应用程序的访问权限。

5. 向您的用户提供 Amazon Web Services 访问门户的登录说明

   Amazon Web Services 访问门户是一个门户网站，可让您的用户无缝访问他们分配的所有应用程序 Amazon Web Services 账户，或两者兼而有之。IAM Identity Center 中的新用户必须先激活其用户证书，然后才能登录 Amazon Web Services 访问门户。

   有关如何登录 Amazon Web Services 访问门户的信息，请参阅《Amazon 登录 用户指南》中的登录 Amazon Web Services 访问门户。要了解 Amazon Web Services 访问门户的登录流程，请参阅登录 Amazon Web Services 访问门户。

IAM Identity Center 先决条件和注意事项

您可以使用 IAM Identity Center 仅访问 Amazon 托管应用程序， Amazon Web Services 账户 也可以仅访问托管应用程序，也可以同时使用这两者。如果您使用 IAM 联合身份验证来管理对的访问权限 Amazon Web Services 账户，则可以在使用 IAM 身份中心进行应用程序访问的同时继续这样做。

在启用 IAM Identity Center 之前，请考虑以下事项：

- Amazon 区域

  您首先在单个支持的区域中为 IAM 身份中心的每个实例启用 IAM 身份中心。如果您想使用 IAM Identity Center 进行单点登录以访问 Amazon 账户，则该区域必须对您组织中的所有用户都可访问。

如果您计划使用 IAM Identity Center 访问应用程序，请注意，某些 Amazon 托管应用程序（例如 SageMaker Amazon AI）只能在其支持的区域运行。此外，大多数 Amazon 托管应用程序都要求 IAM Identity Center 在与应用程序相同的区域中可用。这可以通过将它们放在同一个区域来实现，或者在支持的情况下，通过将 IAM Identity Center 实例复制到 Amazon 托管应用程序的所需部署区域来实现。有关更多信息，请参阅 选择的注意事项 Amazon Web Services 区域。

- 仅应用程序访问

  您只能使用 IAM Identity Center，使用您现有的身份提供商访问应用程序（例如 Kiro）。有关更多信息，请参阅 仅将 IAM Identity Center 用于应用程序的用户访问。

  > **Note**
  >
  > 对应用程序资源的访问由应用程序所有者独立管理。

- IAM 角色的配额

  IAM Identity Center 通过创建 IAM 角色，向用户提供账户资源访问权限。有关更多信息，请参阅 IAM Identity Center 所创建 IAM 角色。

- IAM 身份中心和 Amazon Organizations

  Amazon Organizations 建议在 IAM 身份中心中使用，但不是必需的。如果您还没有设置组织，则不必执行此操作。如果您已经设置 Amazon Organizations 并打算将 IAM Identity Center 添加到您的组织，请确保所有 Amazon Organizations 功能都已启用。有关更多信息，请参阅 IAM 身份中心和 Amazon Organizations。

IAM Identity Center Web 界面，包括访问门户和 IAM Identity Center 控制台，旨在供人类通过支持的 Web 浏览器进行访问。兼容的浏览器包括最新的三个版本的微软 Edge、Mozilla Firefox、谷歌浏览器和苹果 Safari。不支持使用非基于浏览器的路径访问这些端点。要以编程方式访问 IAM 身份中心服务，我们建议使用 IAM 身份中心和身份存储 API 参考指南中 APIs 提供的文档。

选择的注意事项 Amazon Web Services 区域

您可以选择单一启用 IAM Identity Center，该中心可供全球用户使用。 Amazon Web Services 区域 这种全球可用性使您可以更轻松地配置用户对多个 Amazon Web Services 账户 和应用程序的访问权限。以下是选择 Amazon Web Services 区域的关键考虑因素。

- 用户的地理位置-当您选择地理位置最接近大多数最终用户的区域时，他们访问 Amazon Web Services 访问门户和 Amazon 托管应用程序（例如 Amazon A SageMaker I）的延迟将更低。

- 选择加入区域（默认情况下禁用的区域）-选择加入区域是 Amazon Web Services 区域 默认禁用的区域。要使用选择加入区域，您必须首先将其启用。有关更多信息，请参阅在选择加入区域中管理 IAM Identity Center。
- 将 IAM 身份中心复制到其他区域 — 如果您计划将 IAM 身份中心复制到其他区域 Amazon Web Services 区域，则必须选择默认启用的区域。有关更多信息，请参阅 跨多个 IAM 身份中心使用 Amazon Web Services 区域。
- 为 Amazon 托管应用程序选择部署区域- Amazon 托管应用程序只能 Amazon Web Services 区域 在可用的区域内运行。许多 Amazon 托管应用程序也只能在启用 IAM Identity Center 或将其复制到的区域（主区域或其他区域）中运行。要确认您的 IAM 身份中心实例是否支持复制到其他区域，请参阅跨多个 IAM 身份中心使用 Amazon Web Services 区域。如果无法进行复制，请考虑在计划使用 Amazon 托管应用程序的区域启用 IAM 身份中心。
- 数字主权 – 数字主权法规或公司政策可能要求强制使用特定 Amazon Web Services 区域。请咨询公司法律部门。
- 身份源 — 如果您使用Amazon Managed Microsoft AD或您在 Act ive Directory (AD) 中的自行管理目录作为身份源，则其主区域必须与您启用 IAM Identity Center 时所在的区域相匹配。 Amazon Web Services 区域
- 使用 Amazon Simple Email Service 的跨区域电子邮件 - 在某些区域，IAM Identity Center 可能会调用不同区域中的 Amazon Simple Email Service（Amazon SES）来发送电子邮件。在这些跨区域调用中，IAM Identity Center 会将特定用户属性发送到其他区域。有关更多信息，请参阅 使用 Amazon SES 的跨区域电子邮件。
- Amazon Control Tower— 如果您从启用 IAM Identity Center 的组织实例 Amazon Control Tower，则该实例将在与 Amazon Control Tower 着陆区相同的区域中创建。

主题

IAM Identity Center 区域数据存储和操作

了解 IAM Identity Center 如何处理跨 Amazon Web Services 区域的数据存储和操作。

了解 IAM Identity Center 如何存储数据

启用 IAM Identity Center 后，您在 IAM 身份中心配置的所有数据都存储在您启用该功能的区域中。这些数据包括目录配置、权限集、应用程序实例和对 Amazon Web Services 账户 应用程序的用户分配。如果使用的是 IAM Identity Center 身份存储，则您在 IAM Identity Center 中创建的所有用户和组也存储在同一区域中。如果您将 IAM Identity Center 实例复制到其他区域，IAM Identity Center 会自动将用户、群组、权限集及其分配以及其他元数据和配置复制到这些区域。

使用 Amazon SES 的跨区域电子邮件

当尝试使用一次性密码（OTP）作为第二个身份验证因素登录时，以及在发生某些身份和凭证管理事件（例如邀请用户设置初始密码、验证电子邮件地址和重置密码）时，中国（北京）区域的 IAM Identity Center 会向中国（宁夏）地区发出跨区域 API 调用以发送电子邮件。在这些跨区域调用中，用户属性包括：

- 电子邮件地址
- 名
- 姓
- Amazon Web Services 账户 in Amazon Organizations
- Amazon Web Services 访问门户网址
- 用户名
- 目录 ID
- 用户 ID

在选择加入区域（默认禁用的区域）中管理 IAM Identity Center

默认情况下 Amazon Web Services 区域 ，大多数 Amazon 服务都启用了操作功能，但是如果您想使用 IAM Iden tity Center，则必须启用以下可选区域：

- 非洲（开普敦）
- 亚太地区（香港）
- 亚太地区（台北）
- 亚太地区（海得拉巴）
- 亚太地区（雅加达）
- 亚太地区（墨尔本）

- 亚太地区（马来西亚）
- 亚太地区（新西兰）
- 亚太地区（泰国）
- 加拿大西部（卡尔加里）
- 欧洲地区（米兰）
- 欧洲（西班牙）
- 欧洲（苏黎世）
- 以色列（特拉维夫）
- 墨西哥（中部）
- 中东（巴林）
- 中东（阿联酋）：

如果您在选择加入区域中部署 IAM Identity Center，须在想要管理对 IAM Identity Center 的访问权限的所有账户中启用该区域。所有账户都需要此配置，无论您是否将在该区域中创建资源。可为组织中的当前账户启用区域，且在添加新账户时必须重复此操作。有关说明，请参阅《Amazon Organizations 用户指南》中的在您的组织中启用或禁用区域。为避免重复这些附加步骤，可选择在默认启用区域部署 IAM Identity Center。

> **Note**
>
> 您的 Amazon 成员账户必须选择与您的 IAM Identity Center 实例所在的选择加入区域相同的区域，这样您就可以从访问门户 Amazon Web Services 访问该 Amazon 成员账户。

在选择加入区域中存储的元数据

当您在选择加入中为管理账户启用 IAM Identity Center 时 Amazon Web Services 区域，任何成员账户的以下 IAM 身份中心元数据都存储在该区域中。

- 帐户 ID
- 帐户名称
- 帐户电子邮件
- IAM 身份中心在成员账户中创建的 IAM 角色的 Amazon 资源名称 (ARNs)

Amazon Web Services 区域 默认情况下处于启用状态

以下区域默认启用，您可以在这些区域中启用 IAM Identity Center。

- 美国东部（俄亥俄州）
- 美国东部（弗吉尼亚州北部）
- 美国西部（俄勒冈州）
- 美国西部（北加利福尼亚）
- 欧洲地区（巴黎）
- 南美洲（圣保罗）
- 亚太地区（孟买）
- 欧洲地区（斯德哥尔摩）
- 亚太地区（首尔）
- 亚太地区（东京）
- 欧洲地区（爱尔兰）
- 欧洲地区（法兰克福）
- 欧洲地区（伦敦）
- 亚太地区（新加坡）
- 亚太地区（悉尼）
- 加拿大（中部）
- 亚太地区（大阪）

切换 Amazon Web Services 区域

我们建议您将 IAM Identity Center 安装在您计划向用户开放的区域，而不是您可能需要禁用的区域。有关更多信息，请参阅 选择的注意事项 Amazon Web Services 区域。

您只能通过删除当前的 IAM Identity Center 实例并在另一个区域中创建实例来切换 IAM Identity Center 区域。如果您已使用现有的 IAM Identity Center 实例启用了 Amazon 托管应用程序，请在删除 IAM Identity Center 之前禁用该应用程序。有关禁用 Amazon 托管应用程序的说明，请参阅禁用 Amazon 托管应用程序。

> **Note**
>
> 如果您正在考虑切换 IAM 身份中心区域以允许在另一个区域部署 Amazon 托管应用程序，请考虑将您的 IAM 身份中心实例复制到该区域。有关更多信息，请参阅 跨多个 IAM 身份中心使用 Amazon Web Services 区域。

新区域中的配置注意事项

须在新的 IAM Identity Center 实例中重新创建用户、组、权限集、应用程序和分配。您可以使用 IAM Identity Center 账户和应用程序分配APIs来获取配置的快照，然后使用该快照在新区域中重建您的配置。切换到其他区域还会更改Amazon Web Services 访问门户的 URL，该门户为您的用户提供了对其 Amazon Web Services 账户 和应用程序的单点登录访问权限。可能还需要通过新实例管理控制台重新创建 IAM Identity Center 的部分配置。

禁用已启用 IAM 身份中心 Amazon Web Services 区域 的地方

如果您禁用安装了 IAM 身份中心的，则也会禁用 IAM 身份中心。 Amazon Web Services 区域 在某个区域禁用 IAM Identity Center 后，该区域的用户将无法单点登录访问 Amazon Web Services 账户 和应用程序。

要在选择加入模式下重新启用 IAM 身份中心 Amazon Web Services 区域，您必须重新启用该区域。由于 IAM Identity Center 必须重新处理所有暂停的事件，因此重新启用 IAM Identity Center 可能需要一些时间。

> **Note**
>
> IAM Identity Center 只能管理允许在中使用的访问权限 Amazon Web Services 区域。 Amazon Web Services 账户 要管理组织中所有账户的访问权限，请在管理账户中启用 IAM Identity Center，该账户会自动激活以与 IAM Identity Center 配合使用。 Amazon Web Services 区域

有关启用和禁用的更多信息 Amazon Web Services 区域，请参阅《Amazon 一般参考》 Amazon Web Services 区域中的 “管理”。

仅将 IAM Identity Center 用于应用程序的用户访问

您可以使用 IAM 身份中心让用户访问诸如 Kiro 之类的应用程序 Amazon Web Services 账户，或两者兼而有之。可连接现有身份提供者，同步目录中的用户和组，或者直接在 IAM Identity Center 中创

建和管理用户。有关如何将现有身份提供者连接至 IAM Identity Center 的信息，请参阅 IAM Identity Center 身份源教程。

已经在使用 IAM 进行访问了 Amazon Web Services 账户吗？

您无需对当前 Amazon Web Services 账户 的工作流程进行任何更改即可使用 IAM Identity Center 访问 Amazon 托管应用程序。如果您使用与 IAM 的联合身份验证进行 Amazon Web Services 账户 访问，则您的用户可以继续以与往常相同的方式进行访问 Amazon Web Services 账户 ，并且您可以继续使用现有的工作流程来管理该访问权限。

IAM Identity Center 所创建 IAM 角色

当您将用户分配到 Amazon 账户时，IAM Identity Center 会创建 IAM 角色来向用户授予资源访问权限。

当您分配权限集时，IAM Identity Center 会在每个账户中创建由 IAM Identity Center 控制的相应 IAM 角色，并将权限集中指定的策略附加给这些角色。IAM Identity Center 管理角色，并允许您定义的授权用户使用 Amazon Web Services 访问门户或代入该角色。 Amazon CLI在您修改权限集时，IAM Identity Center 会确保相应的 IAM 策略和角色也相应更新。将您的 IAM 身份中心实例复制到其他区域不会影响现有的 IAM 角色，也不会创建新的 IAM 角色。

> **Note**
>
> 权限集不用于向应用程序授予权限。

如果您已经在中配置了 IAM 角色 Amazon Web Services 账户，我们建议您检查您的账户是否已接近 IAM 角色的配额。每个账户的 IAM 角色默认配额为 1000 个角色。有关更多信息，请参阅 IAM 对象限额。

如果您已接近此限额，可以考虑申请增加限额。否则，当您为已超过 IAM 角色限额的帐户预置权限集时，IAM Identity Center 可能会遇到问题。有关如何请求提高限额的信息，请参阅 Service Quotas 用户指南中的请求增加限额。

> **Note**
>
> 如果您正在查看已使用 IAM Identity Center 账户中的 IAM 角色，您可能会注意到以“AWSReservedSSO_” 开头的角色名称。这些角色是 IAM Identity Center 服务在帐户中创建的角色，它们来自向帐户分配权限集。

IAM 身份中心和 Amazon Organizations

Amazon Organizations 建议在 IAM 身份中心中使用，但不是必需的。如果您还没有设置组织，则不必执行此操作。启用 IAM Identity Center 时，您将选择是否使用启用该服务 Amazon Organizations。当你建立组织时，建立 Amazon Web Services 账户 该组织的用户将成为该组织的管理帐户。此时， Amazon Web Services 账户 的根用户将是组织管理账户的所有者。您邀请加入组织的任何其他 Amazon Web Services 账户 均为成员账户。管理账户将创建组织资源、组织单位，以及管理成员账户的策略。权限将通过管理账户委派给成员账户。

> **Note**
>
> 我们建议您使用启用 IAM 身份中心 Amazon Organizations，这将创建 IAM 身份中心的组织实例。组织实例是我们推荐的最佳实践，因为它支持 IAM Identity Center 的所有功能，并提供集中管理能力。有关更多信息，请参阅 IAM Identity Center 的组织实例。

如果您已经设置 Amazon Organizations 并打算将 IAM Identity Center 添加到您的组织，请确保所有 Amazon Organizations 功能都已启用。在创建组织时，默认情况下将启用所有功能。有关更多信息，请参阅《Amazon Organizations 用户指南》中的启用企业中的所有功能。

要启用 IAM Identity Center 的组织实例，您必须以拥有 Amazon Organizations 管理凭证的用户或根用户身份登录管理账户（除非不存在其他管理用户，否则不建议这样做）登录管理账户。 Amazon Web Services 管理控制台 有关更多信息，请参阅《Amazon Organizations 用户指南》中的创建和管理 Amazon 组织。

使用 Amazon Organizations 成员账户的管理证书登录后，您可以启用 IAM Identity Center 的账户实例。账户实例的功能有限，并且绑定到单个 Amazon 账户。

IAM Identity Center 的组织和账户实例

实例是对 IAM Identity Center 的单次部署。IAM Identity Center 有两种可用实例：组织实例和账户实例。

- 组织实例（推荐）

  您在 Amazon Organizations 管理账户中启用的 IAM 身份中心实例。组织实例支持 IAM Identity Center 的所有功能。为减少管理节点数量，建议您部署组织实例而非账户实例。
- 账户实例

绑定到单 Amazon Web Services 账户个 IAM Identity Center 的实例，并且仅在启用该实例的 Amazon Web Services 账户 和 Amazon 区域内可见。账户实例适用于更简单的单账户场景。您可以通过以下任一途径启用账户实例：

- Amazon Web Services 账户 而且不是由管理的 Amazon Organizations
- 中的会员账户 Amazon Organizations

Amazon Web Services 账户 可以启用 IAM 身份中心的类型

要启用 IAM Identit Amazon Web Services 管理控制台 y Center，请使用以下凭证之一登录，具体取决于您要创建的实例类型：

- 您的 Amazon Organizations 管理账户（推荐）— 创建 IAM Identity Center 的组织实例所必需的。使用组织实例，您可以在整个组织内实现多账户权限和应用程序分配。
- 您的 Amazon Organizations 成员账户 — 用于创建 IAM Identity Center 的账户实例，以便在该成员账户中启用应用程序分配。一个组织中可以存在一个或多个具有成员级实例的账户。
- 独立版 Amazon Web Services 账户 — 用于创建 IAM Identity Center 的组织实例或账户实例。独立版 Amazon Web Services 账户 不是由管理的 Amazon Organizations。您只能将一个 IAM Identity Center 实例与独立实例关联， Amazon Web Services 账户 并将该实例用于该独立实例中的应用程序分配 Amazon Web Services 账户。

使用以下表格比较实例类型提供的功能：

能力	Amazon Organizations 管理账户中的实例（推荐）	成员账户中的实例	独立版中的实例 Amazon Web Services 账户
管理用户	✓是	✓是	✓是
Amazon Web Services 访问门户，可通过单点登录访问您的 Amazon 托管应用程序	✓是	✓是	✓是

能力	Amazon Organizations 管理账户中的实例（推荐）	成员账户中的实例	独立版中的实例 Amazon Web Services 账户
OAuth 2.0 (OIDC) 客户管理的应用程序	✓是	✓是	✓是
多账户权限	✓是	✗否	✗否
Amazon Web Services 访问门户，通过单点登录即可访问您的 Amazon Web Services 账户	✓是	✗否	✗否
SAML 2.0 客户管理型应用程序	✓是	✗否	✗否
委派管理员可以管理实例	✓是	✗否	✗否
使用客户管理的 KMS 密钥进行静态加密	✓是	✗否	✗否
将 IAM 身份中心复制到其他区域	✓是	✗否	✗否

有关 Amazon 托管应用程序和 IAM 身份中心的更多信息，请参阅Amazon 可与 IAM 身份中心配合使用的托管应用程序。

主题

- IAM Identity Center 的组织实例
- IAM Identity Center 的账户实例
- 删除 IAM Identity Center 实例

IAM Identity Center 的组织实例

当你同时启用 IAM 身份中心时 Amazon Organizations，你就是在创建 IAM Identity Center 的组织实例。您的组织实例必须在管理账户中启用，您可以通过单个组织实例集中管理用户和组的访问权限。Amazon Organizations中的每个管理账户只能有一个组织实例。

如果您在 2023 年 11 月 15 日之前启用了 IAM Identity Center，则您已经拥有一个 IAM Identity Center 组织实例。

要启用 IAM Identity Center 的组织实例，请参阅启用 IAM Identity Center 的实例。

何时使用组织实例

组织实例是启用 IAM Identity Center 的主要方法，通常情况下，建议使用组织实例。组织实例具有以下优势：

- 支持 IAM Identity Center 的所有功能 — 包括管理组织 Amazon Web Services 账户 中多个用户的权限、分配对客户托管应用程序的访问权限以及多区域复制。
- 减少管理点的数量 - 组织实例只有一个管理点，即管理账户。我们建议您启用组织实例，而不是账户实例，以减少管理点的数量。
- 集中控制账户实例的创建 — 只要您尚未在可选区域（Amazon Web Services 区域 默认情况下处于禁用状态）向组织部署 IAM Identity Center 实例，您就可以控制是否可以由组织中的成员账户创建账户实例。

有关启用 IAM Identity Center 组织实例的说明，请参阅 启用 IAM Identity Center 的实例。

IAM Identity Center 的账户实例

使用 IAM Identity Center 的账户实例，您可以部署支持的 Amazon 托管应用程序和基于 OIDC 的客户托管应用程序。账户实例利用 IAM Identity Center 员工身份和访问门户功能 Amazon Web Services 账户，支持在单个账户中隔离部署应用程序。

账户实例绑定到单个 Amazon Web Services 账户 账户，仅用于管理用户和群组对同一个账户中支持的应用程序的访问权限 Amazon Web Services 区域。每个账户只能使用一个实例 Amazon Web Services 账户。您可以通过以下任一方式创建账户实例：中的成员账户 Amazon Organizations 或不由管理 Amazon Web Services 账户 的独立账户 Amazon Organizations。

有关启用 IAM Identity Center 账户实例的说明，请参阅 启用 IAM Identity Center 的实例 并选择账户选项卡。

何时使用账户实例

在大多数情况下，建议使用组织实例。仅当以下任一场景适用时才使用账户实例：

- 您想对支持的 Amazon 托管应用程序进行临时试用，以确定该应用程序是否适合您的业务需求。
- 您没有计划在整个组织中采用 IAM Identity Center，但您希望支持一个或多个 Amazon 托管应用程序。
- 您拥有一个 IAM Identity Center 组织实例，但希望向一组独立的用户部署受支持的 Amazon 托管应用程序，这些用户需要与组织实例中的用户区分开来。
- 您无法控制您所在的 Amazon 组织。例如，第三方控制管理您的 Amazon 组织 Amazon Web Services 账户。

> **Important**
>
> 如果您计划使用 IAM Identity Center 支持多个账户中的应用程序，请使用组织实例。账户实例不支持此使用案例。

Amazon 支持账户实例的托管应用程序

请参阅Amazon 可与 IAM 身份中心配合使用的托管应用程序以了解哪些 Amazon 托管应用程序支持 IAM Identity Center 的账户实例。使用您的 Amazon 托管应用程序验证创建账户实例的可用性。

成员账户的可用性限制

要在 Amazon Organizations 成员账户中部署 IAM Identity Center 的账户实例，必须满足以下条件之一：

- 组织中没有 IAM Identity Center 的组织实例。
- 您组织中有一个 IAM Identity Center 的组织实例，并且实例管理员已允许创建 IAM Identity Center 的账户实例（适用于 2023 年 11 月 15 日之后创建的组织实例）。
- 组织中有一个 IAM Identity Center 的组织实例，并且实例管理员已手动允许组织中的成员账户创建 IAM Identity Center 的账户实例（适用于 2023 年 11 月 15 日之后创建的组织实例）。有关说明，请参阅允许在成员账户中创建账户实例。

除了满足任一上述条件，还须满足以下所有条件：

- 管理员并未创建服务控制策略阻止成员账户创建账户实例。
- 无论在哪个 Amazon Web Services 区域，您尚未在同一账户中拥有 IAM Identity Center 实例。
- 您正在可用 IAM 身份中心 Amazon Web Services 区域 的地方工作。有关区域的更多信息，请参阅 IAM Identity Center 区域数据存储和操作。

账户实例注意事项

账户实例专为特殊使用案例而设计，并提供组织实例的部分功能。创建账户实例之前，请考虑以下事项：

- 账户实例不支持权限集，因此不支持对 Amazon Web Services 账户的访问。
- 您无法将账户实例转换为或合并到组织实例。
- 只有特定的 Amazon 托管应用程序支持账户实例。
- 将账户实例用于仅在单个账户中使用应用程序的孤立用户，并在所使用应用程序的生命周期内使用。
- 附加到账户实例的应用程序必须始终附加到该账户实例，直到您删除该应用程序及其资源为止。
- 账户实例必须保留在创建 Amazon Web Services 账户 的地方。

允许在成员账户中创建账户实例

如果您在 2023 年 11 月 15 日之前启用了 IAM Identity Center，您就已经拥有了 IAM Identity Center 组织实例，成员账户创建账户实例的功能默认被禁用。您可以通过在 IAM Identity Center 控制台中启用账户实例功能，选择成员账户是否可以创建账户实例。

要允许组织中的成员账户创建账户实例

> **Important**
>
> 为成员账户启用 IAM Identity Center 账户实例属于一次性操作。这表示此操作无法逆转。启用后，您可以通过创建服务控制策略（SCP）限制账户实例创建。有关说明，请参阅通过服务控制策略控制账户实例的创建。

1. 打开 IAM Identity Center 控制台。
2. 选择设置，然后选择管理选项卡。
3. 在 IAM Identity Center 账户实例部分，选择启用 IAM Identity Center 账户实例。

4. 在启用 IAM Identity Center 的账户实例对话框中，选择启用，以确认您希望允许组织中的成员账户创建账户实例。

使用服务控制策略控制账户实例创建

成员账户创建账户实例的权限取决于您启用 IAM Identity Center 的时间：

- 2023 年 11 月之前 – 您必须允许在成员账户中创建账户实例，这是一个无法撤销的操作。
- 2023 年 11 月 15 日之后 - 默认情况下，成员账户可以创建账户实例。

无论哪种情况，您都可以使用服务控制策略 (SCPs) 来：

- 阻止所有成员账户创建账户实例。
- 仅允许特定成员账户创建账户实例。

阻止账户实例

使用以下过程生成阻止成员账户创建 IAM Identity Center 账户实例的 SCP。

1. 打开 IAM Identity Center 控制台。
2. 在控制面板的中央管理部分，选择阻止账户实例按钮。
3. 在附加 SCP 以阻止创建新账户实例对话框中，会为您提供一个 SCP。复制该 SCP，并选择前往 SCP 控制面板按钮。您将被引导到Amazon Organizations 控制台创建 SCP 或将其作为语句附加到现有 SCP。 SCPs 是一项功能 Amazon Organizations。有关附加 SCP 的说明，请参阅 Amazon Organizations 用户指南中的附加和分离服务控制策略。

限制账户实例

该策略不会阻止所有账户实例的创建，而是拒绝任何为*"<ALLOWED-ACCOUNT-ID>"*占位符中明确列出的账户以 Amazon Web Services 账户 外的所有账户创建 IAM Identity Center 账户实例的尝试。

Example：用于限制账户实例创建的拒绝策略

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement" : [
        {
            "Sid": "DenyMemberAccountInstances",
            "Effect": "Deny",
            "Action": "sso:CreateInstance",
            "Resource": "*",
            "Condition": {
                 "StringNotEquals": {
                    "aws:PrincipalAccount": ["<ALLOWED-ACCOUNT-ID>"]
                }
            }
        }
    ]
}
```

- 将 ["<ALLOWED-ACCOUNT-ID>"] 替换为您想要允许创建 IAM Identity Center 账户实例的实际 Amazon Web Services 账户 ID。
- 您可以按数组格式列出多个允许的账户 IDs ：["111122223333", "444455556666"]。
- 将此策略附加到您的组织 SCP，以强制执行对 IAM Identity Center 账户实例创建的集中控制。

  有关附加 SCP 的说明，请参阅 Amazon Organizations 用户指南中的附加和分离服务控制策略。

删除 IAM Identity Center 实例

删除 IAM Identity Center 实例后，该实例中的所有数据都将被删除且无法恢复。下表描述了根据在 IAM Identity Center 中配置的目录类型删除了哪些数据。

哪些数据会被删除	连接的目录- Amazon Managed Microsoft AD、AD Connector 或外部身份提供商	IAM Identity Center 身份存储	
您为其配置的所有权限集 Amazon Web Services 账户	⊙是	⊙是	

哪些数据会被删除	连接的目录- Amazon Managed Microsoft AD、AD Connector 或外部身份提供商	IAM Identity Center 身份存储	
您在 IAM Identity Center 中配置的所有应用程序	⊘是	⊘是	
您为其配置的所有用户分配 Amazon Web Services 账户 和应用程序	⊘是	⊘是	
目录或存储中的所有用户和组	不适用	⊘是	

如果您将 IAM Identity Center 实例复制到其他区域，则必须先移除这些区域，然后再删除该实例。

按照下列步骤删除 IAM Identity Center 实例。

删除 IAM Identity Center 实例

1. 打开 IAM Identity Center 控制台。
2. 在左侧导航窗格中，选择设置。
3. 在“设置 ”页面上，选择“管理” 选项卡。
4. 在“删除 IAM Identity Center 配置”部分中，选择“删除”。
5. 在“删除 IAM Identity Center 配置”对话框中，选中每个复选框，以确认您知道自己的数据将被删除。在文本框中键入您的 IAM Identity Center 实例，然后选择“确认”。

启用 IAM Identity Center

启用 IAM Identity Center 时，您可以选择要启用的 Amazon IAM Identity Center 实例类型。服务的实例是在您的 Amazon 环境中对服务的单一部署。IAM Identity Center 有两种可用实例：组织实例和账户实例。您可以启用的实例类型取决于您登录的账户类型。

以下列表指明了您可以为每种 Amazon Web Services 账户类型启用的 IAM Identity Center 实例类型：

- 您的 Amazon Organizations 管理账户（推荐）— 创建 IAM Identity Center 的组织实例所必需的。使用组织实例，您可以在整个组织内实现多账户权限和应用程序分配。您可以将此实例类型复制到其他区域，以增强账户访问的灵活性以及选择 Amazon 应用程序部署区域的灵活性。
- 您的 Amazon Organizations 成员账户 — 用于创建 IAM Identity Center 的账户实例，以便在该成员账户中启用应用程序分配。一个组织中可以存在一个或多个具有成员级实例的账户。
- 独立版 Amazon Web Services 账户 — 用于创建 IAM Identity Center 的组织实例或账户实例。独立版 Amazon Web Services 账户 不是由管理的 Amazon Organizations。您只能将一个 IAM Identity Center 实例与独立实例关联， Amazon Web Services 账户 并将该实例用于该独立实例中的应用程序分配 Amazon Web Services 账户。

> **Important**
>
> 组织管理账户可以通过使用服务控制策略来控制组织成员账户是否可以创建 IAM Identity Center 的账户实例。
> 如果您使用免费套餐账户，则创建 Amazon 组织会自动将您的账户升级为带 pay-as-you-go 定价的付费套餐。您的免费套餐积分将立即过期。有关更多信息，请参阅 Amazon 免费套餐 FAQs。

有关不同实例类型提供的不同功能的比较，请参阅 IAM Identity Center 的组织和账户实例。

在启用 IAM Identity Center 之前，我们建议您查看 IAM Identity Center 先决条件和注意事项。

启用 IAM Identity Center 的实例

选择与您要启用的 IAM Identity Center 实例类型对应的选项卡（组织实例或账户实例）：

Organization (recommended)

1. 请执行以下一项操作，登录 Amazon Web Services 管理控制台。
   - Amazon （root 用户）新手 — 选择 R oot 用户并输入您的 Amazon Web Services 账户 电子邮件地址，以账户所有者身份登录。在下一页上，输入您的密码。
   - 已使用 Amazon 独立版 Amazon Web Services 账户 （IAM 证书）— 使用具有管理权限的 IAM 凭证登录。
   - 已在使用 Amazon Organizations （IAM 证书）-使用您的管理账户证书登录。
2. 打开 IAM Identity Center 控制台。
3. （可选）如果您想使用客户托管的 KMS 密钥进行静态加密，而不是使用默认的 Amazon 托管密钥，请在用于加密静态的 IAM Identity Center 数据的密钥部分中配置客户托管密钥。有关更多信息，请参阅在中实现客户托管的 KMS 密钥 Amazon IAM Identity Center。

   > **Important**
   >
   > 仅当您已配置使用 KMS 客户自主管理型密钥的必要权限后，才执行此步骤。如果没有适当的权限，此步骤可能会失败或中断 IAM Identity Center 管理和 Amazon 托管应用程序。

4. 在启用 IAM Identity Center下，选择启用。
5. 在结合 Amazon Organizations启用 IAM Identity Center 页面，查看相关信息后选择启用完成操作。

   > **Note**
   >
   > Amazon Organizations 只能在单个 Amazon 区域启用 IAM 身份中心。启用 IAM Identity Center 后，如果您需要更改启用 IAM Identity Center 的区域，则必须删除当前实例并在另一个区域中创建实例。

启用组织实例后，我们建议您执行以下步骤来完成环境设置：

- 确认您正在使用所选择的身份源。若已有分配的身份源，可以继续使用。有关更多信息，请参阅确认 IAM Identity Center 中的身份源。
- 将成员账户注册为委托管理员。有关更多信息，请参阅 委派管理。

- IAM 身份中心为您提供 Amazon 资源访问门户。如果您使用下一代防火墙 (NGFW) 或安全 Web 网关 (SWG) 等 Web 内容过滤解决方案来筛选对特定 Amazon 域或 URL 端点的访问权限，请参阅。更新防火墙和网关以允许访问 Amazon Web Services 访问门户

Account

1. 请执行以下一项操作，登录 Amazon Web Services 管理控制台。
   - Amazon （root 用户）新手 — 选择 R oot 用户并输入您的 Amazon Web Services 账户 电子邮件地址，以账户所有者身份登录。在下一页上，输入您的密码。
   - 已在使用 Amazon （IAM 证书）— 使用具有管理权限的 IAM 凭证登录。
   - 已使用 Amazon Organizations （IAM 证书）-使用您的成员账户管理证书登录。
2. 打开 IAM Identity Center 控制台。
3. 如果您是新手 Amazon 或拥有独立版 Amazon Web Services 账户，请在启用 IAM 身份中心下选择启用。

   您将看到结合 Amazon Organizations启用 IAM Identity Center 页面。我们推荐此选项，但非强制要求。

   选择链接启用 IAM Identity Center 的账户实例。
4. 如果您是 Amazon Organizations 成员账户的管理员，请在启用 IAM Identity Center 的账户实例下，选择启用账户实例。
5. 在启用 IAM Identity Center 账户实例页面上，查看信息并可选地添加要与此账户实例关联的标签。然后选择启用以完成该过程。

   > **Note**
   >
   > 如果您的 Amazon 账户是组织的成员，那么您启用 IAM Identity Center 账户实例的能力可能会受到限制。
   >
   > - 如果您的组织在 2023 年 11 月 15 日之前启用了 IAM Identity Center，成员账户创建账户实例的功能默认禁用，需由组织管理账户手动启用。
   > - 如果您的组织在 2023 年 11 月 15 日之后启用了 IAM Identity Center，成员账户创建账户实例的功能默认启用。但组织可通过服务控制策略禁止创建 IAM Identity Center 账户实例。

有关更多信息，请参阅the section called “允许在成员账户中创建账户实例”和the section called “SCPs 用于创建账户实例”。

确认 IAM Identity Center 中的身份源

您在 IAM Identity Center 中的身份源定义了用户和组的管理位置。启用 IAM Identity Center 后，请确认您使用的是您选择的身份源。若已有分配的身份源，可以继续使用。

如果您已经在管理 Active Directory 或外部 IdP 中的用户和组，我们建议您在启用 IAM Identity Center 和选择身份源时考虑连接此身份源。在默认 Identity Center 目录中创建任何用户和组并进行任何分配之前，应先完成此操作。

如果您已经在 IAM Identity Center 中的一个身份源中管理用户和组，则更改为其他身份源可能会移除您在 IAM Identity Center 中配置的所有用户和组分配。如果发生这种情况，所有用户（包括 IAM Identity Center 中的管理用户）都将失去对其 Amazon Web Services 账户 和应用程序的单点登录访问权限。有关更多信息，请参阅 更改身份源的注意事项。

确认您的身份来源

1. 打开 IAM Identity Center 控制台。
2. 在控制面板页面的推荐设置步骤部分下方，选择确认身份源。您也可以通过选择设置，然后选择身份源选项卡，访问此页面。
3. 如果您想保留已分配的身份源，则无需执行任何操作。如果您想对其做出更改，请选择操作，然后选择更改身份源。

您可以选择以下一个选项作为身份源：

Identity Center 目录

> 您首次启用 IAM Identity Center 后，IAM Identity Center 会自动配置 Identity Center 目录作为您的默认身份源。如果您尚未使用其他外部身份提供商，则可以开始创建您的用户和群组，并分配他们对您的 Amazon Web Services 账户 和应用程序的访问级别。有关使用此身份源的教程，请参阅 使用默认 IAM Identity Center 目录配置用户访问权限。

Active Directory

如果您已经在使用 Amazon Directory Service 或中的自管理 Amazon Managed Microsoft AD 目录中管理用户和群组Active Directory (AD)，我们建议您在启用 IAM Identity Center 时连接该目录。请勿在默认的 Identity Center 目录中创建任何用户和组。IAM Identity Center 使用 Amazon Directory Service 提供的连接将用户、组和成员资格信息从 Active Directory 中的源目录同步到 IAM Identity Center 身份存储。有关更多信息，请参阅 Microsoft AD 目录。

> **Note**
>
> IAM Identity Center 不支持将 SAMBA4基于的 Simple AD 作为身份源。

外部身份提供商

对于外部身份提供商 (IdPs)，例如Okta或Microsoft Entra ID，您可以使用 IAM Identity Center IdPs 通过安全断言标记语言 (SAML) 2.0 标准对身份进行身份验证。SAML 协议不提供查询 IdP 以了解用户和组的方法。您可以通过将这些用户和组预置到 IAM Identity Center，使 IAM Identity Center 了解这些用户和组。在 IdP 支持的情况下，您可以使用跨域身份管理 (SCIM) v2.0 协议系统将用户和组的信息从 IdP 自动预置（同步）到 IAM Identity Center。如果不支持，您可以在 IAM Identity Center 手动输入用户名、电子邮件地址和组，手动预置用户和组。

有关设置身份源的详细说明，请参阅 IAM Identity Center 身份源教程。

> **Note**
>
> 如果您计划使用外部身份提供商，请注意将由外部 IdP（而不是 IAM Identity Center）管理多重身份验证 (MFA) 设置。不支持外部身份提供者使用 IAM Identity Center 中的 MFA。有关更多信息，请参阅 提示用户完成 MFA。

> **Note**
>
> 如果您计划将 IAM Identity Center 复制到其他区域，则需要配置外部身份提供商。有关包括先决条件在内的更多详细信息，请参阅跨多个 IAM 身份中心使用 Amazon Web Services 区域。

更新防火墙和网关以允许访问 Amazon Web Services 访问门户

Amazon Web Services 访问门户为用户提供单点登录访问所有 Amazon Web Services 账户 和最常用的云应用程序，例如 Office 365、Concur、Salesforce 等。只需在门户中选择 Amazon Web Services 账户 或应用程序图标即可快速启动多个应用程序。

> **Note**
>
> Amazon 托管应用程序与 IAM Identity Center 集成并用于身份验证和目录服务，但可能不会使用 Amazon Web Services 访问门户进行应用程序访问。

如果您使用网络内容过滤解决方案（例如下一代防火墙 (NGFW) 或安全 Web 网关 (SWG)）来筛选对特定 Amazon 域或 URL 端点的访问，则必须将与访问门户关联的域和 URL 端点列入许可名单。Amazon Web Services

以下列表提供了要添加到您的网页内容过滤解决方案许可名单中的双栈域名和网址端点。 IPv4

IPv4 允许名单

- *[Directory ID or alias]*.awsapps.com
- *[Identity Center instance ID]*.*[Region]*.portal.amazonaws.com
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.amazonaws.com
- *.sso.amazonaws.com
- *.sso.*[Region]*.amazonaws.com
- *.sso-portal.*[Region]*.amazonaws.com
- *[Region]*.prod.pr.panorama.console.api.aws/panoramaroute
- *[Region]*.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com

双栈允许列表

- *[Identity Center instance ID]*.portal.*[Region]*.app.aws
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.api.aws
- sso.*[Region]*.api.aws
- portal.sso.*[Region]*.api.aws
- *[Region]*.sso.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- cdn.us-east-1.threat-mitigation.aws.amazon.com
- us-east-1.threat-mitigation.aws.amazon.com
- amcs-captcha-prod-us-east-1.s3.dualstack.us-east-1.amazonaws.com

合并允许列表（IPv4 + 具有向后兼容性的双堆栈）

- *[Directory ID or alias]*.awsapps.com
- *[Identity Center instance ID]*.*[Region]*.portal.amazonaws.com
- *[Identity Centers instance ID]*.portal.*[Region]*.app.aws
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.amazonaws.com
- oidc.*[Region]*.api.aws
- *.sso.amazonaws.com
- *.sso.*[Region]*.amazonaws.com
- sso.*[Region]*.api.aws
- *.sso-portal.*[Region]*.amazonaws.com
- portal.sso.*[Region]*.api.aws

- *[Region]*.prod.pr.panorama.console.api.aws/panoramaroute
- *[Region]*.signin.aws
- *[Region]*.sso.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com
- cdn.us-east-1.threat-mitigation.aws.amazon.com
- us-east-1.threat-mitigation.aws.amazon.com
- amcs-captcha-prod-us-east-1.s3.dualstack.us-east-1.amazonaws.com

将域和 URL 端点列入许可列表的注意事项

除了 Amazon Web Services 访问门户的许可名单要求外，您使用的其他服务和应用程序可能还需要将域列入许可名单。

- 要从您的访问 Amazon Web Services 账户门户 Amazon Web Services 访问 Amazon Web Services 管理控制台、和 IAM Identity Center 控制台，您必须将其他域列入许可名单。有关 Amazon Web Services 管理控制台 域名列表，请参阅《Amazon Web Services 管理控制台 入门指南》中的疑难解答。
- 要从您的访问门户 Amazon Web Services 访问 Amazon 托管应用程序，您必须将其各自的域列入许可名单。如需有关指导，请参阅相应服务文档。
- 如果您使用外部软件，例如外部软件 IdPs （ 例如Okta和Microsoft Entra ID ），则需要将其域名包括在许可名单中。

IAM Identity Center 身份源教程

您可以将 Amazon Organizations 管理账户中的现有身份源连接到 IAM Identity Center 的组织实例。如果没有现有身份提供者，可直接在默认 IAM Identity Center 目录中创建并管理用户。每个组织有一个身份源。

本节中的教程介绍如何使用常用身份源设置 IAM Identity Center 的组织实例、如何创建管理用户，以及如何使用 IAM Identity Center 管理对权限集的访问权限 Amazon Web Services 账户、创建和配置权限集。如果仅将 IAM Identity Center 用于应用程序访问，则无需使用权限集。

这些教程并未介绍如何设置 IAM Identity Center 账户实例。可使用账户实例为应用程序分配用户和组，但不能将此实例类型用于管理用户对 Amazon Web Services 账户的访问权限。有关更多信息，请参阅 IAM Identity Center 的账户实例。

> **Note**
>
> 在开始这些教程之前，首先启用 IAM Identity Center。有关更多信息，请参阅 启用 IAM Identity Center。

主题

使用 Active Directory 作为身份源

如果您使用 Amazon Directory Service 或在 A Amazon Managed Microsoft AD ctive Directory (AD) 中管理您的目录中的用户，则可以更改您的 IAM Identity Center 身份源以使用这些用户。我们建议您在

启用 IAM Identity Center 并选择身份源时，考虑连接此身份源。在默认 Identity Center 目录中创建任何用户和组之前执行此操作将有助于避免在以后更改身份源时所需的额外配置。

要使用 Active Directory 作为身份源，您的配置必须满足以下先决条件：

- 如果您正在使用 Amazon Managed Microsoft AD，则必须在设置 Amazon Managed Microsoft AD 目录的同一 Amazon Web Services 区域 位置启用 IAM 身份中心。IAM Identity Center 会将分配数据存储在与目录相同的区域中。要管理 IAM Identity Center，您可能需要切换到配置 IAM Identity Center 的区域。另外，请注意， Amazon Web Services 访问门户使用的访问网址与您的目录相同。
- 使用驻留在管理帐户中的 Active Directory：

  您必须在中设置现有 AD Con Amazon Managed Microsoft AD nector 或目录 Amazon Directory Service，并且该目录必须位于您的 Amazon Organizations 管理账户中。一次只能在 Amazon Managed Microsoft AD 连接一个 AD Connector 目录或一个目录。如果您需要支持多个域或林，请使用 Amazon Managed Microsoft AD。有关更多信息，请参阅:

  - 将目录连接 Amazon Managed Microsoft AD 到 IAM 身份中心
  - 将 Active Directory 中的自行管理目录连接到 IAM Identity Center
- 使用驻留在委派管理员账户中的 Active Directory：

  如果您计划启用 IAM 身份中心委托管理员并使用 Active Directory 作为您的 IAM 身份中心身份源，则可以使用位于委托管理员账户中的现有 AD Connector 或 Amazon Managed Microsoft AD Amazon 目录中设置的目录。

  如果您决定将 IAM Identity Center 身分源从任何其他源更改为 Active Directory，或者将其从 Active Directory 更改为任何其他源，则该目录必须驻留在 IAM Identity Center 委派管理员成员账户（如果存在）中（归该账户所有）；否则，它必须位于管理账户中。

本教程将指导您完成使用 Active Directory 作为 IAM Identity Center 身份源的基本设置。

步骤 1：连接 Active Directory 并指定用户

如果您已经在使用 Active Directory，以下主题可帮助您准备好将目录连接到 IAM Identity Center。

> **Note**
>
> 如果您计划连接 Active Directory 中的 Amazon Managed Microsoft AD 目录或自管理目录，但未将 RADIUS MFA Amazon Directory Service与一起使用，请在 IAM 身份中心启用 MFA。

Amazon Managed Microsoft AD

1. 请查看 Microsoft AD 目录 中的指南。
2. 按照 将目录连接 Amazon Managed Microsoft AD 到 IAM 身份中心 中的步骤操作。
3. 配置 Active Directory 以将您要向其授予管理权限的用户同步到 IAM Identity Center。有关更多信息，请参阅 将管理用户同步到 IAM Identity Center 中。

Active Directory 中的自行管理目录

1. 请查看 Microsoft AD 目录 中的指南。
2. 按照 将 Active Directory 中的自行管理目录连接到 IAM Identity Center 中的步骤操作。
3. 配置 Active Directory 以将您要向其授予管理权限的用户同步到 IAM Identity Center。有关更多信息，请参阅 将管理用户同步到 IAM Identity Center 中。

步骤 2：将管理用户同步到 IAM Identity Center 中

将您的目录连接到 IAM Identity Center 后，您可以指定要向其授予管理权限的用户，然后将该用户从您的目录同步到 IAM Identity Center 中。

1. 打开 IAM Identity Center 控制台。
2. 选择设置。
3. 在设置页面上，选择身份源选项卡，从中选择操作，然后选择管理同步。
4. 在管理同步页面上，选择用户选项卡，然后选择添加用户和组。
5. 在用户选项卡的用户下，输入确切的用户名并选择添加。
6. 在已添加用户和组项下，执行以下操作：
   a. 确认已指定您要向其授予管理权限的用户。
   b. 选中该用户名左边的复选框。
   c. 选择提交。
7. 在管理同步页面中，您指定的用户将显示在同步范围内的用户列表中。
8. 在导航窗格中，选择 Users（用户）。
9. 在用户页面上，您指定的用户可能需要一些时间才会出现在列表中。选择刷新图标以更新用户列表。

此时，您的用户无权访问管理账户。您可以通过创建管理权限集并将用户分配给该权限集来设置对此帐户的管理访问权限。有关更多信息，请参阅 创建权限集。

Setting up SCIM provisioning between CyberArk and IAM Identity Center

IAM Identity Center 支持将用户信息从 CyberArk Directory Platform 自动预置（同步）到 IAM Identity Center。此预置使用跨域身份管理系统 (SCIM) v2.0 协议。有关更多信息，请参阅 对外部身份提供者使用 SAML 和 SCIM 身份联合验证。

在开始部署 SCIM 之前，我们建议您首先查看 使用自动预置的注意事项。然后继续查看下一部分中的其他注意事项。

主题

先决条件

在开始之前，您将需要以下内容：

- CyberArk 订阅或免费试用。报名参加免费试用访问 CyberArk。
- 支持 IAM Identity Center 的帐户（免费）。有关更多信息，请参阅启用 IAM Identity Center。
- 从您的 CyberArk 帐户到 IAM Identity Center 的 SAML 连接，如 IAM Identity Center CyberArk 文档中所述。
- 将 IAM Identity Center 连接器与您想要允许访问 Amazon Web Services 账户的角色、用户和组织相关联。

SCIM 注意事项

以下是对 IAM Identity Center 使用 CyberArk 联合身份验证时的注意事项：

- 只有应用程序预置部分中映射的角色才会同步到 IAM Identity Center。
- 配置脚本仅在默认状态下受支持，一旦更改，SCIM 预置可能会失败。
  - 只能同步一种电话号码属性，默认为“工作电话”。
- 如果 CyberArk IAM Identity Center 应用程序中的角色映射发生更改，则预计会出现以下行为：
  - 如果角色名称发生更改——IAM Identity Center 中的组名称不会发生更改。
  - 如果组名称发生更改——将在 IAM Identity Center 中创建新组，旧组将保留，但没有成员。
- 用户同步和取消预置行为可以从 CyberArk IAM Identity Center 应用程序进行设置，请确保为您的组织设置正确的行为。您可以选择以下选项：
  - 覆盖（或不覆盖）Identity Center 目录中具有相同主体名称的用户。
  - 从 CyberArk 角色中移除用户后，从 IAM Identity Center 取消对该用户的配置。
  - 取消配置用户行为——禁用或删除。

步骤 1：在 IAM Identity Center 中启用预置

在第一步中，您使用 IAM Identity Center 控制台启用自动预置。

在 IAM Identity Center 中启用自动预置

1. 完成先决条件后，打开 IAM Identity Center 控制台。
2. 在左侧导航窗格中选择设置。
3. 在设置页面上，找到自动预置信息框，然后选择启用。这会立即在 IAM Identity Center 中启用自动预置，并显示必要的 SCIM 端点和访问令牌信息。
4. 在入站自动预置对话框中，复制 SCIM 端点和访问令牌。稍后在 IdP 中配置预置时，您需要粘贴这些内容。

   a. SCIM 端点 ——例如，https://scim。*us-east-2*.amazonaws.com/ /scim/v2 *11111111111-2222-3333-4444-555555555555*

   b. 访问令牌 - 选择显示令牌以复制该值。

> **Warning**
>
> 这是唯一可以获取 SCIM 端点与访问令牌的机会。在继续操作之前，务必复制这些值。本教程的后续步骤需要输入这些值，以便在 IdP 中配置自动预置。

5. 选择关闭。

现在您已在 IAM Identity Center 控制台中设置了预置，您需要使用 CyberArk IAM Identity Center 应用程序完成其余任务。以下过程中描述了这些步骤。

步骤2：在 CyberArk 中配置预置

在 CyberArk IAM Identity Center 应用程序中使用以下过程来启用 IAM Identity Center 的预置。此过程假设您已将 CyberArk IAM Identity Center 应用程序添加到 Web 应用程序下的 CyberArk 管理控制台。如果您尚未执行此操作，请参阅 先决条件，然后完成此过程以配置 SCIM 预置。

要在 CyberArk 中配置预置

1. 打开您在为 CyberArk 配置 SAML 过程中添加的 CyberArk IAM Identity Center 应用程序（应用程序 > Web 应用程序）。请参阅 先决条件。
2. 选择 IAM Identity Center 应用程序并转到预置部分。
3. 选中启用此应用程序的预置框并选择实时模式。
4. 在前面的过程中，您从 IAM Identity Center 复制了 SCIM 端点值。将该值粘贴到 SCIM 服务 URL 字段中，在 CyberArk IAM Identity Center 应用程序中将授权类型设置为 Authorization 标头。
5. 将标头类型设置为持有者令牌。
6. 在上一过程中，您复制了 IAM Identity Center 中的访问令牌值。将该值粘贴到 CyberArk IAM Identity Center 应用程序中的持有者令牌字段中。
7. 单击验证以测试和应用配置。
8. 在同步选项下，选择您希望 CyberArk 中的出站预置发挥作用的正确行为。您可以选择覆盖（或不覆盖）具有相似主体名称和取消预置行为的现有 IAM Identity Center 用户。
9. 在角色映射下，设置从名称字段下的 CyberArk 角色到目标组下的 IAM Identity Center 组的映射。
10. 完成后点击底部的保存。
11. 要验证用户是否已成功同步到 IAM Identity Center，请返回 IAM Identity Center 控制台并选择用户。来自 CyberArk 的同步用户将显示在用户页面上。现在可以将这些用户分配给帐户并可以在 IAM Identity Center 中进行连接。

（可选）步骤 3：在 CyberArk 中配置用户属性以在 IAM Identity Center 中进行访问控制 (ABAC)

如果您选择为 IAM Identity Center 配置属性以管理对 Amazon 资源的访问权限，则这是一个可选过程。CyberArk您在 CyberArk 中定义的属性将在 SAML 断言中传递到 IAM Identity Center。然后，您在 IAM Identity Center 中创建权限集，以根据您从 CyberArk 传递的属性管理访问权限。

在开始此过程之前，您必须首先启用 访问控制属性 功能。有关此操作的详细信息，请参阅 启用并配置访问控制属性。

要在 CyberArk 中配置用户属性，用于 IAM Identity Center 的访问控制

1. 打开您在为 CyberArk 配置 SAML 过程中安装的 CyberArk IAM Identity Center 应用程序（应用程序 > Web 应用程序）。
2. 转至 SAML 响应选项。
3. 在属性下，按照以下逻辑将相关属性添加到表中：
   a. 属性名称是来自 CyberArk 的原始属性名称。
   b. 属性值是在 SAML 断言中发送到 IAM Identity Center 的属性名称。
4. 选择保存。

（可选）传递访问控制属性

您可以选择使用 IAM Identity Center 中的 访问控制属性 功能来传递 `Name` 属性设置为 `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` 的 `Attribute` 元素。此元素允许您将属性作为 SAML 断言中的会话标签传递。有关会话标签的更多信息，请参阅 IAM 用户指南在 Amazon STS中的传递会话标签。

要将属性作为会话标签传递，请包含指定标签值的 `AttributeValue` 元素。例如，要传递标签键值对`CostCenter = blue`，请使用以下属性。

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

如果您需要添加多个属性，请为每个标签包含一个单独的 `Attribute` 元素。

使用 IAM Identity Center 与 JumpCloud 目录平台连接

IAM Identity Center 支持将用户信息从 JumpCloud Directory Platform 自动预置（同步）到 IAM Identity Center。此预置使用安全断言标记语言（SAML）2.0协议。有关更多信息，请参阅 对外部身份提供者使用 SAML 和 SCIM 身份联合验证。

您可以使用 IAM Identity Center SCIM 端点和访问令牌在 JumpCloud 中配置此连接。配置 SCIM 同步时，您将在 JumpCloud 中创建用户属性到 IAM Identity Center 中的命名属性的映射。这会导致 IAM Identity Center 和 JumpCloud 之间的预期属性匹配。

本指南基于截至 2021 年 6 月的 JumpCloud。新版本的步骤可能有所不同。本指南包含一些有关通过 SAML 配置用户身份验证的说明。

以下步骤将引导您了解如何使用 SCIM 协议将用户和组从 JumpCloud 自动预置到 IAM Identity Center。

> **Note**
>
> 在开始部署 SCIM 之前，我们建议您首先查看 使用自动预置的注意事项。然后继续查看下一部分中的其他注意事项。

主题

先决条件

在开始之前，您将需要以下内容：

- JumpCloud 订阅或免费试用。报名参加免费试用访问 JumpCloud。

- 启用 IAM 身份中心的账户（免费）。有关更多信息，请参阅启用 IAM Identity Center。
- 从您的 JumpCloud 帐户到 IAM Identity Center 的 SAML 连接，如 IAM Identity Center JumpCloud 文档中所述。
- 如果您将 IAM Identity Center 复制到其他区域，则必须更新您的身份提供商配置以允许访问 Amazon 托管应用程序和 Amazon Web Services 账户 从这些区域访问托管应用程序。有关更多详细信息，请参阅the section called “步骤 3：更新外部 IdP 设置”。有关更多详细信息，请参阅 JumpCloud文档。
- 将 IAM Identity Center 连接器与您想要允许访问 Amazon 帐户的组关联。

SCIM 注意事项

以下是使用 IAM Identity Center 联合身份验证 JumpCloud 时的注意事项。

- 只有与中的 Amazon 单点登录连接器关联的群组才 JumpCloud会与 SCIM 同步。
- 只能同步一种电话号码属性，默认为“工作电话”。
- JumpCloud 目录中的用户必须配置名字和姓氏才能使用 SCIM 同步到 IAM Identity Center。
- 如果用户在 IAM Identity Center 中被禁用但在 JumpCloud 中仍然激活，属性仍然会同步。
- 您可以通过取消选中连接器中的“启用用户组和组成员身份管理”来选择仅对用户信息启用 SCIM 同步。

步骤 1：在 IAM Identity Center 中启用预置

在第一步中，您使用 IAM Identity Center 控制台启用自动预置。

在 IAM Identity Center 中启用自动预置

1. 完成先决条件后，打开 IAM Identity Center 控制台。
2. 在左侧导航窗格中选择设置。
3. 在设置页面上，找到自动预置信息框，然后选择启用。这会立即在 IAM Identity Center 中启用自动预置，并显示必要的 SCIM 端点和访问令牌信息。
4. 在入站自动预置对话框中，复制 SCIM 端点和访问令牌。稍后在 IdP 中配置预置时，您需要粘贴这些内容。

    a. SCIM 端点 ——例如，https://scim。*us-east-2*.amazonaws.com/ /scim/v2 *11111111111-2222-3333-4444-555555555555*

b. 访问令牌 - 选择显示令牌以复制该值。

> **Warning**
>
> 这是唯一可以获取 SCIM 端点与访问令牌的机会。在继续操作之前，务必复制这些值。本教程的后续步骤需要输入这些值，以便在 IdP 中配置自动预置。

5. 选择关闭。

现在您已在 IAM Identity Center 控制台中设置了预配置，您需要使用 JumpCloud IAM Identity Center 连接器完成剩余任务。以下过程中描述了这些步骤。

步骤2：在 JumpCloud 中配置预置

在 JumpCloud IAM Identity Center 连接器中使用以下过程以启用 IAM Identity Center 预置。此过程假设您已将 JumpCloud IAM Identity Center 连接器添加到您的 JumpCloud 管理门户和组。如果您尚未执行此操作，请参阅 先决条件，然后完成此过程来配置 SCIM 预置。

要在 JumpCloud 中配置预置

1. 打开您在为 JumpCloud 配置 SAML 过程中安装的 JumpCloud IAM Identity Center 连接器（用户身份验证 > IAM Identity Center）。请参阅先决条件。
2. 选择 IAM Identity Center 连接器，然后选择第三个选项卡身份管理。
3. 如果您希望组 SCIM 同步，请选中启用此应用程序中的用户组和组成员身份管理复选框。
4. 单击配置。
5. 在上一过程中，您复制了 IAM Identity Center 中的 SCIM 端点值。将该值粘贴到 JumpCloud IAM Identity Center 连接器的基本 URL 字段中。
6. 在上一过程中，您复制了 IAM Identity Center 中的访问令牌值。将该值粘贴到 JumpCloud IAM Identity Center 连接器中的令牌密钥字段中。
7. 单击激活以应用配置。
8. 确保单点登录旁边有一个绿色指示器已激活。
9. 移至第四个选项卡用户组并检查要使用 SCIM 配置的组。
10. 完成后点击底部的保存。

11. 要验证用户是否已成功同步到 IAM Identity Center，请返回 IAM Identity Center 控制台并选择用户。来自 JumpCloud 的同步用户出现在用户页面上。现在可以将这些用户分配到 IAM Identity Center 内的帐户。

（可选）第三步：在 JumpCloud IAM Identity Center 中配置用户属性进行访问控制

如果您选择为 IAM Identity Center 配置属性以管理对 Amazon 资源的访问权限，则这是一个可选过程。JumpCloud您在 JumpCloud 中定义的属性将在 SAML 断言中传递到 IAM Identity Center。然后，您在 IAM Identity Center 中创建权限集，以根据您从 JumpCloud 传递的属性管理访问权限。

在开始此过程之前，您必须首先启用访问控制功能的属性。有关如何执行此操作的详细信息，请参阅启用和配置访问控制属性。

要在 JumpCloud 中配置用户属性，用于 IAM Identity Center 的访问控制

1. 打开您在为 JumpCloud 配置 SAML 过程中安装的 JumpCloud IAM Identity Center 连接器（用户身份验证 > IAM Identity Center）。
2. 选择 IAM Identity Center 连接器。然后，选择第二个选项卡 IAM 身份中心。
3. 在此选项卡底部，您可以选择用户属性映射，选择添加新属性，然后执行以下操作： 您必须对要添加以在 IAM Identity Center 中用于访问控制的每个属性执行这些步骤。

    a. 在服务提供属性名称字段中，输入 `https://aws.amazon.com/SAML/Attributes/AccessControl:` **`AttributeName`**`.` 将 **`AttributeName`** 替换为您在 IAM Identity Center 中期望的属性名称。例如， `https://aws.amazon.com/SAML/Attributes/AccessControl:` **`Email`** 。

    b. 在 JumpCloud 属性名称字段中，从 JumpCloud 目录中选择用户属性。例如，电子邮件（工作）。
4. 选择保存。

（可选）传递访问控制属性

您可以选择使用 IAM Identity Center 中的 访问控制属性 功能来传递 Name 属性设置为 `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`** 的 Attribute 元素。此元素允许您将属性作为 SAML 断言中的会话标签传递。有关会话标签的更多信息，请参阅 IAM 用户指南在 Amazon STS中的传递会话标签。

要将属性作为会话标签传递，请包含指定标签值的 `AttributeValue` 元素。例如，要传递标签键值对`CostCenter = blue`，请使用以下属性。

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

如果您需要添加多个属性，请为每个标签包含一个单独的 `Attribute` 元素。

通过 Microsoft Entra ID 和 IAM Identity Center 配置 SAML 和 SCIM

Amazon IAM Identity Center 支持与安全断言标记语言 (SAML) 2.0 集成，以及使用跨域身份管理系统 (SCIM) 2.0 协议将来自Microsoft Entra ID（以前称为Azure Active Directory或Azure AD）的用户和群组信息自动配置（同步）到 IAM Identity C enter。有关更多信息，请参阅 对外部身份提供者使用 SAML 和 SCIM 身份联合验证。

目标

在本教程中，您将设置测试实验室，并配置 Microsoft Entra ID 和 IAM Identity Center 之间的 SAML 连接和 SCIM 预置。在最初的准备步骤中，您将在 Microsoft Entra ID 和 IAM Identity Center 中创建一名测试用户 (Nikki Wolf)，用于双向测试 SAML 连接。稍后，作为 SCIM 步骤的一部分，您将创建一个不同的测试用户 (Richard Roe)，以验证 Microsoft Entra ID 中的新属性是否按预期同步到 IAM Identity Center。

先决条件

在开始本教程之前，您首先需要设置以下方面：

- Microsoft Entra ID 租户。有关更多信息，请参阅 Microsoft 文档中的快速入门：设置租户。
- Amazon IAM Identity Center已启用的账户。有关更多信息，请参阅 Amazon IAM Identity Center 用户指南中的启用 IAM Identity Center。

注意事项

以下是有关 Microsoft Entra ID 的重要注意事项，它们将影响您计划如何在生产环境中使用 SCIM v2 协议通过 IAM Identity Center 实施自动预置。

自动预置

在开始部署 SCIM 之前，我们建议您首先查看 使用自动预置的注意事项。

访问控制属性

用于访问控制的属性用于权限策略，这些策略决定了您的身份源中的谁可以访问您的 Amazon 资源。如果在 Microsoft Entra ID 中从用户中删除属性，则不会从 IAM Identity Center 中的相应用户中删除该属性。这是 Microsoft Entra ID 中已知的限制。如果用户的属性更改为不同的（非空）值，则该更改将同步到 IAM Identity Center。

嵌套组

Microsoft Entra ID 用户预置服务无法读取或预置嵌套组中的用户。只能读取和预置属于明确分配组的直接成员的用户。Microsoft Entra ID 不会以递归方式解包间接分配的用户或组（属于直接分配的组的成员的用户或组）的组成员身份。有关更多信息，请参阅 Microsoft 文档中的基于分配的范围界定。您也可以使用 IAM Identity Center 可配置 AD 同步功能将 Active Directory 组与 IAM Identity Center 集成。

动态组

Microsoft Entra ID 用户预置服务可以读取和预置动态组中的用户。请参阅下面的示例，该示例显示使用动态组时的用户和组结构以及它们在 IAM Identity Center 中的显示方式。这些用户和组通过 SCIM 从 Microsoft Entra ID 配置到 IAM Identity Center

例如，如果动态组的 Microsoft Entra ID 结构如下：

1. A 组，成员 ua1、ua2
2. B 组，成员 ub1
3. C 组，成员 uc1
4. K组规则包括 A、B、C 组成员
5. L 组，规则包括 B 组和 C 组成员

将 Microsoft Entra ID 中的用户和组信息通过 SCIM 预置到 IAM Identity Center 后，结构如下：

1. A 组，成员 ua1、ua2
2. B 组，成员 ub1
3. C 组，成员 uc1

4. K 组，成员 ua1、ua2、ub1、uc1
5. L组，成员 ub1、uc1

使用动态组配置自动预置时，请记住以下注意事项。

- 动态组可以包括嵌套组。但是，Microsoft Entra ID 预置服务不会扁平化嵌套组。例如，如果您具有以下动态组 Microsoft Entra ID 结构：
  - A 组是 B 组的父组。
  - A 组有 ua1 成员。
  - B 组有 ub1 作为成员。

包含组 A 的动态组将仅包含组 A 的直接成员（即 ua1）。它不会以递归方式包含 B 组的成员。

- 动态组不能包含其他动态组。有关更多信息，请参阅 Microsoft 文档中的预览限制。

步骤 1：准备 Microsoft 租户

在本步骤中，您将介绍如何安装和配置 Amazon IAM Identity Center 企业应用程序以及如何为新创建的Microsoft Entra ID测试用户分配访问权限。

Step 1.1 >

步骤 1.1：在中设置 Amazon IAM Identity Center 企业应用程序 Microsoft Entra ID

在此过程中，您将在中安装 Amazon IAM Identity Center 企业应用程序Microsoft Entra ID。稍后您将需要此应用程序来配置您的 SAML 连接。 Amazon

1. 至少以云应用程序管理员的身份登录 Microsoft Entra 管理中心。
2. 导航到身份 > 应用程序 > 企业应用程序，然后选择新应用程序。
3. 在浏览 Microsoft Entra Gallery页面上，在搜索框中输入 **`Amazon IAM Identity Center`**。
4. 从结果中选择 Amazon IAM Identity Center。
5. 选择创建。

Step 1.2 >

步骤 1.2：在 Microsoft Entra ID 中创建测试用户

Nikki Wolf 是您在此过程中创建的 Microsoft Entra ID 测试用户姓名。

1. 在 Microsoft Entra 管理中心控制台，导航到身份 > 用户 > 所有用户。
2. 选择新用户，然后选择屏幕顶部的创建新用户。
3. 在用户主体名称中，输入 **NikkiWolf**，然后选择您喜欢的域和扩展。例如，NikkiWolf@*example.org*。
4. 在显示名称中，输入 **NikkiWolf**。
5. 在密码中输入高强度密码，或选择眼睛图标，显示自动生成的密码，然后复制或写下显示的值。
6. 选择属性，在名字中输入 **Nikki**。在姓氏中，输入 **Wolf**。
7. 选择审核并创建，然后选择创建。

Step 1.3

步骤 1.3：在 Nikki 分配权限之前，先测试 Nikki 的体验 Amazon IAM Identity Center

在此过程中，您将验证 Nikki 可以成功登录其 Microsoft 我的账户门户中的哪些内容。

1. 在同一个浏览器中打开新标签页，前往我的账户门户登录页面，然后输入 Nikki 的完整电子邮件地址。例如，NikkiWolf@ *example.org*。
2. 出现提示时，输入 Nikki 的密码，然后选择登录。如果密码是自动生成的，系统将提示您更改密码。
3. 在需要执行的操作页面，选择稍后询问，绕过关于其他安全方法的提示。
4. 在我的账户页面的左侧导航窗格中，选择我的应用程序。请注意，除加载项外，此时不会显示任何应用程序。您将添加一个 Amazon IAM Identity Center 应用程序，在稍后的步骤中，其将显示在此处。

Step 1.4

步骤 1.4：在 Microsoft Entra ID 中向 Nikki 分配权限

现在您已验证 Nikki 可以成功访问我的账户门户，请使用此过程将其用户分配至 Amazon IAM Identity Center 应用程序。

1. 在 Microsoft Entra 管理中心控制台，导航到身份 > 应用程序 > 企业应用程序，然后从列表中选择 Amazon IAM Identity Center。

2. 在左侧，选择用户和组。
3. 选择添加用户/组。您可以忽略组不可用于分配的消息。此教程不使用组进行分配。
4. 在添加分配页面，在用户下选择未选择任何对象。
5. 选择 NikkiWolf，然后选择 “选择”。
6. 在添加作业页面上，选择分配。 NikkiWolf 现在出现在分配给该Amazon IAM Identity Center应用程序的用户列表中。

第 2 步：准备 Amazon 账户

在本步骤中，您将了解如何使用 IAM Identity Center 配置访问权限（通过权限集），手动创建相应的 Nikki Wolf 用户，并为其分配管理 Amazon资源所需的权限。

Step 2.1 >

步骤 2.1：在中创建 RegionalAdmin 权限集 IAM Identity Center

此权限集将用于向Nikki授予必要的 Amazon 账户权限，以便从中的账户页面管理区域。 Amazon Web Services 管理控制台默认将拒绝其他所有查看或管理 Nikki 账户其他任何信息的权限。

1. 打开 IAM Identity Center 控制台。
2. 在多帐户权限下，选择权限集。
3. 选择创建权限集。
4. 在选择权限集类型页面，选择自定义权限集，然后选择下一步。
5. 选择内联策略，将其展开，然后使用以下步骤为权限集创建策略：
   a. 选择添加新声明，以创建策略语句。
   b. 在编辑语句下，从列表中选择账户，然后选中以下复选框。
      - **`ListRegions`**
      - **`GetRegionOptStatus`**
      - **`DisableRegion`**
      - **`EnableRegion`**
   c. 在添加资源旁边，选择添加。
   d. 在添加资源页面的资源类型下，选择所有资源，然后选择添加资源。验证您的策略是否如下所示：

```
{
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "account:ListRegions",
                "account:DisableRegion",
                "account:EnableRegion",
                "account:GetRegionOptStatus"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

6. 选择下一步。
7. 在指定权限集详细信息页面的权限集名称下，输入 **RegionalAdmin**，然后选择下一步。
8. 在审核和创建页面，选择创建。您应该看到权限集列表中RegionalAdmin显示了内容。

Step 2.2 >

步骤 2.2：在中创建相应的 NikkiWolf 用户 IAM Identity Center

由于 SAML 协议不提供查询 IdP (Microsoft Entra ID) 并在 IAM Identity Center 自动创建用户的机制，因此请使用以下过程在 IAM Identity Center 手动创建同步了 Microsoft Entra ID 中 Nikki Wolfs 用户核心属性的用户。

1. 打开 IAM Identity Center 控制台。
2. 选择用户，选择添加用户，然后提供以下信息：
   a. 对于用户名和电子邮件地址-输入您在创建Microsoft Entra ID用户时使用的相同 **NikkiWolf@*yourcompanydomain.extension***。例如，NikkiWolf@*example.org*。
   b. 确认电子邮件地址 - 重新输入上一步中的电子邮件地址
   c. 名字 - 输入 **Nikki**
   d. 姓氏 - 输入 **Wolf**

e. 显示名称 – 输入 **`Nikki Wolf`**

3. 选择两次下一步，然后选择添加用户。
4. 选择关闭。

Step 2.3

步骤 2.3：将 Nikki 分配给中设置的 RegionalAdmin 权限 IAM Identity Center

在这里， Amazon Web Services 账户 您可以找到 Nikki 将在其中管理区域，然后为她分配成功 Amazon Web Services 访问门户所需的必要权限。

1. 打开 IAM Identity Center 控制台。
2. 在多帐户权限下，选择 Amazon Web Services 账户。
3. 选中要授予 Nikki 管理区域权限的账户名（例如*`Sandbox`*）旁边的复选框，然后选择 “分配用户和群组”。
4. 在分配用户和组页面，选择用户选项卡，找到并选中 Nikki 旁边的复选框，然后选择下一步。
5. Example

   <caption>On the 选择权限集 page, choose the `RegionalAdmin` permission set created in Step 2.1, and then choose 下一步.</caption>
6. 在查看并提交页面上，查看您的选择，然后选择提交。

步骤 3：配置和测试 SAML 连接

在此步骤中，您将使用 Amazon IAM Identity Center 企业应用程序和 IAM Identity Cent Microsoft Entra ID er 中的外部 IdP 设置来配置 SAML 连接。

Step 3.1 >

步骤 3.1：从 IAM Identity Center 收集所需的服务提供商元数据

在此步骤中，您将从 IAM Identity Center 控制台中启动更改身份源向导，并检索元数据文件和 Microsoft Entra ID在下一步配置连接时需要输入的 Amazon 特定登录 URL。

1. 在 IAM Identity Center 控制台中，选择设置。
2. 在设置页面上，选择身份源选项卡，然后选择操作>更改身份源。

3. 在选择身份源页面，选择外部身份提供商，然后选择下一步。
4. 在 “配置外部身份提供商” 页面上，在 “服务提供者元数据” 下，选择 “默认” IPv4 或 “双栈”。完成身份源更改后，您可以下载服务提供商元数据文件。
5. 在同一部分，找到 Amazon Web Services 访问门户登录 URL 的值，并复制它。在下一步出现提示时，您需要输入该值。
6. 将此页保持打开状态，然后转到下一步 (**`Step 3.2`**)，在中配置 Amazon IAM Identity Center 企业应用程序Microsoft Entra ID。稍后，您将返回此页面，完成整个过程。

Step 3.2 >

步骤 3.2：在中配置 Amazon IAM Identity Center 企业应用程序 Microsoft Entra ID

此过程使用您在上一步获得的元数据文件和登录 URL 的值，在 Microsoft 端完成一半的 SAML 连接设置。

1. 在 Microsoft Entra 管理中心控制台，导航到身份 > 应用程序 > 企业应用程序，然后选择 Amazon IAM Identity Center。
2. 在左侧选择 2. 设置单点登录。
3. 在设置 SAML 单点登录页面，选择 SAML。然后选择上传元数据文件，选择文件夹图标，选择您在上一步中下载的服务提供商元数据文件，然后选择添加。
4. 在 “基本 SAML 配置” 页面上，验证标识符和回复 URL（断言使用者服务 URL）值现在是否都指向中的端点。 Amazon

   - 标识符-这是来自 IAM 身份中心的颁发者 URL。无论您使用的是 IPv4仅限端点还是双栈端点，都适用相同的值。
   - 回复 URL（断言消费者服务 URL）-此处的值包括来自 IAM 身份 IPv4中心所有已启用区域的仅限终端节点和双栈终端节点。您可以使用主要区域的 ACS URL 作为默认区域，这样当用户从中启动 Amazon Web Services 应用程序时，他们就会被重定向到主要区域Microsoft Entra ID。有关 ACS 的更多信息 URLs，请参阅主端点和附加端点中的 ACS 端点 Amazon Web Services 区域。
   - （可选）如果您将 IAM Identity Center 复制到其他区域，则还可以在中Microsoft Entra ID为每个其他区域的 Amazon Web Services 访问门户创建书签应用程序。这使您的用户能够从中 Amazon Web Services 访问其他地区的访问门户Microsoft Entra ID。请务必向您的用户授予访问中的书签应用程序的权限Microsoft Entra ID。有关更多详细信息，请参阅Microsoft Entra ID文档。如果您计划稍后将 IAM Identity Center 复制到其他区域，请访问

以获取Microsoft Entra ID用于访问其他区域的配置有关如何在初始设置后启用对其他区域的访问权限的指导。

5. 在登录 URL（可选）下，粘贴您在上一步（**Step 3.1**）复制的 Amazon Web Services 访问门户登录 URL 值，选择保存，然后点击 X 关闭窗口。
6. 如果系统提示使用测试单点登录 Amazon IAM Identity Center，请选择 “否”，我稍后再测试。您将在稍后的步骤中进行此项验证。
7. 在设置 SAML 单点登录页面的 SAML 证书部分，选择联合身份验证元数据 XML 旁边的下载，将元数据文件保存到您的系统中。在下一步出现提示时，您需要上传此文件。

Step 3.3 >

步骤 3.3：在 Amazon IAM Identity Center配置 Microsoft Entra ID 外部 IdP

在这里，您将返回到 IAM Identity Center 控制台的更改身份源向导，完成 Amazon中 SAML 连接设置的后半部分。

1. 返回在 **Step 3.1** 中，您在 IAM Identity Center 控制台中保留为打开状态的浏览器会话。
2. 在配置外部身份提供商页面的身份提供商元数据部分，选择 IdP SAML 元数据下的选择文件按钮，然后选择您在上一步从 Microsoft Entra ID 下载的身份提供商元数据文件，然后选择打开。
3. 选择下一步。
4. 在阅读免责声明并准备继续操作后，输入 **ACCEPT**。
5. 选择更改身份源，以应用您的更改。

Step 3.4 >

步骤 3.4：测试 Nikki 是否被重定向到 Amazon Web Services 访问门户

在此过程中，您将使用 Nikki 的凭证登录 Microsoft 的我的账户门户，测试 SAML 连接。通过身份验证后，您将选择将 Nikki 重定向到 Amazon Web Services 访问门户的 Amazon IAM Identity Center 应用程序。

1. 前往我的账户门户登录页面，输入 Nikki 的完整电子邮件地址。例如，***NikkiWolf***@*example.org*。
2. 出现提示时，输入 Nikki 的密码，然后选择登录。
3. 在我的账户页面的左侧导航窗格中，选择我的应用程序。

4. 在我的应用程序页面，选择名为 Amazon IAM Identity Center 的应用程序。这应该会提示您进行额外的身份验证。
5. 在微软的登录页面上，选择你的 NikkiWolf 凭据。如果再次提示您进行身份验证，请再次选择您的 NikkiWolf 凭据。这会自动将您重定向到 Amazon Web Services 访问门户。

> **Tip**
>
> 如果您未成功重定向，请进行检查，确保您在 **Step 3.2** 中输入的 Amazon Web Services 访问门户登录 URL 的值与您在 **Step 3.1** 中复制的值相匹配。

6. 确认您的 Amazon Web Services 账户 显示屏。

> **Tip**
>
> 如果页面为空且未 Amazon Web Services 账户 显示，请确认 Nikki 已成功分配给RegionalAdmin权限集（请参阅 **Step 2.3**）。

Step 3.5

步骤 3.5：测试 Nikki 对于管理其 Amazon Web Services 账户的访问权限级别

在此步骤中，您将进行检查，以确定 Nikki 对于管理其 Amazon Web Services 账户区域设置的访问权限级别。Nikki 应该只有刚好足够的管理员权限，可从账户页面管理区域。

1. 在 Amazon Web Services 访问门户中，选择账户选项卡以显示账户列表。将显示与您已定义权限集的任何帐户关联的帐户名 IDs、帐户和电子邮件地址。
2. 选择您应用权限集的帐户名（例如*Sandbox*）（请参阅 **Step 2.3**）。这将展开权限集列表，Nikki 可以从中选择，以管理其账户。
3. 接下来RegionalAdmin选择管理控制台来代入您在RegionalAdmin权限集中定义的角色。这会将您重定向至 Amazon Web Services 管理控制台 主页。
4. 在控制台的右上角，选择您的账户名称，然后选择账户。您将进入账户页面。请注意，此页面上的所有其他部分都会显示一条消息，说明您没有查看或修改这些设置的必要权限。
5. 在账户页面，向下滚动至 Amazon 区域部分。选中表格中任何可用区域的复选框。注意 Nikki 确实拥有必要的权限，可按预期为其账户启用或禁用区域列表。

做得不错！

步骤 1 到步骤 3 帮助您成功实施并测试了 SAML 连接。现在，我们建议您继续执行步骤 4，实现自动预置，以完成本教程。

步骤 4：配置和测试 SCIM 同步

在此步骤中，您将使用 SCIM v2.0 协议，设置将用户信息从 Microsoft Entra ID 自动预置（同步）到 IAM Identity Center。您可以使用 IAM Identity Center 的 SCIM 端点和 IAM Identity Center 自动创建的持有者令牌在 Microsoft Entra ID 中配置此连接。

配置 SCIM 同步时，您将创建从 Microsoft Entra ID 中的用户属性到 IAM Identity Center 中的命名属性的映射。这会导致 IAM Identity Center 和 Microsoft Entra ID 之间的预期属性匹配。

以下步骤将指导您使用 Microsoft Entra ID 中的 IAM Identity Center 应用程序，实现将主要驻留在 Microsoft Entra ID 中的用户自动预置到 IAM Identity Center。

Step 4.1 >

步骤 4.1：在 Microsoft Entra ID 中创建第二名测试用户

出于测试目的，您将在 Microsoft Entra ID 中创建新用户 (Richard Roe)。稍后，在设置 SCIM 同步后，您将测试此用户和所有相关属性是否已成功同步到 IAM Identity Center。

1. 在 Microsoft Entra 管理中心控制台，导航到身份 > 用户 > 所有用户。
2. 选择新用户，然后选择屏幕顶部的创建新用户。
3. 在用户主体名称中，输入 **RichRoe**，然后选择您喜欢的域和扩展。例如，RichRoe@*example.org*。
4. 在显示名称中，输入 **RichRoe**。
5. 在密码中输入高强度密码，或选择眼睛图标，显示自动生成的密码，然后复制或写下显示的值。
6. 选择属性，然后提供以下值：
   - 名字 - 输入 **Richard**
   - 姓氏 - 输入 **Roe**
   - 职位名称 - 输入 **Marketing Lead**

- 部门 - 输入 **Sales**
- 员工 ID - 输入 **12345**

7. 选择审核并创建，然后选择创建。

Step 4.2 >

步骤 4.2：在 IAM Identity Center 启用自动预置

在此过程中，您将使用 IAM Identity Center 控制台，实现将 Microsoft Entra ID 中的用户和组自动预置到 IAM Identity Center。

1. 打开 IAM Identity Center 控制台，在左侧导航窗格中选择设置。
2. 在设置页面的身份源选项卡下，请注意预置方法已设置为手动。
3. 找到自动预置信息框，然后选择启用。这会立即在 IAM Identity Center 中启用自动预置，并显示必要的 SCIM 端点和访问令牌信息。
4. 在入站自动预置对话框中，复制以下选项的每个值。下一步在 Microsoft Entra ID 中配置预置时，您需要粘贴这些值。

   a. SCIM 端点-例如，

      - IPv4: `https://scim.aws-region.amazonaws.com/11111111111-2222-3333-4444-555555555555/scim/v2`
      - 双堆栈：`https://scim.aws-region.api.aws/11111111111-2222-3333-4444-555555555555/scim/v2`

   b. 访问令牌 - 选择显示令牌以复制该值。

> **Warning**
>
> 这是唯一可以获取 SCIM 端点与访问令牌的机会。在继续操作之前，务必复制这些值。

5. 选择关闭。
6. 在身份源选项卡下，请注意预置方法现在设置为 SCIM。

Step 4.3 >

步骤 4.3：在 Microsoft Entra ID 中配置自动预置

现在，您的 RichRoe 测试用户已经准备就绪，并已在 IAM Identity Center 中启用了 SCIM，您可以继续在中配置 SCIM 同步设置。Microsoft Entra ID

1. 在 Microsoft Entra 管理中心控制台，导航到身份 > 应用程序 > 企业应用程序，然后选择 Amazon IAM Identity Center。
2. 选择预置，在管理下，再次选择预置。
3. 在预置模式下，选择自动。
4. 在管理员凭证下的租户 URL 中，粘贴您之前在 **Step 4.2** 中复制的 SCIM 端点 URL 值。在密钥令牌中，粘贴访问令牌的值。
5. 选择测试连接。您应该会看到一条消息，表明经过测试的凭证已成功得到授权，可以启用预置。
6. 选择保存。
7. 在管理下，选择用户和组，然后选择添加用户/组。
8. 在添加分配页面，在用户下选择未选择任何对象。
9. 选择 RichRoe，然后选择 “选择”。
10. 在添加分配页面，选择分配。
11. 选择概述，然后选择开始预置。

Step 4.4

步骤 4.4：验证是否已进行同步

在本节中，您将验证 Richard 的用户是否已成功预置，并且所有属性均显示在 IAM Identity Center 中。

1. 在 IAM Identity Center 控制台中，选择用户。
2. 在 “用户” 页面上，您应该会看到显示您的RichRoe用户。请注意，在创建者列，值将设置为 SCIM。
3. 选择 “配置文件” 下 RichRoe，确认以下属性是从中复制的Microsoft Entra ID。
   - 名字 - **Richard**

- 姓氏 - **Roe**
- 部门 - **Sales**
- 职位 - **Marketing Lead**
- 员工编号 - **12345**

现在，Richard 的用户已在 IAM Identity Center 中创建，您可以将其分配给任何权限集，这样您就可以控制他对您 Amazon 资源的访问权限级别。例如，您可以分配RichRoe给之前使用的**RegionalAdmin**权限集，授予 Nikki 管理区域的权限（请参阅 **Step 2.3**），然后使用**Step 3.5**测试其访问级别。

恭喜您！

你已成功在 Microsoft 和 Microsoft 之间建立了 SAML 连接， Amazon 并已验证自动配置可以使所有内容保持同步。现在，您可以运用所学到的方法，更顺利地设置生产环境。

步骤 5：配置 ABAC – 可选

现在，您已成功配置了 SAML 和 SCIM，可以选择配置基于属性的访问权限控制 (ABAC)。ABAC 是一种基于属性定义权限的授权策略。

通过 Microsoft Entra ID，您可以使用以下两种方法中的任何一种配置 ABAC，与 IAM Identity Center 配合使用。

Configure user attributes in Microsoft Entra ID for access control in IAM Identity Center

在 Microsoft Entra ID 中配置用户属性，用于 IAM Identity Center 的访问控制

在以下步骤中，您将确定 IAM Identity Center Microsoft Entra ID 应使用中的哪些属性来管理对您的 Amazon 资源的访问权限。定义后，Microsoft Entra ID 通过 SAML 断言将这些属性发送到 IAM Identity Center。然后，您需要在 IAM Identity Center 中 创建权限集 根据您从 Microsoft Entra ID 传递的属性来管理访问权限。

在开始此过程之前，您首先需要启用 访问控制属性 功能。有关此操作的详细信息，请参阅 启用并配置访问控制属性。

1. 在 Microsoft Entra 管理中心控制台，导航到身份 > 应用程序 > 企业应用程序，然后选择 Amazon IAM Identity Center。

2. 选择 Single sign-on（单点登录）。
3. 在属性和声明部分，选择编辑。
4. 在属性和声明页面，执行以下操作：
   a. 选择添加新声明
   b. 对于名称，请输入 `AccessControl:`*`AttributeName`*。*`AttributeName`* 替换为您在 IAM Identity Center 中期望的属性的名称。例如 `AccessControl:`**`Department`**。
   c. 对于命名空间，请输入 **`https://aws.amazon.com/SAML/Attributes`**。
   d. 对于源，请选择属性。
   e. 对于来源属性，使用下拉列表选择 Microsoft Entra ID 用户属性。例如 `user.`**`department`**。
5. 对需要在 SAML 断言中发送到 IAM Identity Center 的每个属性重复上一步。
6. 选择保存。

Configure ABAC using IAM Identity Center

使用 IAM Identity Center 配置 ABAC

通过此方法，您可以使用 IAM Identity Center 中的 访问控制属性 功能来传递 Name 属性设置为 `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`** 的 `Attribute` 元素。您可以使用此元素将属性作为 SAML 断言中的会话标记传递。有关会话标签的更多信息，请参阅 IAM 用户指南在 Amazon STS中的传递会话标签。

要将属性作为会话标签传递，请包含指定标签值的 `AttributeValue` 元素。例如，要传递标签键值对 `Department=billing`，请使用以下属性：

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/
AccessControl:Department">
<saml:AttributeValue>billing
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

如果您需要添加多个属性，请为每个标签包含一个单独的 `Attribute` 元素。

将访问权限分配给 Amazon Web Services 账户

仅授予访问权限时才需要执行以下步骤。 Amazon Web Services 账户 授予 Amazon 应用程序访问权限不需要这些步骤。

> **Note**
>
> 要完成此步骤，您需要拥有 IAM Identity Center 的 Organization 实例。有关更多信息，请参阅 IAM Identity Center 的组织和账户实例。

步骤 1：IAM Identity Center：向 Microsoft Entra ID 用户授予账户访问权限

1. 返回 IAM Identity Center 控制台。在 IAM Identity Center 导航窗格的多账户权限下，选择 Amazon Web Services 账户。
2. 在 Amazon Web Services 账户 页面，组织结构将显示您的组织根目录，您的账户将以分层结构列于其下方。选中管理账户对应的复选框，然后选择分配用户或组。
3. 此时将显示分配用户和组工作流程。它包括三个步骤：

   a. 对于步骤 1：选择用户和组，选择将要执行管理员工作职能的用户。然后选择下一步。

   b. 对于步骤 2：选择权限集，选择创建权限集，以打开新的标签页，它将引导您完成创建权限集所涉及的三个子步骤。

      i. 对于步骤 1：选择权限集类型，请完成以下操作：

         - 在权限集类型中，选择预定义权限集。
         - 在预定义权限集的策略中，选择AdministratorAccess。

         选择下一步。

      ii. 对于步骤 2：指定权限集详细信息，保留默认设置，并选择下一步。

         默认设置会创建名为*AdministratorAccess*、会话持续时间设置为一小时的权限集。

      iii. 对于 “步骤 3：查看并创建”，请验证权限集类型是否使用 Amazon 托管策略AdministratorAccess。选择创建。权限集页面会显示通知，告知您权限集已创建。您可以在网络浏览器中关闭此标签页。

      iv. 在分配用户和组浏览器标签页，您仍处于步骤 2：选择权限集，您将在这里启动创建权限集工作流程。

v. 在权限集区域，选择刷新按钮。您创建的*AdministratorAccess*权限集将出现在列表中。选择该权限集的复选框，然后选择下一步。

c. 对于步骤 3：查看并提交，请查看选定的用户和权限集，然后选择提交。

页面更新时会显示一条消息，告知您 Amazon Web Services 账户 正在配置中。等待该过程完成。

您将返回到该 Amazon Web Services 账户 页面。系统会显示一条通知消息，告知您 Amazon Web Services 账户 已重新配置您的权限集，并且已应用更新的权限集。当用户登录时，他们可以选择*AdministratorAccess*角色。

步骤 2Microsoft Entra ID：确认Microsoft Entra ID用户对 Amazon 资源的访问权限

1. 返回到 Microsoft Entra ID 控制台，并导航到您的 IAM Identity Center 基于 SAML 的登录应用程序。
2. 选择用户和组，然后选择添加用户或组。您将把在本教程步骤 4 中创建的用户添加到 Microsoft Entra ID 应用程序。通过添加该用户，您将允许他们登录到 Amazon。搜索您在步骤 4 中创建的用户。如果您遵循了此步骤，该用户应为 **RichardRoe**。

   - 有关演示，请参阅将您现有的 IAM Identity Center 实例与 Microsoft Entra ID 联合

Microsoft Entra ID访问 IAM 身份中心其他区域的配置-可选

如果您将 IAM Identity Center 复制到其他区域，则必须更新您的身份提供商配置，以允许访问 Amazon 托管应用程序和 Amazon Web Services 账户 通过其他区域。以下步骤将指导您完成整个过程。有关本主题的更多详细信息（包括先决条件），请参阅跨多个 IAM 身份中心使用 Amazon Web Services 区域。

1. 从 IAM I URLs dentity Center 控制台检索其他区域的 ACS，如中所述主端点和附加端点中的 ACS 端点 Amazon Web Services 区域。
2. 在 Microsoft Entra 管理中心控制台，导航到身份 > 应用程序 > 企业应用程序，然后选择 Amazon IAM Identity Center。
3. 在左侧选择 2. 设置单点登录。
4. 在 “基本 SAML 配置” 页面的 “回复 URL（断言使用者服务 URL）” 部分下，选择为每个其他区域的 ACS URL 添加回复 URL。您可以将主区域的 ACS URL 保留为默认区域，这样当用户从中启动 Amazon IAM Identity Center 应用程序时，他们就会被重定向到主区域Microsoft Entra ID。

5. 添加 ACS 后 URLs，保存Amazon IAM Identity Center应用程序。
6. 您可以在中Microsoft Entra ID为每个其他区域的 Amazon Web Services 访问门户创建书签应用程序。这使您的用户能够从中 Amazon Web Services 访问其他地区的访问门户Microsoft Entra ID。请务必向您的用户授予访问中的书签应用程序的权限Microsoft Entra ID。有关更多详细信息，请参阅Microsoft Entra ID文档。
7. 确认您可以登录其他每个地区的 Amazon Web Services 访问门户。导航到Amazon Web Services 访问门户 URLs或从中启动书签应用程序Microsoft Entra ID。

问题排查

有关使用 Microsoft Entra ID 对 SCIM 和 SAML 进行一般性问题排查，请参阅以下各部分：

- Microsoft Entra ID 与 IAM Identity Center 的同步问题
- 特定用户无法从外部 SCIM 提供商同步到 IAM Identity Center
- 与 IAM Identity Center 创建的 SAML 断言内容有关的问题
- 使用外部身份提供者预置用户或组时出现重复用户或组错误
- 其他资源

Microsoft Entra ID 与 IAM Identity Center 的同步问题

如果您遇到 Microsoft Entra ID 用户未同步到 IAM Identity Center 的问题，可能是由于在向 IAM Identity Center 添加新用户时，IAM Identity Center 已经标记的语法问题。您可以通过检查 Microsoft Entra ID 审核日志中的失败事件（例如 `'Export'`）来确认这一点。此事件的状态原因将说明：

```
{"schema":["urn:ietf:params:scim:api:messages:2.0:Error"],"detail":"Request is
 unparsable, syntactically incorrect, or violates schema.","status":"400"}
```

您也可以检查 Amazon CloudTrail 失败的事件。这可以通过在 “事件历史记录” 控制台中搜索 CloudTrail 或使用以下过滤器来完成：

```
"eventName":"CreateUser"
```

CloudTrail 事件中的错误将说明以下内容：

```
"errorCode": "ValidationException",
        "errorMessage": "Currently list attributes only allow single item“
```

最终，此异常意味着从 Microsoft Entra ID 传递的某个值包含的值比预期多。该解决方案旨在查看 Microsoft Entra ID 中用户的属性，确保不包含重复值。重复值的一个常见示例是，联系电话（例如手机、工作电话和传真）存在多个值。尽管是单独的值，但它们都会在单父属性 phoneNumbers 下传递到 IAM Identity Center。

有关 SCIM 一般性问题排查的提示，请参阅问题排查。

Microsoft Entra ID 访客账户同步

若想将 Microsoft Entra ID 访客用户同步到 IAM Identity Center，请参阅下列步骤。

Microsoft Entra ID 访客用户的电子邮件有别于 Microsoft Entra ID 用户的电子邮件。尝试与 IAM Identity Center 同步 Microsoft Entra ID 访客账户时，该差异会引发问题。例如，查看访客用户的以下电子邮件地址：

`exampleuser_domain.com#EXT#@domain.onmicrosoft.com.`

IAM Identity Center 不希望电子邮件地址包含该*#EXT#@domain*格式。

1. 登录到 Microsoft Entra 管理中心，导航到身份 > 应用程序 > 企业应用程序，然后选择 Amazon IAM Identity Center
2. 导航到左侧窗格的单点登录选项卡。
3. 选择显示在用户属性和声明旁边的编辑。
4. 依次选择必填声明和唯一用户标识符（姓名 ID）。
5. 将为 Microsoft Entra ID 用户和访客用户创建两个声明条件：

    a. 若为 Microsoft Entra ID 用户，则为源属性设为 `user.userprincipalname` 的成员创建用户类型。

    b. 若为 Microsoft Entra ID 访客用户，则为源属性设为 `user.mail` 的外部访客创建用户类型。

    c. 选择保存，然后重新尝试以 Microsoft Entra ID 访客用户身份登录。

其他资源

- 有关 SCIM 一般性问题排查的提示，请参阅排查 IAM Identity Center 问题。
- 有关 Microsoft Entra ID 问题排查，请参阅 Microsoft 文档。
- 要了解有关跨多重联合的更多信息 Amazon Web Services 账户，请参阅Amazon Web Services 账户 使用进行保护Azure Active Directory Federation。

以下资源可以帮助您在使用时进行故障排除 Amazon：

- Amazon Web Services re:Post-查找 FAQs 并链接到其他资源以帮助您解决问题。
- Amazon Web Services 支持 – 获得技术支持

通过 Okta 和 IAM Identity Center 配置 SAML 和 SCIM

您可以使用跨域身份管理系统（SCIM）2.0 协议将用户和组信息从 Okta 自动预置或同步到 IAM Identity Center。有关更多信息，请参阅 对外部身份提供者使用 SAML 和 SCIM 身份联合验证。

要在 Okta 中配置此连接，您可以使用 IAM Identity Center 的 SCIM 端点和 IAM Identity Center 自动创建的持有者令牌。配置 SCIM 同步时，您将在 Okta 中创建用户属性到 IAM Identity Center 中的命名属性的映射。此映射在 IAM Identity Center 和 Okta 账户之间匹配预期的用户属性。

Okta 通过 SCIM 连接到 IAM Identity Center 时支持以下预置功能：

- 创建用户——在 Okta 中分配给 IAM Identity Center 应用程序的用户是在 IAM Identity Center 中预置的。
- 更新用户属性——在 Okta 中分配给 IAM Identity Center 应用程序的用户的属性更改将在 IAM Identity Center 中更新。
- 停用用户——在 Okta 中从 IAM Identity Center 应用程序取消分配的用户将在 IAM Identity Center 被禁用。
- 组推送——Okta 中的组（及其成员）同步到 IAM Identity Center。

> **Note**
>
> 为了最大限度地减少 Okta 和 IAM Identity Center 的管理开销，我们建议您分配和推送组而不是单个用户。

- 导入用户 — 用户可以从 IAM 身份中心导入Okta。

目标

在本教程中，您将逐步设置与 Okta IAM Identity Center 的 SAML 连接。稍后，您将使用 SCIM 从 Okta 同步用户。在该方案中，您可以管理 Okta 中的所有用户和组。用户通过 Okta 门户登录。要验证所有配置是否正确，完成配置步骤后，您将以Okta用户身份登录并验证对 Amazon 资源的访问权限。

通过 SAML 连接Okta到 IAM 身份中心时，支持以下功能：

- IDP 发起的 SAML 登录 — 用户通过Okta门户登录并获得 IAM 身份中心的访问权限。
- SP 发起的 SAML 登录 — 用户访问 Amazon Web Services 访问门户，该门户会将他们重定向到通过门户登录。Okta

> **Note**
>
> 您可以注册安装了 Okta's IAM Identity Center 应用程序的 Okta 账户（免费试用）。对于付费 Okta 产品，您可能需要确认您的 Okta 许可证支持生命周期管理或类似的功能，以实现出站预置。将 SCIM 从 Okta 配置到 IAM Identity Center 可能需要这些功能。
> 如果您尚未启用 IAM Identity Center，请参阅 启用 IAM Identity Center。

注意事项

- 在 Okta 和 IAM Identity Center 之间配置 SCIM 预置之前，建议先查看 使用自动预置的注意事项。
- 必须已为每位 Okta 用户指定名字、姓氏、用户名和显示名称值。
- 每位 Okta 用户的每个数据属性（如电子邮件地址或电话号码）只有一个值。若用户有多个值，则无法同步。如果用户的属性中有多个值，请先删除重复的属性，然后再尝试在 IAM Identity Center 中预置用户。例如，只能同步一个电话号码属性，因为默认的电话号码属性是“工作电话”，所以即使用户的电话号码是家庭电话号码或移动电话号码，也将使用“工作电话”属性存储其电话号码。
- Okta 与 IAM Identity Center 共用时，IAM Identity Center 通常在 Okta 中配置为应用程序。这样即可将 IAM Identity Center 的多个实例配置为多个应用程序，以此支持在单个 Okta 实例中访问多个 Amazon 组织。
- 不支持权限和角色属性，也无法将其同步到 IAM Identity Center。
- 目前不支持使用相同的 Okta 组进行分配和组推送。要在 Okta 和 IAM Identity Center 之间保持一致的组成员资格，请创建一个单独的组并将其配置为将组推送到 IAM Identity Center。
- 如果您将 IAM Identity Center 复制到其他区域，则必须更新您的身份提供商配置，以允许访问 Amazon 托管应用程序和 Amazon Web Services 账户 通过其他区域。有关包括先决条件在内的更多详细信息，请参阅跨多个 IAM 身份中心使用 Amazon Web Services 区域。OKTA 特定的步骤请参见 Okta用于访问其他区域的配置

步骤 1：Okta：从 Okta 账户获取 SAML 元数据

1. 登录 Okta admin dashboard，展开应用程序，然后选择应用程序。

2. 在应用程序页面，选择浏览应用程序目录。
3. 在搜索框中键入 Amazon IAM Identity Center，选择要添加 IAM Identity Center 应用程序的应用程序。
4. 选择登录选项卡。
5. 在 SAML 签名证书下，选择操作，然后选择查看 IdP 元数据。将打开一个新的浏览器选项卡，显示 XML 文件的文档树。选择从 `<md:EntityDescriptor>` 到 `</md:EntityDescriptor>` 的所有 XML，将其复制到文本文件。
6. 将文本文件保存为 `metadata.xml`。

让 Okta admin dashboard 保持打开状态，因为后续步骤会继续使用此控制台。

步骤 2：IAM Identity Center：将 Okta 配置为 IAM Identity Center 的身份源

1. 以具有管理权限的用户身份打开 IAM Identity Center 控制台。
2. 在左侧导航窗格中，选择设置。
3. 在设置页面，选择操作，然后选择更改身份源。
4. 在选择身份源下选择外部身份提供者，然后选择下一步。
5. 在配置外部身份提供商下，执行以下操作：

   a. 在服务提供商元数据下，将以下项目复制到文本文件以便于访问：

      - IAM Identity Center 断言消费者服务 (ACS) 网址 — 您可以选择 IPv4仅限和双栈 ACS。URLs此外，如果您的 IAM Identity Center 实例已在多个区域启用，则每个其他区域都有自己的 IPv4仅限双栈 ACS。 URLs有关 ACS 的更多信息 URLs，请参阅主端点和附加端点中的 ACS 端点 Amazon Web Services 区域。
      - IAM Identity Center 发布者 URL

      本教程稍后会用到这些值。

   b. 在身份提供者元数据下的 IdP SAML 元数据下，选择选择文件，然后选择您在上一步创建的 `metadata.xml` 文件。

   c. 选择下一步。
6. 阅读免责声明并准备继续操作后，输入接受。
7. 选择更改身份源。

   保持 Amazon 控制台处于打开状态，您将在下一步中继续使用此控制台。

8. 返回Okta admin dashboard并选择 Amazon IAM Identity Center 应用程序的 “登录” 选项卡，然后选择 “编辑”。
9. 在高级登录设置下，输入以下内容：
   - 对于 ACS URL，输入您为 IAM 身份中心断言消费者服务 (ACS) 网址复制的值。您可以使用主要区域的 ACS URL 作为默认区域，这样当用户从中启动 Amazon Web Services 应用程序时，他们就会被重定向到主要区域Okta。
   - （可选）如果您将 IAM Identity Center 复制到其他区域，则还可以在中Okta为每个其他区域的 Amazon Web Services 访问门户创建书签应用程序。这使您的用户能够从中 Amazon Web Services 访问其他地区的访问门户Okta。请务必向您的用户授予访问中的书签应用程序的权限Okta。有关更多详细信息，请参阅Okta文档。如果您计划稍后将 IAM Identity Center 复制到其他区域，请访问以获取Okta用于访问其他区域的配置有关如何在初始设置后启用对其他区域的访问权限的指导。
   - 在发布者 URL 中，输入您复制的 IAM Identity Center 发布者 URL 值
   - 在应用程序用户名格式中，选择菜单中的一个选项。

     确保您选择的值对每个用户来说都是唯一的。在本教程中，选择 Okta 用户名
10. 选择保存。

现在，您可以将用户从 Okta 预置到 IAM Identity Center。让 Okta admin dashboard 保持打开状态，返回 IAM Identity Center 控制台，执行下一步。

步骤 3：IAM Identity Center 和 Okta：预置 Okta 用户

1. 在 IAM Identity Center 控制台的设置页面，找到自动预置信息框，然后选择启用。这会在 IAM Identity Center 中启用自动预置，并显示必要的 SCIM 端点和访问令牌信息。
2. 在入站自动预置对话框中，复制以下选项的各个值：
   a. SCIM 端点-端点格式取决于您的配置：
      - IPv4: https://scim。*us-east-2*.amazonaws.com/ /scim/v2 *11111111111-2222-3333-4444-555555555555*
      - 双栈：https://scim。*us-east-2*.api.aws/ /scim/v2 *11111111111-2222-3333-4444-555555555555*

   b. 访问令牌 - 选择显示令牌以复制该值。

> **Warning**
>
> 这是唯一可以获取 SCIM 端点与访问令牌的机会。在继续操作之前，务必复制这些值。本教程的后续步骤需要输入这些值，以便在 Okta 中配置自动预置。

3. 选择关闭。
4. 返回 Okta admin dashboard，移到 IAM Identity Center 应用程序。
5. 在 IAM Identity Center 应用程序页面，选择预置选项卡，然后在左侧导航栏的设置下选择集成。
6. 选择编辑，然后选中启用 API 集成旁边的复选框，以启用自动预置。
7. Okta使用您在本步骤前面复制的 Amazon IAM Identity Center SCIM 配置值进行配置：
   a. 在基本 URL 字段，输入 SCIM 端点值。
   b. 在 API 令牌字段，输入访问令牌值。
8. 选择测试 API 凭证以验证输入的凭证是否有效。

   将显示 Amazon IAM Identity Center 验证成功！消息。
9. 选择保存。您将移至设置部分，集成为选中状态。
10. 在设置下，选择至应用程序，然后为每个要启用的预置至应用程序功能选择启用复选框。在本教程中，请选择所有选项。
11. 选择保存。

现在，您可以将来自 Okta 的用户与 IAM Identity Center 同步了。

步骤 4：Okta：将来自 Okta 的用户与 IAM Identity Center 同步

默认情况下，未将任何组或用户分配给您的 Okta IAM Identity Center 应用程序。通过预置组，该组的成员用户也会被预置。完成以下步骤，将组和用户与同步 Amazon IAM Identity Center。

1. 在 Okta IAM Identity Center 应用程序页面中，选择分配选项卡。您可以将人员和组分配至 IAM Identity Center 应用程序。
   a. 要分配人员：
      - 在分配页面，选择分配，然后选择分配给人员。

- 选择您想要为其分配 IAM Identity Center 应用程序访问权限的 Okta 用户。选择分配，选择保存并返回，然后选择完成。

这将启动将用户预置到 IAM Identity Center 的过程。

b. 要分配组：

- 在分配页面，选择分配，然后选择分配给组。
- 选择您想要为其分配 IAM Identity Center 应用程序访问权限的 Okta 组。选择分配，选择保存并返回，然后选择完成。

这将启动将组中的用户预置到 IAM Identity Center 的过程。

> **Note**
>
> 如果所有用户记录中都没有该组的属性，您可能需要为该组指定其他属性。为组指定的属性将覆盖任何单独属性的值。

2. 选择推送组选项卡。选择要与 IAM Identity Center 同步的 Okta 组。选择保存。

将组及其成员推送到 IAM Identity Center 后，组状态将更改为活动。

3. 返回分配选项卡。
4. 要向 IAM Identity Center 添加个人 Okta 用户，请执行以下步骤：

a. 在分配页面，选择分配，然后选择分配给人员。

b. 选择您想要为其分配 IAM Identity Center 应用程序访问权限的 Okta 用户。选择分配，选择保存并返回，然后选择完成。

这将启动将单个用户预置到 IAM Identity Center 的过程。

> **Note**
>
> 您也可以从的应用程序页面为 Amazon IAM Identity Center 应用程序分配用户和群组 Okta admin dashboard。要这样做，请选择设置图标，然后选择分配给用户或分配给组，然后指定用户或组。

5. 返回 IAM Identity Center 控制台。在左侧导航栏中，选择用户，您应该会看到用户列表填入了您的 Okta 用户。

恭喜您！

您已成功在Okta和之间建立了 SAML 连接， Amazon 并已验证自动配置正在运行。您现在可以在 IAM Identity Center 中将这些用户分配给账户和应用程序。在本教程的下一步，我们将指定一名用户，通过赋予其对管理账户的管理权限，使其成为 IAM Identity Center 管理员。

传递访问控制属性 – 可选

您可以选择使用 IAM Identity Center 中的 访问控制属性 功能来传递 `Name` 属性设置为 `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` 的 `Attribute` 元素。此元素允许您将属性作为 SAML 断言中的会话标签传递。有关会话标签的更多信息，请参阅 IAM 用户指南在 Amazon STS中的传递会话标签。

要将属性作为会话标签传递，请包含指定标签值的 `AttributeValue` 元素。例如，要传递标签键值对`CostCenter = blue`，请使用以下属性。

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

如果您需要添加多个属性，请为每个标签包含一个单独的 `Attribute` 元素。

将访问权限分配给 Amazon Web Services 账户

仅授予访问权限时才需要执行以下步骤。 Amazon Web Services 账户 授予 Amazon 应用程序访问权限不需要这些步骤。

Note

要完成此步骤，您需要拥有 IAM Identity Center 的 Organization 实例。有关更多信息，请参阅 IAM Identity Center 的组织和账户实例。

步骤 1：IAM Identity Center：向 Okta 用户授予账户访问权限

1. 在 IAM Identity Center 导航窗格的多账户权限下，选择 Amazon Web Services 账户。

2. 在 Amazon Web Services 账户 页面，组织结构将显示您的组织根目录，您的账户将以分层结构列于其下方。选中管理账户对应的复选框，然后选择分配用户或组。
3. 此时将显示分配用户和组工作流程。它包括三个步骤：

   a. 对于步骤 1：选择用户和组，选择将要执行管理员工作职能的用户。然后选择下一步。

   b. 对于步骤 2：选择权限集，选择创建权限集打开新的标签页，该标签页将引导您完成创建权限集所涉及的三个子步骤。

      i. 对于步骤 1：选择权限集类型，请完成以下操作：

         - 在权限集类型中，选择预定义权限集。
         - 在预定义权限集的策略中，选择AdministratorAccess。

         选择下一步。

      ii. 对于步骤 2：指定权限集详细信息，保留默认设置，并选择下一步。

         默认设置会创建名为*AdministratorAccess*、会话持续时间设置为一小时的权限集。

      iii. 对于步骤 3：查看并创建，请验证权限集类型是否使用 Amazon 托管策略AdministratorAccess。选择创建。权限集页面会显示通知，告知您权限集已创建。您可以在网络浏览器中关闭此标签页。

      在分配用户和组浏览器标签页，您仍处于步骤 2：选择权限集，您将在这里启动创建权限集工作流程。

      在权限集区域，选择刷新按钮。您创建的*AdministratorAccess*权限集将出现在列表中。选择该权限集的复选框，然后选择下一步。

   c. 对于步骤 3：查看并提交，请查看选定的用户和权限集，然后选择提交。

      页面更新时会显示一条消息，告知您 Amazon Web Services 账户 正在配置中。等待该过程完成。

      您将返回到该 Amazon Web Services 账户 页面。系统会显示一条通知消息，告知您 Amazon Web Services 账户 已重新配置并应用了更新的权限集。当用户登录时，他们可以选择角色。*AdministratorAccess*

步骤 2Okta：确认Okta用户对 Amazon 资源的访问权限

1. 使用测试用户账户登录 Okta dashboard。
2. 在我的应用程序下，选择 Amazon IAM Identity Center 图标。
3. 你应该会看到图 Amazon Web Services 账户 标。展开该图标可查看用户可以访问的 Amazon Web Services 账户 列表。在本教程中，您只使用了一个账户，因此展开图标只显示一个账户。
4. 选择账户，以显示用户可用的权限集。在本教程中，您创建了AdministratorAccess权限集。
5. 权限集旁边是该权限集可用访问权限类型的链接。创建权限集时，您指定了访问权限 Amazon Web Services 管理控制台 和编程访问权限。选择管理控制台，打开 Amazon Web Services 管理控制台。
6. 用户已登录到 Amazon Web Services 管理控制台。

您也可以使用 Amazon Web Services 访问门户。这会将您重定向到通过Okta门户登录，然后再将您带到 Amazon Web Services 访问门户。此路径遵循由 SP 发起的 SAML 登录流程。

Okta访问 IAM 身份中心其他区域的配置-可选

如果您将 IAM Identity Center 复制到其他区域，则必须更新您的身份提供商配置，以允许访问 Amazon 托管应用程序和 Amazon Web Services 账户 通过其他区域。以下步骤将指导您完成整个过程。有关本主题的更多详细信息（包括先决条件），请参阅跨多个 IAM 身份中心使用 Amazon Web Services 区域。

1. 从 IAM 身份中心控制台检索其他区域的 ACS URLs ，如中所述主端点和附加端点中的 ACS 端点 Amazon Web Services 区域。
2. 在Okta管理控制面板的导航窗格中，选择应用程序，然后在展开的列表中再次选择应用程序。
3. 选择 Amazon IAM Identity Center 应用程序。
4. 选择 Sign On（登录）选项卡。
5. 在 “高级登录设置” 和 “其他可请求的 SSO” 下 URLs，为每个其他区域的 ACS URL 选择添加另一个，然后将 ACS URL 粘贴到文本字段中。
6. 添加 ACS 后 URLs，保存Amazon IAM Identity Center应用程序。
7. 您可以在中Okta为每个其他区域的 Amazon Web Services 访问门户创建书签应用程序。这使您的用户能够从中 Amazon Web Services 访问其他地区的访问门户Okta。请务必向您的用户授予访问中的书签应用程序的权限Okta。有关更多详细信息，请参阅Okta文档。
8. 确认您可以登录其他每个地区的 Amazon Web Services 访问门户。导航到Amazon Web Services 访问门户 URLs或从中启动书签应用程序Okta。

后续步骤

现在，您已在 IAM Identity Center 将 Okta 配置为身份提供商，并预置了用户，您可以：

- 授予访问权限 Amazon Web Services 账户，请参阅为用户或群组分配访问权限 Amazon Web Services 账户。
- 授予对云应用程序的访问权限，请参阅 在 IAM Identity Center 控制台中为用户分配应用程序的访问权限。
- 根据工作职能配置权限，请参阅创建权限集。

问题排查

有关使用 Okta 对 SCIM 和 SAML 进行一般性问题排查，请参阅以下各部分：

- 重新配置从 IAM Identity Center 删除的用户和组
- Okta 中的自动预置错误
- 特定用户无法从外部 SCIM 提供商同步到 IAM Identity Center
- 与 IAM Identity Center 创建的 SAML 断言内容有关的问题
- 使用外部身份提供者预置用户或组时出现重复用户或组错误
- 其他资源

重新配置从 IAM Identity Center 删除的用户和组

- 如果尝试更改 Okta 中已同步后又从 IAM Identity Center 中删除的用户或组，则可能会在 Okta 控制台中收到以下错误消息：
  - 自动将用户个人资料推送*Jane Doe*到应用程序 Amazon IAM Identity Center 失败：尝试推送个人资料更新时出错*jane_doe@example.com*：用户未返回任何用户 *xxxxx-xxxxxx-xxxxx-xxxxxxx*
  - 中缺少关联的群组 Amazon IAM Identity Center。Change the linked group to resume pushing group memberships.
- 对于已同步和删除的 IAM Identity Center 用户或组，还可能在 Okta 的系统日志中收到以下错误消息：
  - Okta 错误：事件失败 application.provision.user.puser.push_profile：用户未返回任何 *xxxxx-xxxxxx-xxxxx-xxxxxxx*

- Okta 错误：application.provision.group_push_push.mapping.update.or.delete.failed.with.error：中缺少链接组。 Amazon IAM Identity Center Change the linked group to resume pushing group memberships.

> **Warning**
>
> 如已使用 SCIM 同步 Okta 和 IAM Identity Center，则应从 Okta 而非 IAM Identity Center 中删除用户和组。

排查已删除的 IAM Identity Center 用户问题

要解决已删除的 IAM Identity Center 用户的这一问题，必须从 Okta 中删除这些用户。如有必要，还需在 Okta 中重新创建这些用户。在 Okta 中重新创建用户时，还会通过 SCIM 将其重新预置到 IAM Identity Center。有关删除用户的更多信息，请参阅 Okta 文档。

> **Note**
>
> 如需移除 Okta 用户对 IAM Identity Center 的访问权限，则应先将其从“组推送”中移除，再将其从 Okta 的分配组中移除。这可确保在 IAM Identity Center 中将用户从关联组成员资格中移除。有关“组推送”问题排查的更多信息，请参阅 Okta 文档。

排查已删除的 IAM Identity Center 组问题

要解决已删除的 IAM Identity Center 组的这一问题，必须从 Okta 中删除组。如有必要，还需要使用“组推送”在 Okta 中重新创建这些组。在 Okta 中重新创建用户时，还会通过 SCIM 将其重新预置到 IAM Identity Center。有关删除组的更多信息，请参阅 Okta 文档。

Okta 中的自动预置错误

如果在 Okta 中收到以下错误消息：

将用户 Jane Doe 自动配置到应用程序 Amazon IAM Identity Center 失败：未找到匹配的用户

有关更多信息，请参阅 Okta 文档。

其他资源

- 有关 SCIM 一般性问题排查的提示，请参阅排查 IAM Identity Center 问题。

以下资源可以帮助您在使用时进行故障排除 Amazon：

- Amazon Web Services re:Post-查找 FAQs 并链接到其他资源以帮助您解决问题。
- Amazon Web Services 支持 – 获得技术支持

在 OneLogin 和 IAM Identity Center 之间设置 SCIM 预置

IAM Identity Center 支持使用跨域身份管理系统 (SCIM) v2.0 协议将用户和组信息从 OneLogin 自动预置（同步）到 IAM Identity Center。有关更多信息，请参阅 对外部身份提供者使用 SAML 和 SCIM 身份联合验证。

> **Note**
>
> OneLogin目前不支持应用程序 URLs中的 SAML 多重断言使用服务 (ACS)。 Amazon IAM Identity Center 要充分利用 IAM Identity Center 中的多区域支持，必须使用此 SAML 功能。如果您计划将 IAM Identity Center 复制到其他区域，请注意，使用单个 ACS URL 可能会影响这些其他区域的用户体验。您的主要区域将继续正常运行。我们建议您与 IdP 供应商合作以启用此功能。有关使用单个 ACS URL 在其他区域的用户体验的更多信息，请参阅the section called “使用没有多个 ACS 的 Amazon 托管应用程序 URLs”和the section called “Amazon Web Services 账户 无需多个 ACS 即可实现访问弹性 URLs”。

您可以在 OneLogin 中使用 IAM Identity Center 的 SCIM 端点和 IAM Identity Center 自动创建的持有者令牌来配置此连接。配置 SCIM 同步时，您将在 OneLogin 中创建用户属性到 IAM Identity Center 中的命名属性的映射。这会导致 IAM Identity Center 和 OneLogin 之间的预期属性匹配。

以下步骤将引导您了解如何使用 SCIM 协议将用户和组从 OneLogin 自动预置到 IAM Identity Center。

> **Note**
>
> 在开始部署 SCIM 之前，我们建议您首先查看 使用自动预置的注意事项。

主题

先决条件

在开始之前，您将需要以下内容：

- 一个 OneLogin 帐户。如果您没有现有帐户，您可以从 OneLogin 网站获取免费试用版或开发者帐户。
- 支持 IAM Identity Center 的帐户（免费）。有关更多信息，请参阅启用 IAM Identity Center。
- 从您的 OneLogin 帐户到 IAM Identity Center 的 SAML 连接。有关详细信息，请参阅 Amazon 合作伙伴网络博客上的在 OneLogin 和 Amazon之间启用单点登录。

步骤 1：在 IAM Identity Center 中启用预置

在第一步中，您使用 IAM Identity Center 控制台启用自动预置。

在 IAM Identity Center 中启用自动预置

1. 完成先决条件后，打开 IAM Identity Center 控制台。
2. 在左侧导航窗格中选择设置。
3. 在设置页面上，找到自动预置信息框，然后选择启用。这会立即在 IAM Identity Center 中启用自动预置，并显示必要的 SCIM 端点和访问令牌信息。
4. 在入站自动预置对话框中，复制 SCIM 端点和访问令牌。稍后在 IdP 中配置预置时，您需要粘贴这些内容。

    a. SCIM 端点 ——例如，https://scim。*us-east-2*.amazonaws.com/ /scim/v2*11111111111-2222-3333-4444-555555555555*

    b. 访问令牌 - 选择显示令牌以复制该值。

> **Warning**
>
> 这是唯一可以获取 SCIM 端点与访问令牌的机会。在继续操作之前，务必复制这些值。本教程的后续步骤需要输入这些值，以便在 IdP 中配置自动预置。

5. 选择关闭。

您现在已在 IAM Identity Center 控制台中设置预置。现在，您需要使用 OneLogin 管理控制台执行其余任务，如以下过程中所述。

步骤2：在 OneLogin 中配置预置

在 OneLogin 管理控制台中使用以下过程来启用 IAM Identity Center 和 IAM Identity Center 应用程序之间的集成。此过程假设您已经在中配置了 Amazon 单点登录应用程序OneLogin以进行 SAML 身份验证。如果您尚未创建此 SAML 连接，请在继续之前创建此连接，然后返回此处完成 SCIM 预置过程。有关使用 OneLogin 配置 SAML 的更多信息，请参阅 Amazon 合作伙伴网络博客上的在 OneLogin 和 Amazon之间启用单点登录。

要在 OneLogin 中配置预置

1. 登录 OneLogin，然后导航至应用程序>应用程序。
2. 在应用程序页面上，搜索您之前创建的应用程序以与 IAM Identity Center 形成 SAML 连接。选择它，然后从导航栏中选择配置。
3. 在上一过程中，您复制了 IAM Identity Center 中的 SCIM 端点值。将该值粘贴到 OneLogin 中的 SCIM Base URL 字段中。此外，在之前的过程中，您复制了 IAM Identity Center 中的访问令牌值。将该值粘贴到 OneLogin 中的 SCIM 持有者令牌字段中。
4. 在API 连接旁边，单击启用，然后单击保存以完成配置。
5. 在导航窗格中，选择 Provisioning（预调配）。
6. 选中启用预置、创建用户、删除用户和更新用户复选框，然后选择保存。
7. 在导航窗格中，选择 Users（用户）。
8. 单击更多操作，然后选择同步登录。您应该收到消息正在使用 Amazon 单点登录同步用户。
9. 再次单击更多操作，然后选择重新应用权限映射。您应该会收到消息映射正在重新应用。
10. 此时，预置过程应该开始。要确认这一点，请导航至活动>事件，并监控进度。成功的预置事件以及错误应该出现在事件流中。
11. 要验证您的用户和组是否已全部成功同步到 IAM Identity Center，请返回 IAM Identity Center 控制台并选择用户。您从 OneLogin 同步的用户出现在用户页面上。您还可以在组页面查看已同步的组。
12. 要将用户更改自动同步到 IAM Identity Center，请导航到配置页面，找到 “执行此操作之前需要管理员批准” 部分，取消选择 “创建用户”、“删除用户”、“ and/or 更新用户”，然后单击 “保存”。

（可选）第三步：在 OneLogin IAM Identity Center 中配置用户属性进行访问控制

OneLogin如果您选择配置将在 IAM Identity Center 中使用的属性来管理对 Amazon 资源的访问权限，则这是一个可选过程。您在 OneLogin 中定义的属性将在 SAML 断言中传递到 IAM Identity Center。然后，您将在 IAM Identity Center 中创建一个权限集，以根据您从 OneLogin 传递的属性来管理访问。

在开始此过程之前，您必须首先启用 访问控制属性 功能。有关此操作的详细信息，请参阅 启用并配置访问控制属性。

要在 OneLogin 中配置用户属性，用于 IAM Identity Center 的访问控制

1. 登录 OneLogin，然后导航至应用程序>应用程序。
2. 在应用程序页面上，搜索您之前创建的应用程序以与 IAM Identity Center 形成 SAML 连接。选择它，然后从导航栏中选择参数。
3. 在必需参数部分中，对您要在 IAM Identity Center 中使用的每个属性执行以下操作：
   a. 选择 +。
   b. 在字段名称中，输入 `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`AttributeName`**，并将 **`AttributeName`** 替换为您在 IAM Identity Center 中期望的属性名称。例如 `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Department`**。
   c. 在标志下，选中包含在 SAML 断言中旁边的框，然后选择保存。
   d. 在值字段中，使用下拉列表选择 OneLogin 用户属性。例如，部门。
4. 选择保存。

（可选）传递访问控制属性

您可以选择使用 IAM Identity Center 中的 访问控制属性 功能来传递 Name 属性设置为 `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`** 的 `Attribute` 元素。此元素允许您将属性作为 SAML 断言中的会话标签传递。有关会话标签的更多信息，请参阅 IAM 用户指南在 Amazon STS中的传递会话标签。

要将属性作为会话标签传递，请包含指定标签值的 `AttributeValue` 元素。例如，要传递标签键值对`CostCenter = blue`，请使用以下属性。

```
<saml:AttributeStatement>
```

```
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

如果您需要添加多个属性，请为每个标签包含一个单独的 `Attribute` 元素。

问题排查

以下内容可以帮助您解决在使用 OneLogin 设置自动预置时可能遇到的一些常见问题。

组未配置到 IAM Identity Center

默认情况下，组可能无法从 OneLogin 配置到 IAM Identity Center。确保您已在 OneLogin 中为 IAM Identity Center 应用程序启用组预置。为此，请登录 OneLogin 管理控制台，并检查以确保在 IAM Identity Center 应用程序的属性（IAM Identity Center 应用程序 > 参数 > 组）下选择了包含在用户预置中选项。有关如何在 OneLogin 中创建组的更多详细信息，包括如何在 SCIM 中将 OneLogin 角色同步为组，请参阅 OneLogin 网站。

尽管所有设置均正确，但没有任何内容从 OneLogin 同步到 IAM Identity Center

除了上面有关管理员批准的注释之外，您还需要重新应用权限映射才能使许多配置更改生效。这可以在应用程序 > 应用程序 > IAM Identity Center 应用程序 > 更多操作中找到。您可以在 OneLogin 中查看大多数操作的详细信息和日志，包括活动 > 事件下的同步事件。

我已删除或禁用 OneLogin 中的一个组，但它仍然出现在 IAM Identity Center 中

OneLogin 目前不支持组的 SCIM DELETE 操作，这意味着该组继续存在于 IAM Identity Center 中。因此，您必须直接从 IAM Identity Center 中删除该组，以确保删除 IAM Identity Center 中该组的任何相应权限。

我在 IAM Identity Center 中删除了一个群组，但没有先将其从中OneLogin删除，现在我遇到了 user/group 同步问题

要解决这种情况，首先确保您没有 OneLogin 中的任何冗余组预置规则或配置。例如，直接分配给应用程序的组以及发布到同一组的规则。接下来，删除 IAM Identity Center 中任何不需要的组。最后，在 OneLogin 中，刷新权限（IAM Identity Center 应用程序 > 预置 > 权限），然后重新应用权限映射（IAM Identity Center 应用程序 > 更多操作）。为了避免将来出现此问题，请首先进行更改以停止预置 OneLogin 中的组，然后从 IAM Identity Center 中删除该组。

将 Ping Identity 产品与 IAM Identity Center 结合使用

以下 Ping Identity 产品已通过 IAM Identity Center 测试。

主题

PingFederate

IAM Identity Center 支持通过 Ping Identity（以下简称“Ping”）将 PingFederate 产品中的用户和组信息自动预置（同步）到 IAM Identity Center。此预置使用跨域身份管理系统 (SCIM) v2.0 协议。有关更多信息，请参阅 对外部身份提供者使用 SAML 和 SCIM 身份联合验证。

您可以使用 IAM Identity Center SCIM 端点和访问令牌在 PingFederate 中配置此连接。配置 SCIM 同步时，您将在 PingFederate 中创建用户属性到 IAM Identity Center 中的命名属性的映射。这会导致 IAM Identity Center 和 PingFederate 之间的预期属性匹配。

本指南基于 PingFederate version 10.2。其他版本的步骤可能有所不同。请联系 Ping，了解有关如何为其他版本的 PingFederate 预置 IAM Identity Center 的更多信息。

以下步骤将引导您了解如何使用 SCIM 协议将用户和组从 PingFederate 自动预置到 IAM Identity Center。

> **Note**
>
> 在开始部署 SCIM 之前，我们建议您首先查看 使用自动预置的注意事项。然后继续查看下一部分中的其他注意事项。

主题

- 问题排查

先决条件

在开始之前，您将需要以下内容：

- 一台正在运行的 PingFederate 服务器。如果您没有现有 PingFederate 服务器，您可以从 Ping Identity 网站获取免费试用版或开发人员帐户。该试用版包括许可证和软件下载以及相关文档。
- 安装在您的 PingFederate 服务器上的 PingFederate IAM Identity Center 连接器软件的副本。有关如何获取该软件的更多信息，请参阅 Ping Identity 网站上的 IAM Identity Center Connector。
- 支持 IAM Identity Center 的帐户（免费）。有关更多信息，请参阅启用 IAM Identity Center。
- 从 PingFederate 实例到 IAM Identity Center 的 SAML 连接。有关如何配置此连接的说明，请参阅 PingFederate 文档。综上所述，推荐的路径是使用 IAM Identity Center Connector 在 PingFederate 中配置“浏览器 SSO”，利用两端的“下载”和“导入”元数据功能在 PingFederate 和 IAM Identity 之间交换 SAML 元数据 中心。
- 如果您将 IAM Identity Center 复制到其他区域，则必须更新您的身份提供商配置以允许访问 Amazon 托管应用程序和 Amazon Web Services 账户 从这些区域访问托管应用程序。有关更多详细信息，请参阅the section called “步骤 3：更新外部 IdP 设置”。有关更多详细信息，请参阅 PingFederate文档。

注意事项

以下是关于 PingFederate 的重要注意事项，它们可能会影响您使用 IAM Identity Center 实施预置的方式。

- 如果从 PingFederate 中配置的数据存储中的用户删除某个属性（例如电话号码），则不会从 IAM Identity Center 中的相应用户中删除该属性。这是 PingFederate’s 置备程序实现中的一个已知限制。如果用户的属性更改为不同的（非空）值，则该更改将同步到 IAM Identity Center。

步骤 1：在 IAM Identity Center 中启用预置

在第一步中，您使用 IAM Identity Center 控制台启用自动预置。

在 IAM Identity Center 中启用自动预置

1. 完成先决条件后，打开 IAM Identity Center 控制台。
2. 在左侧导航窗格中选择设置。

3. 在设置页面上，找到自动预置信息框，然后选择启用。这会立即在 IAM Identity Center 中启用自动预置，并显示必要的 SCIM 端点和访问令牌信息。
4. 在入站自动预置对话框中，复制 SCIM 端点和访问令牌。稍后在 IdP 中配置预置时，您需要粘贴这些内容。

   a. SCIM 端点 ——例如，https://scim。*us-east-2*.amazonaws.com/ /scim/v2 *11111111111-2222-3333-4444-555555555555*

   b. 访问令牌 - 选择显示令牌以复制该值。

> **Warning**
>
> 这是唯一可以获取 SCIM 端点与访问令牌的机会。在继续操作之前，务必复制这些值。本教程的后续步骤需要输入这些值，以便在 IdP 中配置自动预置。

5. 选择关闭。

现在您已在 IAM Identity Center 控制台中设置了预置，您必须使用 PingFederate 管理控制台完成剩余任务。以下过程中描述了这些步骤。

步骤2：在 PingFederate 中配置预置

在 PingFederate 管理控制台中使用以下过程启用 IAM Identity Center 和 IAM Identity Center 连接器之间的集成。此过程假设您已安装 IAM Identity Center Connector 软件。如果您尚未执行此操作，请参阅先决条件，然后完成此过程来配置 SCIM 预置。

> **Important**
>
> 如果您的 PingFederate 服务器之前尚未针对出站 SCIM 配置进行配置，您可能需要更改配置文件才能启用预置。有关更多信息，请参阅 Ping 文档。总之，您必须将 pingfederate-<version>/pingfederate/bin/run.properties 文件中的 `pf.provisioner.mode` 设置修改为 `OFF`（默认值）以外的值，并重新启动服务器（如果当前正在运行）。例如，如果您当前没有 PingFederate 的高可用性配置，您可以选择使用 `STANDALONE`。

要在 PingFederate 中配置预置

1. 登录到 PingFederate 管理控制台。

2. 从页面顶部选择应用程序，然后单击 SP 连接。
3. 找到您之前创建的用于与 IAM Identity Center 形成 SAML 连接的应用程序，然后单击连接名称。
4. 从页面顶部附近的黑色导航标题中选择连接类型。您应该看到已从之前的 SAML 配置中选择了浏览器 SSO。如果没有，您必须先完成这些步骤才能继续。
5. 选中出站预置复选框，选择 IAM Identity Center Cloud Connector 作为类型，然后单击保存。如果 IAM Identity Center Cloud Connector 未显示为选项，请确保您已安装 IAM Identity Center Connector 并已重新启动 PingFederate 服务器。
6. 重复单击下一步，直到到达出站预置页面，然后单击配置预置按钮。
7. 在上一过程中，您复制了 IAM Identity Center 中的 SCIM 端点值。将该值粘贴到 PingFederate 控制台中的 SCIM URL 字段中。此外，在之前的过程中，您复制了 IAM Identity Center 中的访问令牌值。将该值粘贴到 PingFederate 控制台中的访问令牌字段中。单击保存。
8. 在频道配置（配置频道）页面上，单击创建。
9. 输入此新预置频道的频道名称（例如 **`AWSIAMIdentityCenterchannel`**），然后单击下一步。
10. 在源页面上，选择要用于连接到 IAM Identity Center 的活动数据存储，然后单击下一步。动数据存储，然后单击下一步。

> **Note**
>
> 如果您尚未配置数据来源，则必须立即配置。有关如何在 PingFederate 中选择和配置数据来源的信息，请参阅 Ping 产品文档。

11. 在源设置页面上，确认安装的所有值均正确，然后单击下一步。
12. 在源位置页面上，输入适合您的数据来源的设置，然后单击下一步。例如，如果使用 Active Directory 作为 LDAP 目录：

    a. 输入 AD 林的基本 DN（例如 **`DC=myforest,DC=mydomain,DC=com`**）。
    b. 在用户 > 组 DN 中，指定一个包含您要配置到 IAM Identity Center 的所有用户的组。如果不存在这样的单个组，请在 AD 中创建该组，返回到此设置，然后输入相应的 DN。
    c. 指定是否搜索子组（嵌套搜索）以及任何所需的 LDAP 筛选条件。
    d. 在组 > 组 DN 中，指定一个组，其中包含您要配置到 IAM Identity Center 的所有组。在许多情况下，这可能与您在用户部分中指定的 DN 相同。根据需要输入嵌套搜索和筛选条件值。

13. 在属性映射页面上，确保满足以下条件，然后单击下一步：

    a. userName 字段必须映射到格式为电子邮件 (user@domain.com) 的属性。它还必须与用户用于登录 Ping 的值匹配。该值会在联合身份验证期间填充到 SAML `nameId` 声明中，并用

于匹配 IAM Identity Center 中的用户。例如，当使用 Active Directory 时，您可以选择指定 `UserPrincipalName` 作为用户名。

b. 其他以 * 为后缀的字段必须映射到对您的用户来说非空的属性。

14. 在激活和摘要页面上，将频道状态设置为活动，以便在保存配置后立即开始同步。
15. 确认页面上的所有配置值均正确，然后单击完成。
16. 在管理频道页面上，单击保存。
17. 此时，预置开始了。要确认活动，您可以查看 Provisioner.log 文件，该文件默认位于 PingFederate 服务器上的 pingfederate-<version>/pingfederate/log 目录中。
18. 要验证用户和组是否已成功同步到 IAM Identity Center，请返回 IAM Identity Center 控制台并选择用户。来自 PingFederate 的同步用户出现在用户页面上。您还可以在组页面查看同步的组。

（可选）步骤 3：在 IAM Identity C PingFed enter 中按比例配置用户属性以进行访问控制

PingFederate如果您选择配置将在 IAM Identity Center 中使用的属性来管理对 Amazon 资源的访问权限，则这是一个可选过程。您在 PingFederate 中定义的属性将在 SAML 断言中传递到 IAM Identity Center。然后，您将在 IAM Identity Center 中创建一个权限集，以根据您从 PingFederate 传递的属性来管理访问。

在开始此过程之前，您必须首先启用 访问控制属性 功能。有关此操作的详细信息，请参阅 启用并配置访问控制属性。

要在 PingFederate 中配置用户属性，用于 IAM Identity Center 的访问控制

1. 登录到 PingFederate 管理控制台。
2. 从页面顶部选择应用程序，然后单击SP 连接。
3. 找到您之前创建的用于与 IAM Identity Center 形成 SAML 连接的应用程序，然后单击连接名称。
4. 从页面顶部附近的深色导航标题中选择浏览器 SSO。然后单击配置浏览器 SSO。
5. 在配置浏览器 SSO页上，选择断言创建，然后单击配置断言创建。
6. 在配置断言创建页上，选择属性合同。
7. 在属性合同页面的延长合同部分下，通过执行以下步骤添加新属性：

   a. 在文本框中，输入 `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`AttributeName`**，将 **`AttributeName`** 替换为您在 IAM Identity

Center 中期望的属性名称。例如 `https://aws.amazon.com/SAML/Attributes/AccessControl:Department`。

b. 对于属性名称格式，选择 urn:oasis:names:tc:SAML:2.0:attrname-format:uri。

c. 选择添加，然后选择下一步。

8. 在身份验证源映射页面上，选择使用您的应用程序配置的适配器实例。

9. 在属性合同履行页面上，选择属性合同 `https://aws.amazon.com/SAML/Attributes/AccessControl:Department` 的源（数据存储）和值（数据存储属性）。

> **Note**
>
> 如果您尚未配置数据源，则需要立即进行配置。有关如何在 PingFederate 中选择和配置数据来源的信息，请参阅 Ping 产品文档。

10. 重复单击下一步，直到进入激活和摘要页面，然后单击保存。

（可选）传递访问控制属性

您可以选择使用 IAM Identity Center 中的 访问控制属性 功能来传递 Name 属性设置为 `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` 的 Attribute 元素。此元素允许您将属性作为 SAML 断言中的会话标签传递。有关会话标签的更多信息，请参阅 IAM 用户指南在 Amazon STS中的传递会话标签。

要将属性作为会话标签传递，请包含指定标签值的 AttributeValue 元素。例如，要传递标签键值对`CostCenter = blue`，请使用以下属性。

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

如果您需要添加多个属性，请为每个标签包含一个单独的 Attribute 元素。

问题排查

有关使用 PingFederate 对 SCIM 和 SAML 进行一般性问题排查，请参阅以下各部分：

- 特定用户无法从外部 SCIM 提供商同步到 IAM Identity Center
- 与 IAM Identity Center 创建的 SAML 断言内容有关的问题
- 使用外部身份提供者预置用户或组时出现重复用户或组错误
- 有关 PingFederate 的更多信息，请参阅 PingFederate 文档。

以下资源可以帮助您在使用时进行故障排除 Amazon：

- Amazon Web Services re:Post-查找 FAQs 并链接到其他资源以帮助您解决问题。
- Amazon Web Services 支持 – 获得技术支持

PingOne

IAM Identity Center 支持将 Ping Identity 的（以下简称“Ping”）PingOne 产品的用户信息自动调配（同步）到 IAM Identity Center。此预置使用跨域身份管理系统 (SCIM) v2.0 协议。您可以使用 IAM Identity Center SCIM 端点和访问令牌在 PingOne 中配置此连接。配置 SCIM 同步时，您将在 PingOne 中创建用户属性到 IAM Identity Center 中的命名属性的映射。这会导致 IAM Identity Center 和 PingOne 之间的预期属性匹配。

以下步骤将引导您了解如何使用 SCIM 协议将用户从 PingOne 自动预置到 IAM Identity Center。

> **Note**
>
> 在开始部署 SCIM 之前，我们建议您首先查看 使用自动预置的注意事项。然后继续查看下一部分中的其他注意事项。

主题

- 先决条件
- 注意事项
- 步骤 1：在 IAM Identity Center 中启用预置
- 步骤2：在 PingOne 中配置预置
- （可选）第三步：在 PingOne IAM Identity Center 中配置用户属性进行访问控制
- （可选）传递访问控制属性
- 问题排查

先决条件

在开始之前，您将需要以下内容：

- PingOne 订阅或免费试用，具有联合身份验证和预置功能。有关如何获得免费试用，请参阅 Ping Identity 网站。
- 支持 IAM Identity Center 的帐户（免费）。有关更多信息，请参阅启用 IAM Identity Center。
- PingOne IAM Identity Center 应用程序已添加到您的 PingOne 管理门户。您可以从应用程序目录中获取 PingOne IAM Identity Center PingOne 应用程序。有关一般信息，请参阅 Ping Identity 网站上的应用程序目录中添加应用程序。
- 从 PingOne 实例到 IAM Identity Center 的 SAML 连接。将 PingOne IAM Identity Center 应用程序添加到您的 PingOne 管理门户后，您必须使用它来配置从您的 PingOne 实例到 IAM Identity Center 的 SAML 连接。使用两端的“下载”和“导入”元数据功能在 PingOne 和 IAM Identity Center 之间交换 SAML 元数据。有关如何配置此连接的说明，请参阅 PingOne 文档。
- 如果您将 IAM Identity Center 复制到其他区域，则必须更新您的身份提供商配置以允许访问 Amazon 托管应用程序和 Amazon Web Services 账户 从这些区域访问托管应用程序。有关更多详细信息，请参阅the section called “步骤 3：更新外部 IdP 设置”。有关更多详细信息，请参阅PingOne 文档。

注意事项

以下是关于 PingOne 的重要注意事项，它们可能会影响您使用 IAM Identity Center 实施预置的方式。

- PingOne 不支持通过 SCIM 预置组。联系 Ping 获取 SCIM 组支持 PingOne 的最新信息。
- 在 PingOne 管理门户中禁用配置后，用户可以继续从 PingOne 进行配置。如果您需要立即终止配置，请删除相关的 SCIM 持有者令牌，使用 SCIM 从外部身份提供者预置用户和组在 IAM 身份 and/or 中心中将其禁用。
- 如果从 PingOne 中配置的数据存储中删除用户的属性，则不会从 IAM Identity Center 中的相应用户中删除该属性。这是 PingOne’s 置备程序实现中的一个已知限制。如果修改属性，更改将同步到 IAM Identity Center。
- 以下是关于 PingOne 中 SAML 配置的重要注意事项：
  - IAM Identity Center 仅支持 `emailaddress` 作为 `NameId` 格式。这意味着您需要为中的 SAML_SUBJECT 映射选择一个用户属性PingOne，该属性在目录中是唯一的、非空且格式为 email/UPN（例如，user@domain.com）。PingOne电子邮件（工作）是用于带有PingOne 内置目录的测试配置的合理值。

- PingOne 中电子邮件地址包含 + 字符的用户可能无法登录 IAM Identity Center，并出现诸如 `'SAML_215'` 或 `'Invalid input'` 之类的错误。要解决此问题，请在 PingOne 中为属性映射中的 SAML_SUBJECT 映射选择高级选项。然后在下拉菜单中将要发送到 SP: 的名称 ID 格式设置为 urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress。

步骤 1：在 IAM Identity Center 中启用预置

在第一步中，您使用 IAM Identity Center 控制台启用自动预置。

在 IAM Identity Center 中启用自动预置

1. 完成先决条件后，打开 IAM Identity Center 控制台。
2. 在左侧导航窗格中选择设置。
3. 在设置页面上，找到自动预置信息框，然后选择启用。这会立即在 IAM Identity Center 中启用自动预置，并显示必要的 SCIM 端点和访问令牌信息。
4. 在入站自动预置对话框中，复制 SCIM 端点和访问令牌。稍后在 IdP 中配置预置时，您需要粘贴这些内容。

   a. SCIM 端点 ——例如，https://scim。*us-east-2*.amazonaws.com/ /scim/v2 *11111111111-2222-3333-4444-555555555555*

   b. 访问令牌 - 选择显示令牌以复制该值。

   > **Warning**
   >
   > 这是唯一可以获取 SCIM 端点与访问令牌的机会。在继续操作之前，务必复制这些值。本教程的后续步骤需要输入这些值，以便在 IdP 中配置自动预置。

5. 选择关闭。

现在您已在 IAM Identity Center 控制台中设置了预置，您需要使用 PingOne IAM Identity Center 应用程序完成其余任务。以下过程中描述了这些步骤。

步骤2：在 PingOne 中配置预置

在 PingOne IAM Identity Center 应用程序中使用以下过程来启用 IAM Identity Center 的预置。此过程假设您已将 PingOne IAM Identity Center 应用程序添加到 PingOne 管理门户。如果您尚未执行此操作，请参阅 先决条件，然后完成此过程来配置 SCIM 预置。

要在 PingOne 中配置预置

1. 打开您在为 PingOne 配置 SAML 时安装的 PingOne IAM Identity Center 应用程序（应用程序 > 我的应用程序）。请参阅先决条件。
2. 滚动到页面底部。在用户预置下，选择完整链接以导航到连接的用户预置配置。
3. 在预置说明页面上，选择继续下一步。
4. 在上一过程中，您复制了 IAM Identity Center 中的 SCIM 端点值。将该值粘贴到 PingOne IAM Identity Center 应用程序中的 SCIM URL 字段中。此外，在之前的过程中，您复制了 IAM Identity Center 中的访问令牌值。将该值粘贴到 PingOne IAM Identity Center 应用程序中的 ACCESS_TOKEN 字段中。
5. 对于 REMOVE_ACTION，选择已禁用或已删除（有关更多详细信息，请参阅页面上的说明文本）。
6. 在属性映射页面上，按照本页面前面的 注意事项 中的指导，选择用于 SAML_SUBJECT (NameId) 断言的值。然后选择继续下一步。
7. 在 PingOne 应用程序自定义 - IAM Identity Center 页面上，进行任何所需的自定义更改（可选），然后单击继续下一步。
8. 在组访问权限页面上，选择包含您想要启用的用户组，以便预置和单点登录 IAM Identity Center。选择继续下一步。
9. 滚动到页面底部，然后选择完成，开始预置。
10. 要验证用户是否已成功同步到 IAM Identity Center，请返回 IAM Identity Center 控制台并选择用户。来自 PingOne 的同步用户将显示在用户页面上。现在可以将这些用户分配给 IAM Identity Center 内的帐户和应用程序。

    请记住，PingOne 不支持通过 SCIM 预置组或组成员身份。联系 Ping 以获取更多信息。

（可选）第三步：在 PingOne IAM Identity Center 中配置用户属性进行访问控制

PingOne如果您选择为 IAM Identity Center 配置属性以管理对 Amazon 资源的访问权限，则这是一个可选过程。您在 PingOne 中定义的属性将在 SAML 断言中传递到 IAM Identity Center。然后，您在 IAM Identity Center 中创建权限集，以根据您从 PingOne 传递的属性管理访问权限。

在开始此过程之前，您必须首先启用 访问控制属性 功能。有关此操作的详细信息，请参阅 启用并配置访问控制属性。

要在 PingOne 中配置用户属性，用于 IAM Identity Center 的访问控制

1. 打开您在为 PingOne 配置 SAML 时安装的 PingOne IAM Identity Center 应用程序（应用程序 > 我的应用程序）。
2. 选择编辑，然后选择继续下一步，直到进入属性映射页面。
3. 在属性映射页上，选择添加新属性，然后执行以下操作。您必须对要添加的每个属性执行这些步骤，以便在 IAM Identity Center 中使用以进行访问控制。

   a. 在应用程序属性 字段中输入 `https://aws.amazon.com/SAML/Attributes/AccessControl:`*`AttributeName`*。*`AttributeName`* 替换为您在 IAM Identity Center 中期望的属性的名称。例如 `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Email`**。

   b. 在身份关联属性或文本值字段中，从 PingOne 目录中选择用户属性。例如，电子邮件（工作）。
4. 选择下一步几次，然后选择完成。

（可选）传递访问控制属性

您可以选择使用 IAM Identity Center 中的 访问控制属性 功能来传递 Name 属性设置为 `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`** 的 `Attribute` 元素。此元素允许您将属性作为 SAML 断言中的会话标签传递。有关会话标签的更多信息，请参阅 IAM 用户指南在 Amazon STS中的传递会话标签。

要将属性作为会话标签传递，请包含指定标签值的 `AttributeValue` 元素。例如，要传递标签键值对`CostCenter = blue`，请使用以下属性。

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

如果您需要添加多个属性，请为每个标签包含一个单独的 `Attribute` 元素。

问题排查

有关使用 PingOne 对 SCIM 和 SAML 进行一般性问题排查，请参阅以下各部分：

- 特定用户无法从外部 SCIM 提供商同步到 IAM Identity Center
- 与 IAM Identity Center 创建的 SAML 断言内容有关的问题
- 使用外部身份提供者预置用户或组时出现重复用户或组错误
- 有关 PingOne 的更多信息，请参阅 PingOne 文档。

以下资源可以帮助您在使用时进行故障排除 Amazon：

- Amazon Web Services re:Post-查找 FAQs 并链接到其他资源以帮助您解决问题。
- Amazon Web Services 支持 – 获得技术支持

使用默认 IAM Identity Center 目录配置用户访问权限

首次启用 IAM Identity Center 后，它会自动配置 Identity Center 目录作为您的默认身份源，因此您无需选择身份源。如果您的组织使用其他身份提供商，例如 Microsoft Active Directory、Microsoft Entra ID 或 Okta，请考虑将该身份源与 IAM Identity Center 集成，而不是使用默认配置。

目标

在本教程中，您将使用默认目录作为身份源和一个 IAM Identity Center 组织实例来设置和测试管理用户。该管理用户创建和管理用户和组，并通过权限集授予 Amazon 访问权限。在接下来的步骤中，您将创建以下内容：

- 名为的管理用户 *Nikki Wolf*
- 一个名为的群组 *Admin team*
- 名为的权限集 *AdminAccess*

要验证所有内容是否均已正确创建，您需要登录并设置管理用户的密码。完成本教程后，您可以使用此管理用户在 IAM Identity Center 中添加更多用户、创建其他权限集以及设置对应用程序的组织访问权限。或者，如果您想授予用户对应用程序的访问权限，可以遵循此过程的步骤 1 并配置应用程序访问。

先决条件

需要满足以下先决条件才能完成本教程：

- 启用 IAM Identity Center 并拥有一个 IAM Identity Center 组织实例。

- 如果您拥有 IAM Identity Center 账户实例，则可以创建用户和组，并授予他们对应用程序的访问权限。有关更多信息，请参阅应用程序访问。
- 通过以下任一方式登录 Amazon Web Services 管理控制台 并访问 IAM 身份中心控制台：
  - Amazon （root 用户）新手 — 以账户所有者的身份登录，方法是选择 Amazon Web Services 账户 root 用户并输入您的 Amazon Web Services 账户 电子邮件地址。在下一页上，输入您的密码。
  - 已在使用 Amazon （IAM 证书）— 使用具有管理权限的 IAM 凭证登录。
    - 有关登录的更多帮助 Amazon Web Services 管理控制台，请参阅Amazon 登录 指南。
- 您可以为 IAM Identity Center 用户配置多重身份验证。有关更多信息，请参阅 在 IAM Identity Center 中配置 MFA。

步骤 1：添加用户

1. 打开 IAM Identity Center 控制台。
2. 在 IAM Identity Center 导航窗格，选择用户，然后选择添加用户。
3. 在指定用户详细信息页面，填写以下信息：
   - 用户名-对于本教程，请输入*nikkiw*。

     创建用户时，请选择易于记忆的用户名。您的用户必须记住用户名才能登录 Amazon Web Services 访问门户，您以后无法对其进行更改。
   - 密码 - 选择向该用户发送包含密码设置说明的电子邮件（推荐）。

     此选项会向用户发送一封来自 Amazon Web Services 的电子邮件，主题行为邀请加入 IAM Identity Center。电子邮件发自 `no-reply@signin.aws` 或 `no-reply@login.awsapps.com`。将这些电子邮件地址添加到您允许的发件人列表中。
   - 电子邮件地址 - 输入用户电子邮件地址，您可以通过该地址接收电子邮件。然后，再次输入以确认。每个用户的电子邮件地址必须唯一。
   - 名字 - 输入用户的名字。在本教程中，请输入 *Nikki*。
   - 姓氏 - 输入用户姓氏。在本教程中，请输入 *Wolf*。
   - 显示名称 - 默认值为用户的名字和姓氏。如果要更改显示名称，可以输入不同的名称。显示名称会显示在登录门户和用户列表中。
   - 如果需要，请填写可选信息。本教程不会用到它们，您可以稍后更改。

4. 选择下一步。此时将出现将用户添加到组页面。我们将创建一个群组来分配管理权限，而不是直接授予管理权限*Nikki*。

   选择创建组。

   此时将打开一个新的浏览器选项卡，以显示创建组页面。

   a. 在组详细信息下的组名称中，输入组的名称。我们建议输入一个能表明组角色的组名称。在本教程中，请输入 *Admin team*。

   b. 选择创建组。

   c. 关闭组浏览器选项卡，返回添加用户浏览器选项卡

5. 在组区域，选择刷新按钮。该*Admin team*群组出现在列表中。

   选中旁边的复选框*Admin team*，然后选择 “下一步”。

6. 在查看并添加用户页面，确认以下信息：

   - 主要信息会按您的预期显示
   - “组”显示已添加到您创建的组中的用户

   如果需要进行更改，请选择编辑。如果所有详细信息都正确，选择添加用户。

   此时将显示一条通知消息，告知您用户已添加。

接下来，您将为该*Admin team*组添加管理权限*Nikki*，使其能够访问资源。

步骤 2：添加管理权限

> **Important**
>
> 仅当您启用了 IAM Identity Center 组织实例时，才需执行以下步骤。

1. 在 IAM Identity Center 导航窗格的多账户权限下，选择 Amazon Web Services 账户。
2. 在 Amazon Web Services 账户 页面，组织结构将显示您的组织，您的账户将以分层结构列于其下方。选中管理账户对应的复选框，然后选择分配用户或组。
3. 此时将显示分配用户和组工作流程。它包括三个步骤：

a. 对于步骤 1：选择用户和群组，选择您创建的*Admin team*群组。然后选择下一步。

b. 对于步骤 2：选择权限集，选择创建权限集，以打开新的标签页，它将引导您完成创建权限集所涉及的三个子步骤。

   i. 对于步骤 1：选择权限集类型，请完成以下操作：

      - 在权限集类型中，选择预定义权限集。
      - 在预定义权限集的策略中，选择AdministratorAccess。

      选择下一步。

   ii. 对于步骤 2：指定权限集详细信息，保留默认设置，并选择下一步。

      默认设置会创建名为*AdministratorAccess*、会话持续时间设置为一小时的权限集。在权限集名称字段中输入新名称，即可更改权限集的名称。

   iii. 对于步骤 3：查看并创建，请验证权限集类型是否使用 Amazon 托管策略AdministratorAccess。选择创建。权限集页面会显示通知，告知您权限集已创建。您可以在网络浏览器中关闭此标签页。

   在分配用户和组浏览器标签页，您仍处于步骤 2：选择权限集，您将在这里启动创建权限集工作流程。

   在权限集区域，选择刷新按钮。您创建的*AdministratorAccess*权限集将出现在列表中。选择该权限集的复选框，然后选择下一步。

c. 在 “步骤 3：查看并提交作业” 页面上，确认已选择*Admin team*群组并选择*AdministratorAccess*权限集，然后选择提交。

   页面更新时会显示一条消息，告知您 Amazon Web Services 账户 正在配置中。等待该过程完成。

   您将返回到该 Amazon Web Services 账户 页面。系统会显示一条通知消息，告知您 Amazon Web Services 账户 已重新配置并应用了更新的权限集。

恭喜您！

您已成功设置第一个用户、组和权限集。

在本教程的下一部分中，您将通过*Nikki's*使用他们的管理凭据登录 Amazon Web Services 访问门户并设置密码来测试访问权限。现在，注销控制台。

步骤 3：测试用户访问权限

现在，*Nikki Wolf*这是您组织中的用户，他们可以登录并访问根据其权限集获得权限的资源。要验证用户的配置是否正确，在下一步中，您将使用*Nikki's*凭据登录并设置他们的密码。*Nikki Wolf*在步骤 1 中添加用户时，您选择*Nikki*接收一封包含密码设置说明的电子邮件。现在，您可以打开该电子邮件，并执行以下操作：

1. 在电子邮件中，选择接受邀请链接，以接受邀请。

   > **Note**
   >
   > 该电子邮件还包括*Nikki's*用户名和他们将用于登录组织的 Amazon Web Services 访问门户 URL。记录这些信息，以供将来使用。

   您将进入新用户注册页面，您可以在其中设置*Nikki's*密码并注册他们的 MFA 设备。

2. 设置*Nikki's*密码后，您将导航到 “登录” 页面。输入*nikkiw*并选择 “下一步”，然后输入*Nikki's*密码并选择 “登录”。

3. Amazon Web Services 访问门户打开，显示您可以访问的组织和应用程序。

   选择组织将其展开为列表， Amazon Web Services 账户 然后选择该帐户以显示可用于访问该账户中资源的角色。

   每个权限集都有两种管理方法可供使用，即角色和访问密钥。

   - 例如，角色 *AdministratorAccess*-打开 Amazon Web Services Console Home。
   - 访问密钥-提供可用于 Amazon CLI 或和 Amazon SDK 的凭据。包含会自动刷新的短期凭证或短期访问密钥的使用信息。有关更多信息，请参阅 获取 Amazon CLI 或的 IAM Identity Center 用户证书 Amazon SDKs。

4. 选择角色链接登录 Amazon Web Services Console Home。

您已登录并导航到该 Amazon Web Services Console Home 页面。浏览控制台，并确认您拥有预期的访问权限。

后续步骤

现在，您已经在 IAM Identity Center 创建了管理用户，您可以：

- 分配应用程序
- 添加其他用户
- 将用户分配到账户
- 配置其他权限集

> **Note**
>
> 您可以将多个权限集分配给同一个用户。要遵循应用最低权限的最佳实践，请在创建管理用户后，创建一个限制性更强的权限集并将其分配给同一个用户。这样，您就可以仅 Amazon Web Services 账户 使用所需的权限访问您的，而不是管理权限。

在您的用户接受激活账户的邀请并登录 Amazon Web Services 访问门户后，门户中显示的项目仅限于分配给他们的 Amazon Web Services 账户、角色和应用程序。

教程视频

可将以下视频教程作为补充资源，了解有关设置外部身份提供者的更多信息：

- 在外部身份提供商之间迁移 Amazon IAM Identity Center
- 将您的现有 Amazon IAM Identity Center 实例与 Microsoft Entra ID

在 IAM Identity Center 中设置您的员工队伍

IAM Identity Center 是将您的员工用户连接到 Amazon 托管应用程序（例如 Kiro 和 Amazon Quick）以及其他 Amazon 资源的 Amazon 解决方案。您可以连接现有身份提供者，同步目录中的用户和组，或者直接在 IAM Identity Center 中创建和管理用户。

已经在使用 IAM 进行访问了 Amazon Web Services 账户吗？

您无需对当前 Amazon Web Services 账户 的工作流程进行任何更改即可使用 IAM Identity Center 访问 Amazon 托管应用程序。如果您使用与 IAM 的联合身份验证进行 Amazon Web Services 账户 访问，则您的用户可以继续以与往常相同的方式进行访问 Amazon Web Services 账户 ，并且您可以继续使用现有的工作流程来管理该访问权限。

选择最适合您组织的身份管理策略和现有基础架构的方法。

主题

IAM Identity Center 中的用户、组和预置

IAM Identity Center 使您能控制谁可以登录以及他们可以访问哪些资源。必须为用户预置才能登录。然后，您可以仅将访问权限分配给已配置（预置）的用户或组。了解有关 IAM Identity Center 中的用户、组和配置的信息。

用户名和电子邮件地址的唯一性

IAM Identity Center 要求每个用户都具有唯一的用户名。用户名是用户的主要标识符。用户名不必与用户的电子邮件地址匹配。IAM Identity Center 要求您的用户的所有用户名和电子邮件地址均为非空且是唯一的。

组

组是由您定义的用户的逻辑组合。您可以创建组并将用户添加到该组中。IAM Identity Center 不支持嵌套组（组内有组）。在分配对 Amazon Web Services 账户 和应用程序的访问权限时，组非常有用。与

其向每个用户单独分配访问权限，不如向组授予权限。稍后，当您在组中添加或移除用户时，该用户会自动获得或失去对您分配给该组的帐户和应用程序的访问权限。

用户和组预调配

配置是将用户和群组信息提供给 IAM Identity Center 和 Amazon 托管应用程序或客户托管应用程序使用的过程。您可以直接在 IAM Identity Center 中创建用户和组，或者将您的身份源连接到 IAM Identity Center。通过 IAM Identity Center，您能够为用户和组分配对已连接的应用程序和 Amazon Web Services 账户的访问权限。

IAM Identity Center 中的预调配因您使用的身份源而异。有关更多信息，请参阅 管理您的身份源。

用户和组取消配置

取消配置（取消预置/撤销配置）是从 IAM Identity Center 中移除用户和组信息的过程。

如果您将 Active Directory 或外部身份提供者与 IAM Identity Center 一起使用，您应该从这些身份源（而非 IAM Identity Center）中移除用户和组。如果您的身份源是 Active Directory 或外部身份提供者，则删除 IAM Identity Center 中的用户和组并不会完全移除它们。

如果您需要取消配置（取消预置/撤销配置）IAM Identity Center 用户或组，您应首先移除分配给要取消配置的用户或组的任何权限集或应用程序。否则，您的 IAM Identity Center 中将存在未分配的权限集和应用程序分配。

管理您的身份源

您在 IAM Identity Center 中的身份源定义了用户和组的管理位置。配置身份源后，您可以查找用户或群组，以授予他们对应用程序或两者的单点登录访问权限。 Amazon Web Services 账户

在 Amazon Organizations，每个组织只能有一个身份源。您可以选择以下一个选项作为身份源：

- 外部身份提供者 - 如果您要管理外部身份提供者（IdP）（例如 Okta 或 Microsoft Entra ID）中的用户，请选择此选项。
- 您的本地或 Amazon 托管的 Active Directory — 如果要连接，请选择此选项Active Directory (AD)。
- Identity Center 目录 - 首次启用 IAM Identity Center 时，会自动将 Identity Center 目录配置为默认身份源，除非您选择了其他身份源。使用 Identity Center 目录，您可以创建您的用户和群组，并分配他们对您的 Amazon Web Services 账户 和应用程序的访问级别。

> **Note**
>
> IAM Identity Center 不支持将 SAMBA4基于的 Simple AD 作为身份源。

主题

更改身份源的注意事项

尽管您可以随时更改身份源，但我们建议您考虑此更改会如何影响您当前的部署。

如果您已经在一个身份源中管理用户和组，则更改为其他身份源可能会移除您在 IAM Identity Center 中配置的所有用户和组分配。如果发生这种情况，所有用户（包括 IAM Identity Center 中的管理用户）都将失去对其 Amazon Web Services 账户 和应用程序的单点登录访问权限。

在更改 IAM Identity Center 的身份源之前，请先查看以下注意事项，然后再继续。如果您想继续更改身份源，请参阅 更改您的身份源 了解更多信息。

在 IAM Identity Center 目录和 Active Directory 之间进行更改

如果您已经在 Active Directory 中管理用户和组，我们建议您在启用 IAM Identity Center 并选择身份源时考虑连接您的目录。在默认 Identity Center 目录中创建任何用户和组并进行任何分配之前，请执行此操作。

> **Important**
>
> 在 IAM Identity Center 中将身份源类型更改为 Active Directory 或从 Active Directory 更改时，请注意身份存储 ID 将会更改。这可能会产生以下影响：
>
> - 您的默认 Amazon 访问门户 URL 将更改。您需要将新的 URL 告知您的员工，并更新书签、网关或防火墙允许列表以及引用此 URL 的配置。我们建议您在计划的维护时段执行此更改，以尽量减少对用户的干扰。

- 如果您在 IAM Identity Center 中使用客户自主管理型 KMS 密钥进行静态加密，并且已使用加密上下文配置了 KMS 密钥策略，请注意身份存储的加密上下文将会更改。例如，在身份存储 ARN "arn:aws:identitystore::123456789012:identitystore/d-922763e9b3" 中，"d-922763e9b3" 就是身份存储 ID。为防止在此过渡期间服务中断，请临时修改您的 KMS 密钥策略以使用通配符模式："arn:aws:identitystore::123456789012:identitystore/*"。

如果您已在默认 Identity Center 目录中管理用户和组，请考虑以下事项：

- 已删除分配以及已删除的用户和组——将身份源更改为 Active Directory 会从 Identity Center 目录中删除您的用户和组。此更改还会删除您的分配。在这种情况下，更改为 Active Directory 后，必须将 Active Directory 中的用户和组同步到 Identity Center 目录，然后重新应用其分配。

  如果您选择不使用 Active Directory，则必须在 Identity Center 目录中创建用户和组，然后进行分配。
- 删除身份时不会删除分配——当在 Identity Center 目录中删除身份时，相应的分配也会在 IAM Identity Center 中删除。但是，在 Active Directory 中，当删除身份（在 Active Directory 中或同步的身份中）时，不会删除相应的分配。
- 不进行出站同步 APIs — 如果您使用 Active Directory 作为身份源，我们建议您谨慎 APIs 使用创建、更新和删除。IAM Identity Center 不支持出站同步，因此您的身份源不会自动更新您对使用这些内容的用户或群组所做的更改 APIs。
- 访问门户网址将发生变化 — 在 IAM 身份中心和 Active Directory 之间更改您的身份来源也会更改 Amazon Web Services 访问门户的网址。
- 如果使用 Identity Store 在 IAM Identity Center 控制台中删除或禁用用户 APIs，则具有活动会话的用户可以继续访问集成的应用程序和账户。有关身份验证会话持续时间和用户行为的信息，请参阅了解 IAM Identity Center 中的身份验证会话。

有关 IAM Identity Center 如何配置用户和组的信息，请参阅 Microsoft AD 目录。

从 IAM Identity Center 更改为外部 IdP

如果您将身份源从 IAM Identity Center 更改为外部身份提供商 (IdP)，请考虑以下事项：

- 任务和成员资格使用正确的断言 — 只要新 IdP 发送正确的断言（例如 SAML 名称），您的用户分配、小组分配和小组成员资格就会继续起作用。IDs这些断言必须与 IAM Identity Center 中的用户名和组匹配。

- 无出站同步 – IAM Identity Center 不支持出站同步，因此您的外部 IdP 不会自动更新您在 IAM Identity Center 中对用户和组所做的更改。
- SCIM 预置 – 仅当您的身份提供者将这些更改发送到 IAM Identity Center 后，对身份提供者中的用户和组的更改才会反映在 IAM Identity Center 中。请参阅使用自动预置的注意事项。
- 回滚 – 您可以随时将身份源恢复为使用 IAM Identity Center。请参阅从外部 IdP 更改为 IAM Identity Center。
- 现有用户会话将在会话持续时间到期时撤销 – 将身份源更改为外部身份提供者后，活跃用户会话将在控制台中配置的最长会话持续时间的剩余时间内持续存在。例如，如果 Amazon Web Services 访问门户会话持续时间设置为八小时，而您在第四个小时更改了身份源，则活动用户会话将再持续四个小时。要撤销用户会话，请参阅the section called “结束员工用户的活跃会话”。

  如果使用 Identity Store 在 IAM Identity Center 控制台中删除或禁用用户 APIs，则具有活动会话的用户可以继续访问集成的应用程序和账户。有关身份验证会话持续时间和用户行为的信息，请参阅了解 IAM Identity Center 中的身份验证会话。

  > **Note**
  >
  > 删除用户后，您就无法从 IAM Identity Center 控制台撤销用户会话。

有关 IAM Identity Center 如何配置用户和组的信息，请参阅 外部身份提供者。

从外部 IdP 更改为 IAM Identity Center

如果您将身份源从外部身份提供商 (IdP) 更改为 IAM Identity Center，请考虑以下事项：

- IAM Identity Center 会保留您的所有分配。
- 强制密码重置——在 IAM Identity Center 中拥有密码的用户可以继续使用旧密码登录。对于外部 IdP 中但不在 IAM Identity Center 中的用户，管理员必须强制重置密码。
- 现有用户会话将在会话持续时间到期时撤销 – 将身份源更改为 IAM Identity Center 后，活跃用户会话将在控制台中配置的最长会话持续时间的剩余时间内持续存在。例如，如果 Amazon Web Services 访问门户会话持续时间为八小时，而您在第四个小时更改了身份源，则活动用户会话将继续再运行四个小时。要撤销用户会话，请参阅the section called “结束员工用户的活跃会话”。

  如果使用 Identity Store 在 IAM Identity Center 控制台中删除或禁用用户 APIs，则具有活动会话的用户可以继续访问集成的应用程序和账户。有关身份验证会话持续时间和用户行为的信息，请参阅了解 IAM Identity Center 中的身份验证会话。

> **Note**
>
> 删除用户后，您就无法从 IAM Identity Center 控制台撤销用户会话。

- 多区域支持-如果您已将 IAM Identity Center 复制到其他区域或计划这样做，则必须使用外部身份提供商作为身份来源。有关包括其他先决条件在内的更多信息，请参阅跨多个 IAM 身份中心使用 Amazon Web Services 区域。

有关 IAM Identity Center 如何配置用户和组的信息，请参阅 管理 Identity Center 目录中的用户。

从一个外部 IdP 更改为另一外部 IdP

如果您已使用外部 IdP 作为 IAM Identity Center 的身份源并且更改为其他外部 IdP，请考虑以下事项：

- 分配和成员身份与正确的断言配合使用——IAM Identity Center 会保留您的所有分配。只要新 IdP 发送正确的断言（例如 SAML 名称），用户分配、群组分配和群组成员资格就会继续生效。IDs

  当您的用户通过新的外部 IdP 进行身份验证时，这些断言必须与 IAM Identity Center 中的用户名匹配。
- SCIM 预置 – 如果使用 SCIM 预置到 IAM Identity Center 中，建议查看本指南中关于 IdP 的信息以及 IdP 提供的文档，确保启用 SCIM 时新提供者能够正确匹配用户和组。
- 现有用户会话将在会话持续时间到期时撤销 – 将身份源更改为其他外部身份提供者后，活跃用户会话将在控制台中配置的最长会话持续时间的剩余时间内持续存在。例如，如果 Amazon Web Services 访问门户会话持续时间为八小时，而您在第四个小时更改了身份源，则活动用户会话将再持续四个小时。要撤销用户会话，请参阅the section called “结束员工用户的活跃会话”。

  如果使用 Identity Store 在 IAM Identity Center 控制台中删除或禁用用户 APIs，则具有活动会话的用户可以继续访问集成的应用程序和账户。有关身份验证会话持续时间和用户行为的信息，请参阅了解 IAM Identity Center 中的身份验证会话。

> **Note**
>
> 删除用户后，您就无法从 IAM Identity Center 控制台撤销用户会话。

有关 IAM Identity Center 如何配置用户和组的信息，请参阅 外部身份提供者。

在 Active Directory 和外部 IdP 之间进行更改

如果您将身份源从外部 IdP 更改为 Active Directory，或从 Active Directory 更改为外部 IdP，请考虑以下事项：

- 用户、组和分配被删除——所有用户、组和分配都将从 IAM Identity Center 中删除。外部 IdP 或 Active Directory 中的用户或组信息均不会受到影响。
- 预置用户——如果您更改为外部 IdP，则必须配置 IAM Identity Center 来预置您的用户。或者，您必须先手动为外部 IdP 设置用户和组，然后才能配置分配。
- 创建分配和组——如果更改为 Active Directory，则必须使用 Active Directory 目录中的用户和组创建分配。
- 如果使用 Identity Store 在 IAM Identity Center 控制台中删除或禁用用户 APIs，则具有活动会话的用户可以继续访问集成的应用程序和账户。有关身份验证会话持续时间和用户行为的信息，请参阅了解 IAM Identity Center 中的身份验证会话。
- 多区域支持-如果您已将 IAM Identity Center 复制到其他区域或计划这样做，则必须使用外部身份提供商作为身份来源。有关包括其他先决条件在内的更多信息，请参阅跨多个 IAM 身份中心使用 Amazon Web Services 区域。

有关 IAM Identity Center 如何配置用户和组的信息，请参阅 Microsoft AD 目录。

更改您的身份源

以下步骤介绍如何从 IAM Identity Center 提供的目录（默认 Identity Center 目录）更改为 Active Directory 或外部身份提供者，或者反之亦然。在继续操作之前，请查看 更改身份源的注意事项 中的信息。要完成此过程，您需要拥有 IAM Identity Center 的组织实例。有关更多信息，请参阅 IAM Identity Center 的组织和账户实例。

> **Warning**
>
> 根据您当前的部署，此更改可能会删除您在 IAM Identity Center 中配置的所有用户和组分配。此更改还将从您的权限集 IAM 角色中移除 Amazon Web Services 账户。因此，您可能需要更新资源策略，并应确保这不会中断您对 Amazon KMS 密钥和 Amazon EKS 集群的访问。要了解更多信息，请参阅在资源策略、Amazon EKS 集群配置映射和 Amazon KMS 密钥策略中引用权限集。
>
> 发生这种情况时，所有用户和群组（包括 IAM Identity Center 中的管理用户）都将失去对其 Amazon Web Services 账户 和应用程序的单点登录访问权限。

如需更改您的身份源

1. 打开 IAM Identity Center 控制台。
2. 选择设置。
3. 在设置页面上，选择身份源选项卡。选择操作，然后选择更改身份源。
4. 在选择身份源项下，选择要更改的源，然后选择下一步。

   如果您要更改为 Active Directory，请从下一页的菜单中选择可用目录。

   > **Important**
   >
   > 将您的身份源更改为 Active Directory 或从 Active Directory 更改身份源会从 Identity Center 目录中删除用户和组。此更改还会删除您在 IAM Identity Center 配置的所有分配。

   > **Note**
   >
   > 如果您将 IAM Identity Center 复制到其他区域，则无法更改您的身份源类型。您只能用另一个外部 IdP 替换当前的外部 IdP。要更改身份来源类型，您需要先移除所有其他区域。有关更多信息，请参阅 跨多个 IAM 身份中心使用 Amazon Web Services 区域。

   如果要切换为外部身份提供者，我们建议您按照 如何连接到外部身份提供商 中所述的步骤操作。
5. 阅读免责声明并准备好继续后，键入 ACCEPT。
6. 选择更改身份源。如果要将身份源更改为 Active Directory，请继续执行下一步。
7. 将您的身份源更改为 Active Directory 会让您转至设置页面。在设置页面上，执行以下任一操作：
   - 选择启动引导式设置。有关如何完成引导式设置流程的信息，请参阅 引导式设置。
   - 在身份源部分，请选择操作，然后选择管理同步，以配置您的同步范围以及要同步的用户和组列表。

IAM Identity Center 中支持的用户和组

本指南提供 IAM Identity Center 中 SCIM 属性支持的参考信息。它列出了 IAM Identity Center 身份存储中支持的 SCIM 规范中的哪些用户和组属性，并指出了不支持的具体属性和子属性。

属性是各种条目的信息，用于帮助您定义和标识单个用户或组对象，例如 name、email 或 members。IAM Identity Center 通过手动输入和自动 SCIM 配置（预置）支持最常用的属性。

- 有关跨域身份管理系统 (SCIM) 规范的信息，请参阅 https://tools.ietf.org/html /rfc7642。
- 有关手动和自动预调配的信息，请参阅 当用户来自外部 IdP 时进行预置。
- 有关属性映射的更多信息，请参阅 IAM Identity Center 与外部身份提供者目录之间的属性映射。

由于 IAM Identity Center 支持 SCIM 自动预调配使用案例，因此 Identity Center 目录支持 SCIM 规范中列出的所有相同用户和组属性，只有少数例外。以下各节介绍了 IAM Identity Center 不支持哪些属性。

不支持的用户对象

IAM 身份中心身份存储支持 SCIM 用户架构 (https://tools.ietf.org/html/rfc7643 #section -8.3) 中的所有属性，但以下属性除外：

- password
- ims
- photos
- entitlements
- x509Certificates

支持用户的所有子属性，但以下属性除外：

- 任何多值属性的 'display' 子属性（例如，emails 或 phoneNumbers）
- 'meta' 属性的 'version' 子属性

不支持的组对象

支持 SCIM 组架构 (https://tools.ietf.org/html/rfc7643 #section -8.4) 中的所有属性。

支持组的所有子属性，但以下属性除外：

- 任何多值属性（例如，成员）的 'display' 子属性。

外部身份提供者

借助 IAM Identity Center，您可以通过安全断言标记语言 (SAMLIdPs) 2.0 和跨域身份管理系统 (SCIM) 协议，连接来自外部身份提供商 () 的现有员工身份。这使您的用户能够使用其公司凭证登录 Amazon Web Services 访问门户。然后，他们可以导航到为其分配的帐户、角色和托管在外部的应用程序 IdPs。

例如，您可以将 Okta 或 Microsoft Entra ID 等外部 IdP 连接到 IAM Identity Center。然后，您的用户可以使用其现有Okta或Microsoft Entra ID凭据登录 Amazon Web Services 访问门户。要控制用户登录后可以执行的操作，您可以集中为他们分配 Amazon 组织中所有账户和应用程序的访问权限。此外，开发人员只需使用其现有凭证登录 Amazon Command Line Interface (Amazon CLI)，即可从自动生成和轮换短期凭证中受益。

如果您使用的是 Active Directory 或中的自管理目录 Amazon Managed Microsoft AD，请参阅Microsoft AD 目录。

> **Note**
>
> SAML 协议不提供查询 IdP 以了解用户和组的方法。因此，您必须通过将这些用户和组预置到 IAM Identity Center 来使 IAM Identity Center 了解这些用户和组。

当用户来自外部 IdP 时进行预置

使用外部 IdP 时，必须先将所有适用的用户和群组配置到 IAM Identity Center 中，然后才能对 Amazon Web Services 账户 或应用程序进行任何分配。为此，您可以为用户和组配置 使用 SCIM 从外部身份提供者预置用户和组，也可以使用 手动预置。无论您如何配置用户，IAM Identity Center 都会将命令行界面和应用程序身份验证重定向到您的外部 IdP。 Amazon Web Services 管理控制台然后，IAM Identity Center 根据您在 IAM Identity Center 中创建的策略授予对这些资源的访问权限。有关预置的更多信息，请参阅 用户和组预调配。

主题

- 如何连接到外部身份提供商
- 如何在 IAM Identity Center 中更改外部身份提供者元数据
- 对外部身份提供者使用 SAML 和 SCIM 身份联合验证
- SCIM 配置文件和 SAML 2.0 实施

如何连接到外部身份提供商

对于支持的外部设备，有不同的先决条件、注意事项和配置程序 IdPs。有一些 step-by-step教程可供选择 IdPs：

- CyberArk
- JumpCloud
- Microsoft Entra ID
- Okta
- OneLogin
- Ping Identity

有关 IAM Identity Center 支持的外部 IdPs 注意事项的更多信息，请参阅对外部身份提供者使用 SAML 和 SCIM 身份联合验证。

下方概述了所有外部身份提供者使用的过程。

要连接到外部身份提供商

1. 打开 IAM Identity Center 控制台。
2. 选择设置。
3. 在设置页面上，选择身份源选项卡，然后选择操作>更改身份源。
4. 在选择身份源 下，选择外部身份提供程序，然后选择下一步。
5. 在配置外部身份提供商下，执行以下操作：

    a. 在服务提供商元数据下，选择下载元数据文件以下载元数据文件并将其保存在您的系统上。您的外部身份提供商需要 IAM Identity Center SAML 元数据文件。

    > **Note**
    >
    > 您下载的 SAML 元数据文件包含 IPv4仅限和双栈断言消费者服务 (ACS)。 URLs此外，如果您的 IAM 身份中心被复制到其他区域，则元数据文件将包含每个额外区域 URLs 的 ACS。如果您的外部 IdP 对 ACS 的数量有限制 URLs，则需要删除不必要的 ACS。 URLs例如，如果您的组织已完全采用双堆栈终端节点，并且不再使用 IP4v 仅限双堆栈的终端节点，则可以移除后者。另一种方法是不使用元数据文件，而是将 ACS 复制并粘贴 URLs 到外部 IdP 中。

b. 在身份提供者元数据下选择选择文件，然后找到从外部身份提供者下载的元数据文件。然后上传该文件。此元数据文件包含用于信任从 IdP 发送的消息所需的公共 x509 证书。

c. 选择下一步。

> **Important**
>
> 将源更改为 Active Directory 或从 Active Directory 更改源会删除所有现有的用户和组分配。成功更改来源后，您必须手动重新应用分配。

6. 阅读免责声明并准备继续操作后，输入接受。
7. 选择更改身份源。状态消息将通知您，您已成功更改身份源。

如何在 IAM Identity Center 中更改外部身份提供者元数据

您可以更改之前提供给 IAM Identity Center 的外部身份提供者的元数据。这些更改会影响您的用户通过 IAM Identity Center 登录和访问 Amazon 资源的能力。下列过程介绍了如何更新存储在 IAM Identity Center 中的外部 IdP 的元数据。要完成此过程，您需要拥有 IAM Identity Center 的组织实例。有关更多信息，请参阅 IAM Identity Center 的组织和账户实例。

更改外部身份提供者的元数据

1. 打开 IAM Identity Center 控制台。
2. 选择设置。
3. 在设置页面上，选择身份源选项卡。选择操作，然后选择管理身份验证。
4. 在身份提供者元数据部分，选择编辑 IdP 元数据。您可以在此页面上更改外部 IdP 的 IdP 登录 URL 和/或 IdP 发布者 URL。完成所有必要的更改后，选择保存更改。

对外部身份提供者使用 SAML 和 SCIM 身份联合验证

IAM Identity Center 实施以下基于标准的身份联合验证协议：

- 用于用户身份验证的 SAML 2.0
- 用于预置的 SCIM

任何实施这些标准协议的身份提供商 (IdP) 都有望与 IAM Identity Center 成功互操作，但需要注意以下特殊事项：

- SAML
  - IAM Identity Center 要求电子邮件地址采用 SAML NameID 格式（即 `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`）。
  - 断言中 nameID 字段的值必须是符合 RFC 2822 (https://tools.ietf.org/html/rfc2822) addr-spec (“”) 字符串 (/rfc2822 #section -3.4.1)。`name@domain.com` https://tools.ietf.org/html
  - 元数据文件不能超过 75000 个字符。
  - 元数据必须包含 EntityID、X509 证书，并 SingleSignOnService作为登录网址的一部分。
  - 不支持加密密钥。
  - IAM Identity Center 不支持对发送给外部 IdPs的 SAML 身份验证请求进行签名。
  - URLs 如果您计划将 IAM Identity Center 复制到其他区域，并充分利用多区域 IAM 身份中心的优势，IdP 必须支持多断言消费者服务 (ACS)。有关更多信息，请参阅 跨多个 IAM 身份中心使用 Amazon Web Services 区域。使用单个 ACS URL 可能会影响其他区域的用户体验。您的主要区域将继续正常运行。有关使用单个 ACS URL 在其他区域的用户体验的更多信息，请参阅the section called “使用没有多个 ACS 的 Amazon 托管应用程序 URLs”和the section called “Amazon Web Services 账户 无需多个 ACS 即可实现访问弹性 URLs”。

- SCIM
  - IAM Identity Center SCIM 的实施基于 SCIM RFCs 7642 (https://tools.ietf.org/html/rfc7642)、7643 (/rfc7643) 和 7644 (https://tools.ietf.org/html/rfc764 4)，以及 2020 年 3 月基本 https://tools.ietf.org/htmlSCIM Profile 1.0 草案 (#rfc .section.4) 中规定的互操作性要求。 FastFed https://openid.net/specs/fastfed-scim-1_0-02.html这些文档与 IAM Identity Center 中当前实施之间的任何差异均在 IAM Identity Center SCIM 实施开发人员指南的支持的 API 操作部分中进行了描述。

IdPs 不支持不符合上述标准和注意事项的内容。请联系您的 IdP，了解有关其产品是否符合这些标准和注意事项的问题或澄清。

如果您在将 IdP 连接到 IAM Identity Center 时遇到任何问题，我们建议您检查：

- Amazon CloudTrail 通过筛选事件名称来记录日志 L ExternalIdPDirectoryogin
- 特定于 IDP 的日志调试日志 and/or
- 排查 IAM Identity Center 问题

> **Note**
>
> 有些 IdPs产品（例如中的那些）以专为 IAM Identity Center 构建的 “应用程序” 或 “连接器” 的形式为 IAM Identity Center 提供了简化的配置体验。IAM Identity Center 身份源教程如果您的 IdP 提供此选项，我们建议您使用它，并小心选择专为 IAM Identity Center 构建的项目。其他名为 “Amazon”、“Amazon 联合” 或类似的通用 “Amazon” 名称的项目可能使用其他联合方法 and/or 终端节点，并且可能无法按预期与 IAM Identity Center 配合使用。

SCIM 配置文件和 SAML 2.0 实施

SCIM 和 SAML 都是配置 IAM Identity Center 时的重要考虑因素。

SAML 2.0 实施

IAM Identity Center 支持使用 SAML（安全断言标记语言）2.0 进行身份联合验证。这允许 IAM Identity Center 对来自外部身份提供商的身份进行身份验证 (IdPs)。SAML 2.0 是一种用于安全交换 SAML 断言的开放标准。SAML 2.0 在 SAML 授权机构（称为身份提供商或 IdP）和 SAML 使用者（称为服务提供商或 SP）之间传递有关用户的信息。IAM Identity Center 服务使用此信息来提供联合身份验证单点登录。单点登录允许用户根据其现有的身份提供商凭据访问 Amazon Web Services 账户 和配置应用程序。

IAM Identity Center 为您的 IAM 身份中心存储 Amazon Managed Microsoft AD或外部身份提供商添加 SAML IdP 功能。然后，用户可以单点登录支持 SAML 的服务，包括 Amazon Web Services 管理控制台 和第三方应用程序Microsoft 365，例如Concur、和。Salesforce

但是，SAML 协议不提供查询 IdP 以了解用户和组的方法。因此，您必须通过将这些用户和组预置到 IAM Identity Center 来使 IAM Identity Center 了解这些用户和组。

SCIM 配置文件

IAM Identity Center 为跨域身份管理系统 (SCIM) v2.0 标准提供支持。SCIM 使您的 IAM Identity Center 身份与 IdP 的身份保持同步。这包括 IdP 和 IAM Identity Center 之间的任何用户预置、更新和取消预置。

有关如何实施 SCIM 的更多信息，请参阅 使用 SCIM 从外部身份提供者预置用户和组。有关 IAM Identity Center SCIM 实施的更多详细信息，请参阅 IAM Identity Center SCIM 实施开发人员指南。

主题

- 使用 SCIM 从外部身份提供者预置用户和组

- 轮换 SAML 2.0 证书

使用 SCIM 从外部身份提供者预置用户和组

IAM Identity Center 支持使用跨域身份管理系统 (SCIM) v2.0 协议将用户和组信息从身份提供商 (IdP) 自动预置（同步）到 IAM Identity Center。配置 SCIM 同步时，您可以创建身份提供商 (IdP) 用户属性到 IAM Identity Center 中的命名属性的映射。这会导致 IAM Identity Center 和您的 IdP 之间的预期属性匹配。您可以使用 IAM Identity Center 的 SCIM 端点和您在 IAM Identity Center 中创建的持有者令牌，在 IdP 中配置此连接。

主题

- 使用自动预置的注意事项
- 如何监控访问令牌过期
- 生成访问令牌
- 启用自动预置
- 删除访问令牌
- 禁用自动预置
- 轮换访问令牌
- 审计和协调自动预置的资源
- 手动预置

使用自动预置的注意事项

在开始部署 SCIM 之前，我们建议您首先查看以下有关其如何与 IAM Identity Center 配合使用的重要注意事项。有关其他预置注意事项，请参阅相应 IdP 适用的 IAM Identity Center 身份源教程。

- 如果您要预置主电子邮件地址，则此属性值对于每个用户必须是唯一的。在某些 IdPs情况下，主电子邮件地址可能不是真实的电子邮件地址。例如，它可能是看起来像电子邮件的通用主体名称 (UPN)。它们 IdPs 可能有一个包含用户真实电子邮件地址的辅助或 “其他” 电子邮件地址。您必须在 IdP 中配置 SCIM，以将非空唯一电子邮件地址映射到 IAM Identity Center 主电子邮件地址属性。并且您必须将用户的非空唯一登录标识符映射到 IAM Identity Center 用户名属性。检查您的 IdP 是否具有既是登录标识符又是用户电子邮件名称的单一值。如果是这样，您可以将该 IdP 字段映射到 IAM Identity Center 主电子邮件和 IAM Identity Center 用户名。
- 要使 SCIM 同步起作用，必须为每个用户指定名字、姓氏、用户名和显示名称值。如果用户缺少这些值中的任何一个，则不会配置该用户。

- 如果您需要使用第三方应用程序，则首先需要将出站 SAML 主题属性映射到用户名属性。如果第三方应用程序需要可路由的电子邮件地址，您必须向您的 IdP 提供电子邮件属性。
- SCIM 预置和更新间隔由您的身份提供商控制。仅当您的身份提供商将这些更改发送到 IAM Identity Center 后，对身份提供商中的用户和组的更改才会反映在 IAM Identity Center 中。请咨询您的身份提供商，了解有关用户和组更新频率的详细信息。
- 目前，SCIM 未配置多值属性（例如给定用户的多个电子邮件或电话号码）。尝试使用 SCIM 将多值属性同步到 IAM Identity Center 将失败。为了避免失败，请确保为每个属性仅传递一个值。如果您的用户具有多值属性，请删除或修改 IdP 处 SCIM 中的重复属性映射，以连接到 IAM Identity Center。
- 验证 IdP 处的 `externalId` SCIM 映射是否对应于对您的用户而言唯一、始终存在且最不可能更改的值。例如，您的 IdP 可能会提供有保证的 `objectId` 或其他标识符，这些标识符不会受到姓名和电子邮件等用户属性更改的影响。如果是这样，您可以将该值映射到 SCIM `externalId` 字段。这样可以确保您的用户在需要更改姓名或电子邮件时不会丢失 Amazon 授权、分配或权限。
- 尚未分配到应用程序或 Amazon Web Services 账户 无法配置到 IAM Identity Center 的用户。要同步用户和组，请确保将它们分配给代表您的 IdP 与 IAM Identity Center 连接的应用程序或其他设置。
- 用户取消预置行为由身份提供者管理，可能因实现情况而异。请咨询相关身份提供者，了解有关用户取消预置的详细信息。
- 为您的 IdP 设置 SCIM 自动预置后，您将无法再在 IAM Identity Center 控制台中添加或编辑用户。如果您需要添加或修改用户，必须从您的外部 IdP 或身份源执行此操作。

有关 IAM Identity Center SCIM 实施的更多信息，请参阅 IAM Identity Center SCIM 实施开发人员指南。

如何监控访问令牌过期

SCIM 访问令牌的生成有效期为一年。当您的 SCIM 访问令牌设置为 90 天或更短时间后到期时，Amazon 会在 IAM Identity Center 控制台和控制 Amazon Health 面板中向您发送提醒，以帮助您轮换令牌。通过在 SCIM 访问令牌过期之前进行轮换，您可以持续保护用户和组信息的自动预置。如果 SCIM 访问令牌过期，用户和组信息从身份提供商到 IAM Identity Center 的同步将停止，因此自动预置无法再进行更新或创建和删除信息。自动预置中断可能会增加安全风险并影响对服务的访问。

Identity Center 控制台提醒将持续存在，直到您轮换 SCIM 访问令牌并删除任何未使用或过期的访问令牌。 Amazon Health 控制面板事件每周续订 90 到 60 天，每周更新两次，从 60 到 30 天，每周续订三次，从 30 到 15 天，每天续订 15 天，直到 SCIM 访问令牌到期。

生成访问令牌

使用以下过程在 IAM Identity Center 控制台中生成新的访问令牌。

> **Note**
>
> 此过程要求您之前已启用自动预置。有关更多信息，请参阅 启用自动预置。

生成新的访问令牌

1. 在 IAM Identity Center 控制台中，选择左侧导航窗格中的设置。
2. 在设置页面上，选择身份源选项卡，然后选择操作>管理预置。
3. 在自动预置页面的访问令牌下，选择生成令牌。
4. 在生成新的访问令牌对话框中，复制新的访问令牌并将其保存在安全的地方。
5. 选择关闭。

启用自动预置

使用以下过程可使用 SCIM 协议将用户和组从 IdP 自动预置到 IAM Identity Center。

> **Note**
>
> 在开始此过程之前，我们建议您首先查看适用于您的 IdP 的预置注意事项。有关更多信息，请参阅相应 IdP 的 IAM Identity Center 身份源教程。

在 IAM Identity Center 中启用自动预置

1. 完成先决条件后，打开 IAM Identity Center 控制台。
2. 在左侧导航窗格中选择设置。
3. 在设置页面上，找到自动预置信息框，然后选择启用。这会立即在 IAM Identity Center 中启用自动预置，并显示必要的 SCIM 端点和访问令牌信息。
4. 在入站自动预置对话框中，复制 SCIM 端点和访问令牌。稍后在 IdP 中配置预置时，您需要粘贴这些内容。

    a. SCIM 端点 ——例如，https://scim。*us-east-2*.amazonaws.com/ /scim/v2 *11111111111-2222-3333-4444-555555555555*

b. 访问令牌 - 选择显示令牌以复制该值。

> **Warning**
>
> 这是唯一可以获取 SCIM 端点与访问令牌的机会。在继续操作之前，务必复制这些值。本教程的后续步骤需要输入这些值，以便在 IdP 中配置自动预置。

5. 选择关闭。

完成此过程后，您必须在 IdP 中配置自动预置。有关更多信息，请参阅相应 IdP 的 IAM Identity Center 身份源教程。

删除访问令牌

使用以下过程删除 IAM Identity Center 控制台中的现有访问令牌。

删除现有的访问令牌

1. 在 IAM Identity Center 控制台中，选择左侧导航窗格中的设置。
2. 在设置页面上，选择身份源选项卡，然后选择操作>管理预置。
3. 在自动预置页面的访问令牌下，选择要删除的访问令牌，然后选择删除。
4. 在删除访问令牌对话框中，查看信息，键入 DELETE，然后选择删除访问令牌。

禁用自动预置

使用以下过程在 IAM Identity Center 控制台中禁用自动预置。

> **Important**
>
> 在开始此过程之前，您必须删除访问令牌。有关更多信息，请参阅 删除访问令牌。

在 IAM Identity Center 控制台中禁用自动预置

1. 在 IAM Identity Center 控制台中，选择左侧导航窗格中的设置。
2. 在设置页面上，选择身份源选项卡，然后选择操作>管理预置。
3. 在自动预置页面上，选择禁用。

4. 在禁用自动预置对话框中，查看信息，键入禁用，然后选择禁用自动预置。

轮换访问令牌

IAM Identity Center 目录一次最多支持两个访问令牌。要在任何轮换之前生成额外的访问令牌，请删除所有过期或未使用的访问令牌。

如果您的 SCIM 访问令牌即将过期，您可以使用以下过程在 IAM Identity Center 控制台中轮换现有访问令牌。

要轮换访问令牌

1. 在 IAM Identity Center 控制台中，选择左侧导航窗格中的设置。
2. 在设置页面上，选择身份源选项卡，然后选择操作>管理预置。
3. 在自动预置页面的访问令牌下，记下要轮换的令牌的令牌 ID。
4. 按照 生成访问令牌 的步骤创建一个新的令牌。如果您已创建最大数量的 SCIM 访问令牌，则首先需要删除现有令牌之一。
5. 转至身份提供商的网站并为 SCIM 预置预置新的访问令牌，然后使用新的 SCIM 访问令牌测试与 IAM Identity Center 的连接。确认使用新令牌预置成功后，请继续执行此过程中的下一步。
6. 按照 删除访问令牌 中的步骤删除您之前记下的旧访问令牌。您还可以使用令牌的创建日期作为要删除哪个令牌的提示。

审计和协调自动预置的资源

SCIM 使您能够将用户、组和组成员资格从身份源自动预置到 IAM Identity Center。本指南帮助您验证和协调这些资源，以维持准确的同步。

为何要审计您的资源？

定期审计有助于确保您的访问控制保持准确，并且您的身份提供者（IdP）与 IAM Identity Center 保持正确同步。这对于安全合规性和访问管理尤为重要。

您可以审计的资源：

- Users
- 组
- 组成员资格

您可以使用 Ident Amazon ity Store APIs或 CLI 命令进行审计和对账。以下示例使用 Amazon CLI 命令。有关 API 替代方案，请参阅《Identity Store API 参考》中的相应操作。

如何审计资源

以下是如何使用 Amazon CLI 命令审核这些资源的示例。

在开始之前，请确保您满足以下条件：

- 对 IAM Identity Center 的管理员访问权限。
- Amazon CLI 已安装并配置。有关信息，请参阅 Amazon Command Line Interface 用户指南。
- 执行 Identity Store 命令所需的 IAM 权限。

步骤 1：列出当前资源

您可以使用查看您当前的资源 Amazon CLI。

> **Note**
>
> 使用时 Amazon CLI，除非您指定`--no-paginate`，否则会自动处理分页。如果您直接调用 API（例如，使用 SDK 或自定义脚本），请处理响应中的 `NextToken`。这确保您能检索跨多个页面的所有结果。

Example适用于用户

```
aws identitystore list-users \
  --region REGION \
  --identity-store-id IDENTITY_STORE_ID
```

Example适用于组

```
aws identitystore list-groups \
  --region REGION \
  --identity-store-id IDENTITY_STORE_ID
```

Example适用于组成员资格

```
aws identitystore list-group-memberships \
```

```
  --region REGION \
  --identity-store-id IDENTITY_STORE_ID
  --group-id GROUP_ID
```

步骤 2：与您的身份源进行比较

将列出的资源与您的身份源进行比较，以识别任何差异，例如：

- 缺失了本应在 IAM Identity Center 中预置的资源。
- 应从 IAM Identity Center 中移除的额外资源。

Example适用于用户

```
# Create missing users
aws identitystore create-user \
  --identity-store-id IDENTITY_STORE_ID \
  --user-name USERNAME \
  --display-name DISPLAY_NAME \
  --name GivenName=FIRST_NAME,FamilyName=LAST_NAME \
  --emails Value=EMAIL,Primary=true

# Delete extra users
aws identitystore delete-user \
  --identity-store-id IDENTITY_STORE_ID \
  --user-id USER_ID
```

Example适用于组

```
# Create missing groups
aws identitystore create-group \
  --identity-store-id IDENTITY_STORE_ID \
  [group attributes]

# Delete extra groups
aws identitystore delete-group \
  --identity-store-id IDENTITY_STORE_ID \
  --group-id GROUP_ID
```

Example适用于组成员资格

```
# Add missing members
```

```
aws identitystore create-group-membership \
  --identity-store-id IDENTITY_STORE_ID \
  --group-id GROUP_ID \
  --member-id '{"UserId": "USER_ID"}'

# Remove extra members
aws identitystore delete-group-membership \
  --identity-store-id IDENTITY_STORE_ID \
  --membership-id MEMBERSHIP_ID
```

注意事项

- 命令受服务配额和 API 节流的约束。
- 当您在协调过程中发现许多差异时，请逐步对 Ident Amazon ity Store 进行细微的更改。这有助于您避免影响多个用户的错误。
- SCIM 同步可能会覆盖您的手动更改。检查您的 IdP 设置以了解此行为。

手动预置

有些 IdPs 不支持跨域身份管理系统 (SCIM)，或者有不兼容的 SCIM 实现。在这些情况下，您可以通过 IAM Identity Center 控制台手动配置用户。当您将用户添加到 IAM Identity Center 时，请确保将用户名设置为与 IdP 中的用户名相同。您至少必须拥有唯一的电子邮件地址和用户名。有关更多信息，请参阅 用户名和电子邮件地址的唯一性。

您还必须在 IAM Identity Center 中手动管理所有组。为此，您需要创建组并使用 IAM Identity Center 控制台添加它们。这些组不需要与您的 IdP 中存在的组匹配。有关更多信息，请参阅 组。

轮换 SAML 2.0 证书

IAM Identity Center 使用证书在 IAM Identity Center 和您的外部身份提供商 (IdP) 之间建立 SAML 信任关系。当您在 IAM Identity Center 中添加外部 IdP 时，您还必须从外部 IdP 获取至少一个公共 SAML 2.0 X.509 证书。该证书通常在信任创建期间的 IdP SAML 元数据交换期间自动安装。

作为 IAM Identity Center 管理员，您有时需要将旧的 IdP 证书替换为新的 IdP 证书。例如，当证书到期日期临近时，您可能需要更换 IdP 证书。用新证书替换旧证书的过程称为证书轮换。

主题

- 轮换 SAML 2.0 证书
- 证书过期状态指示器

轮换 SAML 2.0 证书

您可能需要定期导入证书，以便轮换身份提供商颁发的无效或过期的证书。这有助于防止身份验证中断或停机。所有导入的证书都将自动激活。仅应在确保相关身份提供商不再使用证书后才将其删除。

您还应该考虑有些证书 IdPs 可能不支持多个证书。在这种情况下，使用这些证书轮换证书的行为 IdPs 可能意味着您的用户服务会暂时中断。当成功重新建立与该 IdP 的信任时，服务就会恢复。如果可能的话，请在非高峰时段仔细计划此操作。

> **Note**
>
> 作为安全最佳实践，一旦现有 SAML 证书出现任何泄露或处理不当的迹象，您应立即删除并轮换该证书。

轮换 IAM Identity Center 证书是一个多步骤过程，涉及以下内容：

- 从 IdP 获取新证书
- 将新证书导入 IAM Identity Center
- 在 IdP 中激活新证书
- 删除旧证书

使用以下所有过程来完成证书轮换过程，同时避免任何身份验证停机。

步骤 1：从 IdP 获取新证书

访问 IdP 网站并下载其 SAML 2.0 证书。确保以 PEM 编码格式下载证书文件。大多数提供商都允许您在 IdP 中创建多个 SAML 2.0 证书。这些很可能会被标记为禁用或不活动。

步骤 2：将新证书导入 IAM Identity Center

按照以下过程使用 IAM Identity Center 控制台导入新证书。

1. 在 IAM Identity Center 控制台中，选择设置。
2. 在设置页面上，选择身份源选项卡，然后选择操作>管理身份验证。
3. 在管理 SAML 2.0 证书页面上，选择导入证书。
4. 在导入 SAML 2.0 证书对话框中，选择选择文件，导航到您的证书文件并将其选中，然后选择导入证书。

此时，IAM Identity Center 将信任从您导入的两个证书签名的所有传入 SAML 消息。

步骤 3：在 IdP 中激活新证书

返回 IdP 网站，将您之前创建的新证书标记为主证书或有效证书。此时，由 IdP 签名的所有 SAML 消息都应使用新证书。

步骤 4：删除旧证书

使用以下过程完成 IdP 的证书轮换过程。必须始终列出至少一个有效的证书，并且无法将其删除。

> **Note**
>
> 在删除该证书之前，请确保您的身份提供商不再使用此证书对 SAML 响应进行签名。

1. 在管理 SAML 2.0 证书页面上，选择要删除的证书。选择删除。
2. 在删除 SAML 2.0 证书对话框中，键入 **DELETE** 进行确认，然后选择删除。
3. 返回 IdP 的网站并执行必要的步骤来删除旧的非活动状态证书。

证书过期状态指示器

管理 SAML 2.0 证书页面在列表中每个证书旁边的到期时间列中显示彩色状态指示器图标。下面介绍了 IAM Identity Center 用来确定每个证书显示哪个图标的标准。

- 红色 – 表示证书已到期。
- 黄色 – 表示证书将在 90 天或更短时间内到期。
- 绿色 – 表示证书目前有效，并且将至少再保持 90 天的有效期。

要检查证书的当前状态

1. 在 IAM Identity Center 控制台中，选择设置。
2. 在设置页面上，选择身份源选项卡，然后选择操作>管理身份验证。
3. 在管理 SAML 2.0 身份验证页面的管理 SAML 2.0 证书下，查看列表中证书的状态，如过期时间列中所示。

Microsoft AD 目录

使用 Amazon IAM Identity Center，您可以使用连接 Active Directory (AD) 中的自管理目录或中的 Amazon Managed Microsoft AD 目录。 Amazon Directory Service此 Microsoft AD 目录定义了管理员在使用 IAM Identity Center 控制台分配单点登录访问权限时可以从中提取的身份池。将您的公司目录连接到 IAM Identity Center 后，您可以向 AD 用户或群组授予对 Amazon Web Services 账户应用程序或两者的访问权限。

Amazon Directory Service 帮助您设置和运行托管在中的独立 Amazon Managed Microsoft AD 目录 Amazon Web Services 云。您还可以使用 Amazon Directory Service 将您的 Amazon 资源与现有的自管理 AD 连接起来。 Amazon Directory Service 要配置为使用自管理 AD，必须先设置信任关系以将身份验证扩展到云端。

IAM Identity Center 使用提供的连接 Amazon Directory Service 对源 AD 实例执行直通身份验证。当您使用 Amazon Managed Microsoft AD 作为身份源时，IAM Identity Center 可以处理来自 Amazon Managed Microsoft AD 或来自通过 AD 信任连接的任何域的用户。如果您想要在四个或更多域中找到用户，则用户在登录 IAM Identity Center 时必须使用 `DOMAIN\user` 语法作为其用户名。

> **注意**
>
> - 作为先决条件，请确保您的 AD Connector 或 Amazon Managed Microsoft AD 中的目录 Amazon Directory Service 位于您的 Amazon Organizations 管理账户中。
> - IAM Identity Center 不支持基于 SAMBA 4 的 Simple AD 作为连接目录。
> - IAM Identity Center 无法同步外部安全委托人 (FSPs)。如果中的群组 Amazon Managed Microsoft AD 包含来自可信域的成员 FSPs，则这些成员将无法同步。

有关将 Active Directory 用作 IAM Identity Center 身份源的过程演示，请观看以下 YouTube 视频：

使用 Active Directory 作为 Amazon IAM Identity Center | Amazon Web Services 的身份源

使用 Active Directory 的注意事项

如果要使用 Active Directory 作为身份源，则您的配置必须满足以下先决条件：

- 如果您正在使用 Amazon Managed Microsoft AD，则必须在设置 Amazon Managed Microsoft AD 目录的同一 Amazon Web Services 区域 位置启用 IAM 身份中心。IAM Identity Center 会将分配数据存储在与目录相同的区域中。要管理 IAM Identity Center，您可能需要切换到配置 IAM Identity Center 的区域。另外，请注意， Amazon Web Services 访问门户使用的访问网址与您的目录相同。

- 使用驻留在管理帐户中的 Active Directory：

  您必须在中设置现有 AD Con Amazon Managed Microsoft AD nector 或目录 Amazon Directory Service，并且该目录必须位于您的 Amazon Organizations 管理账户中。一次只能连接一个 AD Connector Amazon Managed Microsoft AD 目录或一个目录。如果您需要支持多个域或林，请使用 Amazon Managed Microsoft AD。有关更多信息，请参阅:

  - 将目录连接 Amazon Managed Microsoft AD 到 IAM 身份中心
  - 将 Active Directory 中的自行管理目录连接到 IAM Identity Center
- 使用驻留在委托管理员帐户中的 Active Directory：

  如果您计划启用 IAM Identity Center 委托管理员并使用 Active Directory 作为您的 IAM 身份中心身份源，则可以使用位于委托管理员账户中的现有 AD Connector 或 Amazon Managed Microsoft AD Amazon 目录中设置的目录。

  如果您决定将 IAM Identity Center 身份源从任何其他源更改为 Active Directory，或者将其从 Active Directory 更改为任何其他源，则该目录必须驻留在 IAM Identity Center 委托管理员成员帐户（如果存在）中（归该帐户所有）；否则，它必须位于管理帐户中。

连接 Active Directory 并指定用户

如果您已经在使用 Active Directory，以下主题可帮助您准备好将目录连接到 IAM Identity Center。

您可以将 Active Directory 中的 Amazon Managed Microsoft AD 目录或自管理目录与 IAM 身份中心连接。

> **Note**
>
> IAM Identity Center 不支持将 SAMBA4基于的 Simple AD 作为身份源。

Amazon Managed Microsoft AD

1. 请查看 Microsoft AD 目录 中的指南。
2. 按照 将目录连接 Amazon Managed Microsoft AD 到 IAM 身份中心 中的步骤操作。
3. 配置 Active Directory 以将您要向其授予管理权限的用户同步到 IAM Identity Center。有关更多信息，请参阅 将管理用户同步到 IAM Identity Center 中。

Active Directory 中的自行管理目录

1. 请查看 Microsoft AD 目录 中的指南。
2. 按照 将 Active Directory 中的自行管理目录连接到 IAM Identity Center 中的步骤操作。
3. 配置 Active Directory 以将您要向其授予管理权限的用户同步到 IAM Identity Center。有关更多信息，请参阅 将管理用户同步到 IAM Identity Center 中。

外部 IdP

1. 请查看 外部身份提供者 中的指南。
2. 按照 如何连接到外部身份提供商 中的步骤操作。
3. 配置您的 IdP 以将用户预置到 IAM Identity Center 中。

> **Note**
>
> 在设置所有人力身份的基于组的自动预调配（从 IdP 到 IAM Identity Center）之前，我们建议您将要向其授予管理权限的一个用户同步到 IAM Identity Center 中。

将管理用户同步到 IAM Identity Center 中

将您的 Active Directory 连接到 IAM Identity Center 后，您可以指定要向其授予管理权限的用户，然后将该用户从您的目录同步到 IAM Identity Center 中。

1. 打开 IAM Identity Center 控制台。
2. 选择设置。
3. 在设置页面上，选择身份源选项卡，从中选择操作，然后选择管理同步。
4. 在管理同步页面上，选择用户选项卡，然后选择添加用户和组。
5. 在用户选项卡的用户项下，输入确切的用户名并选择添加。
6. 在已添加用户和组项下，执行以下操作：
   a. 确认已指定您要向其授予管理权限的用户。
   b. 选中该用户名左边的复选框。
   c. 选择提交。
7. 在管理同步页面中，您指定的用户将显示在同步范围内的用户列表中。
8. 在导航窗格中，选择 Users（用户）。

9. 在用户页面上，您指定的用户可能需要一些时间才会出现在列表中。选择刷新图标以更新用户列表。

此时，您的用户无权访问管理账户。您可以通过创建管理权限集并将用户分配给该权限集来设置对此帐户的管理访问权限。有关更多信息，请参阅 创建权限集。

当用户来自 Active Directory 时进行预置

IAM Identity Center 使用提供的连接将用户、群组和成员资格信息从 Active Directory 中的源目录同步到 IAM 身份中心身份存储。 Amazon Directory Service 密码信息不会同步到 IAM Identity Center，因为用户身份验证直接通过 Active Directory 中的源目录进行。应用程序可使用此身份数据推进应用程序内的查找、授权和协作场景，无需将 LDAP 活动传递回 Active Directory 中的源目录。

有关预置的更多信息，请参阅 用户和组预调配。

主题

- 将目录连接 Amazon Managed Microsoft AD 到 IAM 身份中心
- 将 Active Directory 中的自行管理目录连接到 IAM Identity Center
- IAM Identity Center 与外部身份提供者目录之间的属性映射
- IAM Identity Center 可配置 AD 同步

将目录连接 Amazon Managed Microsoft AD 到 IAM 身份中心

使用以下步骤将中 Amazon Managed Microsoft AD 由管理的目录连接 Amazon Directory Service 到 IAM Identity Center。

连接 Amazon Managed Microsoft AD 到 IAM 身份中心

1. 打开 IAM Identity Center 控制台。

> **Note**
>
> 在进行下一步之前，请确保 IAM Identity Center 控制台正在使用您的 Amazon Managed Microsoft AD 目录所在的区域之一。

2. 选择设置。
3. 在设置页面上，选择身份源选项卡，然后选择操作>更改身份源。
4. 在选择身份源下，选择活动目录，然后选择下一步。

5. 在连接活动目录下，从列表中的 Amazon Managed Microsoft AD 中选择一个目录，然后选择下一步。
6. 在确认更改下，查看信息，准备就绪后键入接受，然后选择更改身份源。

> **Important**
>
> 要将 Active Directory 中的用户指定为 IAM Identity Center 中的管理用户，您必须首先将要向其授予管理权限的用户从 Active Directory 同步到 IAM Identity Center。为此，请按照将管理用户同步到 IAM Identity Center 中中的步骤进行操作。

将 Active Directory 中的自行管理目录连接到 IAM Identity Center

您在 Active Directory (AD) 中自行管理的目录中的用户也可以通过单点登录访问 Amazon Web Services 账户 权限访问访问 Amazon Web Services 门户中的应用程序。要为这些用户配置单点登录访问，您可以执行以下任一操作：

- 创建双向信任关系-在 AD 中 Amazon Managed Microsoft AD 与自管理目录之间创建双向信任关系时，AD 中自我管理目录中的用户可以使用其公司凭据登录各种 Amazon 服务和业务应用程序。单向信任不适用于 IAM Identity Center。

  Amazon IAM Identity Center 需要双向信任，以便它有权从您的域中读取用户和群组信息，从而同步用户和群组元数据。IAM Identity Center 在分配对权限集或应用程序的访问权限时使用此元数据。应用程序还使用用户和组元数据进行协作，例如当您与其他用户或组共享仪表板时。Microsoft Active Directory 对你的域的信任允许 IAM 身份中心信任你的域进行身份验证。 Amazon Directory Service 相反方向的信任会授予读取用户和群组元数据的 Amazon 权限。

  有关设置双向信任的详细信息，请参阅 Amazon Directory Service 管理指南中的何时创建信任关系。

  > **Note**
  >
  > 为了使用诸如 IAM Identity Center 之类的 Amazon 应用程序从可信域读取 Amazon Directory Service 目录用户，这些 Amazon Directory Service 账户需要对可信用户的 userAccountControl属性拥有权限。如果没有此属性的读取权限， Amazon 应用程序就无法确定是启用还是禁用了该账户。
  > 创建信任时，默认会提供对该属性的读取权限。如果您拒绝对此属性的访问权限（不推荐），会让 Identity Center 等应用程序无法读取可信用户。解决方案是专门允许对预

Amazon 留 OU（前缀为 Amazon_）下的 Amazon 服务帐号的`userAccountControl`属性的读取权限。

- 创建 AD Connector——AD Connector 是一个目录网关，可以将目录请求重定向到您的自行管理 AD，而无需在云中缓存任何信息。有关详细信息，请参阅 Amazon Directory Service 管理指南中的连接到目录。以下是配置 AD Connector 策略时的注意事项：
  - 如果您将 IAM Identity Center 连接到 AD Connector 目录，则任何未来的用户密码重置都必须在 AD 内完成。这意味着用户将无法从 Amazon Web Services 访问门户重置密码。
  - 如果您使用 AD Connector 将 Active Directory 域服务连接到 IAM Identity Center，则 IAM Identity Center 仅有权访问 AD Connector 附加到的单个域的用户和组。如果您需要支持多个域或林，请对 Microsoft Active Directory 使用 Amazon Directory Service 。

> **Note**
>
> IAM 身份中心不适用于 SAMBA4基于 Simple AD 的目录。

IAM Identity Center 与外部身份提供者目录之间的属性映射

属性映射可用于将 IAM Identity Center 中存在的属性类型与 Google Workspace、Microsoft Active Directory (AD) 和 Okta 等外部身份源中的类似属性进行映射。IAM Identity Center 从身份源目录检索用户属性并将其映射到 IAM Identity Center 用户属性。

如果您的 IAM Identity Center 同步使用外部身份提供者（IdP）（如 Google Workspace、Okta 或 Ping）作为身份源，您将需要在 IdP 中映射属性。

IAM Identity Center 在其配置页面上的属性映射选项卡下为您预填充一组属性。IAM Identity Center 使用这些用户属性来填充发送到应用程序的 SAML 断言（作为 SAML 属性）。反过来，系统会从身份源中检索这些用户属性。每个应用程序都会确定为了成功实现单点登录，其所需的 SAML 2.0 属性列表。有关更多信息，请参阅 将应用程序中的属性映射到 IAM Identity Center 属性。

如果将 Active Directory 用作身份源，IAM Identity Center 还会在 Active Directory 配置页面的属性映射部分下为您管理一组属性。有关更多信息，请参阅 在 IAM Identity Center 和 Microsoft AD 目录之间映射用户属性。

支持的外部身份提供商属性

下表列出了所有受支持且可以映射到您在 IAM Identity Center 中配置 访问控制属性 时可以使用的属性的外部身份提供者（IdP）属性。使用 SAML 断言时，您可以使用 IdP 支持的任何属性。

IdP 中支持的属性
${path:userName}
${path:name.familyName}
${path:name.givenName}
${path:displayName}
${path:nickName}
${path:emails[primary eq true].value}
${path:addresses[type eq "work"].streetAddress}
${path:addresses[type eq "work"].locality}
${path:addresses[type eq "work"].region}
${path:addresses[type eq "work"].postalCode}
${path:addresses[type eq "work"].country}
${path:addresses[type eq "work"].formatted}
${path:phoneNumbers[type eq "work"].value}
${path:userType}
${path:title}
${path:locale}
${path:timezone}
${path:enterprise.employeeNumber}
${path:enterprise.costCenter}
${path:enterprise.organization}

IdP 中支持的属性
${path:enterprise.division}
${path:enterprise.department}
${path:enterprise.manager.value}

IAM Identity Center 与 Microsoft AD 之间的默认映射

下表列出了 IAM Identity Center 中的用户属性到 Microsoft AD 目录中的用户属性的默认映射。IAM Identity Center 仅支持 IAM Identity Center 列中的用户属性中的属性列表。

IAM Identity Center 中的用户属性	映射到您的 Active Directory 中的此属性
displayname	${displayname}
emails[?primary].value *	${mail}
externalid	${objectguid}
name.givenname	${givenname}
name.familyname	${sn}
name.middlename	${initials}
sid	${objectsid}
username	${userprincipalname}

* IAM Identity Center 中的电子邮件属性在目录中必须是唯一的。

IAM Identity Center 中的组属性	映射到您的 Active Directory 中的此属性
externalid	${objectguid}
description	${description}

IAM Identity Center 中的组属性	映射到您的 Active Directory 中的此属性
displayname	${samaccountname}@{associateddomain}

注意事项

- 如果您在启用可配置 AD 同步时在 IAM Identity Center 中没有为您的用户和组进行任何分配，则将使用前面表格中的默认映射。有关如何自定义这些映射的信息，请参阅 配置用于同步的属性映射。
- 某些 IAM Identity Center 属性无法修改，因为它们是不可变的，并且默认映射到特定的 Microsoft AD 目录属性。

  例如，username 是 IAM Identity Center 的必填属性。如果将 username 映射到值为空的 AD 目录属性，IAM Identity Center 会将 windowsUpn 值视为 username 的默认值。如果想从当前映射中更改 username 的属性映射，请在更改之前确认与 username 存在依赖关系的 IAM Identity Center 流程会继续按预期运行。

IAM Identity Center 支持的 Microsoft AD 属性

下表列出了所有受支持且可映射到 IAM Identity Center 中的用户属性的 Microsoft AD 目录属性。

Microsoft AD 目录支持的属性
${samaccountname}
${description}
${objectguid}
${objectsid}
${givenname}
${sn}
${initials}
${mail}

Microsoft AD 目录支持的属性
`${userprincipalname}`
`${displayname}`
`${distinguishedname}`
`${proxyaddresses[?type == "SMTP"].value}`
`${proxyaddresses[?type == "smtp"].value}`
`${useraccountcontrol}`
`${associateddomain}`

注意事项

- 您可以指定受支持的 Microsoft AD 目录属性的任意组合以映射到 IAM Identity Center 中的单个可变属性。

Microsoft AD 支持的 IAM Identity Center 属性

下表列出了受支持且可以映射到 Microsoft AD 目录中的用户属性的所有 IAM Identity Center 属性。设置应用程序属性映射后，您可以使用这些相同的 IAM Identity Center 属性来映射到该应用程序使用的实际属性。

IAM Identity Center 中 Active Directory 支持的属性
`${user:AD_GUID}`
`${user:AD_SID}`
`${user:email}`
`${user:familyName}`
`${user:givenName}`

IAM Identity Center 中 Active Directory 支持的属性
`${user:middleName}`
`${user:name}`
`${user:preferredUsername}`
`${user:subject}`

在 IAM Identity Center 和 Microsoft AD 目录之间映射用户属性

您可以使用以下过程指定 IAM Identity Center 中的用户属性应如何映射到 Microsoft AD 目录中对应的属性。

将 IAM Identity Center 中的属性映射到目录中的属性

1. 打开 IAM Identity Center 控制台。
2. 选择设置。
3. 在设置页面上，选择访问控制的属性选项卡，然后选择管理属性。
4. 在管理访问控制属性页面上，在 IAM Identity Center 中找到您要映射的属性，然后在文本框中键入值。例如，您可能希望将 IAM Identity Center 用户属性 **`email`** 映射到 Microsoft AD 目录属性 **`${mail}`**。
5. 选择保存更改。

IAM Identity Center 可配置 AD 同步

IAM Identity Center 可配置的 Active Directory (AD) 同步使您能够显式配置 Microsoft Active Directory 中的身份，这些身份会自动同步到 IAM Identity Center 并控制同步过程。

- 在该同步方法中，您可以执行下述步骤：
  - 通过显式定义 Microsoft Active Directory 中自动同步到 IAM Identity Center 的用户和组来控制数据边界。您可以随时添加用户和组或删除用户和组以更改同步范围。
  - 为同步用户和组分配对 Amazon Web Services 账户的单点登录访问权限或对应用程序的访问权限。这些应用程序可以是 Amazon 托管应用程序或客户管理的应用程序。
  - 通过根据需要暂停和恢复同步来控制同步过程。这可以帮助您调节生产系统的负载。

先决条件和注意事项

在使用可配置的 AD 同步之前，请注意以下先决条件和注意事项：

- 指定 Active Directory 中要同步的用户和组

  在使用 IAM Identity Center 为新用户和群组分配 Amazon 托管应用程序或客户托管应用程序的访问权限之前，您必须在 Active Directory 中指定要同步的用户和群组，然后将其同步到 IAM Identity Center 中。 Amazon Web Services 账户

  - 可配置的 AD 同步——IAM Identity Center 不会直接在域控制器中搜索用户和组。相反，您必须首先指定要同步的用户和组的列表。您可以通过以下方式之一配置此列表（也称为同步范围），具体取决于您的用户和组是否已同步到 IAM Identity Center，或者您有新用户和组是首次使用可配置的 AD 同步进行同步。
    - 现有用户和组：如果您的用户和组已同步到 IAM Identity Center，则可配置 AD 同步中的同步范围将预先填充这些用户和组的列表。要分配新用户或组，您必须专门将它们添加到同步范围。有关更多信息，请参阅 将用户和组添加到您的同步范围。
    - 新用户和组：如果您想要为新用户和组分配对 Amazon Web Services 账户 和应用程序的访问权限，您必须在可配置的 AD 同步中指定要添加到同步范围的用户和组，然后才能使用 IAM Identity Center 进行分配。有关更多信息，请参阅 将用户和组添加到您的同步范围。

- 分配到 Active Directory 中的嵌套组

  作为其他组成员的组称为嵌套组（或子组）。

  - 可配置 AD 同步 – 使用可配置 AD 同步分配 Active Directory 中包含嵌套组的组，可能会扩大有权访问 Amazon Web Services 账户 或应用程序的用户范围。在这种情况下，分配将应用于所有用户，包括嵌套组中的用户。例如，如果您向组 A 分配访问权限，而组 B 是组 A 的成员，则组 B 的成员也会继承此访问权限。

- 更新自动化工作流程

  如果您有自动化工作流程，其使用 IAM Identity Center 身份存储 API 操作和 IAM Identity Center 分配 API 操作来分配新用户和组对帐户和应用程序的访问权限并将其同步到 IAM Identity Center，您必须通过以下方式调整这些工作流程： 2022 年 4 月 15 日，以便它们通过可配置的 AD 同步按预期运行。可配置的 AD 同步可更改用户和组分配和预置发生的顺序以及执行查询的方式。

  - 可配置的 AD 同步——首先进行预置，并且不会自动执行。相反，您必须首先通过将用户和组添加到同步范围来明确将用户和组添加到身份存储。有关自动执行同步配置以实现可配置 AD 同步的建议步骤的信息，请参阅 自动执行同步配置以实现可配置的 AD 同步。

主题

可配置 AD 同步的工作原理

IAM Identity Center 使用以下过程刷新身份存储中基于 AD 的身份数据。要了解有关先决条件的更多信息，请参阅 先决条件和注意事项。

创建

将 Active Directory 中的自我管理 Amazon Managed Microsoft AD 目录或由管理的目录连接 Amazon Directory Service 到 IAM 身份中心后，您可以显式配置要同步到 IAM 身份中心身份存储中的 Active Directory 用户和群组。您选择的身份将每三个小时左右同步到 IAM Identity Center 身份存储中。根据目录的大小，同步过程可能需要更长的时间。

作为其他组成员的组（称为嵌套组或子组）也会写入身份存储。

您只能在新用户或组同步到 IAM Identity Center 身份存储后为其分配访问权限。

更新

通过定期从 Active Directory 中的源目录读取数据，IAM Identity Center 身份存储中的身份数据保持最新。IAM Identity Center 默认会在同步周期内每小时同步来自 Active Directory 的数据。根据 Active Directory 的大小，数据可能需要 30 分钟到 2 小时才能同步到 IAM Identity Center。

同步范围内的用户和组对象及其成员身份在 IAM Identity Center 中创建或更新，以映射到 Active Directory 源目录中的相应对象。对于用户属性，仅在 IAM Identity Center 控制台的访问控制属性部分中列出的属性子集会在 IAM Identity Center 中更新。您在 Active Directory 中所做的任何属性更新，可能需要一个同步周期才能反映在 IAM Identity Center 中。

您还可以更新同步到 IAM Identity Center 身份存储中的用户和组子集。您可以选择将新用户或组添加到此子集中，或将其删除。您添加的任何身份都会在下一次计划的同步时同步。您从子集中删除的身份将停止在 IAM Identity Center 身份存储中更新。超过 28 天未同步的任何用户都将在 IAM Identity

Center 身份存储中被禁用。在下一个同步周期期间，相应的用户对象将在 IAM Identity Center 身份存储中自动禁用，除非它们属于仍属于同步范围的另一个组的一部分。

删除

当从 Active Directory 中的源目录中删除相应的用户或组对象时，用户和组将从 IAM Identity Center 身份存储中删除。或者，您可以使用 IAM Identity Center 控制台从 IAM Identity Center 身份存储中明确删除用户对象。如果您使用 IAM Identity Center 控制台，您还必须从同步范围中删除用户，以确保他们在下一个同步周期内不会重新同步回 IAM Identity Center。

您还可以随时暂停和恢复同步。如果您暂停同步的时间超过 28 天，则所有用户都将被禁用。

配置用于同步的属性映射

有关属性的更多信息，请参阅 IAM Identity Center 与外部身份提供者目录之间的属性映射。

在 IAM Identity Center 中配置到您的目录的属性映射

1. 打开 IAM Identity Center 控制台。
2. 选择设置。
3. 在设置页面上，选择身份源选项卡，从中选择操作，然后选择管理同步。
4. 在管理同步下，选择查看属性映射。
5. 在 Active Directory 用户属性下，配置 IAM Identity Center 身份存储属性和 Active Directory 用户属性。例如，您可能希望将 IAM Identity Center 身份存储属性 `email` 映射到 Active Directory 用户目录属性 `${objectguid}`。

   > **Note**
   >
   > 在组属性下，无法更改 IAM Identity Center 身份存储属性和 Active Directory 组属性。

6. 选择保存更改。这将返回管理同步页面。

首次将 Active Directory 同步到 IAM Identity Center 的设置

如果是首次将用户和组从 Active Directory 同步到 IAM Identity Center，请按照以下步骤操作。或者，您可以遵循 更改您的身份源 中概述的步骤，将身份源从 IAM Identity Center 更改为 Active Directory。

引导式设置

1. 打开 IAM Identity Center 控制台。

> **Note**
>
> 在进入下一步之前，请确保 IAM Identity Center 控制台使用的是您的 Amazon Managed Microsoft AD 目录所在的控制台。 Amazon Web Services 区域

2. 选择设置。
3. 在页面顶部的通知消息中，选择启动引导式设置。
4. 在步骤 1——可选：配置属性映射中，查看默认的用户和组属性映射。如果不需要更改，请选择下一步。如果需要更改，请进行更改，然后选择保存更改。
5. 在步骤 2——可选：配置同步范围中，选择用户选项卡。然后，输入要添加到同步范围的用户的确切用户名，然后选择添加。接下来，选择 组 选项卡。输入要添加到同步范围的组的确切组名称，然后选择添加。然后选择下一步。如果您想稍后将用户和组添加到同步范围，请不进行任何更改并选择下一步。
6. 在步骤 3：查看并保存配置中，确认步骤 1：属性映射中的属性映射以及步骤 2：同步范围中的用户和组。选择 Save configuration。这将带您进入管理同步页面。

将用户和组添加到您的同步范围

> **Note**
>
> 将群组添加到同步范围时，请直接从受信任的本地域同步群组，而不是从域中的群组同步群组。 Amazon Managed Microsoft AD 直接从可信域同步的群组包含 IAM Identity Center 可以成功访问和同步的实际用户对象。

按照以下步骤将 Active Directory 用户和组添加到 IAM Identity Center。

添加用户

1. 打开 IAM Identity Center 控制台。
2. 选择设置。
3. 在设置页面上，选择身份源选项卡，从中选择操作，然后选择管理同步。
4. 在管理同步页面上，选择用户选项卡，然后选择添加用户和组。
5. 在用户选项卡的用户项下，输入确切的用户名并选择添加。
6. 在已添加的用户和组下，查看要添加的用户。

7. 选择提交。
8. 在导航窗格中，选择 Users（用户）。如果列表中未显示您指定的用户，请选择刷新图标更新用户列表。

添加组

1. 打开 IAM Identity Center 控制台。
2. 选择设置。
3. 在设置页面上，选择身份源选项卡，从中选择操作，然后选择管理同步。
4. 在管理同步页面上，选择组选项卡，然后选择添加用户和组。
5. 选择组选项卡。在组下，输入准确的组名称并选择添加。
6. 在已添加的用户和组下，查看要添加的组。
7. 选择提交。
8. 在导航窗格中，选择 组。如果列表中未显示您指定的组，请选择刷新图标更新组列表。

从同步范围中删除用户和组

有关从同步范围中删除用户和组时会发生什么情况的详细信息，请参阅 可配置 AD 同步的工作原理。

删除用户

1. 打开 IAM Identity Center 控制台。
2. 选择设置。
3. 在设置页面上，选择身份源选项卡，从中选择操作，然后选择管理同步。
4. 选择用户选项卡。
5. 在同步范围内的用户下，选中要删除的用户旁边的复选框。要删除所有用户，请选中用户名旁边的复选框。
6. 选择移除 。

移除组

1. 打开 IAM Identity Center 控制台。
2. 选择设置。
3. 在设置页面上，选择身份源选项卡，从中选择操作，然后选择管理同步。

4. 选择组选项卡。
5. 在同步范围内的组下，选中要删除的用户旁边的复选框。要删除所有组，请选中组名称旁边的复选框。
6. 选择移除 。

暂停和恢复同步

暂停同步会暂停所有未来的同步周期，并防止您对 Active Directory 中的用户和组所做的任何更改反映在 IAM Identity Center 中。恢复同步后，同步周期将从下一次计划的同步中获取这些更改。

暂停同步

1. 打开 IAM Identity Center 控制台。
2. 选择设置。
3. 在设置页面上，选择身份源选项卡，从中选择操作，然后选择管理同步。
4. 在管理同步下，选择暂停同步。

恢复同步

1. 打开 IAM Identity Center 控制台。
2. 选择设置。
3. 在设置页面上，选择身份源选项卡，从中选择操作，然后选择管理同步。
4. 在管理同步下，选择恢复同步。

> **Note**
>
> 如果您看到暂停同步而不是恢复同步，则表明从 Active Directory 到 IAM Identity Center 的同步已恢复。

自动执行同步配置以实现可配置的 AD 同步

为了确保您的自动化工作流程通过可配置的 AD 同步按预期工作，我们建议您执行以下步骤来自动化同步配置。

要自动执行同步配置以实现可配置的 AD 同步

1. 在 Active Directory 中，创建一个父同步组以包含您想要同步到 IAM Identity Center 的所有用户和组。例如，您可以为该组命名IAMIdentityCenterAllUsersAndGroups。
2. 在 IAM Identity Center 中，将父同步组添加到您的可配置同步列表中。IAM Identity Center 将同步父同步组中包含的所有用户、组、子组以及所有组的成员。
3. 使用 Microsoft 提供的 Active Directory 用户和组管理 API 操作在父同步组中添加或删除用户和组。

管理 Identity Center 目录中的用户

IAM Identity Center 为您的用户和组提供以下功能：

- 创建您的用户和组。
- 将您的用户作为成员添加到组中。
- 为群组分配您 Amazon Web Services 账户 和应用程序所需的访问权限级别。

要管理 IAM Identity Center 存储中的用户和群组，请 Amazon 支持身份中心操作中列出的 API 操作。

当用户位于 IAM Identity Center 时进行预置

当您直接在 IAM Identity Center 中创建用户和组时，会进行自动预置。这些身份可立即用于进行分配，并由应用程序使用。有关更多信息，请参阅 用户和组预调配。

更改您的身份源

如果您更喜欢在中管理用户 Amazon Managed Microsoft AD，则可以随时停止使用您的身份中心目录，而是使用将 IAM 身份中心连接到 Microsoft AD 中的目录 Amazon Directory Service。有关更多信息，请参阅 在 IAM Identity Center 目录和 Active Directory 之间进行更改 注意事项。

如果您希望在外部身份提供商 (IdP) 中管理用户，您可以将 IAM Identity Center 连接到您的 IdP 并启用自动预置。有关更多信息，请参阅 从 IAM Identity Center 更改为外部 IdP 注意事项。

主题

- 将用户添加到 Identity Center 目录
- 将组添加到 Identity Center 目录

- 将用户添加到组
- 删除 IAM Identity Center 中的组
- 删除 IAM Identity Center 中的用户
- 从组中删除用户
- 编辑 Identity Center 目录用户属性

将用户添加到 Identity Center 目录

您在 Identity Center 目录中创建的用户和组仅在 IAM Identity Center 中可用。使用以下过程将用户添加到您的 Identity Center 目录中。或者，您可以调用 Amazon API 操作CreateUser来添加用户。

Console

如何添加用户

1. 打开 IAM Identity Center 控制台。
2. 选择用户。
3. 选择添加用户并提供以下必需信息：

   a. 用户名-此用户名是登录 Amazon Web Services 访问门户所必需的，以后无法更改。它必须介于 1 到 100 个字符之间。

   b. 密码——您可以发送一封包含密码设置说明的电子邮件（这是默认选项）或生成一次性密码。如果您要创建管理用户并选择发送电子邮件，请确保指定可以访问的电子邮件地址。

      i. 向该用户发送包含密码设置说明的电子邮件 - 此选项会自动向用户发送一封来自 Amazon Web Services 的电子邮件，主题为邀请加入 Amazon IAM Identity Center。该电子邮件代表公司邀请用户访问 IAM Identity Center Amazon Web Services 访问门户，并注册密码。电子邮件邀请会在七天后过期。如果邀请过期，您可以选择重置密码，然后选择向用户发送一封包含重置密码说明的电子邮件，以此重新发送电子邮件。在用户接受邀请之前，您会看到“发送电子邮件验证”链接，该链接用于验证用户的电子邮件地址。不过，此为可选步骤，会在用户接受邀请并注册密码后消失。

      > **Note**
      >
      > 在某些情况下，IAM Identity Center 会进行跨区域 API 调用以向用户发送电子邮件。有关如何发送电子邮件的信息，请参阅 使用 Amazon SES 的跨区域电子邮件。

IAM Identity Center 服务发送的所有电子邮件都将来自地址 `no-reply@signin.aws.com` 或 `no-reply@login.awsapps.com`。我们建议您配置电子邮件系统，以便它接受来自这些发件人电子邮件地址的电子邮件，并且不将它们作为垃圾邮件处理。

ii. 生成可与该用户共享的一次性密码-此选项为您提供 Amazon Web Services 访问门户 URL 和密码详细信息，您可以通过您的电子邮件地址手动将其发送给用户。用户需要验证自己的电子邮件地址。您可以通过选择“发送电子邮件验证”链接启动该过程。电子邮件验证链接会在七天后过期。如果链接过期，您可以选择重置密码，然后选择生成一次性密码并与用户共享密码，以此重新发送电子邮件验证链接。

c. 电子邮件地址——电子邮件地址必须是唯一的。

d. 确认电子邮件地址

e. 名字——必须在此处输入姓名才能使自动预置生效。有关更多信息，请参阅 使用 SCIM 从外部身份提供者预置用户和组。

f. 姓氏——必须在此处输入姓名才能使自动预置生效。

g. 显示名称

> **Note**
>
> （可选）如果适用，您可以指定其他属性的值，例如用户的 Microsoft 365 不可变 ID，以帮助为用户提供对某些业务应用程序的单点登录访问权限。

4. 选择下一步。
5. 如果适用，选择一个或多个要将用户添加到的组，然后选择下一步。
6. 查看您为步骤 1：指定用户详细信息和步骤 2：将用户添加到组——可选指定的信息。选择按任一步骤编辑以进行任何更改。确认为这两个步骤指定了正确的信息后，选择添加用户。

Amazon CLI

如何添加用户

以下 `create-user` 命令会在您的 Identity Center 目录中创建一个新用户。

```
aws identitystore create-user \
    --identity-store-id d-1234567890 \
    --user-name johndoe \
    --name "GivenName=John,FamilyName=Doe" \
```

```
    --display-name "John Doe" \
    --emails "Type=work,Value=johndoe@example.com"
```

输出：

```
{
    "UserId": "1234567890-abcdef",
    "IdentityStoreId": "d-1234567890"
}
```

> **Note**
>
> 使用 `create-user` CLI 命令或 CreateUser API 操作创建用户时，这些用户默认没有密码。您可以更新 IAM Identity Center 中的设置，以便在这些用户首次尝试登录后向他们发送验证电子邮件，以便他们设置密码。如果您不启用此设置，则必须生成一次性密码并与用户共享。有关更多信息，请参阅 向使用 API 或 CLI 创建的用户发送电子邮件一次性密码。

将组添加到 Identity Center 目录

使用以下过程将组添加到您的 Identity Center 目录中。或者，您可以调用 Amazon API 操作CreateGroup来添加群组。

Console

添加组

1. 打开 IAM Identity Center 控制台。
2. 选择组。
3. 选择创建群组。
4. 输入组名称和描述 - 可选。描述应提供有关已分配或将分配给该组的权限的详细信息。在将用户添加到组——可选下，找到要添加为成员的用户。然后选中其中每个用户旁边的复选框。
5. 选择创建群组。

Amazon CLI

添加组

以下 `create-group` 命令会在您的 Identity Center 目录中创建一个新组。

```
aws identitystore create-group \
    --identity-store-id d-1234567890 \
    --display-name "Developers" \
    --description "Group that contains all developers"
```

输出：

```
{
    "GroupId": "1a2b3c4d-5e6f-7g8h-9i0j-1k2l3m4n5o6p",
    "IdentityStoreId": "d-1234567890"
}
```

将此组添加到 Identity Center 目录后，您可以向该组分配单点登录访问权限。有关更多信息，请参阅为用户或群组分配访问权限 Amazon Web Services 账户。

将用户添加到组

使用以下过程将用户添加为之前 Identity Center 目录中创建的组的成员。或者，您可以调用 Amazon API 操作CreateGroupMembership将用户添加为群组成员。

Console

将用户添加为组的成员

1. 打开 IAM Identity Center 控制台。
2. 选择组。
3. 选择您要更新的组名称。
4. 在组详细信息页面上的此组中的用户下，选择将用户添加到组。
5. 在将用户添加到组页面上的其他用户下，找到要添加为成员的用户。然后，选中每个选项旁边的复选框。
6. 选择添加用户。

Amazon CLI

将用户添加为组的成员

以下 `create-group-membership` 命令会将用户添加到您的 Identity Center 目录中的组。

```
aws identitystore create-group-membership \
    --identity-store-id d-1234567890 \
    --group-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222 \
    --member-id UserId=a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

输出：

```
{
    "MembershipId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
    "IdentityStoreId": "d-1234567890"
}
```

删除 IAM Identity Center 中的组

当您删除 IAM Identity Center 目录中的组时，所有身为该组成员的用户对 Amazon Web Services 账户和应用程序的访问权限也会被删除。组删除后无法撤消。使用以下过程删除 Identity Center 目录中的组。

> **Important**
>
> 本页的说明适用于 Amazon IAM Identity Center。它们不适用于 Amazon Identity and Access Management(IAM)。IAM Identity Center 用户、组和用户凭证不同于 IAM 用户、组和 IAM 用户凭证。如果您正在寻找有关在 IAM 中删除组的说明，请参阅 Amazon Identity and Access Management 用户指南中的删除 IAM 用户组。

Console

删除组

1. 打开 IAM Identity Center 控制台。
2. 选择组。
3. 您可以通过两种方式删除组：
   - 在组页面，您可以选择多个组进行删除。选择要删除的组名称，然后选择删除组。
   - 选择您要删除的组名称。在组详细信息页面上，选择删除组。

4. 系统可能会要求您确认删除该组的意图。
   - 如果您一次删除多个组，请通过在删除组对话框中键入 **Delete** 来确认您的意图。
   - 如果您删除包含用户的单个组，请通过在删除组对话框中键入要删除的组的名称来确认您的意图。
5. 选择删除组。如果您选择删除多个组，请选择删除 # 个组。

Amazon CLI

删除组

以下 `delete-group` 命令从您的 Identity Center 目录中删除指定的组。

```
aws identitystore delete-group \
    --identity-store-id d-1234567890 \
    --group-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222
```

删除 IAM Identity Center 中的用户

当您删除 IAM Identity Center 目录中的用户时，其对 Amazon Web Services 账户 和应用程序的访问权限也会被删除。删除用户之后，您无法撤消此操作。使用以下过程删除 Identity Center 目录中的用户。

> **Note**
>
> 当您在 IAM Identity Center 中禁用用户访问权限或删除用户时，该用户将立即被禁止登录 Amazon Web Services 访问门户，也无法创建新的登录会话。有关更多信息，请参阅 了解 IAM Identity Center 中的身份验证会话。

> **Important**
>
> 本页的说明适用于 Amazon IAM Identity Center。它们不适用于 Amazon Identity and Access Management(IAM)。IAM Identity Center 用户、组和用户凭证不同于 IAM 用户、组和 IAM 用户凭证。如果您正在寻找有关在 IAM 中删除用户的说明，请参阅 Amazon Identity and Access Management 用户指南中的删除 IAM 用户。

Console

删除用户

1. 打开 IAM Identity Center 控制台。
2. 选择用户。
3. 有两种方法可以删除用户：
   - 在用户页面上，您可以选择删除多个用户。选择要删除的用户名，然后选择删除用户。
   - 选择您要删除的用户名。在用户详细信息页面上，选择删除用户。
4. 如果您一次删除多个用户，请通过在删除用户对话框中键入 **Delete** 来确认您的意图。
5. 选择删除用户。如果您选择删除多个用户，请选择删除 # 个用户。

Amazon CLI

删除用户

以下 `delete-user` 命令从您的 Identity Center 目录中删除用户。

```
aws identitystore delete-user \
    --identity-store-id d-1234567890 \
    --user-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

从组中删除用户

使用以下过程从组中移除成员。或者，您可以调用 Amazon API 操作DeleteGroupMembership将用户从群组中移除。

Console

从组中移除用户

1. 打开 IAM Identity Center 控制台。
2. 选择组。
3. 选择要更新的组。
4. 在组详细信息页面上，此组中的用户下，选择要移除的用户。
5. 选择从组中移除用户。

6. 在移除用户对话框上，选择从组中移除用户，以确认您要移除这些用户对该组所分配的账户和应用程序的访问权限。

Amazon CLI

从组中移除用户

以下 `delete-group-membership` 命令从组中移除成员资格。

```
aws identitystore delete-group-membership
    --identity-store-id d-1234567890 \
    --membership-id a1b2c3d4-5678-90ab-cdef-EXAMPLE33333
```

编辑 Identity Center 目录用户属性

使用以下过程编辑 Identity Center 目录中的用户的属性。或者，您可以调用 Amazon API 操作 UpdateUser来更新用户属性。

Console

在 IAM Identity Center 中编辑用户属性

1. 打开 IAM Identity Center 控制台。
2. 选择用户。
3. 选择您要编辑的用户。
4. 在用户配置文件页面上的配置文件详细信息旁边，选择编辑。
5. 在编辑配置文件详细信息页面上，根据需要更新属性。然后选择 Save changes（保存更改）。

> **Note**
>
> （可选）您可以修改其他属性，例如员工编号和 Office 365 Immutable ID，以帮助将 IAM Identity Center 中的用户身份与用户需要使用的某些业务应用程序进行映射。

> **Note**
>
> 电子邮件地址属性是一个可编辑字段，您提供的值必须是唯一的。

Amazon CLI

在 IAM Identity Center 中编辑用户属性

以下 `update-user` 命令更新用户的昵称。

```
aws identitystore update-user \
    --identity-store-id d-1234567890 \
    --user-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --operations '{"AttributePath":"nickName","AttributeValue":"Johnny"}'
```

设置员工对 Amazon 资源的访问权限

设置员工用户如何通过 IAM 身份中心进行身份验证和访问 Amazon 资源。本节涵盖管理员工用户访问您的 Amazon 环境的以下组件：

- 身份验证会话：了解 IAM Identity Center 如何管理不同类型的用户会话，从交互式门户会话到后台应用程序会话，以及它们之间如何交互。
- 用户访问管理：配置会话持续时间、禁用用户账户并实施组织范围的访问阻止，以维护安全性和合规性。
- 密码管理：对于在 Identity Center 目录中创建的用户，设置密码要求、处理用户凭证设置以及管理用户密码重置。
- 多重身份验证：对于在 Identity Center 目录中创建的用户，使用验证器应用程序、安全密钥或内置验证器进行 MFA 以增强安全性，保护用户登录。

主题

了解 IAM Identity Center 中的身份验证会话

当用户登录 Amazon Web Services 访问门户时，IAM Identity Center 会创建一个代表用户已验证身份的身份验证会话。

经过身份验证后，用户无需额外登录即可访问其所有已分配 Amazon Web Services 账户、Amazon托管的应用程序以及管理员授予其使用权限的客户管理的应用程序。

身份验证会话的类型

用户交互式会话

用户登录 Amazon Web Services 访问门户后，IAM Identity Center 会创建用户交互式会话。此会话代表用户在 IAM Identity Center 内的已验证状态，并作为创建其他会话类型的基础。用户交互式会话的持续时间可以在 IAM Identity Center 中配置，最长可达 90 天。

用户交互式会话是主要的身份验证机制。当用户注销或管理员终止其会话时，这些会话结束。应根据组织的安全要求仔细配置这些会话的持续时间。

有关配置用户交互式会话持续时间的信息，请参阅 the section called “配置会话持续时间”。

应用程序会话

应用程序会话是 IAM Identity Center 通过单点登录建立的用户与 Amazon 托管应用程序（例如 Kiro 或 Amazon Quick）之间经过身份验证的连接。

默认情况下，应用程序会话的有效期为一小时，但只要基础的用户交互式会话仍然有效，它们就会自动刷新。这种刷新机制在保持安全控制的同时，为用户提供了无缝的体验。当用户交互式会话结束时（无论是通过用户注销还是管理员操作），应用程序会话将在下一次尝试刷新时结束，通常是在 30 分钟内。

用户后台会话

用户后台会话是持续时间较长的会话，专为需要连续运行数小时或数天的进程的应用程序而设计。目前，这种会话类型主要适用于 Amazon SageMaker Studio，数据科学家可能会在那里运行需要数小时才能完成的机器学习训练作业。

有关配置用户后台会话持续时间的信息，请参阅用户后台会话。

Kiro 会议

您可以延长 Kiro 会话，允许使用 Kiro 的开发者 IDEs 将身份验证保持长达 90 天。此功能可在您编写代码时减少登录中断。

这些会话独立于其他会话类型，并且不会影响用户交互式会话或其他 Amazon 托管应用程序。根据您启用 IAM Identity Center 的时间，此功能可能默认启用。

有关配置扩展 Kiro 会话的信息，请参阅???。

IAM Identity Center 创建的 IAM 角色会话

当用户访问 Amazon Web Services 管理控制台 或时，IAM Identity Center 会创建不同类型的会话 Amazon CLI。在这些情况下，IAM Identity Center 使用登录会话，通过担任用户权限集中指定的 IAM 角色来获取 IAM 会话。

> **Important**
>
> 与应用程序会话不同，IAM 角色会话一旦建立便独立运行。它们的持续时间根据权限集中的配置而定，最长可达 12 小时，与原始登录会话的状态无关。这种行为确保了长时间运行的 CLI 操作或控制台会话不会意外终止。

在 IAM Identity Center 中结束用户会话的方法

用户启动

当用户退出 Amazon Web Services 访问门户时，登录会话将结束，从而阻止用户访问任何新资源。

然而，现有的应用程序会话不会立即结束。相反，它们会在下次尝试刷新并发现登录会话不再有效时结束，通常在大约 30 分钟内。现有的 IAM 角色会话会持续到根据权限集配置到期为止，这可能长达 12 小时之后。

由管理员启动

您组织中拥有 IAM Identity Center 管理权限的任何人员（通常是 IT 管理员或安全团队）都可以结束用户的会话。此操作与用户自行注销的工作方式相同，允许管理员在需要时要求用户重新登录。当安全策略更改或检测到可疑活动时，此功能非常有用。

当 IAM Identity Center 管理员删除用户或禁用用户的访问权限时，用户将失去对 Amazon Web Services 访问门户的访问权限，并且无法重新登录以启动新的应用程序或 IAM 角色会话。用户将在 30 分钟内失去对现有应用程序会话的访问权限。任何现有的 IAM 角色会话将根据 IAM Identity Center 权限集中配置的会话持续时间继续运行。最长会话持续时间可为 12 小时。

结束会话时用户访问权限会发生什么变化

本参考提供了有关采取管理操作时 IAM Identity Center 会话行为的详细信息。本节中的表格显示了用户管理操作和权限更改对访问门户、应用程序和 Amazon Web Services 账户 会话 Amazon Web Services 访问权限的持续时间和影响。

User management

此表汇总了用户管理变更如何影响对 Amazon 资源、应用程序会话和 Amazon 账户会话的访问。

Action	用户失去 IAM Identity Center 访问权限	用户无法创建新的应用程序会话	用户无法访问现有应用程序会话	用户无法访问现有 Amazon Web Services 账户 会话
用户的访问权限被禁用	立即生效	立即生效	30 分钟内	12 小时或更短。持续时间取决于为权限集配置的 IAM 角色会话到期持续时间。
用户被删除	立即生效	立即生效	30 分钟内	12 小时或更短。持续时间取决于为权限集配置的 IAM 角色会话到期持续时间。
用户会话被撤销	用户必须重新登录才能恢复访问权限	立即生效	30 分钟内	12 小时或更短。持续时间取决于为权限集配置的 IAM 角色会话到期持续时间。
用户注销	用户必须重新登录才能恢复访问权限	立即生效	30 分钟内	12 小时或更短。持续时间取决于为权限集配置的 IAM 角色会话到期持续时间。

组成员资格

此表汇总了用户权限和群组成员资格的更改如何影响对 Amazon 资源、应用程序会话和 Amazon 账户会话的访问。

Action	用户失去 IAM Identity Center 访问权限	用户无法创建新的应用程序会话	用户无法访问现有应用程序会话	用户无法访问现有 Amazon Web Services 账户 会话
已删除用户的应用程序或 Amazon Web Services 账户 访问权限	否 - 用户可以继续访问 IAM Identity Center	立即生效	1 小时内	12 小时或更短。持续时间取决于为权限集配置的 IAM 角色会话到期持续时间。
用户已从已分配应用程序或 Amazon Web Services 账户的组中移除	否 - 用户可以继续访问 IAM Identity Center	1 小时内	2 小时内	12 小时或更短。持续时间取决于为权限集配置的 IAM 角色会话到期持续时间。
已从组中移除应用程序或 Amazon Web Services 账户 访问权限	否 - 用户可以继续访问 IAM Identity Center	立即生效	1 小时内	12 小时或更短。持续时间取决于为权限集配置的 IAM 角色会话到期持续时间。

> **Note**
>
> Amazon Web Services 访问门户 Amazon CLI 将在您在该群组中添加或移除用户后的 1 小时内反映更新的用户权限。

了解时间差异

- 立即生效 - 需要立即重新进行身份验证的操作。
- 30 分钟至 2 小时内 - 应用程序会话需要时间与 IAM Identity Center 核对并发现任何更改。
- 12 小时或更短 - IAM 角色会话独立运行，仅在配置的持续时间到期时结束。

单点注销

IAM Identity Center 不支持由作为您身份源的身份提供者发起的 SAML 单点注销（一种协议，当用户从一个应用程序注销时，会自动将其从所有连接的应用程序中注销）。此外，它不会向使用 IAM Identity Center 作为身份提供者的 SAML 2.0 应用程序发送 SAML 单点注销。

会话管理的最佳实践

有效的会话管理需要周密的配置和监控。组织应根据其安全要求配置会话持续时间，通常对敏感的应用程序和环境使用较短的持续时间。

实施在用户更改角色或离开组织时终止会话的流程，对于维护安全边界至关重要。应将定期审查活跃会话纳入安全监控实践，以检测可能表明安全问题的异常行为，例如异常的访问模式、意外的登录时间或地点，或访问正常职务功能之外的资源。

在 IAM Identity Center 中配置会话持续时间

当员工用户使用 Amazon Web Services 访问门户 和与 IAM Identity Center 配合使用的应用程序（包括 Kiro）时，您可以为他们配置会话持续时间。IAM Identity Center 提供以下会话类型：用户交互式会话、用户后台会话和 Kiro 的扩展会话。

主题

用户交互式会话

用户交互式会话是指与用户登录 Amazon Web Services 访问门户或访问Amazon 托管应用程序相关的会话。对 Amazon Web Services 访问门户 和应用程序进行身份验证的会话持续时间是用户无需重新进行身份验证即可登录的最大时长。如果您结束活动 Amazon Web Services 访问门户会话，则这些托管应用程序的所有会话也会随之结束。

用户交互式会话的默认会话持续时间为 8 小时。您可以指定不同的持续时间，从最少 15 分钟到最长 90 天不等。自定义持续时间值必须以分钟为单位输入，并且介于 15 分钟到 129,600 分钟（90 天）之间。有关更多信息，请参阅 了解 IAM Identity Center 中的身份验证会话。

有关诸如 IAM Identity Center 身份源如何影响用户交互会话持续时间等注意事项，请参阅the section called “身份源、 Amazon CLI 和 Amazon SDKs”。

配置用户交互式会话的持续时间

1. 打开 IAM Identity Center 控制台。
2. 选择设置。
3. 在设置页面上，选择身份验证选项卡。
4. 在身份验证下,会话持续时间旁边，选择配置。这时会出现一个配置会话持续时间对话框。
5. 在配置会话持续时间对话框的用户交互式会话下，点击下拉箭头选择用户的最大会话时长。选择会话时长，然后选择保存。

> **Note**
>
> 对会话持续时间的更改仅适用于新会话。当前会话保持原始持续时间。

6. 您将返回到身份验证选项卡。选项卡上方会出现一条绿色的通知消息，指示会话设置已成功更新。

用户后台会话

用户后台会话允许用户在 Amazon 托管应用程序（例如 Amazon SageMaker Studio）上启动长时间运行的作业，而无需在任务运行时保持登录状态。作业立即运行，并利用 IAM Identity Center 的可信身份传播功能，确保在后台运行作业时保持用户的权限。即使用户关闭计算机、IAM Identity Center 登录会话过期或用户退出 Amazon Web Services 访问门户，该作业仍可以继续运行。此功能使数据科学家、机器学习工程师和其他人员能够启动在后台运行的分析和机器学习工作流，而无需用户主动参与。

默认情况下，支持 Amazon 托管应用程序（例如 Amazon SageMaker Studio）启用用户后台会话。但是，要使用此功能，您必须在创建或更新域时在 Amazon SageMaker Studio 中启用可信身份传播。有关更多信息，请参阅在您的 Amazon A SageMaker I 域中启用可信身份传播。

用户后台会话的默认会话持续时间为 7 天。您可以指定不同的持续时间，从最少 15 分钟到最长 90 天不等。自定义持续时间值必须以分钟为单位输入，并且介于 15 分钟到 129,600 分钟（90 天）之间。

请记住以下关于用户后台会话的注意事项：

- 只有当用户在 Amazon SageMaker Studio 中手动启动任务时，才能创建用户后台会话。自动化、计划的工作流不支持此功能。
- 有关支持用户后台会话的 Amazon 区域列表，请参阅支持的 Amazon 区域。
- 您可以在中查看用户后台会话 CloudTrail。有关信息，请参阅识别用户后台会话详细信息。
- 您也可以结束组织中用户的活跃会话。相关信息，请参阅结束员工用户的活跃会话。

配置用户后台会话的持续时间

1. 打开 IAM Identity Center 控制台。
2. 选择设置。
3. 在设置页面上，选择身份验证选项卡。
4. 在身份验证下,会话持续时间旁边，选择配置。这时会出现一个配置会话持续时间对话框。
5. 在配置会话持续时间对话框中，如果启用用户后台会话复选框未勾选，请勾选该选项。取消勾选可禁用用户后台会话。

> **Note**
>
> 禁用用户后台会话不会影响当前活跃会话。

6. 在用户后台会话下，点击下拉箭头选择最大会话持续时间。选择会话时长，然后选择保存。

> **Note**
>
> 对会话持续时间的更改仅适用于新会话。当前会话保持原始持续时间。

7. 您将返回到身份验证选项卡。选项卡上方会出现一条绿色的通知消息，指示会话设置已成功更新。

> **Note**
>
> 客户管理型应用程序无法创建用户后台会话。

Kiro 的延长会话

如果您的开发人员将 Kiro 用作集成开发环境 (IDE) 的一部分，则可以将 Kiro 的会话持续时间设置为 90 天。根据您启用 IAM Identity Center 的时间，默认情况下可能会启用 Kiro 的延长会话持续时间。此延长会话不会影响 Amazon Web Services 访问门户或其他 Amazon 托管应用程序的会话持续时间。

有关诸如 IAM Identity Center 身份源如何影响延长的会话持续时间之类的注意事项，请参阅the section called “身份源、 Amazon CLI 和 Amazon SDKs”。

> **Note**
>
> Kiro 可通过设置为商用 Amazon Web Services 区域 且默认处于启用状态的主机进行访问。如果您的 IAM Identity Center 实例位于当前无法访问 Kiro 的区域，则启用 90 天延长会话持续时间不会覆盖默认设置。这意味着，是否启用 90 天延长会话持续时间，会话持续时间都保持不变。有关信息，请参阅 Kiro 支持的 Amazon 区域。

延长 Kiro 的会话

1. 打开 IAM Identity Center 控制台。
2. 选择设置。
3. 在设置页面上，选择身份验证选项卡。
4. 在身份验证下,会话持续时间旁边，选择配置。这时会出现一个配置会话持续时间对话框。
5. 在 “配置会话持续时间” 对话框中，选中 “为 Kiro 启用扩展会话” 复选框。清除该复选框可禁用 Kiro 的扩展会话会话。
6. 选择保存以返回设置页面。

查看和结束员工用户的活跃会话

作为 IAM Identity Center 管理员，您可查看员工用户的活跃会话列表，并在需要时结束用户的一个或多个会话。例如，在以下情况下您可能需要结束用户的会话：

- 用户不再需要这些会话。
- 用户不应该保持其当前的身份验证状态。当他们离开公司或权限发生变更时，可能会发生这种情况。

您可使用 IAM Identity Center 控制台查看和结束这些会话。您的用户还可以使用 Amazon Web Services 访问门户查看和结束自己的会话。有关您的员工用户如何在无需管理员协助的情况下查看和结束其会话的信息，请参阅 查看和结束活跃会话。

> **Note**
>
> 结束 IAM Identity Center 用户的活动会话不会结束 Amazon Web Services 管理控制台 或中任何活跃的 IAM 角色会话 Amazon CLI。有关更多信息，请参阅 了解 IAM Identity Center 中的身份验证会话。

结束员工用户的活跃会话（IAM Identity Center 控制台）

1. 打开 IAM Identity Center 控制台。
2. 选择用户。
3. 在用户页面上，选择要管理其会话的用户的用户名。这会让您转至包含用户信息的页面。
4. 在用户页面上，选择活跃会话选项卡。活跃会话旁边括号中的数字表示该用户处于活跃状态的会话数。
5. 搜索用户后台会话（可选）

   要按使用该会话的作业的 Amazon 资源名称（ARN）搜索会话，请在会话类型列表中选择用户后台会话，然后在搜索框中输入作业 ARN。

   > **Note**
   >
   > 您只能结束已加载的活跃会话。如果用户有许多会话，请选择加载更多活跃会话，以显示其他会话。

6. 选择要结束的每个会话旁边的复选框，然后选择结束会话。
7. 这时会出现一个对话框，确认您正在结束该用户的活跃会话。查看信息，如果要继续，请键入 `confirm`，然后选择结束会话。
8. 您将返回到用户的页面。此时会出现绿色通知消息，表示所选会话已成功结束。

使用身份源、 Amazon CLI 和的会话持续时间注意事项 Amazon SDKs

如果您使用 Microsoft Active Directory (AD) 或外部身份提供者 (IdP) 作为身份源，或者使用 Amazon 软件开发套件 (SDKs) 或其他 Amazon 开发工具以编程方式访问 Amazon 服务，则配置会话持续时间的注意事项如下。 Amazon Command Line Interface

微软 Active Directory、用户交互会话和 Kiro 的扩展会话

如果您使用 Microsoft Active Directory (AD) 作为身份源，并为 Kiro 配置用户交互会话或扩展会话的会话持续时间，请记住以下注意事项。

> **Note**
>
> 这些注意事项不适用于用户后台会话。

无论你使用 Amazon Managed Microsoft AD 还是在中配置的 AD Connector Amazon Directory Service，Microsoft AD 中定义的用户 Kerberos 票证的最大生命周期都会影响 Kiro 的用户交互会话和延长会话的有效期。有关此设置的更多信息，请参阅 Microsoft 网站上的用户票证的最长使用寿命。

- Amazon Managed Microsoft AD：如果您使用中 Amazon Managed Microsoft AD 配置的 Amazon Directory Service，则用户 Kerberos 票证的最长使用寿命固定为 10 小时。因此，用户交互会话持续时间设置为 IAM Identity Center 设置中较短的一个，即 10 小时。例如，如果您将用户交互会话持续时间设置为 12 小时，则您的用户必须在 10 小时后在 Amazon Web Services 访问门户中重新进行身份验证。同样的 10 小时限制也适用于 Kiro 的延长会话。
- AD Con nector：如果您使用中配置的 AD Connector Amazon Directory Service，则用户 Kerberos 票证的最大使用寿命在 AD Connector 后面的 Microsoft AD 中定义。默认值为 10 小时，它对用户交互会话和延长会话的影响与实际效果相同 Amazon Managed Microsoft AD。尽管可以在 Microsoft AD 中配置此限制，但我们建议您与 IT 管理员一起考虑风险，尤其是因为此设置可能会影响其他 Microsoft AD 客户端应用程序的会话时长。

Kiro 的外部身份提供商、用户交互会话和扩展会话

如果您使用外部身份提供商 (IdP)，并为 Kiro 配置用户交互会话或扩展会话的会话持续时间，请记住以下注意事项。

> **Note**
>
> 这些注意事项不适用于用户后台会话。

IAM Identity Center 使用 SAML 断言中的 `SessionNotOnOrAfter` 属性帮助确定会话在多长时间内有效。

- 如果未在 SAML 断言中通过，`SessionNotOnOrAfter`则 Amazon Web Services 访问门户（用户交互）会话和扩展会话的持续时间不受外部 IdP 会话持续时间的影响。例如，如果您的 IdP 会话持续时间为 24 小时，并且您在 IAM Identity Center 中设置了 18 小时的会话时长，则您的用户必须在 18 小时后在 Amazon Web Services 访问门户中重新进行身份验证。同样，如果您为 Kiro 设置了 90 天的延长会话，则您的 Kiro 用户需要在 90 天后重新进行身份验证。
- 如果在 SAML 断言中传递，`SessionNotOnOrAfter`则会话持续时间值将设置为 Amazon Web Services 访问门户（用户交互）会话或延长的会话持续时间以及您的 SAML IdP 会话持续时间中较短的一个。如果您在 IAM Identity Center 中设置了 72 小时的会话时长，并且您的 IdP 的会话持续时间为 18 小时，则您的用户将可以在您的 IdP 中定义的 18 小时内访问 Amazon 资源。同样，如果您为 Kiro 设置了 90 天的延长会话，则您的 Kiro 用户需要在 18 小时后在 Kiro 中重新进行身份验证。
- 如果您 IdP 的会话持续时间长于 IAM Identity Center 中设置的持续时间，由于您 IdP 的登录会话仍然有效，用户无需重新输入凭证即可启动新的 IAM Identity Center 会话。

Amazon CLI 和 SDK 会话

如果您使用 Amazon CLI 或其他 Amazon 开发工具以编程方式访问 Amazon 服务，则必须满足以下先决条件才能设置 Amazon Web Services 访问门户和 Amazon 托管应用程序的会话持续时间。 Amazon SDKs

- 您必须在 IAM Identity Center 控制台中配置 Amazon Web Services 访问门户会话持续时间。
- 您必须在共享配置文件中为单点登录设置定义 Amazon 配置文件。此配置文件用于连接到 Amazon Web Services 访问门户。我们建议您使用 SSO 令牌提供程序配置。使用此配置，您的 Amazon SDK 或工具可以自动检索刷新的身份验证令牌。有关更多信息，请参阅Amazon SDK 和工具参考指南中的 SSO 令牌提供商配置。
- 用户必须运行支持会话管理的版本 Amazon CLI 或 SDK。

支持会话管理的最低版本 Amazon CLI

以下是支持会话管理的最低版本。 Amazon CLI

- Amazon CLI V2 2.9 或更高版本
- Amazon CLI V1 1.27.10 或更高版本

> **Note**
>
> 对于账户访问用例，如果您的用户正在运行 Amazon CLI，如果您在 IAM Identity Center 会话设置为到期之前刷新权限集，并且会话持续时间设置为 20 小时，而权限集持续时间设置为 12 小时，则 Amazon CLI 会话最长运行时间为 20 小时加 12 小时，总计 32 小时。有关 IAM Identity Center CLI 的更多信息，请参阅 Amazon CLI 命令参考。

支持 IAM 身份中心会话管理的最低版本 SDKs

以下是支持 IAM Identity Center 会话管理的最低版本。 SDKs

SDK	最低版本
Python	1.26.10
PHP	3.245.0
Ruby	aws-sdk-core 3.167.0
Java V2	Amazon 适用于 Java 的 SDK v2 (2.18.13)
Go V2	整个 SDK：2022-11-11 版本和特定的 Go 模块：1.18.0 credentials/v1.13.0, config/v
JS V2	2.1253.0
JS V3	v3.210.0
C++	1.9.372
.NET	v3.7.400.0

禁用用户对 IAM 身份中心中的应用程序的访问权限 Amazon Web Services 账户

当您在 IAM Identity Center 目录中禁用用户访问权限时，您无法编辑其用户详细信息、重置其密码、将用户添加到组或查看其组成员身份。禁用用户访问权限会阻止他们登录 Amazon Web Services 访问门户，并且他们将无法再访问分配给他们的应用程序 Amazon Web Services 账户 和应用程序。当您以后可能需要恢复访问权限时，使用禁用用户访问来进行临时访问权限移除。

通过以下过程，通过 IAM Identity Center 控制台禁用 Identity Center 目录中的用户访问权限。

> **Note**
>
> 当您在 IAM Identity Center 中禁用用户访问权限或删除用户时，该用户将立即被禁止登录 Amazon Web Services 访问门户，也无法创建新的登录会话。有关更多信息，请参阅 了解 IAM Identity Center 中的身份验证会话。

在 IAM Identity Center 中禁用用户访问

1. 打开 IAM Identity Center 控制台。

   > **Important**
   >
   > 本页的说明适用于 Amazon IAM Identity Center。它们不适用于 Amazon Identity and Access Management(IAM)。IAM Identity Center 用户、组和用户凭证不同于 IAM 用户、组和 IAM 用户凭证。如果您正在寻找有关在 IAM 中停用用户的说明，请参阅 Amazon Identity and Access Management 用户指南中的管理 IAM 用户。

2. 选择用户。
3. 选择您要禁用其访问权限的用户的用户名。
4. 在要禁用访问权限的用户的用户名下方，从一般信息部分中选择禁用用户访问权限。
5. 在禁用用户访问对话框中，选择禁用用户访问。

使用服务控制策略拒绝用户访问

要在 IAM Identity Center 用户的访问被禁用或用户被删除时立即拒绝其进行授权的 API 调用，您可以：

1. 通过为所有资源的所有操作添加显式的 Deny 效果，来添加或更新分配给用户的权限集的内联策略。
2. 指定 aws:userid 或 identitystore:userid 条件键。

或者，您可以使用服务控制策略来拒绝该用户访问您组织中的所有成员账户。

Example拒绝访问的 SCP 示例

此拒绝策略会阻止特定用户的所有 Amazon 操作，无论他们可能在其他地方获得的其他权限如何。此策略会覆盖任何 Allow 策略。

JSON

```
{
    "Version":"2012-10-17",
    "Statement" : [
        {
            "Effect": "Deny",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                 "StringLike": {
                    "aws:UserId": "*:deleteduser@domain.com"
                }
            }
        }
    ]
}
```

JSON

```
{
    "Version":"2012-10-17",
    "Statement" : [
        {
            "Effect": "Deny",
            "Action": "*",
            "Resource": "*",
            "Condition": {
```

```
                "StringEquals": {
                    "identitystore:UserId": "DELETEDUSER_ID"
                }
            }
        }
    ]
}
```

管理 Identity Center 目录中用户的访问权限

了解如何为 IAM Identity Center 目录中的用户管理密码和多重身份验证（MFA）。这些安全功能有助于保护用户账户。

> **Note**
>
> 这些功能不适用于 Active Directory 用户或外部身份提供者用户。

管理员可以通过 IAM Identity Center 控制台管理密码与 MFA。这些安全功能仅适用于内置 Identity Center 目录。

密码管理

密码管理包括以下功能：

- 通过电子邮件说明重置密码
- 生成一次性密码
- 为通过 API 创建的用户配置自动电子邮件验证

Amazon 强制执行固定的安全要求，包括复杂性规则和密码重用限制。

MFA

MFA 默认启用，每个用户最多支持八台设备。

支持的设备类型包括：

- 身份验证器应用程序
- 安全密钥

- 内置生物识别验证器

管理员可以为用户注册并管理 MFA 设备。

主题

- 设置用户密码
- Identity Center 目录用户的多重身份验证

设置用户密码

对于在 Identity Center 目录中创建的用户，管理员可以管理密码策略、处理没有初始密码的用户以及在需要时重置密码。这些密码管理功能仅适用于内置 Identity Center 目录中的用户。如果您使用 Active Directory 或外部身份提供者，则必须在这些系统中管理密码。

密码管理选项

- 密码要求：用户在设置或更改密码时必须满足的安全要求。这包括复杂性规则与重用限制。
- 一次性密码设置：为通过 API 或 CLI 创建且没有初始密码的用户配置电子邮件验证。您也可以生成临时密码以供立即访问。
- 密码重置 - 为被锁定或需要新凭证的用户重置密码。您可通过电子邮件发送重置说明或生成一次性密码。

主题

- 在 IAM Identity Center 中管理身份时的密码要求
- 向使用 API 或 CLI 创建的用户发送电子邮件一次性密码
- 重置最终用户的 IAM Identity Center 用户密码

在 IAM Identity Center 中管理身份时的密码要求

> **Note**
>
> 这些要求仅适用于在 Identity Center 目录中创建的用户。如果您配置了 IAM Identity Center 以外的身份源进行身份验证，例如 Active Directory 或外部身份提供者，用户的密码策略将在这些系统中而不是在 IAM Identity Center 中定义和实施。如果您的身份来源是 Amazon Managed Microsoft AD，请参阅管理密码策略 Amazon Managed Microsoft AD以了解更多信息。

当您使用 IAM Identity Center 作为身份源时，用户必须遵守以下密码要求才能设置或更改其密码：

- 密码区分大小写。
- 密码长度必须在 8 到 64 个字符之间。
- 密码必须包含下列四种类别中每种类别的至少一个字符：
  - 小写字母 (a-z)
  - 大写字母 (A-Z)
  - 数字 (0-9)
  - 非字母数字字符 (~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/)
- 不能与最近使用的三个密码重复。
- 不能使用通过第三方泄露的数据集公开的密码。

向使用 API 或 CLI 创建的用户发送电子邮件一次性密码

使用 CreateUser API 操作或 `create-user` CLI 命令创建用户时，这些用户默认没有密码。如果您在创建用户时为其指定了电子邮件，则可以更新 IAM Identity Center 中的设置，以便在这些用户首次尝试登录后向他们发送验证电子邮件。收到验证电子邮件后，用户必须设置密码才能登录。

如果您不启用此设置，则必须生成一次性密码并与使用 CreateUser API 或 `create-user` CLI 命令创建的用户共享。

向使用 CreateUser API 或 **`create-user`** CLI 命令创建的用户发送电子邮件地址验证邮件

1. 打开 IAM Identity Center 控制台。
2. 选择设置。
3. 在设置页面上，选择身份验证选项卡。
4. 在标准身份验证部分中，选择配置。
5. 在 配置标准身份验证对话框中，选中发送电子邮件 OTP 复选框。然后，选择保存。状态从禁用更新为启用。

重置最终用户的 IAM Identity Center 用户密码

此过程适用于需要重置 IAM Identity Center 目录中的用户密码的管理员。您将使用 IAM Identity Center 控制台重置密码。

身份提供商和用户类型的注意事项

- Microsoft Active Directory 或外部提供商 - 如果您将 IAM Identity Center 连接到 Microsoft Active Directory 或外部提供者，则必须从 Active Directory 或外部提供商内部完成用户密码重置。这意味着无法从 IAM Identity Center 控制台重置这些用户的密码。
- IAM Identity Center 目录中的用户 - 如果您是 IAM Identity Center 用户，您可以重置您自己的 IAM Identity Center 密码，请参阅 重置您的 Amazon Web Services 访问门户用户密码。

重置 IAM Identity Center 最终用户的密码

> **Important**
>
> 本页的说明适用于 Amazon IAM Identity Center。它们不适用于 Amazon Identity and Access Management(IAM)。IAM Identity Center 用户、组和用户凭证不同于 IAM 用户、组和 IAM 用户凭证。如果您正在寻找有关更改 IAM 用户密码的说明，请参阅 Amazon Identity and Access Management 用户指南中的管理 IAM 用户密码。

1. 打开 IAM Identity Center 控制台。
2. 选择用户。
3. 选择您要重置其密码的用户的用户名。
4. 在用户详细信息页面上，选择重置密码。
5. 在重置密码对话框中，选择以下选项之一，然后选择重置密码：

   a. 向用户发送包含重置密码说明的电子邮件——此选项会自动向用户发送一封来自 Amazon Web Services 的电子邮件，指导他们如何重置密码。

   > **Warning**
   >
   > 作为安全最佳实践，请在选择此选项之前验证该用户的电子邮件地址是否正确。如果将此密码重置电子邮件发送到错误或配置错误的电子邮件地址，则恶意收件人可能会利用它来未经授权访问您的 Amazon 环境。

   b. 生成一次性密码并与用户共享密码——此选项为您提供密码详细信息，您可以将其从您的电子邮件地址手动发送给用户。

Identity Center 目录用户的多重身份验证

> **Important**
>
> 目前，外部身份提供者不支持 IAM Identity Center 中的 MFA。

IAM Identity Center 已预先配置为默认开启多重身份验证（MFA），因此所有用户除了使用用户名和密码外，还必须使用 MFA 登录。这可确保用户必须使用以下两个因素登录 Amazon Web Services 访问门户：

- 其用户名和密码。这是第一个因素，也是用户所熟知的。
- 可以是密码、安全密钥或生物识别。这是第二个因素，也是用户所拥有（占有）或本身存在（生物识别）的因素。第二个因素可能是用户的移动设备生成的身份验证码、连接到其计算机的安全密钥或用户的生物识别扫描。

除非成功完成有效的 MFA 挑战，否则这多种因素可以防止未经授权访问您的 Amazon 资源，从而提高安全性。

每位用户最多可以注册两个虚拟身份验证器应用程序（即安装在您的移动设备或平板电脑上的一次性密码身份验证器应用程序），以及六个 FIDO 身份验证器（包括内置身份验证器和安全密钥），用于总共八台 MFA 设备。了解有关 适用于 IAM Identity Center 的可用 MFA 类型 的更多信息。

主题

适用于 IAM Identity Center 的可用 MFA 类型

多重身份验证（MFA）是一种简单而有效的机制，可以增强用户的安全性。用户的第一个因素（他们的密码）是他们记住的秘密，也称为知识因素。其他因素可以是占有因素（您拥有的事物，例如安全密钥）或固有因素（您的身份，例如生物识别扫描）。强烈建议您配置 MFA，以便为您的帐户额外添加一层保护。

IAM Identity Center MFA 支持以下设备类型。所有的 MFA 类型均支持基于浏览器的控制台访问以及使用 Amazon CLI v2 和 IAM 身份中心。

- FIDO2 身份验证器，包括内置的身份验证器和安全密钥
- 虚拟身份验证器应用程序
- 你自己的RADIUS MFA实现通过以下方式连接 Amazon Managed Microsoft AD

一个用户最多可以将八台 MFA 设备注册到一个 Amazon Web Services 账户，其中包括最多两个虚拟身份验证器应用程序和六个 FIDO 身份验证器。您还可以配置 MFA 设置，以要求用户在尝试从新设备或浏览器登录时，或者从未知 IP 地址登录时进行 MFA。有关如何为您的用户配置 MFA 设置的更多信息，请参阅 选择用户身份验证适用的 MFA 类型 和 配置 MFA 设备实施。

FIDO2 身份验证器

FIDO2是一个包括 CTAP2 WebAuthn和基于公钥加密的标准。FIDO 凭证具有防网络钓鱼功能，因为它们是创建凭证的网站所独有的，例如 Amazon。

Amazon 支持 FIDO 身份验证器的两种最常见外形规格：内置身份验证器和安全密钥。有关最常见的 FIDO 身份验证器类型的更多信息，请参阅下文。

主题

- 内置身份验证器
- 安全密钥
- 密码管理器、密钥提供商和其他 FIDO 身份验证器

内置身份验证器

多个现代化计算机和移动电话配有内置身份验证器，例如 Macbook 上的 TouchID 或与 Windows Hello 兼容的摄像机。如果您的设备具有兼容 FIDO 的内置身份验证器，则可以使用指纹、面部或设备 PIN 码作为第二个因素。

安全密钥

安全密钥是兼容 FIDO 的外部硬件身份验证器，您可以通过 USB、BLE 或 NFC 购买并连接到您的设备。您收到 MFA 的提示时，只需使用密钥的传感器完成手势即可。安全密钥的一些示例包括 YubiKeys 和 Feitian 密钥，最常见的安全密钥会创建绑定设备的 FIDO 凭证。有关所有经过 FIDO 认证的安全密钥的列表，请参阅经过 FIDO 认证的产品。

密码管理器、密钥提供商和其他 FIDO 身份验证器

多个第三方提供商支持移动应用程序中的 FIDO 身份验证，例如密码管理器中的功能、带有 FIDO 模式的智能卡以及其他外形规格。这些兼容 FIDO 的设备可以与 IAM Identity Center 配合使用，但我们建议您在为 MFA 启用此选项之前亲自测试 FIDO 身份验证器。

> **Note**
>
> 有些 FIDO 身份验证器可以创建可发现的 FIDO 凭证，称为密钥。密钥可以绑定到创建密钥的设备，也可以同步并备份到云端。例如，您可以在支持的 Macbook 上使用 Apple Touch ID 注册密钥，然后按照登录时屏幕上的提示使用 Google Chrome，在 iCloud 中使用密钥从 Windows 笔记本电脑登录网站。有关哪些设备支持可同步密钥以及操作系统和浏览器之间当前密钥互操作性的更多信息，请参阅 passkeys.dev 上的设备支持资源，该资源由 FIDO 联盟和万维网联盟 (W3C) 负责维护。

虚拟身份验证器应用程序

身份验证器应用程序本质上是基于一次性密码（OTP）的第三方身份验证器。您可将安装在移动装置或平板电脑上的身份验证器应用程序用作授权的 MFA 设备。第三方身份验证器应用程序必须符合 RFC 6238，这是一种标准的基于时间的一次性密码（TOTP）算法，且能够生成六位数身份验证码。

提示进行多重身份验证时，用户必须在显示的输入框中输入来自其身份验证器应用程序的有效代码。分配给用户的每台 MFA 设备必须是唯一的。可为任意给定用户注册两个身份验证器应用程序。

经过测试的身份验证器应用程序

任何符合 TOTP 标准的应用程序都可使用 IAM Identity Center MFA。下表列出常见的第三方身份验证器应用程序以供选择。

操作系统	经过测试的身份验证器应用程序
Android	Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator
iOS	Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator

RADIUS MFA

远程身份验证拨入用户服务 (RADIUS) 是一种行业标准的客户端-服务器协议，它提供身份验证、授权和记账管理，因此用户可以连接到网络服务。 Amazon Directory Service 包括一个 RADIUS 客户端，该客户端可连接到您实施了 MFA 解决方案的 RADIUS 服务器。有关更多信息，请参阅为 Amazon Managed Microsoft AD启用多重身份验证。

您可以在 IAM Identity Center 中使用 RADIUS MFA 或 MFA 来登录用户门户，但不能同时使用两者。如果您想要使用 Amazon 原生双因素身份验证来访问门户，IAM 身份中心中的 MFA 是 RADIUS MFA 的替代方案。

您在 IAM Identity Center 中启用 MFA 时，您的用户需要一台 MFA 设备才能登录 Amazon Web Services 访问门户。如果您之前使用过 RADIUS MFA，则在 IAM 身份中心启用 MFA 实际上会覆盖登录访问门户的用户的 RADIUS MFA。 Amazon Web Services 但是，当用户登录所有其他可与之配合使用的应用程序（例如适用于 SQL Server 的 Amazon RDS for SQL Server）时 Amazon Directory Service，RADIUS MFA 会继续向他们提出质疑。

如果您的 MFA 在 IAM 身份中心控制台上被禁用，并且您已将 RADIUS MFA 配置为，则 Amazon Directory Service RADIUS MFA 将控制访问门户的登录。 Amazon Web Services 这意味着，如果禁用 MFA，IAM Identity Center 将回退到 RADIUS MFA 配置。

在 IAM Identity Center 中配置 MFA

当您的身份源配置了 IAM 身份中心的身份存储 Amazon Managed Microsoft AD或 AD Connector 时，您可以在 IAM 身份中心配置多重身份验证 (MFA) 功能。目前，外部身份提供者不支持 IAM Identity Center 中的 MFA。

以下是一般的 MFA 建议，具体取决于您的 IAM Identity Center 设置和组织偏好。

- 鼓励用户为所有启用的 MFA 类型注册多个备份身份验证器。这种做法可以防止在 MFA 设备损坏或放错位置时失去访问权限。
- 如果您的用户必须登录 Amazon Web Services 访问门户才能访问他们的电子邮件，请不要选择 “要求他们提供通过电子邮件发送的一次性密码” 选项。例如，您的用户可以在 Amazon Web Services 访问门户Microsoft 365中使用来阅读他们的电子邮件。在这种情况下，用户将无法检索验证码，也无法登录 Amazon Web Services 访问门户。有关更多信息，请参阅 配置 MFA 设备实施。
- 如果您已经在使用配置的 RADIUS MFA Amazon Directory Service，则无需在 IAM 身份中心内启用 MFA。对于 IAM Identity Center 的 Microsoft Active Directory 用户，IAM Identity Center 中的 MFA 可以作为 RADIUS MFA 的替代方案。有关更多信息，请参阅 RADIUS MFA。
- 以下 YouTube 视频概述了 MFA 和 IAM 身份中心：

IAM 身份中心：新实例的多重身份验证默认设置

主题

提示用户完成 MFA

您可以使用以下步骤来确定员工用户在尝试登录访问门户时被提示进行多重身份验证 (MFA) 的频率。Amazon Web Services 在开始之前，我们建议您首先了解 适用于 IAM Identity Center 的可用 MFA 类型。

> **Important**
>
> 本部分中的说明适用于 Amazon IAM Identity Center。它们不适用于 Amazon Identity and Access Management (IAM)。IAM Identity Center 用户、组和用户凭证不同于 IAM 用户、组和 IAM 用户凭证。如果您正在寻找有关为 IAM 用户停用 MFA 的说明，请参阅 Amazon Identity and Access Management 用户指南中的停用 MFA 设备。

> **Note**
>
> 如果您使用的是外部 IdP，则多重身份验证部分将不可用。您的外部 IdP 管理 MFA 设置，而不是 IAM 身份中心管理这些设置。

配置 MFA

1. 打开 IAM Identity Center 控制台。
2. 在左侧导航窗格中，选择设置。
3. 在设置页面上，选择身份验证选项卡。
4. 在多重身份验证部分，选择配置。
5. 在配置多重身份验证页面的提示用户完成 MFA 项下，根据您的业务所需的安全级别选择以下身份验证模式之一：

- 他们每次登录时（始终开启）

  在此模式（默认设置）下，IAM Identity Center 要求拥有已注册 MFA 设备的用户每次登录时都会收到提示。这是最安全的设置，它要求他们每次登录 Amazon Web Services 访问门户时都使用 MFA，从而确保您的组织或合规政策得到执行。例如，PCI DSS 强烈建议在每次登录时完成 MFA，以访问支持高风险支付交易的应用程序。

- 仅当他们的登录上下文发生变化时（上下文感知）

  在此模式下，IAM Identity Center 为用户提供了在登录期间信任其设备的选项。在用户表示要信任某设备后，IAM Identity Center 会提示用户进行一次 MFA，然后分析登录上下文（例如设备、浏览器和位置），以便用户后续登录。对于后续登录，IAM Identity Center 会确定用户是否使用先前信任的上下文登录。如果用户的登录上下文发生变化，除了电子邮件地址和密码凭证外，IAM Identity Center 还会提示用户完成 MFA。

  此模式为经常从工作场所登录的用户提供了易用性，但安全性低于始终开启选项。只有当用户的登录上下文发生变化时，才会提示他们完成 MFA。

- 从不（已禁用）

  在此模式下，所有用户仅使用其标准用户名和密码登录。选择此选项将禁用 IAM Identity Center MFA，不建议这样做。

  虽然您的身份中心目录为用户禁用 MFA，但您无法在其用户详细信息中管理 MFA 设备，并且身份中心目录用户无法从访问门户管理 MFA 设备。 Amazon Web Services

  > **Note**
  >
  > 如果您已经在使用 RADIUS MFA Amazon Directory Service，并希望继续将其用作默认 MFA 类型，则可以将身份验证模式保留为禁用状态，以绕过 IAM Identity Center 中的 MFA 功能。从禁用模式更改为上下文感知或始终开启模式将覆盖现有的 RADIUS MFA 设置。有关更多信息，请参阅 RADIUS MFA。

6. 选择保存更改。

相关主题

- 选择用户身份验证适用的 MFA 类型
- 配置 MFA 设备实施
- 允许用户注册自己的 MFA 设备

选择用户身份验证适用的 MFA 类型

在访问门户中提示用户进行多重身份验证 (MFA) 时，使用以下步骤选择用户可以进行身份验证 Amazon Web Services 的设备类型。

如需为您的用户配置 MFA 类型

1. 打开 IAM Identity Center 控制台。
2. 在左侧导航窗格中，选择设置。
3. 在设置页面上，选择身份验证选项卡。
4. 在多重身份验证部分，选择配置。
5. 在配置多重身份验证页面的用户可以使用这些 MFA 类型进行身份验证项下，根据您的业务需求选择以下 MFA 类型之一。有关更多信息，请参阅 适用于 IAM Identity Center 的可用 MFA 类型。
   - 安全密钥和内置验证器
   - 身份验证器应用程序
6. 选择保存更改。

配置 MFA 设备实施

使用以下步骤来确定您的用户在登录 Amazon Web Services 访问门户时是否必须拥有已注册的 MFA 设备。

有关 IAM 中 MFA 的更多信息，请参阅 IAM 中的Amazon 多重身份验证。

如需为您的用户配置 MFA 设备实施

1. 打开 IAM Identity Center 控制台。
2. 在左侧导航窗格中，选择设置。
3. 在设置页面上，选择身份验证选项卡。
4. 在多重身份验证部分，选择配置。
5. 在配置多重身份验证页面的如果用户还没有已注册的 MFA 设备项下，根据您的业务需求选择以下选项之一：
   - 要求他们在登录时注册 MFA 设备

     这是您首次为 IAM Identity Center 配置 MFA 时的默认设置。如果您希望要求尚未注册 MFA 设备的用户在成功进行密码身份验证后在登录期间自行注册设备，请使用此选项。这使您可以使

用 MFA 保护组织 Amazon 环境，而不必单独注册身份验证设备并将其分发给用户。在自行注册期间，您的用户可以注册您之前启用的可用 适用于 IAM Identity Center 的可用 MFA 类型 中的任何设备。完成注册后，用户可以选择为其新注册的 MFA 设备起一个友好名称，之后 IAM Identity Center 会将用户重定向到其原始目标。如果用户的设备丢失或被盗，您只需将该设备从其帐户中移除即可，IAM Identity Center 将要求他们在下次登录时自行注册新设备。

- 要求他们提供电子邮件发送的一次性密码才能登录

  如果您想通过电子邮件向用户发送验证码，请使用此选项。由于电子邮件未与特定设备绑定，因此此选项不符合行业标准的多重身份验证的标准。但是，与单独使用密码相比，它确实可以提高安全性。只有当用户尚未注册 MFA 设备时，才会请求电子邮件验证。如果启用了上下文感知身份验证方法，则用户将有机会将接收电子邮件的设备标记为信任设备。之后，用户在使用该设备、浏览器和 IP 地址组合登录时，无需再验证电子邮件代码。

  > **Note**
  >
  > 如果您使用 Active Directory 作为 IAM Identity Center 启用的身份源，则电子邮件地址将始终基于 Active Directory `email` 属性。自定义 Active Directory 属性映射不会覆盖此行为。

- 阻止他们登录

  如果您想强制每位用户在登录 Amazon之前使用 MFA，请使用阻止他们登录选项。

  > **Important**
  >
  > 如果您的身份验证方法设置为上下文感知，则用户可以在登录页面上选中这是信任设备复选框。在这种情况下，即使您启用了阻止他们登录设置，也不会提示该用户完成 MFA。如果您想让这些用户收到提示，请将您的身份验证方法更改为始终开启。

- 允许他们登录

  使用此选项表示您的用户无需使用 MFA 设备即可登录 Amazon Web Services 访问门户。选择注册 MFA 设备的用户仍会收到完成 MFA 的提示。

6. 选择保存更改。

允许用户注册自己的 MFA 设备

IAM Identity Center 管理员可以允许用户自行注册 MFA 设备。

如需允许用户注册自己的 MFA 设备

1. 打开 IAM Identity Center 控制台。
2. 在左侧导航窗格中，选择设置。
3. 在设置页面上，选择身份验证选项卡。
4. 在多重身份验证部分，选择配置。
5. 在配置多重身份验证页面的谁可以管理 MFA 设备项下，选择用户可以添加并管理自己的 MFA 设备选项。
6. 选择保存更改。

> **Note**
>
> 为用户设置自助注册后，您可能需要向他们发送转至步骤 注册设备进行 MFA 的链接。本主题提供有关用户如何设置自己的 MFA 设备的说明。

注册用户的 MFA 设备

IAM Identity Center 管理员可以设置新的 MFA 设备，供特定用户在 IAM Identity Center 控制台中访问。管理员必须拥有对用户 MFA 设备的物理访问权限，才能注册设备。例如，如果您为使用在智能手机上运行的 MFA 设备的用户配置 MFA，则您需要对该智能手机的物理访问权限才能完成注册流程。或者，您可以允许用户配置和管理他们自己的 MFA 设备。有关更多信息，请参阅 允许用户注册自己的 MFA 设备。

如需注册 MFA 设备

1. 打开 IAM Identity Center 控制台。
2. 在左侧导航窗格中，选择 用户。在列表中，选择一个用户。在此步骤中，请勿选中用户旁边的复选框。
3. 在用户详细信息页面上，选择 MFA 设备选项卡，然后选择注册 MFA 设备。
4. 在注册 MFA 设备页面上，选择以下 MFA 设备类型之一，然后按照说明进行操作：

   - 身份验证器应用程序
     1. 在设置身份验证器应用程序页面上，IAM Identity Center 将显示新 MFA 设备的配置信息，包括二维码图形。该图表示可在不支持 QR 码的设备上手动输入的密钥。
     2. 使用物理 MFA 设备，执行以下操作：

a. 打开兼容的 MFA 身份验证器应用程序。有关可以在 MFA 设备上使用的经过测试的应用程序的列表，请参阅 虚拟身份验证器应用程序。如果 MFA 应用支持多个帐户（多个 MFA 设备），请选择创建新帐户（新的 MFA 设备）的选项。

b. 确定 MFA 应用程序是否支持 QR 码，然后在设置身份验证器应用程序页面上执行以下操作之一：

i. 选择显示 QR 代码，然后使用该应用程序扫描 QR 代码。例如，您可选择摄像头图标或选择类似于 Scan code（扫描代码）的选项，然后使用装置的摄像头扫描此代码。

ii. 选择显示密钥，然后将该密钥键入到 MFA 应用程序中。

> **Important**
>
> 当您为 IAM Identity Center 配置 MFA 设备时，我们建议您将 QR 码或密钥的副本保存在安全的位置。如果指定用户丢失了手机或者必须重新安装 MFA 身份验证器应用程序，这可能会有所帮助。如果出现上述任一情况，您可以快速重新配置应用程序，使其使用相同的 MFA 配置。这样便无需在 IAM Identity Center 中为用户创建新的 MFA 设备。

3. 在设置身份验证器应用程序页面的身份验证器代码项下，输入物理 MFA 设备上当前显示的一次性密码。

> **Important**
>
> 生成代码之后立即提交您的请求。如果在生成代码后等待很长时间才提交请求，MFA 设备将成功与用户关联，但 MFA 设备不同步。这是因为基于时间的一次性密码（TOTP）很快会过期。这种情况下，您可以重新同步设备。

4. 选择分配 MFA。MFA 设备现在可以开始生成一次性密码，现在可以与之配合使用了。Amazon

- 安全密钥

1. 在注册用户的安全密钥页面上，按照浏览器或平台提供的说明进行操作。

> **Note**
>
> 此处的体验因不同的操作系统和浏览器而异，因此请按照浏览器或平台显示的说明进行操作。成功注册用户设备后，您可以选择将友好显示名称与用户新注册的设备相关

联。如果要更改此设置，请选择重命名，输入新名称，然后选择保存。如果您启用了允许用户管理自己的设备的选项，则用户将在 Amazon Web Services 访问门户中看到此友好名称。

重命名或删除 IAM Identity Center 中的 MFA 设备

IAM Identity Center 管理员可以按照下列步骤重命名或删除用户的 MFA 设备。

重命名 MFA 设备

1. 打开 IAM Identity Center 控制台。
2. 在左侧导航窗格中，选择 用户。在列表中选择用户。在此步骤中，请勿选中用户旁边的复选框。
3. 在用户详细信息页面上，选择 MFA 设备选项卡，选择设备，然后选择重命名。
4. 收到提示后，输入新名称，然后选择重命名。

删除 MFA 设备

1. 打开 IAM Identity Center 控制台。
2. 在左侧导航窗格中，选择 用户。在列表中选择用户。
3. 在用户详细信息页面上，选择 MFA 设备选项卡，选择设备，然后选择删除。
4. 要确认，请键入 DELETE，然后选择删除。

配置对应用程序的访问

使用 Amazon IAM Identity Center，您可以控制谁可以单点登录访问您的应用程序。用户使用其目录凭证登录后，就可以无缝访问这些应用程序。

IAM Identity Center 通过 IAM Identity Center 与应用程序的服务提供商之间的可信关系与这些应用程序安全地通信。根据应用程序的类型，这种信任可以通过不同的方式建立。

IAM Identity Center 支持两种应用程序类型：Amazon 托管应用程序和客户托管应用程序。 Amazon 托管应用程序可以直接从相关的应用程序控制台中进行配置，也可以通过应用程序 API 进行配置。客户托管的应用程序必须添加到 IAM Identity Center 控制台，并为 IAM Identity Center 和服务提供商配置合适的元数据。

将应用程序配置为与 IAM Identity Center 协同使用后，您可以管理哪些用户或组可以访问这些应用程序。默认不会向应用程序分配任何用户。

您还可以授予员工访问组织 Amazon Web Services 账户 中特定 Amazon Web Services 管理控制台 人员的访问权限。有关更多信息，请参阅 配置对的访问权限 Amazon Web Services 账户。

主题

Amazon 托管应用程序

Amazon IAM Identity Center 简化并简化了将员工用户连接到 Kiro 和 Amazon Quick 等 Amazon 托管应用程序的任务。借助 IAM Identity Center，您可以连接现有身份提供者一次并同步目录中的用户和

组，或者直接在 IAM Identity Center 中创建和管理用户。通过提供一个联合身份验证点，IAM Identity Center 将免除为每个应用程序设置联合身份验证或用户和组同步的需要，以此减少您的管理工作。您还可以大致查看用户和组分配。

有关与 IAM 身份中心配合使用的 Amazon 应用程序表，请参阅Amazon 可与 IAM 身份中心配合使用的托管应用程序。

控制访问权限 Amazon 托管应用程序

通过两种方式控制对 Amazon 托管应用程序的访问：

- 应用程序的初始入口

  IAM Identity Center 通过对应用程序的分配对此进行管理。默认情况下， Amazon 托管应用程序需要分配。如果您是应用程序管理员，可以选择是否需要针对应用程序进行分配。

  如果需要分配，当用户登录 Amazon Web Services 访问门户时，只有直接或通过组分配分配至应用程序的用户才能查看应用程序磁贴。

  如果不需要分配，您可以允许所有 IAM Identity Center 用户进入应用程序。在这种情况下，应用程序将管理对资源的访问权限，访问 Amazon Web Services 访问门户的所有用户都可以看到该应用程序磁贴。

  > **Important**
  >
  > 如果您是 IAM 身份中心管理员，则可以使用 IAM 身份中心控制台删除对 Amazon 托管应用程序的分配。在删除分配之前，我们建议您与应用程序管理员进行协调。如果您计划修改决定是否需要进行分配的设置，或者计划自动完成应用程序分配，也应该与应用程序管理员进行协调。

- 对应用程序资源的访问权限

  应用程序通过其控制的独立资源分配对此进行管理。

Amazon 托管应用程序提供了一个管理用户界面，您可以使用该界面来管理对应用程序资源的访问权限。例如，Quick 管理员可以根据用户的群组成员资格为其分配访问仪表板的权限。大多数 Amazon 托管应用程序还提供允许您将用户分配给应用程序的 Amazon Web Services 管理控制台 体验。这些应用程序的控制台体验也许可以整合这两种功能，将用户分配功能与管理应用程序资源访问权限的能力结合起来。

共享身份信息

在中共享身份信息的注意事项 Amazon Web Services 账户

IAM Identity Center 支持各种应用程序中最常用的属性。这些属性包括名字和姓氏、电话号码、电子邮件地址、住址和首选语言。请仔细考虑哪些应用程序和哪些账户可以使用这些个人身份信息。

您可以通过以下任一方式控制对此信息的访问：

- 您可以选择仅在 Amazon Organizations 管理账户中启用访问权限，也可以选择在中的所有账户中启用访问权限 Amazon Organizations。
- 您也可以使用服务控制策略（SCP）控制哪些应用程序可以访问 Amazon Organizations中哪些账户里的信息。

例如，如果您仅在 Amazon Organizations 管理账户中启用访问权限，则成员账户中的应用程序将无法访问信息。但是，如果您在所有帐户中启用访问权限，则可以使用 SCP 禁止除您想要授予权限的应用程序之外的其他应用程序进行访问。

服务控制策略是的一项功能 Amazon Organizations。有关附加 SCP 的说明，请参阅 Amazon Organizations 用户指南中的附加和分离服务控制策略。

配置 IAM Identity Center 以共享身份信息

IAM Identity Center 提供了身份存储，其中包含用户和组属性，但不包括登录凭证。您可以使用以下任一方法来更新您的 IAM Identity Center 身份存储中的用户和组：

- 使用 IAM Identity Center 身份存储作为您的主身份源。如果您选择此方法，则可以从 IAM Identity Center 控制台或 Amazon Command Line Interface (Amazon CLI) 中管理您的用户、他们的登录凭证和群组。有关更多信息，请参阅 管理 Identity Center 目录中的用户。
- 将来自以下任一身份源的用户和组预调配（同步）到您的 IAM Identity Center 身份存储：
  - Active Directory - 有关更多信息，请参阅 Microsoft AD 目录。
  - 外部身份提供商 - 有关更多信息，请参阅 外部身份提供者。

  如果您选择这种预调配方法，则可以继续从您的身份源中管理您的用户和组，这些更改将同步到 IAM Identity Center 身份存储。

无论您选择哪种身份来源，IAM Identity Center 都可以与 Amazon 托管应用程序共享用户和群组信息。这样，您就可以将身份源连接到 IAM Identity Center 一次，然后与 Amazon Web Services 云中的

多个应用程序共享身份信息。这样就无需为每个应用程序单独设置联合身份验证和身份预调配。此共享功能还可以让用户轻松访问不同 Amazon Web Services 账户中的许多应用程序。

限制使用 Amazon 托管应用程序

首次启用 IAM Identity Center 时，它将作为身份源供您 Amazon Organizations中所有账户的 Amazon 托管应用程序使用。要限制应用程序的使用，必须实施服务控制策略（SCP）。SCP 是一项功能 Amazon Organizations ，您可以使用它来集中控制组织中的身份（用户和角色）可以拥有的最大权限。您可以使用 SCP 阻止对 IAM Identity Center 用户和组信息的访问，并阻止除指定账户以外的账户启动应用程序。有关更多信息，请参阅《Amazon Organizations 用户指南》中的服务控制策略（SCP）。

以下 SCP 示例将阻止对 IAM Identity Center 用户和组信息进行访问，并阻止除指定账户（111111111111 和 222222222222）以外的账户启动应用程序。

```
{
  "Sid": "DenyIdCExceptInDesignatedAWSAccounts",
  "Effect": "Deny",
  "Action": [
    "identitystore:*",
    "sso:*",
    "sso-directory:*",
    "sso-oauth:*"
  ],
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "aws:PrincipalAccount": [
        "111111111111",
        "222222222222"
      ]
    }
  }
}
```

Amazon 可与 IAM 身份中心配合使用的托管应用程序

IAM Identity Center 允许您连接现有身份源或一次性创建用户。这样，应用程序管理员就可以管理对以下 Amazon 托管应用程序的访问权限，而无需单独的联合体或用户和组同步。

下表中的所有 Amazon 托管应用程序都与 IAM Identity Center 的组织实例集成。该表还提供了有关支持的 Amazon 托管应用程序的以下内容的信息：

- 应用程序是否也与 IAM Identity Center 的账户实例集成
- 应用程序是否可以通过 IAM Identity Center 启用可信身份传播？
- 应用程序是否支持配置了客户自主管理型 KMS 密钥的 IAM Identity Center
- 应用程序是否支持在 IAM 身份中心的其他区域部署

> **Note**
>
> 支持在 IAM 身份中心其他区域部署的应用程序还支持使用客户托管 KMS 密钥配置的 IAM 身份中心。此处列出的每个 Amazon 托管应用程序都支持在主区域部署。有关更多信息，请参阅 the section called “跨多个 Amazon 托管应用程序部署和管理托管应用程序 Amazon Web Services 区域”。

Amazon 与 IAM 身份中心集成的托管应用程序

Amazon 托管应用程序	与 IAM Identity Center 的账户实例集成	通过 IAM Identity Center 启用可信身份传播	支持配置了客户自主管理型 KMS 密钥的 IAM Identity Center	支持在 IAM 身份中心的其他区域进行部署
Amazon Athena SQL	是	是	是	是
Amazon CodeCatalyst	是	没有	是	没有
Amazon DataZone	是	是	是	没有
Amazon EKS 功能	是	是	是	没有
EC2 上的 Amazon EMR	是	是	是	是
Amazon EMR on EKS	是	是	是	是
Amazon EMR Serverless	是	是	是	是

Amazon 托管应用程序	与 IAM Identity Center 的账户实例集成	通过 IAM Identity Center 启用可信身份传播	支持配置了客户自主管理型 KMS 密钥的 IAM Identity Center	支持在 IAM 身份中心的其他区域进行部署
Amazon EMR Studio	是	是	是	是
Amazon Kendra	没有	没有	是	没有
Amazon Managed Grafana	没有	没有	是	没有
Amazon Monitron	没有	没有	没有	没有
亚马逊 OpenSearch 服务	是	是	是	没有
亚马逊 OpenSearch 服务 Serverless Service	是	是	是	没有
Amazon Q Business	是	是	是	没有
Amazon Quick	是	是	是	没有
Amazon Redshift	是[2]	是	是	是
Amazon S3 Access Grants	是	是	是	是
亚马逊 SageMaker Studio	没有	是	是	没有
亚马逊 SageMaker 联合工作室	是	是	是	是
Amazon WorkMail	是	是	是	没有
Amazon WorkSpaces	是	没有	是	没有
Amazon WorkSpaces Secure Browser	没有	没有	是	没有
Amazon App Studio	是	没有	没有	没有
Amazon Deadline Cloud	是	没有	是	是

Amazon 托管应用程序	与 IAM Identity Center 的账户实例集成	通过 IAM Identity Center 启用可信身份传播	支持配置了客户自主管理型 KMS 密钥的 IAM Identity Center	支持在 IAM 身份中心的其他区域进行部署
Amazon DevOps 代理	是	是	是	没有
Amazon Glue	是	是	是	是
Amazon IoT Events	没有	没有	没有	没有
Amazon IoT SiteWise	没有	没有	没有	没有
Amazon Lake Formation	是	是	是	是
Amazon re:Post 私人版	是	没有	是	没有
Amazon Supply Chain	是	没有	是	没有
Amazon 安全代理	是	是	是	没有
Amazon Systems Manager	没有	没有	是	是-舰队管理器远程桌面
Amazon Transfer Family 网络应用程序	是	是	是	是
Amazon 转换	是	没有	是	没有
Amazon Verified Access	没有	没有	是	没有
Kiro	是[1]	是	是	没有
Multi-party 批准	没有	是	是	没有
OpenSearch user interface (Dashboards)	是	是	是	没有

[1] 对于 Kiro，除非您的用户需要访问网站上的 Amazon 全套 Kiro 功能，否则支持 IAM 身份中心的账户实例。有关更多信息，请参阅 Kiro 用户指南中的设置 Kiro。

[2] 对于 Amazon Redshift，支持 IAM 身份中心的账户实例，但查询编辑器 v2 等需要权限集的应用程序除外，账户实例不支持权限集。

> **Note**
>
> 有些 Amazon 服务（例如 Connect Custom Amazon Client VPN er）未在此表中列出，但您可以将其与 IAM Identity Center 配合使用。这是因为它们仅使用 SAML 与 IAM Identity Center 集成，因此被归类为客户托管的应用程序。

快速入门：设置 IAM 身份中心进行测试 Amazon 托管应用程序

如果您的管理员尚未向您提供访问 IAM Identity Center 的权限，则可以使用本主题中的步骤设置 IAM Identity Center 来测试 Amazon 托管应用程序。您将学习如何启用 IAM Identity Center、直接在 IAM Identity Center 中创建用户，以及如何将该用户分配给 Amazon 托管应用程序。

本主题提供了通过以下任意一种方式启用 IAM Identity Center 的快速入门步骤：

- 使用 Amazon Organizations — 如果您选择此选项，则会创建 IAM Identity Center 的组织实例。
- 仅在您的具体情况下 Amazon Web Services 账户— 如果您选择此选项，则会创建 IAM Identity Center 的账户实例。

有关这些实例类型的更多信息，请参阅 IAM Identity Center 的组织和账户实例。

先决条件

启用 IAM Identity Center 之前，请确认以下事项：

- 你有一个 Amazon Web Services 账户 — 如果你没有 Amazon Web Services 账户，请参阅《Amazon 账户管理参考指南》 Amazon Web Services 账户中的 “入门”。
- Amazon 托管应用程序可与 IAM Iden tity Center 配合使用 — 查看列表Amazon 可与 IAM 身份中心配合使用的托管应用程序以确认您要测试的 Amazon 托管应用程序可与 IAM 身份中心配合使用。
- 您已查看区域注意事项 — 确保启用 IAM Identity Center 的 Amazon Web Services 区域 位置支持您要测试的 Amazon 托管应用程序。有关更多信息，请参阅 Amazon 托管应用程序的文档。

> **Note**
>
> 您必须在计划启用 IAM Identity Center 的同一区域部署 Amazon 托管应用程序。

设置 IAM 身份中心的组织实例进行测试 Amazon 托管应用程序

> **Note**
>
> 本主题介绍如何使用启用 IAM 身份中心 Amazon Organizations，这是启用 IAM 身份中心的推荐方法。

确认您的权限

要启用 IAM Identity Center Amazon Organizations，您必须通过以下任一方式登录 Amazon 管理控制台：

- 在将通过 Amazon Organizations启用 IAM Identity Center 的 Amazon Web Services 账户 中具有管理权限的用户。
- 根用户（除非不存在其他管理用户，否则不推荐使用）。

> **Important**
>
> root 用户有权访问账户中的所有 Amazon 服务和资源。作为安全最佳实践，除非您没有其他证书，否则请勿使用账户的根证书访问 Amazon 资源。这些凭证可提供不受限的账户访问且难以撤销。

步骤 1：使用启用 IAM 身份中心 Amazon Organizations

1. 请执行以下一项操作，登录 Amazon Web Services 管理控制台。

   - Amazon （root 用户）新手 — 选择 R oot 用户并输入您的 Amazon Web Services 账户 电子邮件地址，以账户所有者身份登录。在下一页上，输入您的密码。
   - 已使用 Amazon 独立版 Amazon Web Services 账户 （IAM 证书）— 使用具有管理权限的 IAM 凭证登录。

2. 在 Amazon 管理控制台主页上，选择 IAM 身份中心服务或导航到 IAM 身份中心控制台。
3. 选择启用，然后使用启用 IAM 身份中心 Amazon Organizations。执行此操作时，您正在创建 IAM Identity Center 的组织实例。

步骤 2：创建 IAM Identity Center 中的管理用户

此过程介绍如何直接在内置的 Identity Center 目录中创建用户。此目录未连接到管理员可能用于管理工作用户的任何其他目录。在 IAM Identity Center 中创建用户后，您需要为此用户指定新凭证。当您以该用户身份登录以测试您的 Amazon 托管应用程序时，您将使用新的凭据登录，而不是使用任何用于访问公司资源的现有凭据登录。

> **Note**
>
> 建议您仅出于测试目的使用此方法创建用户。

1. 在 IAM Identity Center 控制台的导航窗格中，选择用户，然后选择添加用户。
2. 请按照控制台中的指导添加用户。保持选中向该用户发送包含密码设置说明的电子邮件，并确保指定您有权访问的电子邮件地址。
3. 在导航窗格中，选择 Amazon Web Services 账户，选中账户旁边的复选框，然后选择分配用户或群组。
4. 选择用户选项卡，选中您刚添加的用户旁边的复选框，然后选择下一步。
5. 选择创建权限集，然后按照控制台中的指导创建预定义的 `AdministratorAccess` 权限集。
6. 完成后，新的权限集会显示在列表中。关闭浏览器窗口中的权限集选项卡，返回分配用户和组选项卡，然后选择创建权限集旁边的刷新图标。
7. 在分配用户和组浏览器选项卡中，新的权限集会显示在列表中。选中权限集名称旁边的复选框，选择下一步，然后选择提交。
8. 注销 Console。

步骤 3：登录 Amazon Web Services 以管理用户身份访问门户

Amazon Web Services 访问门户是一个 Web 门户，可让您创建的用户访问 Amazon 管理控制台。在登录 Amazon Web Services 访问门户之前，您必须接受加入 IAM Identity Center 的邀请并激活用户凭证。

1. 检查您的电子邮件，查找主题为邀请加入 Amazon IAM Identity Center 的邮件。

2. 选择接受邀请，然后按照注册页面上的指导设置新密码、登录并为您的用户注册 MFA 设备。
3. 注册 MFA 设备后， Amazon Web Services 访问门户打开。
4. 在 Amazon Web Services 访问门户中，选择您的， Amazon Web Services 账户 然后选择AdministratorAccess。随后您将被重定向至 Amazon 管理控制台。

步骤 4：配置 Amazon 使用 IAM 身份中心的托管应用程序

1. 登录 Amazon 管理控制台后，打开计划使用的 Amazon 托管应用程序的控制台。
2. 按照控制台中的指导将 Amazon 托管应用程序配置为使用 IAM Identity Center。在此过程中，您可以将创建的用户分配给该应用程序。

设置 IAM 身份中心的账户实例进行测试 Amazon 托管应用程序

> **Note**
>
> IAM Identity Center 的账户实例将部署范围限定在单个 Amazon Web Services 账户内。您必须在与要测试的 Amazon 应用程序 Amazon Web Services 区域 相同的情况下启用此实例。

确认您的应用程序

所有与 IAM 身份中心配合使用的 Amazon 托管应用程序均可与 IAM 身份中心的组织实例一起使用。但是，只有其中部分应用程序可以与 IAM Identity Center 的账户实例一起使用。查看 Amazon 可与 IAM 身份中心配合使用的托管应用程序 列表。

步骤 1. 启用 IAM Identity Center 的账户实例

1. 请执行以下一项操作，登录 Amazon Web Services 管理控制台。
   - Amazon （ root 用户 ）新手 — 选择 R oot 用户并输入您的 Amazon Web Services 账户 电子邮件地址，以账户所有者身份登录。在下一页上，输入您的密码。
   - 已使用 Amazon 独立版 Amazon Web Services 账户 （ IAM 证书 ）— 使用具有管理权限的 IAM 凭证登录。
2. 在 Amazon 管理控制台主页上，选择 IAM 身份中心服务或导航到 IAM 身份中心控制台。
3. 请选择启用。
4. 在使用 Amazon Organizations启用 IAM Identity Center 页面上，选择启用 IAM Identity Center 的账户实例。

5. 在启用 IAM Identity Center 账户实例页面上，查看信息并可选地添加要与此账户实例关联的标签。然后选择 Enable。

步骤 2：在 IAM Identity Center 中创建用户

此过程介绍如何直接在内置的 Identity Center 目录中创建用户。此目录未连接到管理员可能用于管理工作用户的任何其他目录。在 IAM Identity Center 中创建用户后，您需要为此用户指定新凭证。当您以该用户身份登录以测试您的 Amazon 托管应用程序时，您将使用新的凭据登录。新凭证不允许您访问其他企业资源

> **Note**
>
> 建议您仅出于测试目的使用此方法创建用户。

1. 在 IAM Identity Center 控制台的导航窗格中，选择用户，然后选择添加用户。
2. 请按照控制台中的指导添加用户。保持选中向该用户发送包含密码设置说明的电子邮件，并确保指定您有权访问的电子邮件地址。
3. 注销 Console。

步骤 3：登录 Amazon Web Services 以 IAM 身份中心用户身份访问门户

Amazon Web Services 访问门户是一个 Web 门户，可让您创建的用户访问 Amazon 管理控制台。在登录 Amazon Web Services 访问门户之前，您必须接受加入 IAM Identity Center 的邀请并激活用户凭证。

1. 检查您的电子邮件，查找主题为邀请加入 Amazon IAM Identity Center 的邮件。
2. 选择接受邀请，然后按照注册页面上的指导设置新密码、登录并为您的用户注册 MFA 设备。
3. 注册 MFA 设备后， Amazon Web Services 访问门户打开。当应用程序对您可用时，您可以在应用程序选项卡下找到它们。

> **Note**
>
> Amazon 支持账户实例的应用程序允许用户无需额外权限即可登录应用程序。因此，账户选项卡将保持为空。

步骤 4：配置 Amazon 使用 IAM 身份中心的托管应用程序

1. 登录 Amazon 管理控制台后，打开计划使用的 Amazon 托管应用程序的控制台。
2. 按照控制台中的指导将 Amazon 托管应用程序配置为使用 IAM Identity Center。在此过程中，您可以将创建的用户分配给该应用程序。

查看和更改有关某人的详细信息 Amazon 托管应用程序

使用应用程序的控制台或 API 将 Amazon 托管应用程序连接到 IAM Identity Center 后，该应用程序将在 IAM Identity Center 中注册。应用程序注册到 IAM Identity Center 后，您可以在 IAM Identity Center 控制台查看和更改有关该应用程序的详细信息。

关于应用程序的信息包括是否需要分配用户和组，如果适用，还包括分配的用户和组，以及用于身份传播的可信应用程序。有关可信身份传播的信息，请参阅 可信身份传播概述。

查看和更改有关某人的信息 Amazon IAM 身份中心控制台中的托管应用程序

1. 打开 IAM Identity Center 控制台。
2. 选择应用程序。
3. 选择 Amazon 托管选项卡。
4. 选择要打开和查看的托管应用程序的链接。
5. 如果要更改有关 Amazon 托管应用程序的信息，请选择操作，然后选择编辑详细信息。
6. 应用程序的显示名称、描述以及用户和组分配方法都可以更改。

    a. 要更改显示名称，请在显示名称字段中输入所需名称，然后选择保存更改。
    b. 要更改描述，请在描述字段中输入所需描述，然后选择保存更改。
    c. 要更改用户和组的分配方法，请进行所需更改，然后选择保存更改。有关更多信息，请参阅 the section called “用户、组和预调配”。

禁用 Amazon 托管应用程序

要防止用户对 Amazon 托管应用程序进行身份验证，您可以在 IAM Identity Center 控制台中禁用该应用程序。

要禁用 Amazon 托管应用程序

1. 打开 IAM Identity Center 控制台。

2. 选择应用程序。
3. 在应用程序页面上的 Amazon 托管的应用程序下，选择要禁用的应用程序。
4. 选择应用程序后，选择操作，然后选择禁用。
5. 在禁用应用程序对话框中，选择禁用。
6. 在 Amazon 托管的应用程序列表中，应用程序的状态会显示为非活动。

> **Note**
>
> 如果 Amazon 托管应用程序处于禁用状态，则可以通过选择 “操作” 和 “启用” 来恢复用户对该应用程序进行身份验证的能力。

启用身份增强的控制台会话

控制台的身份增强会话通过提供一些额外的用户上下文来个性化用户的体验，从而增强用户的 Amazon 控制台会话。目前，Kiro Pro 用户在 Amazon 应用程序和网站上支持 Kiro 功能。

您可以启用身份增强型控制台会话，而无需对现有访问模式进行任何更改或与控制台联 Amazon 合。如果您的用户使用 IAM 登录 Amazon 控制台（例如，如果他们以 IAM 用户身份登录或通过 IAM 联合访问登录），则他们可以继续使用这些方法。如果您的用户登录 Amazon Web Services 访问门户，他们可以继续使用他们的 IAM Identity Center 用户证书。

主题

- 先决条件和注意事项
- 如何启用身份增强控制台会话
- 身份增强控制台会话的工作原理

先决条件和注意事项

在启用身份增强控制台会话之前，请先查看以下先决条件和注意事项：

- 如果您的用户通过订阅 Kiro Pro 在 Amazon 应用程序和网站上访问 Kiro，则必须启用身份增强型主机会话。

> **Note**
>
> Kiro 用户无需身份增强会话即可访问 Kiro，但他们将无法访问 Kiro Pro 订阅。

- Identity-enhanced 控制台会话需要 IAM 身份中心的组织实例。
- 如果您选择 Amazon Web Services 区域启用 IAM 身份中心，则不支持与 Kiro 集成。
- 要启用身份增强控制台会话，必须具有以下权限：
  - `sso:CreateApplication`
  - `sso:GetSharedSsoConfiguration`
  - `sso:ListApplications`
  - `sso:PutApplicationAssignmentConfiguration`
  - `sso:PutApplicationAuthenticationMethod`
  - `sso:PutApplicationGrant`
  - `sso:PutApplicationAccessScope`
  - `signin:CreateTrustedIdentityPropagationApplicationForConsole`
  - `signin:ListTrustedIdentityPropagationApplicationsForConsole`
- 要让用户使用身份增强控制台会话，必须在基于身份的策略中向他们授予 `sts:setContext` 权限。有关信息，请参阅授予使用者使用身份增强控制台会话的权限。

如何启用身份增强控制台会话

您可以在 Kiro 控制台或 IAM Identity Center 控制台中启用身份增强控制台会话。

在 Kiro 控制台中启用身份增强型控制台会话

在启用身份增强控制台会话之前，您必须拥有连接了身份源的 IAM Identity Center 组织实例。如果已经配置 IAM Identity Center，请跳到步骤 3。

1. 打开 IAM Identity Center 控制台。选择启用，然后创建 IAM Identity Center 的组织实例。有关信息，请参阅启用 IAM Identity Center。
2. 将身份源连接到 IAM Identity Center 并将用户预置到 IAM Identity Center 中。您可以将现有身份源连接到 IAM Identity Center；如果尚未使用其他身份源，也可以使用 Identity Center 目录。有关更多信息，请参阅 IAM Identity Center 身份源教程。

3. 完成设置 IAM 身份中心后，打开 Kiro 控制台并按照《K iro 用户指南》中订阅中的步骤进行操作。务必启用身份增强控制台会话。

> **Note**
>
> 如果您没有足够的权限启用身份增强控制台会话，则可能需要让 IAM Identity Center 管理员在 IAM Identity Center 控制台中代为执行此任务。有关该过程的更多信息，请参阅接下来的步骤。

在 IAM Identity Center 控制台中启用身份增强控制台会话

如果您是 IAM Identity Center 管理员，其他管理员可能会让您在 IAM Identity Center 控制台中启用身份增强控制台会话。

1. 打开 IAM Identity Center 控制台。
2. 在导航窗格中，选择设置。
3. 在启用身份增强会话下，选择启用。
4. 在第二条消息中选择启用。
5. 完成启用身份增强控制台会话后，设置页面的顶部会显示一条确认消息。
6. 在 “详细信息” 部分中，Identity-enhanced 会话的状态为 “已启用”。

身份增强控制台会话的工作原理

IAM Identity Center 可增强用户当前的控制台会话，使其包含活跃的 IAM Identity Center 用户的 ID 和 IAM Identity Center 会话 ID。

Identity-enhanced 控制台会话包括以下三个值：

- 身份存储用户 ID（identitystore：UserId）：此值用于唯一标识连接到 IAM Identity Center 的身份源中的用户。
- 身份存储目录 ARN（identitystore：IdentityStoreArn）：此值是连接到 IAM Identity Center 的身份存储的 ARN，可在其中查找 `identitystore:UserId` 的属性。
- IAM Identity Center 会话 ID：此值表示用户的 IAM Identity Center 会话是否仍然有效。

这些值虽然相同，但以不同方式获得，且在过程的不同时刻添加，具体取决于用户的登录方式：

- IAM 身份中心（Amazon Web Services 访问门户）：在这种情况下，活跃的 IAM 身份中心会话中已经提供了用户的身份存储用户 ID 和 ARN 值。IAM Identity Center 通过仅添加会话 ID 增强当前会话。
- 其他登录方法：如果用户以 IAM 用户、IAM 角色或 IAM 的联合用户身份登录 Amazon ，则不提供这些值。IAM Identity Center 通过添加身份存储用户 ID、身份存储目录 ARN 和会话 ID 增强当前会话。

客户托管的应用程序

IAM Identity Center 充当员工用户和组的中央身份服务。如果您已经使用了身份提供商 (IdP)，IAM Identity Center 可以与您的 IdP 集成，以便您将用户和组预置到 IAM Identity Center，并使用您的 IdP 进行身份验证。通过单个连接，IAM Identity Center 在多个连接前面代表您的 IdP， Amazon Web Services 服务 并使您的 OAuth 2.0 应用程序能够代表您的用户请求访问这些服务中的数据。您还可以使用 IAM Identity Center 为用户分配对 SAML 2.0 应用程序的访问权限。这包括诸如Connect Customer和之类的 Amazon 服务 Amazon Client VPN，这些服务仅使用SAML与IAM身份中心集成，因此被归类为客户托管的应用程序。

- 如果您的应用程序支持 JSON Web 令牌 (JWT)，则可以使用 IAM Identity Center 的可信身份传播功能使您的应用程序能够 Amazon Web Services 服务 代表您的用户请求访问数据。可信身份传播功能基于 OAuth 2.0 授权框架构建，该功能包含一个选项，可供应用程序将来自外部 OAuth 2.0 授权服务器的身份令牌与 IAM Identity Center 颁发并由 Amazon Web Services 服务识别的令牌交换。有关更多信息，请参阅 可信身份传播应用场景。
- 如果应用程序支持 SAML 2.0，则可以将其连接到 IAM Identity Center 的组织实例。您可以使用 IAM Identity Center 分配对 SAML 2.0 应用程序的访问权限。

> **Note**
>
> 将客户托管的应用程序与使用客户托管 KMS 密钥的 IAM 身份中心实例集成时，请验证应用程序是否调用 IAM 身份中心服务 API。如果是，请参阅基准 KMS 密钥策略以获取所需权限。

主题

- 对 SAML 2.0 和 OAuth 2.0 应用程序的单点登录访问
- 设置客户托管的 SAML 2.0 应用程序

对 SAML 2.0 和 OAuth 2.0 应用程序的单点登录访问

IAM Identity Center 使您能够为用户提供对 SAML 2.0 或 OAuth 2.0 应用程序的单点登录访问权限。以下主题提供了对 SAML 2.0 和 OAuth 2.0 的综合概述。

主题

SAML 2.0

SAML 2.0 是一种用于安全交换 SAML 断言的行业标准，它在 SAML 机构（称为身份提供商或 IdP）与 SAML 2.0 使用者（称为服务提供商或 SP）之间传递用户的相关信息。IAM Identity Center 使用这些信息为有权在访问门户中使用应用程序的用户提供联合单点登录 Amazon Web Services 访问权限。

> **Note**
>
> IAM Identity Center 不支持验证来自 SAML 应用程序的传入 SAML 身份验证请求的签名。

OAuth 2.0

OAuth 2.0 协议允许应用程序在不共享密码的情况下安全地访问和共享用户数据。这项功能提供了一种安全、标准化的方式，让用户允许应用程序访问其资源。通过不同的 OAuth 2.0 授予流程，访问变得更加便利。

IAM Identity Center 允许在公共客户端上运行的应用程序检索临时证书，以便以编程方式代表其用户访问 Amazon Web Services 账户 和服务。公共客户端通常是用于在本地运行应用程序的台式机、笔记本电脑或其他移动设备。在公共客户端上运行的 Amazon 应用程序的示例包括 Amazon Command Line Interface (Amazon CLI) Amazon Toolkit、和 Amazon 软件开发套件 (SDK)。为了让这些应用程序能够获得凭证，IAM Identity Center 支持以下 OAuth 2.0 流程的部分内容：

- 采用代码交换验证密钥（Proof Key for Code Exchange，PKCE）的授权码授予（RFC 6749 和 RFC 7636）
- 设备授权授予（RFC 8628）

> **Note**
>
> 这些授权类型只能用于支持此功能 Amazon Web Services 服务 的授予类型。这些服务可能并非在所有 Amazon Web Services 区域中都支持此授权类型。有关地区差异， Amazon Web Services 服务 请参阅相关文档。

OpenID Connect（OIDC）是基于 OAuth 2.0 框架的身份验证协议。OIDC 指定了如何使用 OAuth 2.0 进行身份验证。通过 IAM Identity Center OIDC 服务 API，应用程序会注册一个 OAuth 2.0 客户端，并使用其中一个流程获取访问令牌，该令牌为受 IAM Identity Center 保护的 API 提供权限。应用程序会指定访问范围，声明其预期的 API 用户。在您以 IAM Identity Center 管理员身份配置身份源之后，应用程序最终用户必须完成登录过程（如果他们尚未这么做）。然后，最终用户必须给予同意，才能允许应用程序进行 API 调用。这些 API 调用是使用用户的权限进行的。作为响应，IAM Identity Center 会向应用程序返回一个访问令牌，其中包含用户同意的访问范围。

使用 OAuth 2.0 授予流程

OAuth 2.0 拨款流只能通过支持这些流程的 Amazon 托管应用程序获得。要使用 OAuth 2.0 流程，您的 IAM Identity Center 实例和您使用的任何 Amazon 受支持的托管应用程序都必须部署在单个流程中。 Amazon Web Services 区域请参阅每个应用程序的文档， Amazon Web Services 服务 以确定 Amazon 托管应用程序的区域可用性以及您要使用的 IAM Identity Center 实例。

要使用会使用 OAuth 2.0 流的应用程序，最终用户必须输入该应用程序将连接的 URL，并在 IAM Identity Center 实例中注册。根据应用程序的不同，作为管理员的您必须向用户提供 Amazon Web Services 访问门户 URL 或 IAM Identity Center 实例的发布者 URL。您可以在 IAM Identity Center 控制台的 设置页面上找到这两个设置。有关配置客户端应用程序的其他信息，请参阅相应的应用程序文档。

最终用户登录应用程序和给予同意的体验取决于应用程序使用的是 具有 PKCE 的授权代码授予，还是 设备授权授予。

具有 PKCE 的授权代码授予

此流程由在装有浏览器的设备上运行的应用程序使用。

1. 打开浏览器窗口。
2. 如果用户尚未进行身份验证，浏览器会重定向用户来完成用户身份验证。
3. 完成身份验证后，用户会看到一个同意屏幕，其中显示以下信息：
   - 应用程序的名称

- 应用程序请求同意使用的访问范围

4. 用户可以取消同意过程，也可以给予同意，然后应用程序会根据用户的权限继续进行访问。

设备授权授予

此流程可能由在装有或未装浏览器的设备上运行的应用程序使用。当应用程序启动该流时，应用程序会提供一个 URL 和一个用户代码，用户必须稍后在流中对其进行验证。用户代码是必要的，因为启动流程的应用程序可能在不是用户给予同意的设备上运行。该代码可确保用户同意他们在另一台设备上启动的流程。

> **Note**
>
> 如果您的客户端使用 `device.sso.region.amazonaws.com`，则必须更新授权流程以使用代码交换的证明密钥（PKCE）。有关更多信息，请参阅《Amazon Command Line Interface 用户指南》中的使用 Amazon CLI配置 IAM Identity Center 身份验证。

1. 当流程从装有浏览器的设备启动时，会打开一个浏览器窗口。当流程从未装浏览器的设备启动时，用户必须在另一台设备上打开浏览器，然后前往应用程序提供的 URL。
2. 无论是哪种情况，如果用户尚未进行身份验证，浏览器会重定向用户来完成用户身份验证。
3. 完成身份验证后，用户会看到一个同意屏幕，其中显示以下信息：
   - 应用程序的名称
   - 应用程序请求同意使用的访问范围
   - 应用程序提供给用户的用户代码
4. 用户可以取消同意过程，也可以给予同意，然后应用程序会根据用户的权限继续进行访问。

访问范围

范围定义了可通过 OAuth 2.0 流访问的服务的访问权限。范围是服务（也称为资源服务器）对与操作和服务资源相关的权限进行分组的一种方式，指定了 OAuth 2.0 客户端可以请求的粗粒度操作。在 OAuth 2.0 客户端向 IAM Identity Center OIDC 服务注册时，该客户端会指定范围来声明其预期操作，用户必须同意才能执行这些操作。

OAuth 2.0 客户端使用 OAuth 2.0（RFC 6749）第 3.3 节中定义的 `scope` 值指定要为访问令牌请求哪些权限。在请求访问令牌时，客户端最多可以指定 25 个范围。当用户在采用 PKCE 的授权码授予流程或设备授权授予流程中给予同意时，IAM Identity Center 会将范围编码到其返回的访问令牌中。

Amazon 将范围添加到 IAM 身份中心以获得支持 Amazon Web Services 服务。下表列出了注册公共客户端时，IAM Identity Center OIDC 服务支持的范围。

注册公共客户端时，IAM Identity Center OIDC 服务支持的访问范围

Scope	说明	支持的服务
`sso:account:access`	访问 IAM Identity Center 管理型帐户和权限集。	IAM Identity Center
`codewhisperer:analysis`	启用对 Kiro 代码分析的访问权限。	Amazon 构建者 ID 和 IAM 身份中心
`codewhisperer:completions`	启用对 Kiro 内联代码建议的访问权限。	Amazon 构建者 ID 和 IAM 身份中心
`codewhisperer:conversations`	启用对 Kiro 聊天的访问权限。	Amazon 构建者 ID 和 IAM 身份中心
`codewhisperer:taskassist`	允许访问 Kiro Agent 以进行软件开发。	Amazon 构建者 ID 和 IAM 身份中心
`codewhisperer:transformations`	启用对 Kiro 代理的访问权限以进行代码转换。	Amazon 构建者 ID 和 IAM 身份中心
`codecatalyst:read_write`	读取和写入您的 Amazon CodeCatalyst 资源，允许访问您的所有现有资源。	Amazon 构建者 ID 和 IAM 身份中心
`verified_access:application:connect`	启用 Amazon Verified Access	Amazon Verified Access
`redshift:connect`	连接到 Amazon Redshift	Amazon Redshift

Scope	说明	支持的服务
`datazone:domain:access`	访问您的 DataZone 域名执行角色	Amazon DataZone
`nosqlworkbench:datamodeladviser`	创建与读取数据模型	NoSQL Workbench
`transform:read_write`	启用对 Amazon 转换代理的访问权限以进行代码转换	Amazon 转换

设置客户托管的 SAML 2.0 应用程序

如果您使用的客户托管应用程序支持 SAML 2.0，则可以通过 SAML 2.0 将您的 IdP 与 IAM Identity Center 联合起来，并使用 IAM Identity Center 管理用户对这些应用程序的访问。您可以在 IAM Identity Center 控制台中从常用应用程序目录中选择一个 SAML 2.0 应用程序，也可以设置自己的 SAML 2.0 应用程序。

> **Note**
>
> 如果您有支持 OAuth 2.0 的客户托管应用程序，并且您的用户需要从这些应用程序进行访问 Amazon Web Services 服务，则可以使用可信身份传播。通过可信身份传播，用户可以登录应用程序，而该应用程序可以在请求中传递用户的身份，以访问 Amazon Web Services 服务中的数据。

主题

- 设置来自 IAM Identity Center 应用程序目录的应用程序
- 设置您自己的 SAML 2.0 应用程序

设置来自 IAM Identity Center 应用程序目录的应用程序

您可以使用 IAM Identity Center 控制台中的应用程序目录添加许多可与 IAM Identity Center 配合使用的常用 SAML 2.0 应用程序。例如，其中包括 Salesforce、Box 和 Microsoft 365。

大多数应用程序都会提供详细信息，介绍如何设置 IAM Identity Center 与应用程序服务提供商之间的信任。在目录中选择应用程序后，您可在应用程序的配置页面中找到此信息。配置应用程序后，您可以根据需要，向 IAM Identity Center 中的用户或组分配访问权限。

请使用此过程在 IAM Identity Center 和应用程序的服务提供商之间设置 SAML 2.0 信任关系。

开始执行此过程之前，获得服务提供者的元数据交换文件将很有帮助，这样可以让您更有效地设置信任。如果您没有此文件，仍可以使用此过程手动配置信任。

要添加并配置应用程序目录中的应用程序

1. 打开 IAM Identity Center 控制台。
2. 选择应用程序。
3. 选择客户托管选项卡。
4. 选择添加应用程序。
5. 在选择应用程序类型页面，选择设置首选项下的我想从目录中选择应用程序。
6. 在应用程序目录下，开始在搜索框中键入要添加的应用程序名称。
7. 当应用程序出现在搜索结果中时，从列表中选择该应用程序的名称，然后选择下一步。
8. 在配置应用程序页面，显示名称和描述字段会预先填充应用程序的相关详细信息。您可以编辑这些信息。
9. 在 IAM Identity Center 元数据下，执行以下操作：

    a. 在 IAM Identity Center SAML 元数据文件下，选择下载以下载身份提供商元数据。

    b. 在 IAM Identity Center 证书下，选择下载证书以下载身份提供商证书。

    > **Note**
    >
    > 稍后通过服务提供商的网站设置应用程序时，您会用到这些文件。按照该提供商的说明进行操作。

10. （可选）在应用程序属性下，您可以指定应用程序启动 URL、中继状态和会话持续时间。有关更多信息，请参阅 了解 IAM Identity Center 控制台中的应用程序属性。
11. 在应用程序元数据下，执行以下操作之一：

    a. 如果您有元数据文件，请选择上传应用程序 SAML 元数据文件。然后，选择选择文件以查找并选择元数据文件。

b. 如果您没有元数据文件，请选择手动键入元数据值，然后提供应用程序 ACS URL 和应用程序 SAML 受众值。

12. 选择提交。您将进入刚刚添加的应用程序的详细信息页面。

设置您自己的 SAML 2.0 应用程序

您可以自行设置允许使用 SAML 2.0 进行身份联合验证的应用程序，然后将其添加到 IAM Identity Center。要设置自己的 SAML 2.0 应用程序，其大部分步骤与在 IAM Identity Center 控制台设置应用程序目录中的 SAML 2.0 应用程序相同。但是，您还必须为自己的 SAML 2.0 应用程序提供额外的 SAML 属性映射。这些映射将使 IAM Identity Center 为您的应用程序正确填充 SAML 2.0 断言。您可以在首次设置应用程序时提供此附加 SAML 属性映射。您还可以在 IAM Identity Center 控制台的应用程序详细信息页面上提供 SAML 2.0 属性映射。

请使用以下过程在 IAM Identity Center 和您的 SAML 2.0 应用程序服务提供商之间设置 SAML 2.0 信任关系。开始执行此过程之前，请确保您拥有服务提供商的证书和元数据交换文件，以便您完成信任的设置。

要设置您自己的 SAML 2.0 应用程序

1. 打开 IAM Identity Center 控制台。
2. 选择应用程序。
3. 选择客户托管选项卡。
4. 选择添加应用程序。
5. 在选择应用程序类型页面，选择设置首选项下的我有想设置的应用程序。
6. 在应用程序类型下，选择 SAML 2.0。
7. 选择下一步。
8. 在配置应用程序页面上的配置应用程序下，输入应用程序的显示名称，例如 **MyApp**。然后，输入描述。
9. 在 IAM Identity Center 元数据下，执行以下操作：

   a. 在 IAM Identity Center SAML 元数据文件下，选择下载以下载身份提供商元数据。

   b. 在 IAM Identity Center 证书下，选择下载，以下载身份提供商证书。

> **Note**
>
> 稍后在您通过服务提供商的网站设置自定义应用程序时，您会用到这些文件。

10. （可选）在应用程序属性下，您也可以指定应用程序启动 URL、中继状态和会话持续时间。有关更多信息，请参阅 了解 IAM Identity Center 控制台中的应用程序属性。
11. 在应用程序元数据下，选择手动键入您的元数据值。然后，提供应用程序 ACS URL 和应用程序 SAML 受众值。
12. 选择提交。您将进入刚刚添加的应用程序的详细信息页面。

可信身份传播概述

可信身份传播是 IAM Identity Center 的一项功能，让 Amazon Web Services 服务 的管理员可以根据用户属性（例如组关系）授予权限。通过可信身份传播，可以向 IAM 角色添加身份上下文，以识别请求访问 Amazon 资源的用户。此上下文会传播到其他 Amazon Web Services 服务上下文。

身份上下文包含在他们收到访问请求时 Amazon Web Services 服务 用于做出授权决策的信息。这些信息包括识别请求者（例如，IAM 身份中心用户）、请求访问权限的元数据（例如 Amazon Redshift）和访问范围（例如，只读权限）的元数据。 Amazon Web Services 服务 接收方 Amazon Web Services 服务 使用此上下文以及分配给用户的任何权限来授权访问其资源。

可信身份传播的优势

可信身份传播允许管理员使用员工的 Amazon Web Services 服务 企业身份授予对资源（例如数据）的权限。此外，他们还可以通过查看服务日志或来审核谁访问了哪些数据 Amazon CloudTrail。如果您是 IAM Identity Center 管理员，其他 Amazon Web Services 服务 管理员可能会要求您启用可信身份传播。

启用可信身份传播

启用可信身份传播的流程包括以下两个步骤：

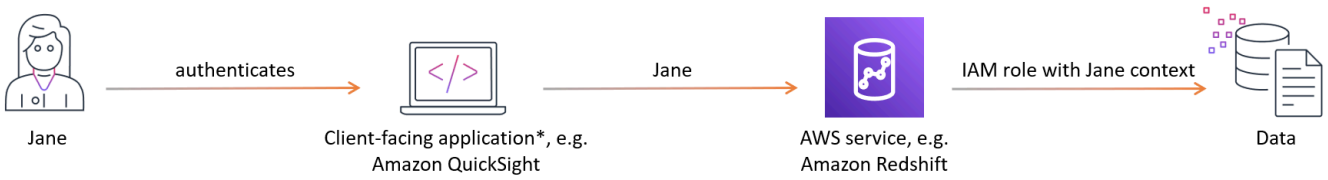
1. 启用 IAM Identity Center 并将您现有的身份来源连接到 IAM Identity Center-您将继续使用现有身份来源管理员工身份；将其连接到 IAM Identity Center 可创建对您的员工的引用，供您的用例 Amazon Web Services 服务 中的所有人共享。数据所有者也可在未来的使用案例中使用该引用。

2. 将@@ 您的用例中的 IAM Identity Center 连接到 IAM Identity Center-可信身份传播用例中的管理员遵循相应服务文档中的指导将服务连接到 IAM Identity Center。 Amazon Web Services 服务 Amazon Web Services 服务

> **Note**
>
> 如果您的使用案例涉及第三方或客户开发的应用程序，您可以通过在验证应用程序用户身份的身份提供者和 IAM Identity Center 之间配置信任关系来启用可信身份传播。这样，您的应用程序就能利用前文所述的可信身份传播流程。
> 有关更多信息，请参阅 通过可信令牌发布者使用应用程序。

可信身份传播如何工作

下图展示了可信身份传播的高层级工作流：

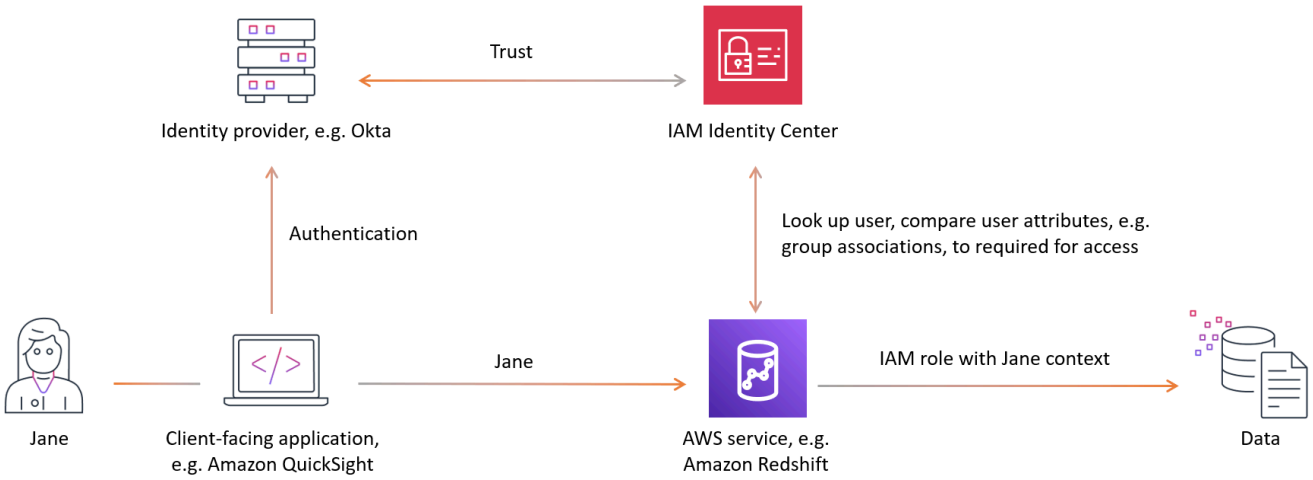


1. 用户使用面向客户端的应用程序（例如 Quick）进行身份验证。
2. 面向客户的应用程序请求访问权限以使用 Amazon Web Services 服务 来查询数据，并包含有关用户的信息。

> **Note**
>
> 一些可信身份传播用例涉及与 Amazon Web Services 服务 使用服务驱动程序进行交互的工具。您可以在使用案例指南中查看这是否适用于您的使用案例。

3. 使用 IAM Identity Center Amazon Web Services 服务 验证用户身份，并将用户属性（例如群组关联）与访问所需的属性进行比较。只要用户或其组具有必要的权限，就会 Amazon Web Services 服务 授予访问权限。
4. Amazon Web Services 服务 可能会将用户标识符记录在服务日志中 Amazon CloudTrail 和服务日志中。有关详细信息，请参阅相应服务文档。

下图概述了前文所述的可信身份传播工作流步骤：



主题

先决条件和注意事项

在设置可信身份传播之前，请先查看以下先决条件和注意事项。

主题

先决条件

要使用可信身份传播，请确保您的环境满足以下先决条件：

- 启用和预置 IAM Identity Center
  - 要使用可信身份传播，您必须在启用用户将要访问的 Amazon 应用程序和服务的相同 Amazon Web Services 区域 位置启用 IAM Identity Center。有关信息，请参阅启用 IAM Identity Center。

    - 推荐使用 IAM Identity Center 组织实例 - 我们建议您使用在 Amazon Organizations管理账户中启用的 IAM Identity Center 组织实例。您可以将 IAM Identity Center 组织实例的管理权限委托给成员账户。如果您选择 IAM Identity Center 的账户实例，则所有希望用户通过可信身份传播访问的 Amazon Web Services 服务 必须位于您启用 IAM Identity Center 的同一 Amazon Web Services 账户 中。有关更多信息，请参阅 IAM Identity Center 的账户实例。
  - 将您现有的身份提供者连接到 IAM Identity Center，并将用户和组配置到 IAM Identity Center 中。有关更多信息，请参阅 IAM Identity Center 身份源教程。
- 将您的可信身份传播用例中的 Amazon 托管应用程序和服务连接到 IAM Identity Center。要使用可信身份传播， Amazon 托管应用程序必须连接到 IAM 身份中心。

注意事项

配置和使用可信身份传播时，请记住以下注意事项：

- IAM Identity Center 的组织和账户实例
  - IAM Identity Center 的组织实例能为您提供最大的控制权和灵活性，支持将使用案例扩展到多个 Amazon Web Services 账户、用户和 Amazon Web Services 服务。如果您无法使用组织实例，您的使用案例可能支持通过 IAM Identity Center 的账户实例实现。有关您使用案例中的哪些 Amazon Web Services 服务 支持 IAM Identity Center 账户实例，请参阅 Amazon 可与 IAM 身份中心配合使用的托管应用程序。
- Multi-account 不需要权限（权限集）
  - 可信身份传播不需要您设置多账户权限（权限集）。您可以启用 IAM Identity Center，仅将其用于可信身份传播。

客户自主管理型应用程序的注意事项

即使您的用户与不由 Amazon您定制开发的应用程序管理的面向客户的应用程序进行交互，您的员工也可以从可信的身份Tableau传播中受益。这些应用程序的用户可能未在 IAM Identity Center 中配置。为了顺利识别和授权用户访问 Amazon 资源，IAM Identity Center 允许您在对用户进行身份验证的身份提供商与 IAM Identity Center 之间配置可信关系。有关更多信息，请参阅 通过可信令牌发布者使用应用程序。

此外，为您的应用程序配置可信身份传播还需满足以下要求：

- 您的应用程序必须使用 OAuth 2.0 框架进行身份验证。可信身份传播不支持 SAML 2.0 集成。
- 您的应用程序必须获得 IAM Identity Center 的认可。请遵循您的使用案例专属指引。

可信身份传播应用场景

作为 IAM Identity Center 管理员，您可能需要协助配置从面向用户的应用程序到 Amazon Web Services 服务的可信身份传播。为支持此请求，您需要以下信息：

- 您的用户将使用哪个面向客户端的应用程序？
- Amazon Web Services 服务 哪些用于查询数据和授权访问数据？
- 哪个 Amazon Web Services 服务 授权访问数据？

在启用不涉及第三方应用程序或自定义开发应用程序的可信身份传播使用案例时，您的职责包括：

1. 启用 IAM 身份中心。
2. 将现有身份源连接到 IAM Identity Center。

这些用例的可信身份配置的其余步骤将在连接 Amazon Web Services 服务 的应用程序中执行。已连接 Amazon Web Services 服务 或应用程序的管理员应参阅相应的用户指南，以获得全面的服务特定指导。

在启用涉及第三方应用程序或自定义开发应用程序的可信身份传播使用案例时，您的职责包括 启用 IAM Identity Center 和连接身份源的步骤，以及：

1. 配置身份提供者（IdP）与第三方或自定义开发应用程序的连接。
2. 使 IAM Identity Center 能够识别该第三方或自定义开发应用程序。
3. 在 IAM Identity Center 中将您的 IdP 配置为可信令牌颁发者。有关更多信息，请参阅 通过可信令牌发布者使用应用程序。

所连接应用程序的管理员 Amazon Web Services 服务 应参阅相应的用户指南，以获得全面的服务特定指导。

分析、数据湖仓和机器学习使用案例

您可以通过以下分析和机器学习服务启用可信传播使用案例：

- Amazon Redshift - 有关指导，请参阅 使用 Amazon Redshift 的可信身份传播。
- Amazon EMR - 有关指导，请参阅 使用 Amazon EMR 的可信身份传播。
- Amazon Athena - 有关指导，请参阅 使用 Amazon Athena 的可信身份传播。

- SageMaker Studio-有关指导，请参阅使用 Amazon SageMaker Studio 进行可信身份传。

其他使用案例

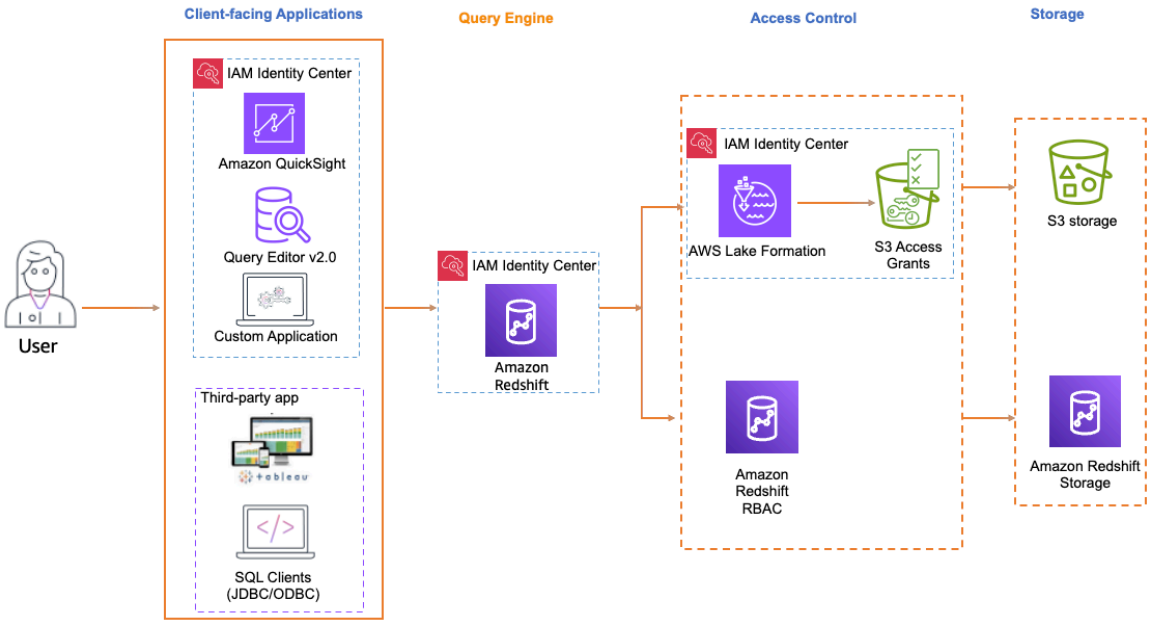
您还可以通过以下 Amazon Web Services 服务启用 IAM Identity Center 和可信身份传播：

- Amazon Q Business - 有关指导，请参阅：
  - 使用 IAM Identity Center 的应用程序的管理员工作流
  - 使用 IAM Identity Center 配置 Amazon Q Business 应用程序。
  - 使用 IAM Identity Center 可信身份传播配置 Amazon Q Business。
- Amazon OpenSearch 服务-有关指导，请参阅：
  - IAM Identity Center 可信身份传播支持 Amazon OpenSearch 服务。
  - Amazon OpenSearch 服务的集中式 OpenSearch 用户界面（控制面板）。
- Amazon Transfer Family - 有关指导，请参阅：
  - Transfer Family Web 应用程序。

主题

使用 Amazon Redshift 的可信身份传播

启用可信身份传播的步骤取决于您的用户是与托管应用程序交互还是与客户 Amazon 托管的应用程序进行交互。下图显示了面向客户端的应用程序（无论是 Amazon 托管的还是外部的）的可信身份传播配置，这些应用程序通过Amazon Redshift或授权服务（例如Amazon S3）提供的访问控制来查询 Amazon Redshift 数据。 Amazon Amazon Lake Formation Access Grants



启用面向 Amazon Redshift 的可信身份传播后，Redshift 管理员可以将 Redshift 配置为自动创建角色（以 IAM Identity Center 作为身份提供者）、将 Redshift 角色映射到 IAM Identity Center 中的组，并使用 Redshift 基于角色的访问控制授予访问权限。

支持的面向客户端的应用程序

Amazon 托管应用程序

以下面向客户的 Amazon 托管应用程序支持向 Amazon Redshift 传播可信身份：

- Amazon RedshiftQuery Editor V2
- 快点

> **Note**
>
> 如果您使用 Amazon Redshift Spectrum 访问 Amazon Glue Data Catalog中的外部数据库或表，建议设置 Lake Formation 和 Amazon S3 Access Grants 以提供细粒度访问控制。

客户托管的应用程序

以下客户自主管理型应用程序支持面向 Amazon Redshift 的可信身份传播：

- Tableau，包括 Tableau Desktop、Tableau Server 和 Tableau Prep

  - 要为 Tableau 用户启用可信身份传播，请参阅《Amazon 大数据博客》中的使用 IAM Identity Center 将 Tableau 和 Okta 与 Amazon Redshift 集成。
- SQL 客户端（DBeaver 和 DBVisualizer）
  - 要为 SQL 客户端（DBeaver和DBVisualizer）用户启用可信身份传播，请参阅大数据博客中使用 IAM Identity Center 将身份提供商 (IdP) 与 Amazon Redshift 查询编辑器 V2 和 SQL 客户端集成，实现无缝 Sign-On单一。Amazon

设置 Amazon Redshift 查询编辑器 V2 的可信身份传播

以下过程将引导您实现从 Amazon Redshift 查询编辑器 V2 到 Amazon Redshift 的可信身份传播。

先决条件

在开始本教程之前，您需要设置以下方面：

1. 启用 IAM 身份中心。建议使用组织实例。有关更多信息，请参阅 先决条件和注意事项。
2. 将身份源中的用户和组配置到 IAM Identity Center。

启用可信身份传播涉及两项操作：IAM Identity Center 管理员在 IAM Identity Center 控制台执行的任务，以及 Amazon Redshift 管理员在 Amazon Redshift 控制台执行的任务。

IAM Identity Center 管理员需执行的任务

IAM Identity Center 管理员需完成以下任务：

1. 在 Amazon Redshift 集群或无服务器实例所在的账户中，创建 IAM 角色 并附加以下权限策略。有关更多信息，请参阅 IAM 角色创建。

   - 以下策略示例包含完成本教程所需的权限。要使用此政策，请将示例策略*italicized placeholder text*中的替换为您自己的信息。有关详细操作指引，请参阅创建策略或编辑策略。

     权限策略：

     JSON

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

```
        {
            "Sid": "AllowRedshiftApplication",
            "Effect": "Allow",
            "Action": [
                "redshift:DescribeQev2IdcApplications",
                "redshift-serverless:ListNamespaces",
                "redshift-serverless:ListWorkgroups",
                "redshift-serverless:GetWorkgroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowIDCPermissions",
            "Effect": "Allow",
            "Action": [
                "sso:DescribeApplication",
                "sso:DescribeInstance"
            ],
            "Resource": [
                "arn:aws:sso:::instance/Your-IAM-Identity-Center-Instance
 ID",
                "arn:aws:sso::111122223333:application/Your-IAM-Identity-
Center-Instance-ID/*"
            ]
        }
    ]
}
```

信任政策：

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "redshift-serverless.amazonaws.com",
                    "redshift.amazonaws.com"
```

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

2. 在启用 IAM Identity Center 的 Amazon Organizations 管理账户中创建权限集。下一步将使用该权限集允许联合用户访问 Redshift 查询编辑器 V2。

   a. 前往 IAM Identity Center 控制台，在 “Multi-Account 权限” 下，选择 “权限集”。

   b. 选择创建权限集。

   c. 选择自定义权限集，然后选择下一步。

   d. 在 Amazon 托管策略下，选择 **AmazonRedshiftQueryEditorV2ReadSharing**。

   e. 在内联策略下，添加以下策略：

      JSON

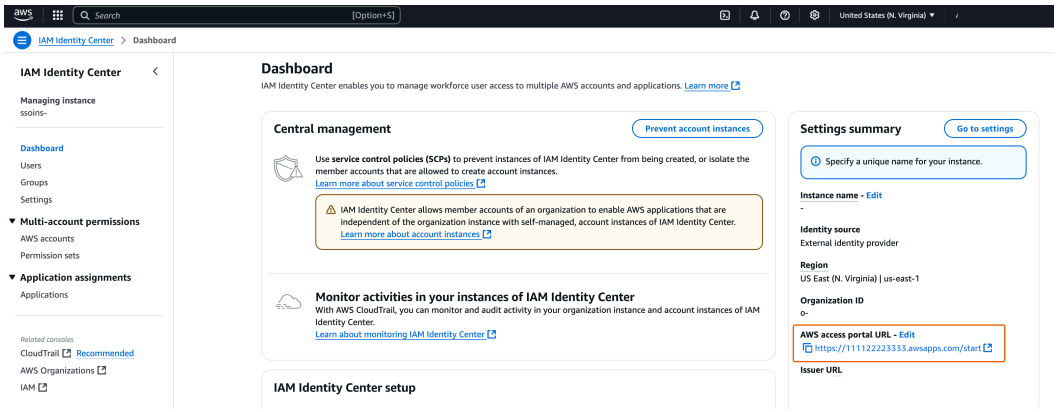
```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "redshift:DescribeQev2IdcApplications",
                "redshift-serverless:ListNamespaces",
                "redshift-serverless:ListWorkgroups",
                "redshift-serverless:GetWorkgroup"
            ],
            "Resource": "*"
        }
    ]
}
```

   f. 选择下一步，然后为权限集命名。例如 **Redshift-Query-Editor-V2**。

g. 在中继状态 - 可选下，将默认中继状态设置为查询编辑器 V2 URL，格式为：`https://your-region.console.aws.amazon.com/sqlworkbench/home`。

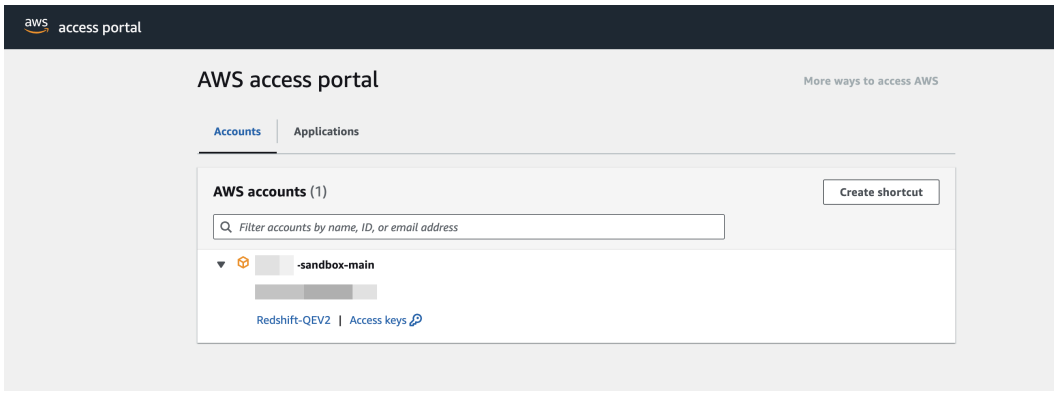
h. 检查设置，然后选择创建。

i. 导航到 IAM Identity Center 仪表板，并从设置摘要部分复制 Amazon Web Services 访问门户 URL。



j. 打开一个新的隐身浏览器窗口并粘贴该 URL。

这将带您 Amazon Web Services 进入访问门户，确保您使用的是 IAM Identity Center 用户登录。



有关权限集的更多信息，请参阅 Amazon Web Services 账户 使用权限集进行管理。

3. 启用联合用户访问 Redshift 查询编辑器 V2。

a. 在 Amazon Organizations 管理账户中，打开 IAM 身份中心控制台。

b. 在导航窗格的 “Multi-account权限” 下，选择Amazon Web Services 账户。

c. 在 Amazon Web Services 账户 页面上，选择 Amazon Web Services 账户 要为其分配访问权限的。

d. 选择分配用户或组。

e. 在分配用户和组页面上，选择要为其创建权限集的用户和/或组。然后选择下一步。

f. 在分配权限集页面上，选择您在上一步中创建的权限集。然后选择下一步。

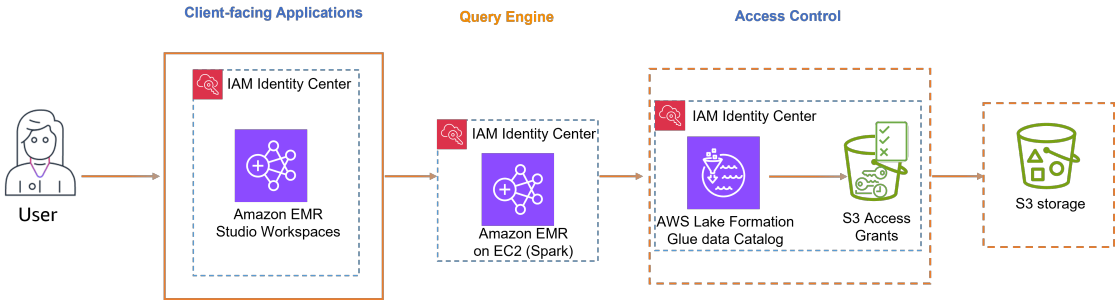
g. 在查看并提交分配页面上，查看您的选择，选择提交。

Amazon Redshift 管理员执行的任务

启用面向 Amazon Redshift 的可信身份传播，需要 Amazon Redshift 集群管理员或 Amazon Redshift Serverless 管理员在 Amazon Redshift 控制台执行多项操作。有关更多信息，请参阅大数据博客中使用 IAM Identity Center 将身份提供商 (IdP) 与 Amazon Redshift 查询编辑器 V2 和 SQL 客户端集成，实现无缝 Sign-On单一。Amazon

使用 Amazon EMR 的可信身份传播

下图显示了 Amazon EMR Studio 的可信身份传播配置，使用亚马逊 EC2 上的 Amazon EMR，访问控制由和 Amaz Amazon Lake Formation on S3 提供。Access Grants



支持的面向客户端的应用程序

- Amazon EMR Studio

如需启用可信身份传播，请执行以下步骤：

- 设置 Amazon EMR Studio 作为 Amazon EMR 集群的面向客户端应用程序。
- 设置搭载 Apache Spark 的 Amazon EC2 上的 Amazon EMR 集群。
- 推荐：Amazon Lake Formation以及 Amazon S3 Access Grants，以提供对 S3 中底层数据位置 Amazon Glue Data Catalog 和底层数据位置的精细访问控制。

设置 Amazon EMR Studio 的可信身份传播

以下过程将引导您设置 Amazon EMR Studio，以实现对 Amazon Athena 工作组或运行 Apache Spark 的 Amazon EMR 集群执行查询时的可信身份传播。

先决条件

在开始本教程之前，您需要设置以下方面：

1. 启用 IAM 身份中心。建议使用组织实例。有关更多信息，请参阅 先决条件和注意事项。
2. 将身份源中的用户和组配置到 IAM Identity Center。

要完成 Amazon EMR Studio 的可信身份传播配置，EMR Studio 管理员必须执行以下步骤。

步骤 1：为 EMR Studio 创建所需的 IAM 角色

本步骤中，Amazon EMR Studio 管理员需为 EMR Studio 创建 IAM 服务角色和 IAM 用户角色。

1. 创建 EMR Studio 服务角色 - EMR Studio 将通过该 IAM 角色安全管理工作区和笔记本、连接集群并处理数据交互。

   a. 导航到 IAM 控制台 (https://console.aws.amazon.com/iam/) 并创建 IAM 角色。
   b. 选择 Amazon Web Services 服务 作为可信实体，然后选择 Amazon EMR。附加以下策略以定义该角色的权限和信任关系。

      要使用这些政策，请将示例策略*italicized placeholder text*中的替换为您自己的信息。有关详细操作指引，请参阅创建策略或编辑策略。

      JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ObjectActions",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::Your-S3-Bucket-For-EMR-Studio/*"
            ],
            "Condition": {
                "StringEquals": {
```

```
                    "aws:ResourceAccount": "Your-AWS-Account-ID"
                }
            }
        },
        {
            "Sid": "BucketActions",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetEncryptionConfiguration"
            ],
            "Resource": [
                "arn:aws:s3:::Your-S3-Bucket-For-EMR-Studio"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "Your-AWS-Account-ID"
                }
            }
        }
    ]
}
```

有关服务角色的所有权限参考，请参阅 EMR Studio 服务角色权限。

2. 创建用于 IAM Identity Center 身份验证的 EMR Studio 用户角色 - 当用户通过 IAM Identity Center 登录以管理工作区、EMR 集群、作业和 Git 代码库时，EMR Studio 将使用该角色。该角色用于启动可信身份传播工作流。

> **Note**
>
> EMR Studio 用户角色不需要包含访问目录中 Amazon Glue 表的 Amazon S3 位置的权限。 Amazon Lake Formation 权限和注册的湖泊位置将用于获得临时权限。

以下示例策略可用于允许 EMR Studio 用户通过 Athena 工作组运行查询的角色。

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDefaultEC2SecurityGroupsCreationInVPCWithEMRTags",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSecurityGroup"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:vpc/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/for-use-with-amazon-emr-managed-
policies": "true"
                }
            }
        },
        {
            "Sid": "AllowAddingEMRTagsDuringDefaultSecurityGroupCreation",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/for-use-with-amazon-emr-managed-
policies": "true",
                    "ec2:CreateAction": "CreateSecurityGroup"
                }
            }
        },
        {
            "Sid": "AllowSecretManagerListSecrets",
            "Action": [
                "secretsmanager:ListSecrets"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Sid": "AllowSecretCreationWithEMRTagsAndEMRStudioPrefix",
            "Effect": "Allow",
```

```
            "Action": "secretsmanager:CreateSecret",
            "Resource": "arn:aws:secretsmanager:*:*:secret:emr-studio-*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/for-use-with-amazon-emr-managed-
policies": "true"
                }
            }
        },
        {
            "Sid": "AllowAddingTagsOnSecretsWithEMRStudioPrefix",
            "Effect": "Allow",
            "Action": "secretsmanager:TagResource",
            "Resource": "arn:aws:secretsmanager:*:*:secret:emr-studio-*"
        },
        {
            "Sid": "AllowPassingServiceRoleForWorkspaceCreation",
            "Action": "iam:PassRole",
            "Resource": [
                "arn:aws:iam::111122223333:role/service-
role/AmazonEMRStudio_ServiceRole_Name"
            ],
            "Effect": "Allow"
        },
        {
            "Sid": "AllowS3ListAndLocationPermissions",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::*",
            "Effect": "Allow"
        },
        {
            "Sid": "AllowS3ReadOnlyAccessToLogs",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::aws-logs-Your-AWS-Account-ID-Region/
elasticmapreduce/*"
            ],
            "Effect": "Allow"
```

```
        },
        {
            "Sid": "AllowAthenaQueryExecutions",
            "Effect": "Allow",
            "Action": [
                "athena:StartQueryExecution",
                "athena:GetQueryExecution",
                "athena:GetQueryResults",
                "athena:StopQueryExecution",
                "athena:ListQueryExecutions",
                "athena:GetQueryResultsStream",
                "athena:ListWorkGroups",
                "athena:GetWorkGroup",
                "athena:CreatePreparedStatement",
                "athena:GetPreparedStatement",
                "athena:DeletePreparedStatement"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowGlueSchemaManipulations",
            "Effect": "Allow",
            "Action": [
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:GetTable",
                "glue:GetTables",
                "glue:GetPartition",
                "glue:GetPartitions"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowQueryEditorToAccessWorkGroup",
            "Effect": "Allow",
            "Action": "athena:GetWorkGroup",
            "Resource": "arn:aws:athena:*:111122223333:workgroup*"
        },
        {
            "Sid": "AllowConfigurationForWorkspaceCollaboration",
            "Action": [
                "elasticmapreduce:UpdateEditor",
                "elasticmapreduce:PutWorkspaceAccess",
                "elasticmapreduce:DeleteWorkspaceAccess",
```

```
                "elasticmapreduce:ListWorkspaceAccessIdentities"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "elasticmapreduce:ResourceTag/creatorUserId":
 "${aws:userId}"
                }
            }
        },
        {
            "Sid": "DescribeNetwork",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ListIAMRoles",
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AssumeRole",
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": "*"
        }
    ]
}
```

以下信任策略允许 EMR Studio 扮演该角色：

> **Note**
>
> 使用 EMR Studio 工作区和 EMR 笔记本需额外配置权限。有关更多信息，请参阅为 EMR Studio 用户创建权限策略。

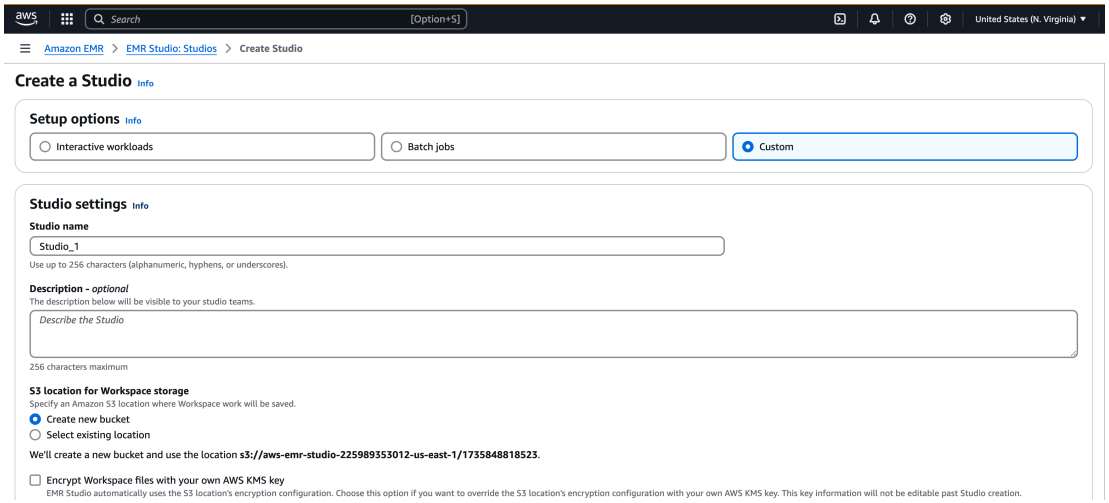
您可通过以下链接获取更多信息：

- 使用客户管理型策略定义自定义 IAM 权限
- EMR Studio 服务角色权限

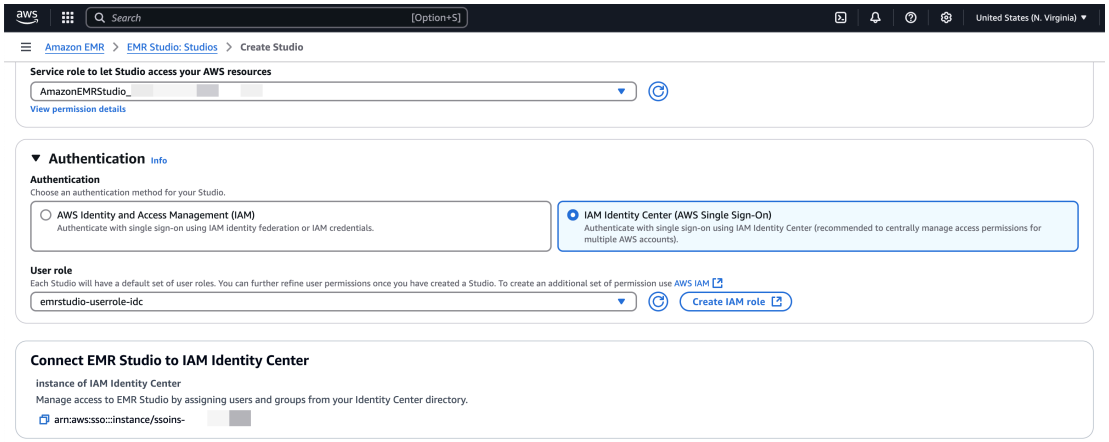
步骤 2：创建并配置 EMR Studio

本步骤中，您将在 EMR Studio 控制台创建 Amazon EMR Studio，并使用在 步骤 1：为 EMR Studio 创建所需的 IAM 角色 中创建的 IAM 角色。

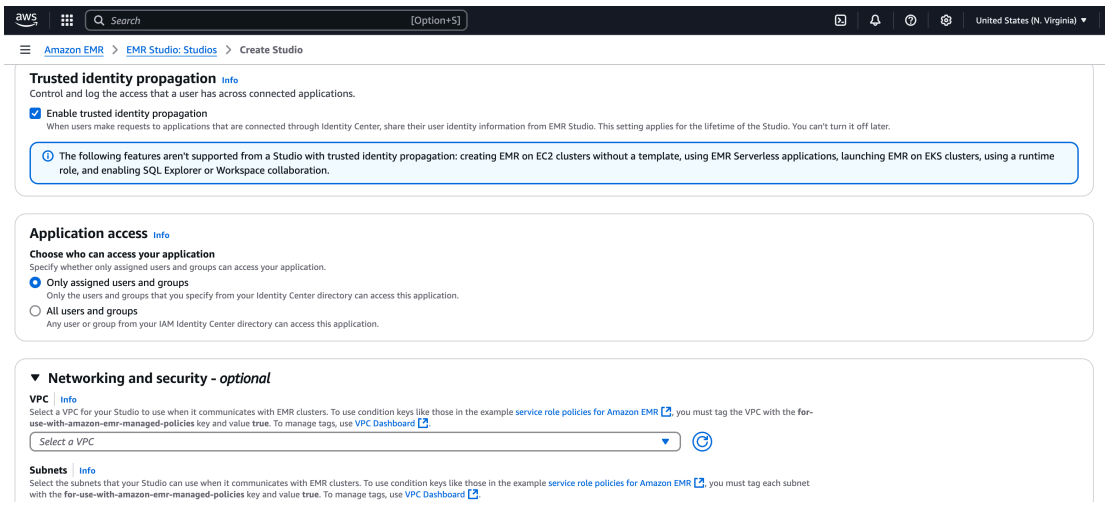
1. 访问 EMR Studio 控制台，选择创建 Studio 并选择自定义设置选项。您可以创建新的 S3 存储桶或使用现有存储桶。您可勾选使用自己的 KMS 密钥加密工作区文件选项。有关更多信息，请参阅 Amazon Key Management Service。



2. 在允许 Studio 访问您资源的服务角色下，从下拉菜单中选择在 步骤 1：为 EMR Studio 创建所需的 IAM 角色 中创建的服务角色。
3. 在身份验证下选择 IAM Identity Center。选择在 步骤 1：为 EMR Studio 创建所需的 IAM 角色 中创建的用户角色。



4. 勾选可信身份传播选项框。在应用程序访问部分选择仅已分配的用户和组，这样仅授权的用户和组可访问该 Studio。
5. （可选）– 如果您将该 Studio 与 EMR 集群配合使用，可配置 VPC 和子网。

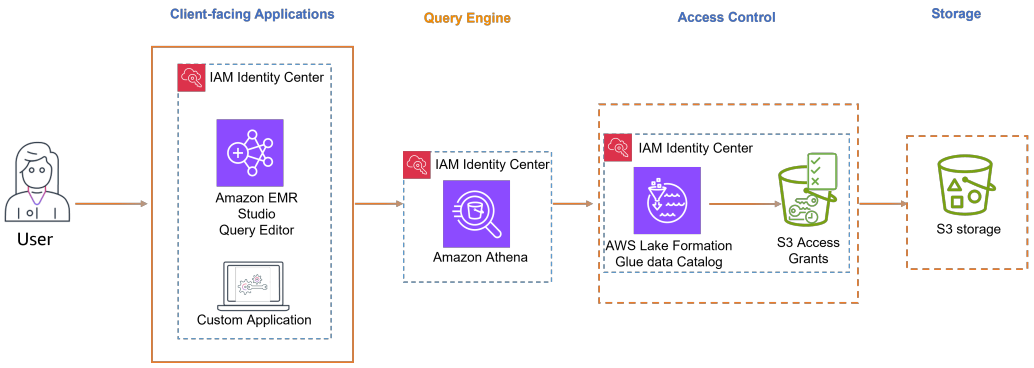


6. 审核所有详细信息并选择创建 Studio。
7. 配置 Athen WorkGroup a 或 EMR 集群后，请登录 Studio 的 URL，以：
   a. 通过查询编辑器运行 Athena 查询。
   b. 在工作区中通过 Jupyter Notebook 运行 Spark 作业。

使用 Amazon Athena 的可信身份传播

启用可信身份传播的步骤取决于您的用户是与托管应用程序交互还是与客户 Amazon 托管的应用程序进行交互。下图显示了面向客户端的应用程序（无论是 Amazon 托管应用程序还是外部应用程序）的可信身份传播配置，该配置使用 Amazon Athena 通过 Amazon Lake Formation 和 Amazon S3 提供的访问控制来 Amazon 查询 Amazon S3 数据。Access Grants

> **Note**
>
> - Amazon Athena 的可信身份传播需使用 Trino。
> - 不支持通过 ODBC 和 JDBC 驱动程序连接到 Amazon Athena 的 Apache Spark 和 SQL 客户端。



Amazon 托管应用程序

以下面向客户端的 Amazon 托管应用程序支持通过 Athena 进行可信身份传播：

- Amazon EMR Studio

如需启用可信身份传播，请执行以下步骤：

- 设置 Amazon EMR Studio 作为 Athena 的面向客户端应用程序。启用可信身份传播后，需通过 EMR Studio 中的查询编辑器运行 Athena 查询。
- 设置 Athena 工作组。
- 设置 Amazon Lake Formation为根据 IAM Identity Center 中的用户或群组对 Amazon Glue 表启用精细访问控制。
- 设置 Amazon S3 Access Grants，以便允许临时访问 S3 中的底层数据位置。

> **Note**
>
> Lake Formation 和 Amazon S3 Access Grants 都需要对亚马逊 S3 中的 Athena 查询结果进行访问控制。 Amazon Glue Data Catalog

客户托管的应用程序

要为自定义开发的应用程序的用户启用可信身份传播，请参阅Amazon 安全博客中的使用可信身份传播 Amazon Web Services 服务 以编程方式访问。

设置 Amazon Athena 工作组的可信身份传播

以下过程将引导您设置 Amazon Athena 工作组以实现可信身份传播。

先决条件

在开始本教程之前，您需要设置以下方面：

1. 启用 IAM 身份中心。建议使用组织实例。有关更多信息，请参阅 先决条件和注意事项。
2. 将身份源中的用户和组配置到 IAM Identity Center。
3. 该配置需要依赖 Amazon EMR Studio、Amazon Lake Formation 和 Amazon S3 访问权限管控。

设置 Athena 的可信身份传播

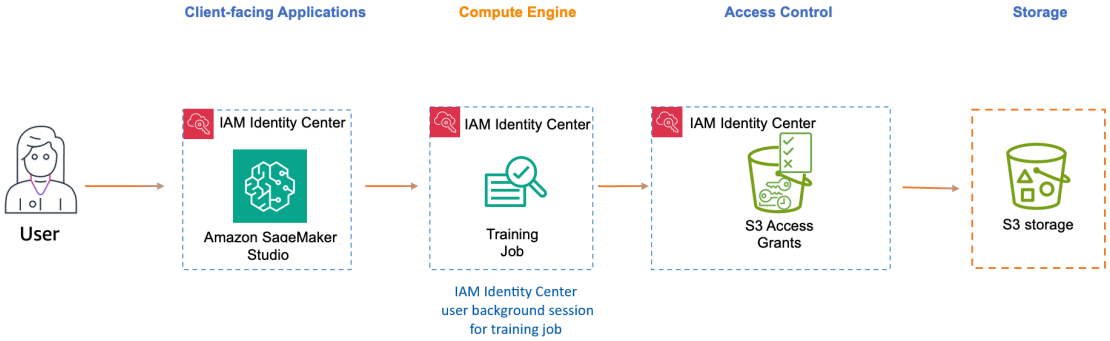
要设置 Athena 的可信身份传播，Athena 管理员必须：

1. 查看使用已启用 IAM Identity Center 的 Athena 工作组的注意事项和限制。
2. 创建启用 IAM Identity Center 的 Athena 工作组。

使用 Amazon SageMaker Studio 进行可信身份传

A@@ mazon SageMaker Studio 与 IAM 身份中心集成，它支持用户后台会话和可信身份传播。用户后台会话允许用户在 SageMaker Studio 上启动长时间运行的作业，而无需在作业运行时保持登录状态。作业将立即在后台运行，并使用启动作业的用户的权限。即使用户关闭计算机、IAM Identity Center 登录会话过期或用户退出 Amazon Web Services 访问门户，该作业仍可以继续运行。用户后台会话的默认持续时间为 7 天，但您可以指定最长 90 天的持续时间。可信身份传播支持基于用户身份或组成员身份，为 Amazon S3 存储桶等 Amazon 资源提供细粒度访问权限。

下图显示了 SageMaker Studio 的可信身份传播配置，可访问存储在 Amazon S3 存储桶中的数据。IAM Identity Center 已启用用户后台会话，这允许 SageMaker Studio 训练作业在后台运行。训练数据的访问控制由 Amazon S3 Access Grants 提供。



Amazon 托管应用程序

以下面向客户端的 Amazon 托管应用程序支持可信身份传播：

- 亚马逊 SageMaker Studio

如需启用可信身份传播和用户后台会话，请执行以下步骤：

- 将 SageMaker Studio 设置为面向客户端的应用程序。
- 设置 Amazon S3 Access Grants，以便允许临时访问 Amazon S3 中的底层数据位置。

使用 SageMaker Studio 设置可信身份传播

以下过程将引导您完成设置 SageMaker Studio 以进行可信身份传播和用户后台会话的过程。

先决条件

开始本教程之前，您需要完成以下任务：

1. 启用 IAM 身份中心。需使用组织实例。有关更多信息，请参阅 先决条件和注意事项。
2. 将身份源中的用户和组配置到 IAM Identity Center。
3. 在 IAM Identity Center 控制台中确认已启用用户后台会话。默认情况下，用户后台会话处于启用状态，会话持续时间设置为 7 天。您可以修改此持续时间。

要从 SageMaker Studio 设置可信身份传播， SageMaker Studio 管理员必须执行以下步骤。

步骤 1：在新的 Studio 域或现有 SageMaker Studio 域中启用可信身份传播

SageMaker Studio 使用域来组织用户个人资料、应用程序及其相关资源。要启用可信身份传播，必须按照以下步骤创建 SageMaker Studio 域或修改现有域。

1. 打开 SageMaker AI 控制台，导航到“域”，然后执行以下任一操作。

   - 使用组织安装程序创建新的 SageMaker Studio 域。

     选择为组织设置，然后执行以下操作：

     - 选择 Amazon Identity Center 作为身份验证方式。
     - 勾选为该域上的所有用户启用可信身份传播复选框。
   - 修改现有的 SageMaker Studio 域名。
     - 选中使用 IAM Identity Center 进行身份验证的现有域。

       > **Important**
       >
       > 仅在使用 IAM 身份中心进行身份验证的 SageMaker Studio 域中支持可信身份传播。如果该域使用 IAM 进行身份验证，则无法更改身份验证方式，因此也无法启用可信身份传播。

     - 编辑域设置。编辑身份验证和权限设置，启用可信身份传播。
2. 继续执行步骤 2：配置默认域执行角色。 SageMaker Studio 域的用户需要此角色才能访问其他 Amazon 服务，例如 Amazon S3。

步骤 2：配置默认域执行角色与角色信任策略

域执行角色是 SageMaker Studio 域代表网域中所有用户担任的 IAM 角色。您分配给该角色的权限决定了 SageMaker Studio 可以执行的操作。

1. 要创建或选择域执行角色，请执行以下任一操作：

   - 通过组织设置创建或选择角色。
     - 打开 SageMaker AI 控制台，按照步骤 2：配置角色和机器学习活动中的控制台指南创建新的域执行角色或选择现有角色。
     - 完成其余设置步骤以创建您的 SageMaker Studio 域名。
   - 手动创建执行角色。

- 打开 IAM 控制台并自行创建执行角色。

2. 更新附加到域执行角色的信任策略，使其包含以下两个操作：sts:AssumeRole 和 sts:SetContext。有关如何查找 SageMaker Studio 域的执行角色的信息，请参阅获取域执行角色。

   信任策略用于指定可以扮演该角色的身份。此策略是允许 SageMaker Studio 服务担任域执行角色所必需的。添加这两个操作，使其在策略中显示如下。

```
{

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


    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "sagemaker.amazonaws.com"
                ]
            },
            "Action": [
                "sts:AssumeRole",
                "sts:SetContext"
            ]
        }
    ]
}
```

步骤 3：验证域执行角色所需的 Amazon S3 访问权限管控权限

要使用 Amazon S3 访问授权，您必须将包含以下权限的 SageMaker Studio 域执行角色附加权限策略（内联策略或客户托管策略）。

```
{

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

    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": [
                "s3:GetDataAccess",
                "s3:GetAccessGrantsInstanceForPrefix"
                ],
            "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
        }
    ]
}
```

如果您暂无包含这些权限的策略，请参阅《Amazon Identity and Access Management 用户指南》中的添加和移除 IAM 身份权限。

步骤 4：为域分配组和用户

按照添加群组和用户中的步骤将群组和用户分配到 SageMaker Studio 域。

步骤 5：设置 Amazon S3 访问权限管控

要设置 Amazon S3 访问权限管控，请遵循通过 IAM Identity Center 配置可信身份传播的 Amazon S3 访问权限管控中的步骤。按照分步指引完成以下任务：

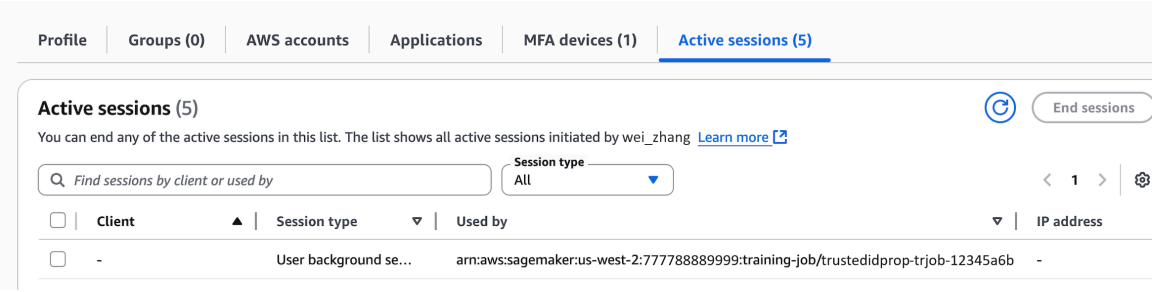
1. 创建 Amazon S3 访问权限管控实例。
2. 在该实例中注册位置。
3. 创建授权，允许特定 IAM Identity Center 用户或组访问指定的 Amazon S3 位置或这些位置内的子集（例如特定前缀）。

步骤 6：提交 SageMaker 训练作业并查看用户后台会话详情

在 SageMaker Studio 中，启动新的 Jupyter 笔记本并提交训练作业。作业运行期间，完成以下步骤以查看会话信息并验证用户后台会话上下文是否处于活跃状态。

1. 打开 IAM Identity Center 控制台。
2. 选择用户。
3. 在用户页面上，选择要管理其会话的用户的用户名。这会让您转至包含用户信息的页面。
4. 在用户页面上，选择活跃会话选项卡。活跃会话旁边括号中的数字表示该用户处于活跃状态的会话数。
5. 要按使用该会话的作业的 Amazon 资源名称（ARN）搜索会话，请在会话类型列表中选择用户后台会话，然后在搜索框中输入作业 ARN。

以下示例展示了使用用户后台会话的训练作业在用户的活跃会话选项卡中的显示形式。



步骤 7：查看 CloudTrail 日志以验证可信身份的传播 CloudTrail

启用可信身份传播后，操作会显示在onBehalfOf元素下方 CloudTrail 的事件日志中。userId 字段将显示启动训练作业的 IAM Identity Center 用户的 ID。以下 CloudTrail 事件捕获了可信身份传播的过程。

```
                        "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA123456789EXAMPLE:SageMaker",
    "arn": "arn:aws:sts::111122223333:assumed-role/SageMaker-
ExecutionRole-20250728T125817/SageMaker",
    "accountId": "111122223333",
    "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
    "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AROA123456789EXAMPLE",
            "arn": "arn:aws:iam::111122223333:role/service-role/SageMaker-
ExecutionRole-20250728T125817",
            "accountId": "111122223333",
            "userName": "SageMaker-ExecutionRole-20250728T125817"
        },
        "attributes": {
            "creationDate": "2025-07-29T17:17:10Z",
            "mfaAuthenticated": "false"
        }
    },
    "onBehalfOf": {
        "userId": "2801d3e0-f0e1-707f-54e8-f558b19f0a10",
        "identityStoreArn": "arn:aws:identitystore::777788889999:identitystore/
d-1234567890"
    }
},
```

运行时系统注意事项

如果管理员将长时间运行的训练或处理作业设置MaxRuntimeInSeconds为低于用户后台会话持续时间， SageMaker Studio 会运行该作业的时间至少为用户后台会话持续时间中的一个MaxRuntimeInSeconds 或一个。

有关更多信息 MaxRuntimeInSeconds，请参阅 Amazon SageMaker API 参考中的`CreateTrainingJob`StoppingCondition参数指南。

授权服务

在所有分析和数据湖仓使用案例中，您可以通过以下服务实现细粒度访问控制：

- Amazon Lake Formation -有关指导，请参阅设置 Amazon Lake Formation 使用 IAM 身份中心。
- Amazon S3 Access Grants - 有关指导，请参阅 使用 IAM Identity Center 设置 Amazon S3 访问权限管控。

设置 Amazon Lake Formation 使用 IAM 身份中心

Amazon Lake Formation 是一项托管服务，可简化 Amazon上数据湖的创建和管理。它可自动化数据收集、编目和安全配置，为存储和分析多种数据类型提供集中式存储库。Lake Formation 提供精细的访问控制并与各种 Amazon 分析服务集成，使组织能够高效地设置、保护数据湖并从中获取见解。

按照以下步骤配置 Lake Formation，使其能够通过 IAM Identity Center 和可信身份传播，基于用户身份授予数据权限。

先决条件

在开始本教程之前，您需要设置以下方面：

- 启用 IAM 身份中心。建议使用组织实例。有关更多信息，请参阅 先决条件和注意事项。

设置可信身份传播的步骤

1. 集成 IAM Identity Center 与 Amazon Lake Formation，请遵循将 Lake Formation 与 IAM Identity Center 连接中的指引。

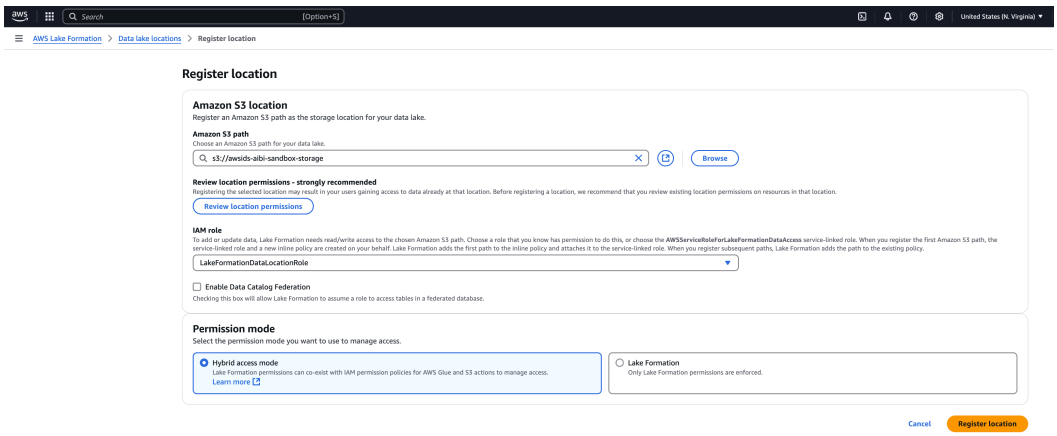
> **Important**
>
> 如果您暂无 Amazon Glue Data Catalog 表，则必须创建这些表才能通过 Amazon Lake Formation 向 IAM Identity Center 用户和组授予访问权限。有关更多信息，请参阅在 Amazon Glue Data Catalog中创建对象。

2. 注册数据湖位置。

   注册 Glue 表数据所在的 S3 位置。这样，Lake Formation 将在查询表时提供对所需 S3 位置的临时访问权限，从而无需在服务角色中包含 S3 权限（例如，上配置的 Athena 服务角色）。WorkGroup

   a. 导航到 Amazon Lake Formation 控制台导航窗格中 “管理” 部分下的数据湖位置。选择注册位置。

      这将允许 Lake Formation 生成具有访问 S3 数据位置所需权限的临时 IAM 凭据。



   b. 在 Amazon S3 路径字段中，输入 Amazon Glue 表数据位置的 S3 路径。

   c. 在 IAM 角色部分，如果要配合可信身份传播使用，请不要选择服务关联角色。创建具有以下权限的单独角色。

      要使用这些政策，请用您自己的信息替换示例*italicized placeholder text*中的策略。有关详细操作指引，请参阅创建策略或编辑策略。权限策略应授予对路径中指定的 S3 位置的访问权限：

      i. 权限策略：

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "LakeFormationDataAccessPermissionsForS3",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::Your-S3-Bucket/*"
            ]
        },
        {
            "Sid":
 "LakeFormationDataAccessPermissionsForS3ListBucket",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::Your-S3-Bucket"
            ]
        },
        {
            "Sid": "LakeFormationDataAccessServiceRolePolicy",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": [
                "arn:aws:s3:::*"
            ]
        }
    ]
}
```

ii. 信任关系：应包含 `sts:SectContext`（可信身份传播的必需操作）。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "lakeformation.amazonaws.com"
            },
            "Action": [
                "sts:AssumeRole",
                "sts:SetContext"
            ]
        }
    ]
}
```

> **Note**
>
> 向导创建的 IAM 角色为服务关联角色，不包含 `sts:SetContext` 操作权限。

d. 创建 IAM 角色后，选择注册位置。

使用 Lake Formation 进行可信身份传播 Amazon Web Services 账户

Amazon Lake Formation 支持使用 Amazon Resource Access Manager (RAM) 共享表，当授予者账户 Amazon Web Services 账户 和被授权者账户处于相同 Amazon Web Services 区域、相同且共享相同的 IAM Identity Center 组织实例时 Amazon Organizations，它可以进行可信身份传播。有关更多信息，请参阅 Lake Formation 中的Cross-account 数据共享。

使用 IAM Identity Center 设置 Amazon S3 访问权限管控

Amazon S3 Access Grants 提供灵活的基于身份的细粒度访问控制能力，可用于授权访问 S3 位置。您可以通过 Amazon S3 Access Grants，直接向企业用户和组授予 Amazon S3 存储桶的访问权限。按照以下步骤启用 S3 Access Grants 与 IAM Identity Center 的集成，实现可信身份传播。

先决条件

在开始本教程之前，您需要设置以下方面：

- 启用 IAM 身份中心。建议使用组织实例。有关更多信息，请参阅 先决条件和注意事项。

通过 IAM Identity Center 配置可信身份传播的 S3 访问权限管控

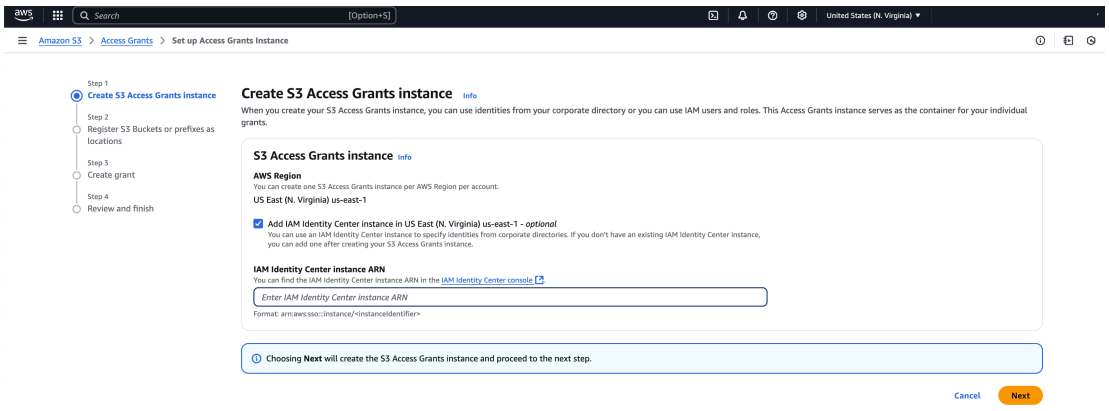
如果你已经有一台 Amazon S3 Access Grants 具有注册位置的实例，请按照以下步骤操作：

1. 关联您的 IAM Identity Center 实例。
2. 创建授权。

如果您尚未创建 Amazon S3 Access Grants 但是，请按照以下步骤操作：

1. 创建 S3 Access Grants 实例-您可以为每个Access Grants实例创建一个 S3 实例 Amazon Web Services 区域。创建 S3 Access Grants 实例时，请务必勾选添加 IAM Identity Center 实例选项框，并提供您的 IAM Identity Center 实例 ARN。选择下一步。

   下图展示了 Amazon S3 Access Grants 控制台中的“创建 S3 Access Grants 实例”页面：



2. 注册营业地点-在您的账户中创建 Amazon S3 Access Grants 实例后，您就可以在该实例中注册一个 S3 地点。 Amazon Web Services 区域 S3 Access Grants 位置会将默认 S3 区域（`S3://`）、存储桶或前缀映射到某个 IAM 角色。S3 Access Grants 代入此 Amazon S3 角色，来向正在访问该特定位置的被授权者提供临时凭证。您必须先在 S3 Access Grants 实例中注册至少一个位置，然后才能创建访问权限管控。

对于位置范围，请指定 `s3://`，其中包含该区域内的所有存储桶。这是大多数使用案例的推荐位置范围。如果您有高级访问管理使用案例，可将位置范围设置为特定存储桶 `s3://bucket` 或存储桶内的前缀 `s3://bucket/prefix-with-path`。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的注册位置。

> **Note**
>
> 确保您要授予访问权限的 Amazon Glue 表的 S3 位置包含在此路径中。

该过程要求您为该位置配置 IAM 角色。该角色应包含访问该位置范围的权限。您可以通过 S3 控制台向导创建该角色。您需要在该 IAM 角色的策略中指定您的 S3 Access Grants 实例 ARN。您的 S3 Access Grants 实例 ARN 的默认值为 `arn:aws:s3:Your-Region:Your-AWS-Account-ID:access-grants/default`。

以下权限策略示例为您创建的 IAM 角色授予 Amazon S3 权限。后续的信任策略示例允许 S3 Access Grants 服务主体扮演该 IAM 角色。

a. 权限策略

要使用这些政策，请用您自己的信息替换示例*italicized placeholder text*中的策略。有关详细操作指引，请参阅创建策略或编辑策略。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ObjectLevelReadPermissions",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion",
                "s3:GetObjectAcl",
                "s3:GetObjectVersionAcl",
                "s3:ListMultipartUploadParts"
            ],
            "Resource": [
```

```
                "arn:aws:s3:::*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "111122223333"
                },
                "ArnEquals": {
                    "s3:AccessGrantsInstanceArn": [
                    "arn:aws:s3:::access-grants/instance-id"
                    ]
                }
            }
        },
        {
            "Sid": "ObjectLevelWritePermissions",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectVersionAcl",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:AbortMultipartUpload"
            ],
            "Resource": [
                "arn:aws:s3:::*"
            ],
            "Condition": {
                "StringEquals": {
                "aws:ResourceAccount": "111122223333"
                },
                "ArnEquals": {
                    "s3:AccessGrantsInstanceArn": [
                    "arn:aws:s3:::access-grants/instance-id"
                    ]
                }
            }
        },
        {
            "Sid": "BucketLevelReadPermissions",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
```

```
            "Resource": [
                "arn:aws:s3:::*"
            ],
            "Condition": {
                "StringEquals": {
                "aws:ResourceAccount": "111122223333"
                },
                "ArnEquals": {
                    "s3:AccessGrantsInstanceArn": [
                    "arn:aws:s3:::access-grants/instance-id"
                    ]
                }
            }
        },
        {
            "Sid": "OptionalKMSPermissionsForSSEEncryption",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

b. 信任策略

在 IAM 角色信任策略中，向 S3 访问权限管控服务 (access-grants.s3.amazonaws.com)主体授予对您创建的 IAM 角色的访问权限。为此，您可以创建一个包含以下语句的 JSON 文件。要将信任策略添加到您的账户，请参阅使用自定义信任策略创建角色。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1234567891011",
```

```
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole",
                "sts:SetSourceIdentity"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333",
                    "aws:SourceArn": "Your-Custom-Access-Grants-Location-
ARN"
                }
            }
        },

        {
            "Sid": "Stmt1234567891012",
            "Effect": "Allow",
            "Action": "sts:SetContext",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333",
                    "aws:SourceArn": "Your-Custom-Access-Grants-Location-
ARN"
                },
                "ForAllValues:ArnEquals": {
                    "sts:RequestContextProviders":
 "arn:aws:iam::aws:contextProvider/IdentityCenter"
                }
            }
        }
    ]
}
```

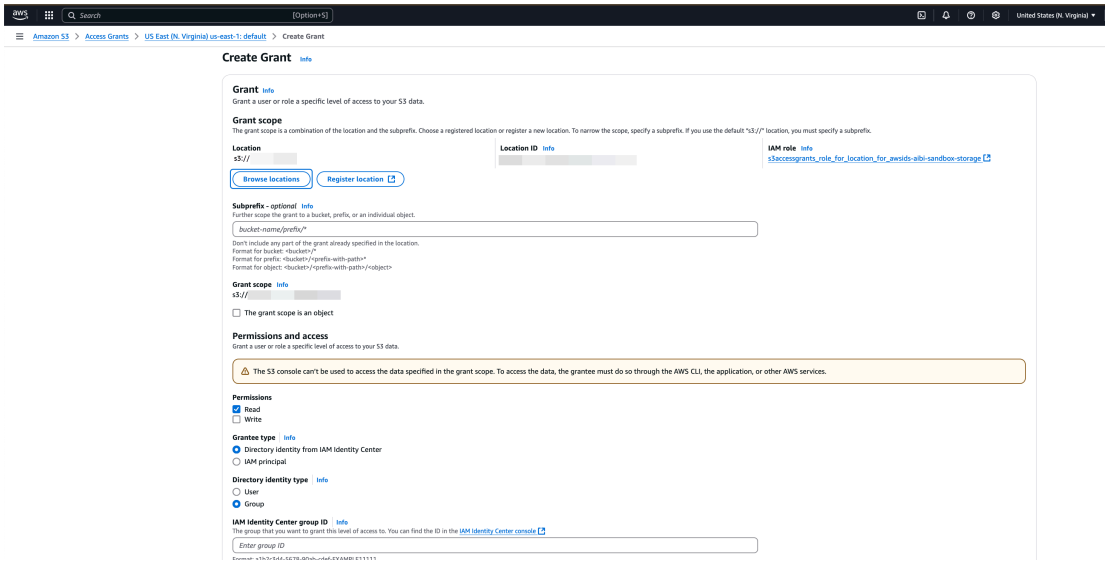
创建 Amazon S3 访问权限管控

如果您已创建带有已注册位置的 Amazon S3 Access Grants 实例，且已关联 IAM Identity Center 实例，则可以创建授权。在 S3 控制台的创建授权页面，完成以下操作：

创建授权

1. 选择上一步创建的位置。您可以通过添加子前缀缩小授权范围。子前缀可以是 `bucket`、`bucket/prefix` 或存储桶中的对象。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的子前缀。
2. 在权限和访问下，根据需求选择读取和/或写入。
3. 在授权方类型中，选择来自 IAM Identity Center 的目录身份。
4. 提供 IAM Identity Center 用户或组 ID。您可以在 IAM Identity Center 控制台的用户和组区域中找到用户和组 ID。选择下一步。
5. 在审核并完成页面，确认 S3 Access Grant 的设置，然后选择创建授权。

   下图展示了 Amazon S3 Access Grants 控制台中的“创建授权”页面：



设置您自己的 OAuth 2.0 应用程序

可信身份传播使客户托管的应用程序能够代表用户请求访问 Amazon 服务中的数据。对数据访问的管理基于用户身份，因此，管理员可以根据用户的现有用户和组成员资格，授予访问权限。用户的身份、代表他们执行的操作以及其他事件都记录在服务特定的日志和 CloudTrail事件中。

通过可信身份传播，用户可以登录客户自主管理型应用程序，而该应用程序可以在请求中传递用户的身份，以访问 Amazon Web Services 服务中的数据。

> **Important**
>
> 要访问客户托管的应用程序 Amazon Web Services 服务，必须从 IAM Identity Center 外部的可信令牌发行者那里获取令牌。可信令牌发布者是可创建签名令牌的 OAuth 2.0 授权服务器。这些令牌授权发起访问请求 Amazon Web Services 服务（接收应用程序）的应用程序。有关更多信息，请参阅 通过可信令牌发布者使用应用程序。

主题

设置客户托管的 OAuth 2.0 应用程序以使用可信身份传播

要设置客户托管的 OAuth 2.0 应用程序，以实现可信身份传播，您必须先将其添加到 IAM Identity Center。使用以下过程将您的应用程序添加到 IAM Identity Center。

主题

步骤 1：选择应用程序类型

1. 打开 IAM Identity Center 控制台。
2. 选择应用程序。
3. 选择客户托管选项卡。
4. 选择添加应用程序。
5. 在选择应用程序类型页面，选择设置首选项下的我有想设置的应用程序。
6. 在应用程序类型下，选择 OAuth 2.0。

7. 选择下一步，进入下一页：步骤 2：指定应用程序详细信息。

步骤 2：指定应用程序详细信息

1. 在指定应用程序详细信息页面的应用程序名称和描述下，输入应用程序的显示名称，如 **MyApp**。然后，输入描述。
2. 在用户和组分配方法下，选择下列选项之一：

   - 需要分配 - 仅允许分配给此应用程序的 IAM Identity Center 用户和组访问该应用程序。

     应用程序图块可见性-只有直接或通过群组分配分配到应用程序的用户才能在访问门户中查看应用程序图块，前提是应用程序在 Amazon Web Services 访问门户中的 Amazon Web Services 可见性设置为 “可见”。

   - 不需要分配 - 允许所有授权的 IAM Identity Center 用户和组访问此应用程序。

     应用程序图块可见性-除非应用程序在 Amazon Web Services 访问门户中的可见性设置为 “不可见”，否则登录 Amazon Web Services 访问门户的所有用户都可以看到应用程序图块。

3. 在Amazon Web Services 访问门户下，输入用户可以访问应用程序的 URL，并指定应用程序图块在 Amazon Web Services 访问门户中是可见还是不可见。如果选择不可见，则即使已分配的用户也无法查看应用程序磁贴。
4. 在标签（可选）下，选择添加新标签，然后为键和值（可选）指定值。

   有关标签的信息，请参阅 为资源添加标签 Amazon IAM Identity Center。
5. 选择下一步，进入下一页：步骤 3：指定身份验证设置。

步骤 3：指定身份验证设置

要将支持 OAuth 2.0 的客户托管应用程序添加到 IAM Identity Center，您必须指定可信令牌发布者。可信令牌发布者是可创建签名令牌的 OAuth 2.0 授权服务器。这些令牌用于对发起请求以访问 Amazon 托管应用程序（接收端应用程序）的应用程序（请求端应用程序）进行授权。

1. 在指定身份验证设置页面的可信令牌发布者下，执行以下任一操作：

   - 使用现有的可信令牌发布者：

     在要使用的可信令牌发布者的名称旁边，选择其复选框。

   - 添加新的可信令牌发布者：

1. 选择创建可信令牌发布者。
2. 将打开一个新的浏览器标签页。按照 如何向 IAM Identity Center 控制台添加可信令牌发布者 中的步骤 5 至步骤 8 操作。
3. 完成这些步骤后，返回您正用于设置应用程序的浏览器窗口，然后选择刚刚添加的可信令牌发布者。
4. 在可信令牌发布者列表中，选中刚刚添加的可信令牌发布者名称旁边的复选框。

   选择可信令牌发布者后，将出现配置选定的可信令牌发布者部分。

2. 在配置选定的可信令牌发布者下，输入 Aud 声明。Aud 声明用于确定可信令牌发布者生成的令牌的目标受众（接收者）。有关更多信息，请参阅 Aud 声明。
3. 要让用户在使用此应用程序时无需重新进行身份验证，请选择启用刷新令牌授予。选中后，此选项将每 60 分钟刷新一次会话的访问令牌，直到会话过期或用户结束会话。
4. 选择下一步，进入下一页：步骤 4：指定应用程序凭证。

步骤 4：指定应用程序凭证

完成此过程中的步骤，为应用程序指定用于与可信应用程序执行令牌交换操作的凭证。这些凭证将在一个基于资源的策略中使用。该策略要求您指定一个主体，该主体必须有权执行该策略中指定的操作。即使可信应用程序位于同一个 Amazon Web Services 账户中，您也必须指定一个主体。

> **Note**
>
> 在使用策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限权限。

该策略需要使用 `CreateTokenWithIAM` API 操作。有关该策略的更多信息以及可根据您的环境需求调整的示例，请参阅 Resource-based IAM 身份中心 IAM 身份中心的策略示例。

1. 在指定应用程序凭证页面，执行以下任一操作：

   - 要快速指定一个或多个 IAM 角色：
     1. 选择输入一个或多个 IAM 角色。
     2. 在输入 IAM 角色下，指定现有 IAM 角色的 Amazon 资源名称 (ARN)。要指定 ARN，请使用以下语法。由于 IAM 资源是全球资源，因此，ARN 的区域部分是空的。

```
arn:aws:iam::account:role/role-name-with-path
```

有关更多信息，请参阅Amazon Identity and Access Management 用户指南中的使用基于资源的策略和 IAM ARN 进行Cross-account 访问。

- 要手动编辑策略（如果指定非Amazon 凭据，则为必填项），请执行以下操作：
  1. 选择编辑应用程序策略。
  2. 在 JSON 文本框中键入或粘贴文本，修改策略。
  3. 解决策略验证过程中产生的任何安全警告、错误或常规警告。有关更多信息，请参阅 Amazon Identity and Access Management 用户指南中的验证 IAM 策略。

2. 选择下一步，进入下一页：步骤 5：审核和配置。

步骤 5：审核和配置

1. 在审查和配置页面中，审查您所做的选择。要进行更改，请选择所需的配置部分，选择编辑，然后进行所需的更改。
2. 完成后，选择添加应用程序。
3. 您添加的应用程序将显示在客户托管的应用程序列表中。
4. 在 IAM Identity Center 中设置客户托管的应用程序后 Amazon Web Services 服务，必须指定一个或多个用于身份传播的受信任的应用程序。这样，用户就能够登录客户托管的应用程序，并访问可信应用程序中的数据。

   有关更多信息，请参阅 指定可信的应用程序。

指定可信的应用程序

设置客户托管的应用程序后，必须为身份传播指定一个或多个可信 Amazon 服务或可信应用程序。指定一项 Amazon 服务，该服务包含客户托管应用程序的用户需要访问的数据。当您的用户登录客户托管的应用程序时，该应用程序会将用户的身份传递给可信的应用程序。

使用以下过程选择服务，然后为该服务指定要信任的单个应用程序。

1. 打开 IAM Identity Center 控制台。
2. 选择应用程序。
3. 选择客户托管选项卡。

4. 在客户托管的应用程序列表中，选择要发起访问请求的 OAuth 2.0 应用程序。这是用户要登录的应用程序。
5. 在详细信息页面的用于身份传播的可信应用程序下，选择指定可信应用程序。
6. 在设置类型下，选择单个应用程序并指定访问权限，然后选择下一步。
7. 在选择服务页面，选择拥有所需应用程序的 Amazon 服务，客户托管的应用程序可以信任这些应用程序进行身份传播，然后选择下一步。

   您选择的服务定义了可以信任的应用程序。您将在下一个步骤中选择应用程序。
8. 在选择应用程序页面，选择单个应用程序，为每个可以接收访问请求的应用程序选择复选框，然后选择下一步。
9. 在配置访问权限页面的配置方法下，执行以下任一操作：

   - 选择每个应用程序的访问权限 - 选择此选项可为每个应用程序配置不同的访问权限级别。选择要为其配置访问权限级别的应用程序，然后选择编辑访问权限。在要应用的访问权限级别中，根据需要更改访问权限级别，然后选择保存更改。
   - 对所有应用程序应用相同的访问权限级别 - 如果不需要针对每个应用程序配置访问权限级别，请选择此选项。
10. 选择下一步。
11. 在审查配置页面中，审查您所做的选择。要进行更改，请选择所需的配置部分，选择编辑访问权限，然后进行所需的更改。
12. 完成后，选择信任应用程序。

通过可信令牌发布者使用应用程序

可信令牌发行者使您能够在外部进行身份验证的应用程序中使用可信身份传播。 Amazon通过可信令牌发行机构，您可以授权这些应用程序代表其用户提出访问 Amazon 托管应用程序的请求。

以下主题介绍了可信令牌发布者的工作方式，并提供了设置指导。

主题

- Identity-enhanced IAM 角色会话

可信令牌发布者概述

可信身份传播提供了一种机制，允许在外部进行身份验证的 Amazon 应用程序使用可信令牌颁发者代表其用户发出请求。可信令牌发布者是可创建签名令牌的 OAuth 2.0 授权服务器。这些令牌授权那些发起请求（请求应用程序）以访问 Amazon Web Services 服务（接收应用程序）的应用程序。请求端应用程序代表经过可信令牌发布者验证身份的用户发起访问请求。可信令牌发布者和 IAM Identity Center 都知道这些用户。

Amazon Web Services 服务 接收请求的用户根据身份中心目录中显示的用户和群组成员资格来管理对其资源的精细授权。 Amazon Web Services 服务 不能直接使用来自外部令牌发行者的代币。

为了解决这个问题，IAM Identity Center 为请求端应用程序或请求端应用程序使用的 Amazon 驱动程序提供了一种方法，将可信令牌发布者发布的令牌交换为 IAM Identity Center 生成的令牌。IAM Identity Center 生成的令牌指向相应的 IAM Identity Center 用户。请求端应用程序或驱动程序使用新令牌向接收端应用程序发起请求。由于新令牌引用了 IAM Identity Center 中的相应用户，因此接收端应用程序可以根据 IAM Identity Center 中显示的用户或其组成员资格，对请求的访问权限授权。

> **Important**
>
> 选择将 OAuth 2.0 授权服务器添加为可信令牌发布者是一项需要仔细考虑的安全决定。仅选择您信任的可信令牌发布者执行以下任务：
>
> - 对令牌中指定的用户进行身份验证。
> - 授权该用户访问接收端应用程序。
> - 生成一个令牌，让 IAM Identity Center 可以将它交换成 IAM Identity Center 创建的令牌。

针对可信令牌发布者的先决条件和注意事项

在设置可信令牌发布者之前，请先查看以下先决条件和注意事项。

- 可信令牌发布者的配置

  您必须配置 OAuth 2.0 授权服务器（可信令牌发布者）。尽管可信令牌发布者通常是您用作 IAM Identity Center 身份源的身份提供者，但也存在其他情况。有关如何设置可信令牌发布者的信息，请参阅相关身份提供者的文档。

> **Note**
>
> 您最多可以配置 10 个可信令牌发布者，将它们与 IAM Identity Center 搭配使用，为此，您只需将可信令牌发布者中每个用户的身份映射到 IAM Identity Center 中的相应用户即可。

- 创建令牌的 OAuth 2.0 授权服务器（可信令牌发布者）必须具有 OpenID Connect (OIDC) 发现端点，IAM Identity Center 可以使用该端点获取用于验证令牌签名的公钥。有关更多信息，请参阅 OIDC 发现端点 URL（发布者 URL）。
- 由可信令牌发布者颁发的令牌

  来自可信令牌发布者的令牌必须满足以下要求：

  - 令牌必须经过签名，并采用使用 RS256 算法的 JSON Web 令牌（JWT）格式。
  - 令牌必须包含以下声明：
    - 发布者（iss）– 颁发令牌的实体。此值必须与可信令牌发布者的 OIDC 发现端点（发布者 URL）中配置的值相匹配。
    - 主体（sub）– 经过身份验证的用户。
    - 受众（aud）– 令牌的预期接收者。将令牌与来自 IAM Identity Center 的令牌交换后会访问的 Amazon Web Services 服务 。有关更多信息，请参阅 Aud 声明。
    - 到期时间（exp）– 令牌到期的时间。
  - 令牌可以是身份令牌，也可以是访问令牌。
  - 令牌必须包含一个与一名 IAM Identity Center 用户具有唯一对应关系的属性。

  > **Note**
  >
  > 不支持对来自 Microsoft Entra ID 的 JWT 使用自定义签名密钥。如果要将 Microsoft Entra ID 令牌与可信令牌发布者配合使用，请勿使用自定义签名密钥。

- 可选声明

  IAM Identity Center 支持 RFC 7523 中定义的所有可选声明。有关更多信息，请参阅此 RFC 的第 3 节：JWT 格式和处理要求。

  例如，令牌可以包含 JTI (JWT ID) 声明。此声明（如果存在）可以防止具有相同 JTI 的令牌被重复用于令牌交换。有关 JTI 声明的更多信息，请参阅 JTI 声明详细信息。

- 使 IAM Identity Center 与可信令牌发布者协同工作的配置

您还必须启用 IAM Identity Center，为 IAM Identity Center 配置身份源，并预置与可信令牌发布者目录中的用户对应的用户。

为此，您必须执行以下任一操作：

- 使用身份管理系统 (SCIM) 2.0 协议，将用户同步到 IAM Cross-domain 身份中心。
- 直接在 IAM Identity Center 创建用户。

JTI 声明详细信息

如果 IAM Identity Center 收到交换令牌的请求，而该令牌已经被 IAM Identity Center 交换过，该请求将失败。要检测并防止重复使用令牌进行交换，您可以添加 JTI 声明。IAM Identity Center 可根据令牌中的声明，防止令牌被重放。

并非所有 OAuth 2.0 授权服务器都会向令牌添加 JTI 声明。有些 OAuth 2.0 授权服务器可能不允许您添加 JTI 作为自定义声明。支持使用 JTI 声明的 OAuth 2.0 授权服务器可能会仅将此声明添加到身份令牌或仅限访问令牌，也可能将其添加到两者。有关更多信息，请参阅 OAuth 2.0 授权服务器的文档。

有关构建交换令牌的应用程序信息，请参阅 IAM Identity Center API 文档。有关配置客户托管应用程序以获取和交换正确令牌的信息，请参阅该应用程序的文档。

可信令牌发布者的配置设置

以下各节描述了设置和使用可信令牌发布者所需的设置。

主题

OIDC 发现端点 URL（发布者 URL）

向 IAM Identity Center 控制台添加可信令牌发布者时，必须指定 OIDC 发现端点 URL。此 URL 通常是指其相对 URL，即 `/.well-known/openid-configuration`。在 IAM Identity Center 控制台，此 URL 称为发布者 URL。

> **Note**
>
> 必须粘贴发现端点 URL 中直至 `.well-known/openid-configuration` 前面的部分。如果 `.well-known/openid-configuration` 包含在 URL 中，则可信令牌发布者配置将不起作用。因为 IAM Identity Center 不会验证此 URL，所以，如果 URL 的格式不正确，则可信令牌发布者的设置将失败，且不会发出通知。
> OIDC 发现端点 URL 只能通过端口 80 和 443 进行访问。

IAM Identity Center 使用此 URL 获取有关可信令牌发布者的其他信息。例如，IAM Identity Center 使用此 URL 获取所需的信息，以验证可信令牌发布者生成的令牌。向 IAM Identity Center 添加可信令牌发布者时，必须指定此 URL。要查找 URL，请参阅用于为应用程序生成令牌的 OAuth 2.0 授权服务器的提供商文档，或者直接联系提供商寻求帮助。

属性映射

IAM Identity Center 能够使用属性映射，将可信令牌发布者发布的令牌所代表的用户与 IAM Identity Center 中的单个用户相匹配。向 IAM Identity Center 添加可信令牌发布者时，您必须指定属性映射。此属性映射用于可信令牌发布者生成的令牌中的声明。声明中的值用于搜索 IAM Identity Center。搜索使用指定的属性检索 IAM Identity Center 中的单个用户，该用户将被用作 Amazon中的用户。您选择的声明必须映射到 IAM Identity Center 身份存储中可用属性固定列表中的一个属性。您可以选择以下 IAM Identity Center 身份存储属性之一：用户名、电子邮件和外部 ID。对于每个用户，您在 IAM Identity Center 指定的属性值必须唯一。

Aud 声明

Aud 声明将确定令牌的目标受众（接收者）。当请求访问权限的应用程序通过未联合到 IAM Identity Center 的身份提供商进行身份验证时，必须将该身份提供商设置为可信令牌发布者。接收访问请求的应用程序（接收端应用程序）必须将可信令牌发布者生成的令牌与 IAM Identity Center 生成的令牌交换。

有关如何获取接收端应用程序在可信令牌发布者处注册的受众声明值，请参阅可信令牌发布者的文档，或联系可信令牌发布者管理员寻求帮助。

设置可信令牌发布者

要为在 IAM Identity Center 外部进行身份验证的应用程序启用可信身份传播，必须由一名或多名管理员设置可信令牌发布者。可信令牌发布者是一种 OAuth 2.0 授权服务器，向发起请求的应用程序（请求端应用程序）发布令牌。令牌授权这些应用程序代表其用户向接收应用程序发起请求 (a Amazon Web Services 服务)。

主题

协调管理角色和职责

在某些情况下，一名管理员可能会执行设置可信令牌发布者所需的所有必要任务。如果有多名管理员执行这些任务，则需要密切协调。下表描述了多个管理员如何协调设置可信令牌发行者并配置 Amazon 服务以使用该令牌。

> **Note**
>
> 该应用程序可以是任何与 IAM Identity Center 集成并支持可信身份传播的 Amazon 服务。

有关更多信息，请参阅 设置可信令牌发布者的任务。

角色	执行这些任务	协调对象
IAM Identity Center 管理员	将外部 IdP 作为可信令牌发布者添加到 IAM Identity Center 控制台。 帮助在 IAM Identity Center 和外部 IdP 之间设置正确的属性映射。 当可信令牌颁发者添加到 IAM Identity Center 控制台时，通知 Amazon 服务管理员。	外部 IdP（可信令牌发布者）管理员 Amazon 服务管理员
外部 IdP（可信令牌发布者）管理员	配置外部 IDP，以颁发令牌。 帮助在 IAM Identity Center 和外部 IdP 之间设置正确的属性映射。	IAM Identity Center 管理员 Amazon 服务管理员

角色	执行这些任务	协调对象
	向 Amazon 服务管理员提供受众名称（Aud 声明）。	
Amazon 服务管理员	检查 Amazon 服务控制台中是否有受信任的令牌发行者。在 IAM Identity Center 管理员将其添加到 IAM Identity Center 控制台后，可信令牌颁发者将在 Amazon 服务控制台中可见。 将 Amazon 服务配置为使用可信令牌发行者。	IAM Identity Center 管理员 外部 IdP（可信令牌发布者）管理员

设置可信令牌发布者的任务

要设置可信令牌发布者，IAM Identity Center 管理员、外部 IdP（可信令牌发布者）管理员和应用程序管理员必须完成以下任务。

> **Note**
>
> 该应用程序可以是任何与 IAM Identity Center 集成并支持可信身份传播的 Amazon 服务。

1. 将可信令牌发布者添加到 IAM Identity Center - IAM Identity Center 管理员使用 IAM Identity Center 控制台或 API 添加可信令牌发布者。此配置需要指定以下内容：
   - 可信令牌发布者的名称。
   - OIDC 发现端点 URL（在 IAM Identity Center 控制台中，此 URL 称为发布者 URL）。发现端点只能通过端口 80 和 443 进行访问。
   - 供用户查询的属性映射。此属性映射用于可信令牌发布者生成的令牌中的声明。声明中的值用于搜索 IAM Identity Center。搜索使用指定的属性检索 IAM Identity Center 中的单个用户。
2. 将@@ Amazon 服务连接到 IAM Identit y Center — Amazon 服务管理员必须使用应用程序或应用程序 API 的控制台将应用程序连接到 IAM 身份中心。

   将可信令牌颁发者添加到 IAM Identity Center 控制台后，它也会在 Amazon 服务控制台中可见，可供 Amazon 服务管理员选择。

3. 配置令牌交换的使用-在 Amazon 服务控制台中， Amazon 服务管理员将 Amazon 服务配置为接受可信令牌发行者发行的令牌。这些令牌将与 IAM Identity Center 生成的令牌交换。这需要指定步骤 1 中受信任的代币发行者的名称，以及与该 Amazon 服务对应的澳元索赔值。

   受信任的代币发行者在其发行的代币中放置澳元索赔值，以表明该代币打算供该 Amazon 服务使用。要获取此值，请联系可信令牌发布者管理员。

如何向 IAM Identity Center 控制台添加可信令牌发布者

在拥有多名管理员的组织中，此任务由 IAM Identity Center 管理员执行。如果您是 IAM Identity Center 管理员，则必须选择使用哪个外部 IdP 作为可信令牌发布者。

要向 IAM Identity Center 控制台添加可信令牌发布者

1. 打开 IAM Identity Center 控制台。
2. 选择设置。
3. 在设置页面上，选择身份验证选项卡。
4. 在可信令牌发布者下，选择创建可信令牌发布者。
5. 在设置外部 IdP 以发布可信令牌页面的可信令牌发布者详细信息下，执行以下操作：

   - 在发布者 URL中，指定将为可信身份传播发布令牌的外部 IdP 的 OIDC 发现 URL。必须指定发现端点 URL 中直至 `.well-known/openid-configuration` 前面的部分。外部 IdP 的管理员可以提供此 URL。

     > **Note**
     >
     > 注意：此 URL 必须与为可信身份传播颁发的令牌中的发布者 (iss) 声明中的 URL 相匹配。

   - 在可信令牌发布者名称中，输入一个名称，以便在 IAM Identity Center 和应用程序控制台中识别该可信令牌发布者。
6. 在映射属性下，执行以下操作：

   - 对于身份提供商属性，从列表中选择一个属性，以映射到 IAM Identity Center 身份存储中的属性。
   - 对于 IAM Identity Center 属性，为属性映射选择相应的属性。
7. 在标签（可选）下，选择添加新标签，为键和值（可选）指定值。

有关标签的信息，请参阅 为资源添加标签 Amazon IAM Identity Center。

8. 选择创建可信令牌发布者。
9. 创建完可信令牌发布者后，请联系应用程序管理员，告知他们可信令牌发布者的名称，以便他们可以确认可信令牌发布者在适用的控制台中可见。
10. 应用程序管理员必须在适用的控制台中选择此可信令牌发布者，才能允许用户从为可信身份传播配置的应用程序中访问其他应用程序。

如何在 IAM Identity Center 控制台中查看或编辑可信令牌发布者设置

将可信令牌发布者添加到 IAM Identity Center 控制台后，您可以查看和编辑相关设置。

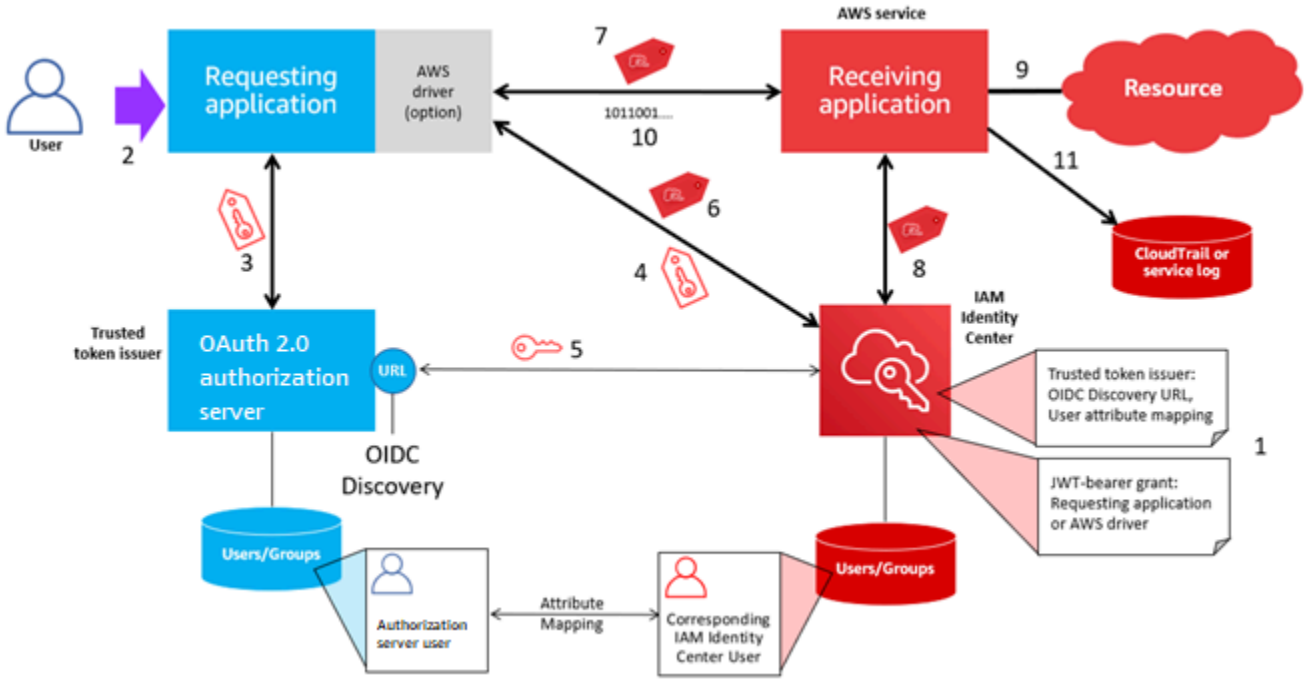
如果您计划编辑可信令牌发布者设置，请注意，这样做可能会导致用户无法访问任何配置为使用可信令牌发布者的应用程序。为避免中断用户访问，我们建议您在编辑设置之前，与配置为使用可信令牌发布者的应用程序管理员进行协调。

要在 IAM Identity Center 控制台中查看或编辑可信令牌发布者设置

1. 打开 IAM Identity Center 控制台。
2. 选择设置。
3. 在设置页面上，选择身份验证选项卡。
4. 在可信令牌发布者下，选择要查看或编辑的可信令牌发布者。
5. 选择操作，然后选择编辑。
6. 在编辑可信令牌发布者页面，根据需要查看或编辑设置。您可以编辑可信令牌发布者名称、属性映射和标签。
7. 选择保存更改。
8. 在编辑可信令牌发布者对话框中，系统会提示您确认是否要进行更改。选择确认。

使用可信令牌发布者的应用程序的设置过程和请求流程

本节介绍使用可信令牌发布者进行可信身份传播的应用程序的设置过程和请求流程。下图提供了此过程的概述。



以下步骤提供了有关此过程的更多信息。

1. 设置 IAM Identity Center 和接收 Amazon 托管应用程序以使用可信令牌颁发者。有关信息，请参阅设置可信令牌发布者的任务。
2. 当用户打开请求端应用程序时，请求流程开始。
3. 发出请求的应用程序向可信令牌颁发者请求令牌，以向接收的 Amazon 托管应用程序发起请求。如果用户尚未进行身份验证，此过程会触发身份验证流程。令牌包含以下信息：
   - 用户的主体 (Sub)。
   - IAM Identity Center 用于在 IAM Identity Center 查找相应用户的属性。
   - 受众 (Aud) 声明，其中包含可信令牌发布者与接收端 Amazon 托管应用程序相关联的值。如果存在其他声明，IAM Identity Center 将不会使用它们。
4. 发出请求的应用程序或其使用的 Amazon 驱动程序将令牌传递给 IAM Identity Center，并请求将该令牌交换为 IAM Identity Center 生成的令牌。如果您使用 Amazon 驱动程序，可能需要为此用例配置驱动程序。有关更多信息，请参阅相关 Amazon 托管应用程序的文档。
5. IAM Identity Center 使用 OIDC 发现端点获取可用于验证令牌真实性的公钥。然后，IAM Identity Center 会执行以下操作：
   - 验证令牌。
   - 搜索 Identity Center 目录。为此，IAM Identity Center 会使用令牌中指定的映射属性。

- 验证用户是否被授权访问接收端应用程序。如果将 Amazon 托管应用程序配置为要求向用户和组分配任务，则用户必须对应用程序进行直接分配或基于群组的分配；否则请求将被拒绝。如果 Amazon 托管应用程序配置为不需要用户和组分配，则处理将继续进行。

> **Note**
>
> Amazon 服务具有默认设置配置，用于确定是否需要为用户和组进行分配。如果您计划将这些应用程序用于可信身份传播，我们建议不要修改它们的需要分配设置。即使您配置了允许用户访问特定应用程序资源的细粒度权限，修改需要分配设置也可能会导致意外行为，包括中断用户对这些资源的访问。

- 验证发出请求的应用程序是否已配置为使用接收 Amazon 托管应用程序的有效范围。

6. 如果前面的验证步骤成功，IAM Identity Center 将创建一个新令牌。新令牌是不透明（加密）的令牌，其中包括 IAM Identity Center 中相应用户的身份、接收 Amazon 托管应用程序的受众 (Aud)，以及请求的应用程序在向接收 Amazon 托管应用程序发出请求时可以使用的范围。
7. 请求端应用程序或其使用的驱动程序向接收端应用程序发起资源请求，并将 IAM Identity Center 生成的令牌传递给接收端应用程序。
8. 接收端应用程序调用 IAM Identity Center 获取用户身份和在令牌中编码的范围。它还可能请求从 Identity Center 目录中获取用户属性或用户的组成员资格。
9. 接收端应用程序使用其授权配置来确定用户是否得到授权，可访问所请求的应用程序资源。
10. 如果用户有权访问所请求的应用程序资源，接收端应用程序会对请求做出响应。
11. 用户的身份、代表他们执行的操作以及其他事件都记录在接收的应用程序日志和 CloudTrail 事件中。记录这些信息的具体方式因应用程序而异。

Identity-enhanced IAM 角色会话

Amazon Security Token Service(STS) 使应用程序能够获得身份增强型 IAM 角色会话。 Identity-enhanced 角色会话具有一个附加的身份上下文，该上下文将用户标识符带到它 Amazon Web Services 服务 所调用的上。 Amazon Web Services 服务 可以在 IAM Identity Center 中查找用户的群组成员资格和属性，并使用它们来授权用户访问资源。

Amazon 应用程序通过向 Amazon STS AssumeRoleAPI 操作发出请求并在请求的`ProvidedContexts`参数中传递带有用户标识符 (`userId`) 的上下文断言来获取身份增强型角色会话。`AssumeRole`该上下文断言是从响应 `CreateTokenWithIAM` SSO OIDC 请求而收到的 `idToken` 声明中获取的。当 Amazon 应用程序使用身份增强型角色会话访问资源时，会 CloudTrail 记录`userId`、启动会话和采取的操作。有关更多信息，请参阅 Identity-enhanced IAM 角色会话记录。

主题

身份增强型 IAM 角色会话的类型

Amazon STS 可以创建两种不同类型的身份增强型 IAM 角色会话，具体取决于为请求提供的上下文断言。AssumeRole已从 IAM Identity Center 获取身份令牌的应用程序，可向 IAM 角色会话添加 sts:identiy_context（推荐）或 sts:audit_context（为向后兼容提供支持）。身份增强型 IAM 角色会话只能采用这些上下文断言中的一个，不能同时采用两者。

Identity-enhanced 使用 sts 创建的 IAM 角色会话:identity_cont **ex**

当身份增强型角色会话包含 sts:identity_context 时，被调用的 Amazon Web Services 服务 会决定资源授权是基于角色会话中代表的用户，还是基于角色。支持基于用户的授权的 Amazon Web Services 服务 ，可为应用程序管理员提供向用户或用户所属组分配访问权限的控制。

Amazon Web Services 服务 不支持基于用户的授权的，请忽略。sts:identity_context CloudTrail 记录 IAM Identity Center 用户的用户 ID 以及该角色采取的所有操作。有关更多信息，请参阅 Identity-enhanced IAM 角色会话记录。

要从中获取此类身份增强型角色会话 Amazon STS，应用程序使用AssumeRole请求参数在请求中提供该sts:identity_context字段的ProvidedContexts值。使用 arn:aws:iam::aws:contextProvider/IdentityCenter 作为 ProviderArn 的值。

有关授权行为的更多信息，请参阅接收 Amazon Web Services 服务文档。

Identity-enhanced 使用 **sts**: audit_context 创建的 IAM 角色

过去sts:audit_context，用于启用 Amazon Web Services 服务 记录用户身份，而不用它来做出授权决定。 Amazon Web Services 服务 现在能够使用单一上下文-sts:identity_context-来实现这一目标并做出授权决定。我们建议在所有新的可信身份传播部署中使用 sts:identity_context。

Identity-enhanced IAM 角色会话记录

向 Amazon Web Services 服务 使用身份增强型 IAM 角色会话的用户发出请求时，用户的 IAM 身份中心userId将登录到该onBehalfOf元素 CloudTrail 中。事件的登录方式 CloudTrail 因而异 Amazon Web Services 服务。并非所有 Amazon Web Services 服务 都会记录 onBehalfOf 元素。

以下是向 Amazon Web Services 服务 使用身份增强角色会话发出的请求如何登录的示例。 CloudTrail

```
"userIdentity": {
      "type": "AssumedRole",
      "principalId": "AROAEXAMPLE:MyRole",
      "arn": "arn:aws:sts::111111111111:assumed-role/MyRole/MySession",
      "accountId": "111111111111",
      "accessKeyId": "ASIAEXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AROAEXAMPLE",
            "arn": "arn:aws:iam::111111111111:role/MyRole",
            "accountId": "111111111111",
            "userName": "MyRole"
        },
        "attributes": {
            "creationDate": "2023-12-12T13:55:22Z",
            "mfaAuthenticated": "false"
        }
    },
    "onBehalfOf": {
        "userId": "11111111-1111-1111-1111-1111111111",
        "identityStoreArn": "arn:aws:identitystore::111111111111:identitystore/
d-111111111"
    }
}
```

轮换 IAM Identity Center 证书

IAM Identity Center 使用证书在 IAM Identity Center 和您的应用程序服务提供商之间建立 SAML 信任关系。当您在 IAM Identity Center 中添加应用程序时，系统会自动创建一个 IAM Identity Center 证书，以便在设置过程中与该应用程序一起使用。默认情况下，此自动生成的 IAM Identity Center 证书的有效期为五年。

作为 IAM Identity Center 管理员，您有时需要将给定应用程序的旧证书替换为新证书。例如，当证书到期日期临近时，您可能需要更换证书。用新证书替换旧证书的过程称为证书轮换。

轮换证书之前的注意事项

在开始在 IAM Identity Center 中轮换证书之前，请考虑以下事项：

- 认证轮换过程要求您重新建立 IAM Identity Center 和服务提供商之间的信任。要重新建立信任，请使用 轮换 IAM Identity Center 证书 中提供的程序。
- 向服务提供商更新证书可能会导致用户的服务暂时中断，直到成功重新建立信任为止。如果可能的话，请在非高峰时段仔细计划此操作。

轮换 IAM Identity Center 证书

轮换 IAM Identity Center 证书是一个多步骤过程，涉及以下内容：

- 生成新证书
- 将新证书添加到服务提供商的网站
- 将新证书设置为活跃状态
- 删除非活跃状态证书

按以下顺序使用以下所有过程来完成给定应用程序的证书轮换过程。

步骤 1：生成新证书

可以将您生成的新 IAM Identity Center 证书配置为使用以下属性：

- 有效期——指定新 IAM Identity Center 证书到期之前分配的时间（以月为单位）。
- 密钥大小——确定密钥在加密算法中必须使用的位数。您可以将此值设置为 1024 位 RSA 或 2048 位 RSA。有关密码学中密钥大小的工作原理的一般信息，请参阅密钥大小。
- 算法-指定 IAM 身份中心在签署 SAML assertion/response 时使用的算法。您可以将此值设置为 SHA-1 或 SHA-256。 Amazon 除非您的服务提供商要求，否则建议尽可能使用 SHA-256 SHA-1。有关密码算法工作原理的一般信息，请参阅Public-key 密码学。

1. 打开 IAM Identity Center 控制台。
2. 选择应用程序。
3. 在应用程序列表中，选择要为其生成新证书的应用程序。
4. 在应用程序详细信息页面上，选择配置选项卡。在 IAM Identity Center 元数据下，选择管理证书。 如果您没有 “配置” 选项卡或配置设置不可用，则无需轮换此应用程序的证书。
5. 在 IAM Identity Center 证书页面上，选择生成新证书。
6. 在生成新的 IAM Identity Center 证书对话框中，为有效期、算法和密钥大小指定相应的值。然后选择生成。

步骤 2：更新服务提供商的网站

使用以下步骤重新建立与应用程序服务提供商的信任。

> **Important**
>
> 当您将新证书上传到服务提供商时，您的用户可能无法通过身份验证。要纠正这种情况，请按下一步所述将新证书设置为活跃状态。

1. 在 IAM Identity Center 控制台中，选择您刚刚为其生成新证书的应用程序。
2. 在应用程序详细信息页面上，选择编辑配置。
3. 选择查看说明，然后按照特定应用程序服务提供商网站的说明添加新生成的证书。

步骤 3：将新证书设置为活跃状态

一个应用程序最多可以分配两个证书。IAM Identity Center 将使用设置为活动状态的证书签署所有 SAML 断言。

1. 打开 IAM Identity Center 控制台。
2. 选择应用程序。
3. 在应用程序列表中，选择您的应用程序。
4. 在应用程序详细信息页面上，选择配置选项卡。在 IAM Identity Center 元数据下，选择管理证书。
5. 在 IAM Identity Center 证书页面上，选择要设置为活跃的证书，选择操作，然后选择设置为活跃。
6. 在将所选证书设置为活跃状态对话框中，确认您了解将证书设置为活动可能需要重新建立信任，然后选择设为活跃。

步骤 4：删除旧证书

使用以下过程完成应用程序的证书轮换流程。您只能删除处于非活跃状态的证书。

1. 打开 IAM Identity Center 控制台。
2. 选择应用程序。
3. 在应用程序列表中，选择您的应用程序。

4. 在应用程序详细信息页面上，选择配置选项卡。在 IAM Identity Center 元数据下，选择管理证书。
5. 在 IAM Identity Center 证书页面上，选择要删除的证书。选择操作，然后选择删除。
6. 在删除证书对话框中，选择删除。

证书过期状态指示器

在 IAM Identity Center 控制台中，应用程序页面会在每个应用程序的属性中显示状态指示器图标。这些图标显示在列表中每个证书旁边的到期时间列中。下面介绍了 IAM Identity Center 用来确定每个证书显示哪个图标的标准。

- 红色——表示证书当前已过期。
- 黄色——表示证书将在 90 天或更短时间后过期。
- 绿色——表示证书当前有效，并且将至少再保持 90 天的有效期。

检查证书的状态

1. 打开 IAM Identity Center 控制台。
2. 选择应用程序。
3. 在应用程序列表中，按照过期时间列中所示查看列表中证书的状态。

了解 IAM Identity Center 控制台中的应用程序属性

在 IAM Identity Center 中，您可以通过配置应用程序启动 URL、中继状态和会话持续时间来自定义用户体验。

应用程序启动 URL

您可以使用应用程序启动 URL来启动与应用程序的联合身份验证过程。典型用途是仅支持服务提供商 (SP) 发起的绑定的应用程序。

以下步骤和图表说明了当用户在 Amazon Web Services 访问门户中选择应用程序时应用程序启动 URL 身份验证工作流程：

1. 用户的浏览器使用应用程序起始 URL 的值重定向身份验证请求（在本例中为https://example.com）。

2. 应用程序向 IAM Identity Center 发送HTMLPOST带有。SAMLRequest

3. 然后，IAM Identity Center 将 HTML POST 和 SAMLResponse 发送回应用程序。

中继状态

在联合身份验证过程中，中继状态重定向应用程序内的用户。对于 SAML 2.0，此值按原样传递给应用程序。配置应用程序属性后，IAM Identity Center 将中继状态值以及 SAML 响应发送到应用程序。

会话持续时间

会话持续时间是应用程序用户会话保持有效的时间长度。对于 SAML 2.0，此属性用于设置 SAML 断言元素 saml2:AuthNStatement 的 SessionNotOnOrAfter 日期。

应用程序可按以下任一方式解释会话持续时间：

- 应用程序可以使用它来确定允许用户进行会话的最长时间。应用程序可能会生成持续时间较短的用户会话。当应用程序仅支持其持续时间短于已配置会话长度的用户会话时，可能会发生这种情况。
- 应用程序可以使用它作为确切的持续时间，可能不允许管理员配置该值。当应用程序仅支持特定的会话长度时，可能会发生这种情况。

有关如何使用会话持续时间的更多信息，请参阅特定体应用程序的文档。

在 IAM Identity Center 控制台中为用户分配应用程序的访问权限

您可以为用户分配对应用程序目录中的 SAML 2.0 应用程序或自定义 SAML 2.0 应用程序的单点登录访问权限。

组分配的注意事项：

- 直接向组分配访问权限。为了帮助简化访问权限的管理，我们建议您将访问权限直接分配给组而不是单个用户。通过组，您可以向用户组授予或拒绝权限，而不是将这些权限应用于每个人。如果用户移至其他组织，则只需将该用户移至其他组即可。然后，用户会自动获得新组织所需的权限。
- 不支持嵌套组。在为应用程序分配用户访问权限时，IAM Identity Center 不支持将用户添加到嵌套组。如果用户被添加到嵌套组，他们可能会在登录期间收到“您没有任何应用程序”消息。必须针对用户所属的直属组进行分配。

要分配用户或组对应用程序的访问权限

> **Important**
>
> 对于 Amazon 托管应用程序，您必须直接从相关的应用程序控制台或通过 API 添加用户。

1. 打开 IAM Identity Center 控制台。

   > **Note**
   >
   > 如果您在中管理用户 Amazon Managed Microsoft AD，请确保 IAM Identity Center 控制台使用您的 Amazon Managed Microsoft AD 目录所在的 Amazon 区域，然后再采取下一步行动。

2. 选择应用程序。
3. 在应用程序列表中，选择要为其分配访问权限的应用程序名称。
4. 在应用程序详细信息页面上的已分配用户部分中，选择分配用户。
5. 在分配用户对话框中，输入用户的显示名称名或组名。您可以指定多个用户或组，方法是当其显示在搜索结果中时选择适用的帐户。
6. 选择 分配用户。

删除用户对 SAML 2.0 应用程序的访问权限

使用此过程删除用户对应用程序目录中 SAML 2.0 应用程序或自定义 SAML 2.0 应用程序的访问权限。有关身份验证会话和持续时间的更多信息，请参阅了解 IAM Identity Center 中的身份验证会话。

要从应用程序中删除用户访问权限

1. 打开 IAM Identity Center 控制台。
2. 选择应用程序。
3. 在应用程序列表中，选择要删除用户访问权限的应用程序。
4. 在应用程序详细信息页面上的已分配的用户部分中，选择要删除的用户或组，然后选择删除访问权限按钮。
5. 在 Remove access (删除访问权限) 对话框中，检查相应的用户名或组名。然后选择 Remove access (删除访问权限)。

将应用程序中的属性映射到 IAM Identity Center 属性

有些服务提供商需要自定义 SAML 断言来传递有关用户登录的其他数据。在这种情况下，请使用以下过程指定您的应用程序用户属性应如何映射到 IAM Identity Center 中的相应属性。

将应用程序属性映射到 IAM Identity Center 中的属性

1. 打开 IAM Identity Center 控制台。
2. 选择应用程序。
3. 在应用程序列表中，选择您要映射属性的应用程序。
4. 在应用程序的详细信息页面上，选择操作，然后选择编辑属性映射。
5. 选择添加新属性映射。
6. 在第一个文本框中，输入应用程序属性。
7. 在第二个文本框中，输入 IAM Identity Center 中您想要映射到应用程序属性的属性。例如，您可能希望将应用程序属性 **`Username`** 映射到 IAM Identity Center 用户属性 **`email`**。如需查看 IAM Identity Center 允许的用户属性列表，请参见 IAM Identity Center 与外部身份提供者目录之间的属性映射 中的表格。
8. 在表的第三列中，从菜单中为属性选择适当的格式。
9. 选择保存更改。

配置对的访问权限 Amazon Web Services 账户

Amazon IAM Identity Center 与集成 Amazon Organizations，这使您 Amazon Web Services 账户 无需手动配置每个帐户即可集中管理多个帐户的权限。您可以 Amazon Web Services 账户 使用 IAM Identity Center 的组织实例定义权限并将这些权限分配给员工用户，以控制他们对特定用户的访问权限。IAM Identity Center 的账户实例不支持账户访问。

Amazon Web Services 账户 类型

有两种类型 Amazon Web Services 账户 的 Amazon Organizations：

- 管理账户-用于创建组织的账户。 Amazon Web Services 账户
- 成员账户- Amazon Web Services 账户 属于组织的其余账户。

有关 Amazon Web Services 账户 类型的更多信息，请参阅Amazon Organizations 用户指南中的Amazon Organizations 术语和概念。

您也可以选择将成员帐户注册为 IAM Identity Center 的委派管理员。此帐户中的用户可以执行大多数 IAM Identity Center 管理任务。有关更多信息，请参阅 委派管理。

对于每种任务和帐户类型，下表指明了帐户中的用户是否可以执行 IAM Identity Center 管理任务。

IAM Identity Center 管理任务	成员帐户	委托管理员帐户	管理帐户
读取用户或组（阅读组本身和组的成员资格）	✓ 是	✓ 是	✓ 是
添加、编辑或删除用户或组	✗否	✓ 是*	✓ 是
启用或禁用用户访问权限	✗否	✓ 是	✓ 是
启用、禁用或管理传入属性	✗否	✓ 是	✓ 是

IAM Identity Center 管理任务	成员帐户	委托管理员帐户	管理帐户
更改或管理身份源	⊗否	⊙ 是	⊙ 是
创建、编辑或删除客户管理型应用程序	⊗否	⊙ 是	⊙ 是
创建、编辑或删除 Amazon 托管应用程序	⊙ 是	⊙ 是	⊙ 是
配置 MFA	⊗否	⊙ 是	⊙ 是
管理管理帐户中未配置的权限集	⊗否	⊙ 是	⊙ 是
管理管理帐户中已配置的权限集	⊗否	⊗否	⊙ 是
启用 IAM Identity Center	⊗否	⊗否	⊙ 是
删除 IAM Identity Center 配置	⊗否	⊗否	⊙ 是
在管理帐户中启用或禁用用户访问权限	⊗否	⊗否	⊙ 是
将成员帐户作为委派管理员注册或取消注册	⊗否	⊗否	⊙ 是

*请参考有关向管理账户分配用户和组的委托管理最佳实践。

分配 Amazon Web Services 账户 访问权限

您可以使用权限集来简化向组织中的用户和组分配 Amazon Web Services 账户访问权限的方式。权限集存储在 IAM Identity Center 中，定义用户和组对 Amazon Web Services 账户的访问级别。您可以创

建单个权限集并将其分配给组织 Amazon Web Services 账户 内的多个权限集。您也可以将多个权限集分配给同一个用户。

有关权限集的更多信息，请参阅创建、管理和删除权限集。

> **Note**
>
> 您还可以为用户分配对应用程序的单点登录访问权限。有关信息，请参阅配置对应用程序的访问。

最终用户体验

Amazon Web Services 访问门户为 IAM Identity Center 用户提供通过门户网站对其分配的所有应用程序 Amazon Web Services 账户 和应用程序的单点登录访问权限。 Amazon Web Services 访问门户不同于 Amazon Web Services 管理控制台，后者是一组用于管理 Amazon 资源的服务控制台。

创建权限集时，您为该权限集指定的名称会作为可用角色出现在 Amazon Web Services 访问门户中。用户登录 Amazon Web Services 访问门户，选择一个 Amazon Web Services 账户，然后选择角色。选择角色后，他们可以使用访问 Amazon 服务 Amazon Web Services 管理控制台 或检索临时凭证以编程方式访问 Amazon 服务。

要打开 Amazon Web Services 管理控制台 或检索临时凭证以 Amazon 编程方式进行访问，用户需要完成以下步骤：

1. 用户打开浏览器窗口，使用您提供的登录 URL 导航到 Amazon Web Services 访问门户。
2. 他们使用其目录凭据登录 Amazon Web Services 访问门户。
3. 身份验证后，在 Amazon Web Services 访问门户页面上，他们选择 “帐户” 选项卡 Amazon Web Services 账户 以显示他们有权访问的列表。
4. 然后，用户选择 Amazon Web Services 账户 他们想要使用的。
5. 在的名称下方 Amazon Web Services 账户，向其分配用户的所有权限集都显示为可用角色。例如，如果您`john_stiles`为用户分配了`PowerUser`权限集，则该角色在 Amazon Web Services 访问门户中显示为`PowerUser/john_stiles`。分配有多个权限集的用户选择要使用的角色。用户可以选择其访问 Amazon Web Services 管理控制台的角色。
6. 除角色外， Amazon Web Services 访问门户用户还可以通过选择访问密钥来检索命令行或编程访问的临时证书。

有关您可以向员工用户提供的 step-by-step指导，请参阅设置和使用 Amazon Web Services 访问门户和获取 Amazon CLI 或的 IAM Identity Center 用户证书 Amazon SDKs。

强制和限制访问权限

启用 IAM Identity Center 后，IAM Identity Center 会创建一个与服务相关的角色。您也可以使用服务控制策略 (SCPs)。

委派和强制访问权限

服务相关角色是一种直接链接到 Amazon 服务的 IAM 角色。启用 IAM Identity Center 后，IAM Identity Center 可以在组织 Amazon Web Services 账户 中的每个角色中创建一个服务相关角色。此角色提供预定义的权限，允许 IAM Identity Center 委派和强制执行哪些用户对组织 Amazon Web Services 账户中的 Amazon Organizations特定用户具有单点登录访问权限。您需要分配一个或多个具有帐户访问权限的用户，才能使用此角色。有关更多信息，请参阅 了解 IAM Identity Center 中的服务相关角色 和 使用 IAM Identity Center 的服务相关角色。

限制成员帐户对身份存储的访问权限

对于 IAM Identity Center 使用的身份存储服务，有权访问成员帐户的用户可以使用需要读取权限的 API 操作。成员帐户有权访问 sso 目录和 identitystore 命名空间上的 读取操作。有关更多信息，请参阅《服务授权参考》中的Amazon IAM Identity Center 目录的操作、资源和条件密钥以及 Ident Amazon ity Store 的操作、资源和条件密钥。

为防止成员帐户中的用户在身份存储中使用 API 操作，您可以附加服务控制策略（SCP）。SCP 是一种组织策略，可用于管理组织中的权限。以下示例 SCP 阻止成员帐户中的用户访问身份存储中的任何 API 操作。

```
{
    "Sid": "ExplicitlyBlockIdentityStoreAccess",
    "Effect": "Deny",
    "Action": ["identitystore:*", "sso-directory:*"],
    "Resource": "*"
}
```

> **Note**
>
> 为确保您的 Amazon 托管应用程序在 IAM Identity Center 中正常运行，您应避免将此 SCP 应用于部署这些应用程序 Amazon Web Services 账户 的位置。此外，如果您使用委托管理，请勿将此 SCP 应用于委托管理账户。有关更多信息，请参阅 最佳实践。

有关更多信息，请参阅《Amazon Organizations 用户指南》中的服务控制策略 (SCPs)。

委派管理

委派管理为注册成员帐户中的分配用户提供了一种便捷的方式，来执行大多数 IAM Identity Center 管理任务。启用 IAM 身份中心后，默认情况下，将在中的管理账户中 Amazon Organizations 创建您的 IAM 身份中心实例。最初是这样设计的，以便 IAM Identity Center 可以在组织的所有成员帐户中配置、取消配置和更新角色。尽管您的 IAM Identity Center 实例必须始终位于管理账户中，但您可以选择将 IAM Identity Center 的管理委托给中的成员账户 Amazon Organizations，从而扩展从管理账户之外管理 IAM Identity Center 的能力。

启用委派管理具有以下优势：

- 最大限度地减少需要访问管理帐户的人员数量，以帮助缓解安全问题
- 允许选定的管理员将用户和组分配给应用程序和组织的成员帐户

有关 IAM 身份中心如何使用的更多信息 Amazon Organizations，请参阅配置对的访问权限 Amazon Web Services 账户。要了解更多信息并查看展示如何配置委派管理的公司情景的示例，请参阅Amazon 安全博客中的开始使用 IAM Identity Center 委派管理。

主题

最佳实践

以下是配置委派管理之前需要考虑的一些最佳实践：

- 向管理帐户授予最小权限 – 我们知道管理帐户是一个高权限帐户，为了遵守最小权限原则，我们强烈建议您将管理帐户的访问权限限制为尽可能少的人。委派管理员功能旨在最大限度地减少需要访问管理帐户的人数。您还可以考虑使用临时提升权限，仅在需要时授予访问权限。
- 为管理账户配置专用权限集 - 为管理账户使用专用的权限集。出于安全考虑，用于访问管理账户的权限集只能由管理账户中的 IAM Identity Center 管理员修改。委派管理员无法更改管理账户中配置的权限集。
- 仅向管理账户中的权限集分配用户（而非群组）-由于管理账户具有特殊权限，因此在控制台或 Amazon Command Line Interface (CLI) 中为该账户分配访问权限时必须谨慎行事。如果您将群组分配给有权访问管理帐户的权限集，则有权修改这些群组中成员资格的任何人都可以 add/remove 使用 to/from 这些群组，从而影响谁有权访问管理帐户。这包括任何对您的身份源拥有控制权的组管理员，例如身份提供者（IdP）管理员、Microsoft Active Directory 域服务（AD DS）管理员或 IAM Identity Center 管理员。因此，您应将用户直接分配到授予管理账户访问权限的权限集，避免使用组分配。如果您确实需要使用组管理对管理账户的访问权限，请确保在 IdP 中设置适当的控制措施，限制有权修改这些组的人员，并确保对这些组的更改（或管理账户中用户凭据的更改）被记录并根据需要进行审核。
- 考虑您的 Active Directory 位置 – 如果您计划使用 Active Directory 作为 IAM Identity Center 身份源，请在启用了 IAM Identity Center 委派管理员功能的成员帐户中找到该目录。如果您决定将 IAM Identity Center 身份来源从任何其他来源更改为 Active Directory，或者将其从 Active Directory 更改为任何其他来源，则该目录必须驻留在 IAM Identity Center 委派管理员成员账户中。如果您希望将 Active Directory 部署在管理账户中，则必须在管理账户中完成设置，因为委托管理员没有完成该操作所需的权限。

限制使用外部身份源的委托管理账户中的 IAM Identity Center 身份存储操作

如果您使用外部身份源（例如 IdP 或） Amazon Directory Service，则应实施策略，限制 IAM Identity Center 管理员可以在委托的管理账户中执行的身份存储操作。应谨慎对待写入和删除操作。通常，外部身份源是用户及其属性以及组成员身份的权威来源。如果您使用身份存储 APIs 或控制台修改这些内容，则在正常同步周期中，您的更改将被覆盖。最好将这些操作交由您的权威身份源独家控制。这还可以防止 IAM Identity Center 管理员通过修改组成员身份来授予对组分配的权限集或应用程序的访问权限，确保组成员身份控制权保留在 IdP 管理员手中。您还应限制谁可以从委托管理账户创建 SCIM 承载令牌，因为这些令牌可能允许成员账户管理员通过 SCIM 客户端修改组和用户。

某些情况下，从委托管理账户执行写入或删除操作可能是合适的。例如，您可以创建一个不含成员的组，然后向权限集分配该组，而无需等待 IdP 管理员创建该组。在 IdP 管理员配置该组且 IdP 同步过程完成组成员设置之前，无人能通过该分配获得访问权限。此外，如果您无法等待 IdP 同步过程移除用户或组的访问权限，临时删除该用户或组以阻止登录或授权可能也是合适的。但滥用此权限可能会对用户造成影响。分配身份存储权限时，应遵循最低权限原则。您可以通过服务控制策略（SCP）控制委托管理账户管理员可执行的身份存储操作。

下面的示例 SCP 可防止通过 Identity Store API 将用户分配到群组 Amazon Web Services 管理控制台，当您的身份源为外部时，建议使用此方法。这不会影响用户与外部 IdP 的同步（通过 SCIM）。Amazon Directory Service

> **Note**
>
> 尽管您使用外部身份源，但您的组织可能完全或部分依赖Identity Stor APIs e来配置用户和群组。因此，在激活此 SCP 之前，您应确认您的用户配置流程不使用此身份存储 API 操作。有关如何将组成员身份管理限制到特定组的信息，请参阅下一节。

```
{
  "Version": "2012-10-17",
  "Statement": [
    { "Effect": "Deny",
      "Action": ["identitystore:CreateGroupMembership"],
      "Resource": [ "*" ] }
  ]
}
```

如果您希望仅阻止向授予管理账户访问权限的组添加用户，可通过以下格式的组 ARN 引用这些特定组：`arn:${Partition}:identitystore:::group/${GroupId}`。该资源类型以及身份存储中可用的其他资源类型记录在《服务授权参考》中 Ident Amazon ity Store 定义的资源类型中。您也可以考虑在 SCP APIs 中添加其他身份存储。有关更多信息，请参阅《Identity Store API 参考》中的操作。

通过向 SCP 添加以下策略语句，可阻止委托管理员创建 SCIM 承载令牌。此配置适用于两种外部身份源场景。

> **Note**
>
> 如果您的委托管理员需要通过 SCIM 配置用户预置，或执行定期的 SCIM 承载令牌轮换，则需要临时允许访问此 API，以便委托管理员完成这些任务。

```
    { "Effect": "Deny",
      "Action": ["sso-directory:CreateBearerToken"],
      "Resource": [ "*" ]
    }
```

限制本地管理用户的委托管理账户中的 IAM Identity Center 身份存储操作

如果您直接在 IAM Identity Center 中创建用户和群组，而不是使用外部 IdP 或 Amazon Directory Service，则应注意谁可以创建用户、重置密码和控制群组成员资格。这些操作赋予管理员极大的权限，可决定谁能登录以及谁能通过组成员身份获得访问权限。这些策略最好在您用于 IAM Identity Center 管理员的权限集内作为内联策略来实施，而不是按 SCPs照。以下内嵌策略示例具有两个目标。首先，阻止向特定组添加用户。您可通过此策略防止委托管理员向授予管理账户访问权限的组添加用户。其次，阻止颁发 SCIM 承载令牌。

```
{
  "Version": "2012-10-17",
  "Statement": [
  { "Effect": "Deny",
    "Action": ["identitystore:CreateGroupMembership"],
    "Resource": [ arn:${Partition}:identitystore:::group/${GroupId1},
                  arn:${Partition}:identitystore:::group/${GroupId2}
                ]
   }
  ],
  { "Effect": "Deny",
    "Action": ["sso-directory:CreateBearerToken"],
    "Resource": [ "*" ] }
  ]
}
```

将 IAM 身份中心配置管理与管理分开 PermissionSet

通过在管理账户中创建独立的管理员权限集，将外部身份源修改、SCIM 令牌管理、会话超时配置等管理任务，与权限集的创建、修改和分配任务分离。

限制 SCIM 承载令牌的颁发

当 IAM Identity Center 的身份源为 Okta 或 Entra ID 等外部 IdP 时，SCIM 承载令牌允许外部身份源通过 SCIM 协议配置用户、组和组成员身份。您可配置以下服务控制策略（SCP），防止委托管理员创建 SCIM 承载令牌。如果您的委托管理员需要通过 SCIM 配置用户预置，或执行定期的 SCIM 承载令牌轮换，则需临时允许访问此 API，以便委托管理员完成相关任务。

```
    { "Effect": "Deny",
      "Action": ["sso-directory:CreateBearerToken"],
      "Resource": [ "*" ]
}
```

使用权限集标签和账户列表委托特定账户的管理权限

您可创建权限集并分配给 IAM Identity Center 管理员，以委托谁能创建权限集，以及谁能在哪些账户中分配哪些权限集。此操作通过为权限集添加标签，并在分配给管理员的权限集中设置策略条件实现。例如，您可创建权限集，允许用户创建带有特定标签的权限集。您还可创建策略，允许管理员在指定账户中分配带有特定标签的权限集。这有助于您委托账户管理权限，同时避免授予管理员修改其自身在委托管理账户中访问权限的特权。例如，通过为仅在委托管理账户中使用的权限集添加标签，您可指定策略，仅允许特定人员修改影响委托管理账户的权限集和分配。您还可授予其他人管理委托管理账户之外的账户列表的权限。有关更多信息，请参阅《Amazon 安全博客》中的在 Amazon IAM Identity Center 中委托权限集管理和账户分配。

先决条件

在将帐户注册为委派管理员之前，必须先部署以下环境：

- Amazon Organizations 除了您的默认管理账户外，还必须启用并配置至少一个成员帐户。
- 如果您的身份源设置为 Active Directory，则必须启用 IAM Identity Center 可配置 AD 同步 功能。

注册成员帐户

要配置委派管理，必须先将组织中的成员帐户注册为委派管理员。该成员帐户中拥有足够权限的用户将拥有对 IAM Identity Center 的管理访问权限。成员账户成功注册委派管理后，它被称为委派管理员账户。要详细了解委派管理员帐户可以执行的任务，请参阅 Amazon Web Services 账户 类型。

IAM Identity Center 一次仅支持将一个成员帐户注册为委派管理员。只有使用管理帐户的凭证登录后，您才能注册成员帐户。

通过将 Amazon 组织中的特定成员账户注册为委托管理员，使用以下步骤授予对 IAM Identity Center 的管理访问权限。

> **Important**
>
> 此操作将 IAM Identity Center 管理权限委派给该成员帐户中的管理员用户。对此委派管理员帐户拥有足够权限的所有用户都可以从该帐户执行所有 IAM Identity Center 管理任务，但以下任务除外：
>
> - 启用 IAM Identity Center
> - 删除 IAM Identity Center 配置
> - 管理管理账号中配置的权限集
> - 将其他成员账号作为委派管理员注册或取消注册
> - 在管理帐户中启用或禁用用户访问权限
>
> 委派管理员可以编辑组成员资格。

注册成员帐户

1. Amazon Web Services 管理控制台 使用您的管理账户的凭据登录 Amazon Organizations。需要管理账户凭据才能运行 RegisterDelegatedAdministratorAPI。
2. 选择启用 IAM Identity Center 的区域，然后打开 IAM Identity Center 控制台。
3. 选择设置，然后选择管理选项卡。
4. 在 委派管理员 部分，选择 注册帐户。
5. 在 “注册委托管理员” 页面上，选择 Amazon Web Services 账户 要注册的，然后选择 “注册账户”。

取消注册成员帐户

只有使用管理帐户的凭证登录后，您才能取消注册成员帐户。

使用以下步骤取消 Amazon 组织中以前被指定为委托管理员的成员账户的注册，从而从 IAM Identity Center 中移除管理权限。

> **Important**
>
> 当您取消注册帐户时，您实际上移除了所有管理员用户从该帐户管理 IAM Identity Center 的能力。因此，他们无法再通过该帐户管理 IAM Identity Center 身份、访问管理、身份验证或应用程序访问权限。此操作不会影响在 IAM Identity Center 中配置的任何权限或分配，因此不会对您的最终用户产生任何影响，因为他们将继续在 Amazon Web Services 访问门户 Amazon Web Services 账户 中访问其应用程序。

取消注册成员帐户

1. Amazon Web Services 管理控制台 使用您的管理账户的凭据登录 Amazon Organizations。需要管理账户凭据才能运行 DeregisterDelegatedAdministratorAPI。
2. 选择启用 IAM Identity Center 的区域，然后打开 IAM Identity Center 控制台。
3. 选择设置，然后选择管理选项卡。
4. 在委派管理员部分，选择取消注册帐户。
5. 在取消注册帐户对话框中，查看安全隐患，然后输入成员帐户的名称以确认您已理解。
6. 选择取消注册帐户。

查看哪个成员账号已注册为委派管理员

使用以下步骤查找您的哪个成员账户 Amazon Organizations 已配置为 IAM Identity Center 的委托管理员。

查看已注册的成员帐户

1. 打开 IAM Identity Center 控制台。
2. 选择设置。
3. 在详细信息部分的委派管理员下找到注册的帐户名。您也可以通过选择管理选项卡，然后在授权管理员部分下查看来查找此信息。

的临时提升访问权限 Amazon Web Services 账户

对您的所有访问权限都 Amazon Web Services 账户 涉及一定级别的权限。更改生产环境的配置等敏感操作，因范围和潜在影响需要特殊处理。临时提升访问权限（也称为 just-in-time访问权限）是一种请求、批准和跟踪在指定时间内执行特定任务的权限使用情况的方法。临时提升的访问权限补充了其他形式的访问控制，例如权限集和多重身份验证。

> **Note**
>
> 为确保业务连续性，我们建议您设置对 Amazon Web Services 管理控制台的紧急访问权限。

为了满足客户的一系列需求，请与 Amazon 安全能力合作伙伴的解决方案 Amazon IAM Identity Center 集成。 Amazon 验证这些解决方案是否满足了一组常见的临时提升访问权限要求。建议仔细审查每个合作伙伴解决方案，以便选择最适合您独特需求和偏好（包括业务、云环境架构和预算）的解决方案。

经过验证的解决方案包括 Apono 访问管理平台、CyberArk 安全云访问、Okta 访问请求和 T enable（之前为 Ermetic）。

合作伙伴可以使用 “合作伙伴中心” 中的 “ Amazon 安全能力” 应用程序来提名解决方案。有关更多信息，请参阅 Amazon 安全能力合作伙伴。

> **Note**
>
> 如果您使用的是基于资源的Amazon Elastic Kubernetes Ser Amazon Key Management Service vice，或者，请在选择解决方案之前参阅在资源策略、Amazon EKS 集群配置映射 Amazon KMS 和密钥策略中引用权限集。 just-in-time

单点登录访问权限 Amazon Web Services 账户

您可以 Amazon Organizations 根据常见的工作职能，将连接目录中的用户分配给组织中的管理账户或成员账户的权限。或者，您可以使用自定义权限，以满足特定的安全需求。例如，您可以在开发帐户中授予数据库管理员广泛的 Amazon RDS 权限，但限制其在生产帐户中的权限。IAM Identity Center 自动在您的 Amazon Web Services 账户 帐户中配置所有必要的用户权限。

> **Note**
>
> 您可能需要向用户或群组授予使用 Amazon Organizations 管理账户进行操作的权限。由于它是高权限帐户，因此其他安全限制要求您先拥有IAMFull访问策略或同等权限，然后才能进行设置。您 Amazon 组织中的任何成员账户都不需要这些额外的安全限制。

主题

为用户或群组分配访问权限 Amazon Web Services 账户

使用以下过程为已连接目录中的用户和组分配单点登录访问权限，并使用权限集确定其访问级别。

要查看现有用户和组的访问权限，请参阅查看和更改权限集。

> **Note**
>
> 为了简化访问权限的管理，建议您直接向组（而非各个用户）分配访问权限。通过组，您可以授予或拒绝用户组的权限，而不是必须为每个用户应用这些权限。如果用户移动到不同的组织，您只需将该用户移动到不同的组，他们会自动接收新组织所需的权限。

为用户或组分配访问权限 Amazon Web Services 账户

1. 打开 IAM Identity Center 控制台。

   > **Note**
   >
   > 确保 IAM Identity Center 控制台使用的区域是您的 Amazon Managed Microsoft AD 目录所在的区域，然后再继续执行下一步骤。

2. 在导航窗格中的多帐户权限下，选择 Amazon Web Services 账户。

3. 在 Amazon Web Services 账户 页面上，将显示贵组织的树状视图列表。选中要为其分配访问权限的 Amazon Web Services 账户 旁边的复选框。如果您要为 IAM Identity Center 设置管理访问权限，请选中管理账户旁边的复选框。

> **Note**
>
> 向用户和群组分配单点登录访问权限时，每个权限集一次最多可以选择 10 Amazon Web Services 账户 个。要向同一组用户和组分配 10 个 Amazon Web Services 账户 以上的用户，请根据需要为其他帐户重复此过程。出现提示时，选择相同的用户、组和权限集。

4. 选择分配用户或组。
5. 对于 “步骤 1：选择用户和组”，在 “将用户和组分配给***Amazon-account-name***” 页面上，执行以下操作：

   1. 在用户选项卡上，选择一个或多个要向其授予单点登录访问权限的用户。

      要筛选结果，请开始在搜索框中键入所需用户的名称。

   2. 在组选项卡上，选择一个或多个要向其授予单点登录访问权限的组。

      要筛选结果，请开始在搜索框中键入所需组的名称。

   3. 要显示您选择的用户和组，请选择选定的用户和组旁边的横向三角形。
   4. 确认选择了正确的用户和组后，选择下一步。
6. 对于 “步骤 2：选择权限集”，在 “将权限集分配给***Amazon-account-name***” 页面上，执行以下操作：

   1. 选择一个或多个权限集。如有需要，您可以创建和选择新的权限集。
      - 要选择一个或多个现有权限集，请在权限集下，选择要应用于在上一步中选择的用户和组的权限集。
      - 要创建一个或多个新权限集，请选择创建权限集，然后按照 创建权限集 中的步骤操作。创建要应用的权限集后，在 IAM Identity Center 控制台中，返回到 Amazon Web Services 账户 并按照说明进行操作，直到进入步骤 2：选择权限集。完成此步骤后，选择您创建的新权限集，然后继续执行此过程的下一步。
   2. 确认选择了正确的权限集后，选择下一步。
7. 对于步骤 3：审阅并提交，在 “查看并提交作业***Amazon-account-name***” 页面上，执行以下操作：

   1. 查看选定的用户、组和权限集。

2. 确认选择了正确的用户、组和权限集之后，选择提交。

注意事项

- 用户和组的分配过程可能需要几分钟才能完成。等到此过程成功完成再关闭该页面。
-

> **Note**
>
> 您可能需要向用户或群组授予使用 Amazon Organizations 管理账户进行操作的权限。由于它是高权限帐户，因此其他安全限制要求您先拥有IAMFull访问策略或同等权限，然后才能进行设置。您 Amazon 组织中的任何成员账户都不需要这些额外的安全限制。

8. 如果符合以下任一条件，请按照 提示用户完成 MFA 中的步骤为 IAM Identity Center 启用 MFA：

- 您正在使用默认的 Identity Center 目录作为身份源。
- 您使用的是 Active Directory 中的 Amazon Managed Microsoft AD 目录或自我管理目录作为身份源，但没有将 RADIUS M Amazon Directory Service FA 与一起使用。

> **Note**
>
> 如果您正在使用外部身份提供者，请注意由外部 IdP（而不是 IAM Identity Center）管理 MFA 设置。外部不支持使用 IAM 身份中心中的 MFA。 IdPs

当您为管理用户设置帐户访问权限时，IAM Identity Center 会创建相应的 IAM 角色。此角色由 IAM Identity Center 控制 Amazon Web Services 账户，在相关版本中创建，权限集中指定的策略将附加到该角色。

或者，您可以使用 Amazon CloudFormation 创建和分配权限集，并将这些权限集分配给用户。然后，用户可以登录 Amazon 访问门户或使用 Amazon Command Line Interface（Amazon CLI）命令。

移除用户和群组对的访问权限 Amazon Web Services 账户

使用此过程可以删除所连接目录中一个或多个用户和组 Amazon Web Services 账户 对的的单点登录访问权限。或者，您也可以使用 delete-account-assignment Amazon CLI。

> **Note**
>
> 当您需要注销 IAM Identity Center 用户或组时，应先从用户和组中移除所有权限集分配，再删除用户和组。

删除用户和群组对的访问权限 Amazon Web Services 账户

1. 打开 IAM Identity Center 控制台。
2. 在导航窗格中的多帐户权限下，选择 Amazon Web Services 账户。
3. 在 Amazon Web Services 账户 页面上，将显示您的组织的树视图列表。选择 Amazon Web Services 账户 包含要删除其单点登录访问权限的用户和群组的名称。
4. 在 “概述” 页面的 “分配的用户和组” 下 Amazon Web Services 账户，选择一个或多个用户或组的名称，然后选择 “移除访问权限”。
5. 在移除访问权限对话框中，确认用户或组的名称是否正确，然后选择移除访问权限。

撤销由权限集创建的活跃 IAM 角色会话

撤销活跃的 IAM Identity Center 用户权限集会话的一般过程如下。该过程假设您要移除凭证受损的用户或系统中恶意行为者的所有访问权限。先决条件是遵循 准备撤销由权限集创建的活跃 IAM 角色会话 中的指导。我们假设服务控制策略（SCP）中存在“全部拒绝策略”。

> **Note**
>
> Amazon 建议您构建自动化以处理除仅限控制台的操作之外的所有步骤。

1. 获取必须撤销其访问权限之人的用户 ID。您可以使用身份存储 APIs 按用户名查找用户。
2. 更新“拒绝策略”，将步骤 1 中的用户 ID 添加到服务控制策略（SCP）中。完成此步骤后，目标用户会失去访问权限，无法对受该策略影响的任何角色执行操作。
3. 移除该用户的所有权限集分配。如果通过组成员资格分配访问权限，请将该用户从所有组和所有直接权限集分配中移除。此步骤可防止用户代入其他 IAM 角色。如果用户拥有有效的 Amazon Web Services 访问门户会话，而您禁用了该用户，则他们可以继续扮演新角色，直到您删除其访问权限。
4. 如果您将身份提供者（IdP）或 Microsoft Active Directory 用作身份源，请在身份源中禁用该用户。禁用该用户可以防止创建其他 Amazon Web Services 访问门户会话。参阅 IdP 或 Microsoft

Active Directory API 文档，了解如何自动执行此步骤。如果将 IAM Identity Center 目录用作身份源，切勿禁用用户访问权限。在步骤 6 中禁用用户访问权限。

5. 在 IAM Identity Center 控制台中，找到用户并删除其活跃会话。

   a. 选择用户。

   b. 选择要删除其活跃会话的用户。

   c. 在用户详细信息页面上，选择活跃会话选项卡。

   d. 选中要删除的会话旁边的复选框，然后选择删除会话。

   删除用户会话后，用户将立即失去对访问门户的 Amazon Web Services 访问权限。了解会话持续时间。

6. 在 IAM Identity Center 控制台中禁用用户访问权限。

   a. 选择用户。

   b. 选择要禁用访问权限的用户。

   c. 在用户详细信息页面上展开一般信息，然后选择禁用用户访问权限按钮，防止该用户继续登录。

7. 保留“拒绝策略”至少 12 小时。否则，拥有活跃 IAM 角色会话的用户将恢复对 IAM 角色的操作。如果等待 12 小时，活跃会话会过期，用户无法再次访问 IAM 角色。

> **Important**
>
> 如果在停止用户会话之前禁用了用户的访问权限（在未完成步骤 5 的情况下完成了步骤 6），则无法再通过 IAM Identity Center 控制台停止用户会话。如果在停止用户会话之前无意中禁用了用户访问权限，则可以重新启用用户，停止其会话，然后再次禁用其访问权限。

现在，如果用户密码被盗用，您可以更改用户凭证并恢复其分配。

委派谁可以为管理账号中的用户和组分配单点登录访问权限

使用 IAM Identity Center 控制台为主帐户分配单点登录访问管理帐户的权限。默认情况下，只有附加 Amazon Web Services 账户根用户了AmazonSSOMasterAccountAdministrator和IAMFullAccess Amazon 托管策略的用户才能向管理账户分配单点登录访问权限。AmazonSSOMasterAccountAdministrator和IAMFullAccess策略管理对 Amazon Organizations 组织内管理账户的单点登录访问权限。

或者，您可以使用 Amazon CLI 创建权限集、将策略附加到权限集和分配权限集。以下列出了每个步骤对应的命令：

- 要创建权限集，请执行以下操作：create-permission-set
- 要附加 Amazon Managed Policy到权限集，请执行以下操作：attach-managed-policy-to-permission- set
- 要将客户托管策略附加到权限集，请执行以下操作：attach-customer-managed-policy-to-permission-set
- 要将权限集分配给委托人，请执行以下操作：create-account-assignment

使用以下步骤委派权限来管理您的目录中用户和组的单点登录访问权限。

授予权限来管理您的目录中的用户和组的单点登录访问权限

1. 以管理帐户的根用户身份或具有管理员权限的另一个管理用户的身份登录到 IAM Identity Center 控制台。
2. 按照 创建权限集 中的步骤创建权限集，然后执行以下操作：
    1. 在创建新权限集页面上，选中创建自定义权限集复选框，然后选择下一步：详细信息。
    2. 在“创建新权限集”页面上，指定自定义权限集的名称和描述（可选）。如有需要，可以修改会话持续时间并指定中继状态 URL。

        > **Note**
        >
        > 对于中继状态 URL，必须指定位于 Amazon Web Services 管理控制台中的 URL 。例如：
        > **`https://console.aws.amazon.com/ec2/`**
        > 有关更多信息，请参阅 设置中继状态以便快速访问 Amazon Web Services 管理控制台。

    3. 在您要在权限集中包含哪些策略？下，选中附加 Amazon 管理型策略复选框。
    4. 在 IAM 策略列表中，选择AWSSSOMasterAccountAdministrator和IAMFullAccess Amazon 托管策略。这些策略向以后将拥有此权限集的访问权限的任何用户和组授予权限。
    5. 选择下一步：标签。
    6. 在添加标签（可选）下，指定密钥和值（可选）的值，然后选择下一步：查看。有关标签的更多信息，请参阅为资源添加标签 Amazon IAM Identity Center。

7. 检查您的选择，然后选择创建。

3. 按照 为用户或群组分配访问权限 Amazon Web Services 账户 中的步骤将相应的用户和组分配给您刚刚创建的权限集。
4. 向已分配的用户传送以下信息：当已分配的用户登录 Amazon Web Services 访问门户并选择账户选项卡时，必须选择适当的角色名以使用刚委派的权限进行身份验证。

Amazon Web Services 账户 使用权限集进行管理

权限集是您创建和维护的模板，用于定义一个或多个 IAM 策略的集合。权限集简化了组织中用户和群组的 Amazon Web Services 账户 访问权限分配。例如，您可以创建一个数据库管理员权限集，其中包括用于管理 Amazon RDS、DynamoDB 和 Aurora 服务的策略，并使用该权限集向数据库管理员授予对组织内 Amazon Web Services 账户Amazon 目标列表的访问权限。

IAM Identity Center 使用权限集向一个或多个 Amazon Web Services 账户 用户或群组分配访问权限。当您分配权限集时，IAM Identity Center 会在每个帐户中创建 IAM Identity Center 控制的相应 IAM 角色，并将权限集中指定的策略附加到这些角色。IAM Identity Center 使用 IAM Identity Center 用户门户或 Amazon CLI 管理角色，并允许您定义的授权用户代入该角色。 在您修改权限集时，IAM Identity Center 会确保相应的 IAM 策略和角色也相应更新。

您可以将 Amazon 管理型策略、客户管理型策略、内联策略和适用于工作职能的Amazon 管理型策略添加到您的权限集中。您也可以指定 Amazon 管理型策略或客户管理型策略作为权限边界。

要创建权限集，请参阅创建、管理和删除权限集。

创建应用最低权限的权限集

要遵循应用最低权限的最佳实践，请在创建管理权限集之后，创建一个限制性更强的权限集并将其分配给一个或多个用户。在之前过程中创建的权限集将提供一个起点，让您评估为用户访问所需的资源分配多少访问权限。要切换到最低权限权限，您可以运行 IAM Access Analyzer 来监控使用 Amazon 托管策略的委托人。了解他们使用的权限后，您可以编写自定义策略或生成仅包含团队所需权限的策略。

借助 IAM Identity Center，您可以为同一个用户分配多个权限集。您还应该为管理用户分配其他限制性更强的权限集。这样，他们就可以仅 Amazon Web Services 账户 凭所需的权限访问您的，而不必总是使用他们的管理权限。

例如，如果您是一名开发人员，在 IAM Identity Center 中创建管理用户后，您可以创建一个授予 `PowerUserAccess` 权限的新权限集，然后将该权限集分配给您自己。不同于使用

AdministratorAccess 权限的管理权限集，PowerUserAccess 权限集不允许管理 IAM 用户和组。当你登录 Amazon 访问门户访问你的 Amazon 账户时，你可以选择PowerUserAccess而不是在AdministratorAccess账户中执行开发任务。

请注意以下事项：

- 要快速开始创建限制性更强的权限集，请使用预定义的权限集而不是自定义权限集。

  使用使用预定义权限的预定义权限集，您可以从可用策略列表中选择单个 Amazon 托管策略。每项策略都授予对 Amazon 服务和资源的特定级别的访问权限或对常见工作职能的权限。有关每项策略的信息，请参阅针对工作职能的Amazon 管理型策略。
- 您可以为权限集配置会话持续时间，以控制用户登录 Amazon Web Services 账户的时间长度。

  当用户联合到他们的管理控制台或命令行界面 (CLI) Amazon Web Services 账户 并使用 Amazon 管理控制台或 Amazon 命令行界面 (Amazon CLI) 时，IAM Identity Center 会使用权限集上的会话持续时间设置来控制会话的持续时间。默认情况下，“会话持续时间” 的值设置为一小时，该值决定了用户在退出会话 Amazon Web Services 账户 之前 Amazon 可以登录的时间长度。可以指定的最大值为 12 小时。有关更多信息，请参阅 将会话持续时间设置为 Amazon Web Services 账户。
- 您还可以配置 Amazon 访问门户会话持续时间以控制员工用户登录门户的时间长度。

  默认情况下，“最大会话持续时间” 的值为八小时，该值决定了员工用户在必须重新进行身份验证之前可以登录 Amazon 访问门户的时间长度。可以将最大值指定为 90 天。有关更多信息，请参阅 在 IAM Identity Center 中配置会话持续时间。
- 登录 Amazon 访问门户时，选择提供最低权限权限的角色。

  您创建并分配给用户的每个权限集在 Amazon 访问门户中显示为可用角色。当您以该用户身份登录门户时，请选择与可用于在帐户中执行任务的最严格的权限集相对应的角色，而不是 AdministratorAccess。
- 您可以将其他用户添加到 IAM Identity Center，并为这些用户分配现有或新的权限集。

  有关信息，请参阅为用户或群组分配访问权限 Amazon Web Services 账户。

主题

Amazon 托管策略的预定义权限

您可以使用 Amazon 托管策略创建预定义的权限集。

创建具有预定义权限的权限集时，可以从 Amazon 托管策略列表中选择一个策略。在可用策略中，您可以从常见权限策略和工作职能策略中进行选择。

常见权限策略

从 Amazon 托管策略列表中进行选择，使您可以访问整个托管策略 Amazon Web Services 账户。您可以添加以下策略之一：

- AdministratorAccess
- PowerUserAccess
- ReadOnlyAccess
- ViewOnlyAccess

工作职能策略

从 Amazon 托管策略列表中进行选择，这些策略允许访问您中 Amazon Web Services 账户 可能与组织内某项工作相关的资源。您可以添加以下策略之一：

- Billing
- DataScientist
- DatabaseAdministrator
- NetworkAdministrator
- SecurityAudit
- SupportUser
- SystemAdministrator

有关可用常见权限策略和工作职能策略的详细说明，请参阅 Amazon Identity and Access Management 用户指南中的适用于工作职能的Amazon 管理型策略。

有关如何创建权限集的说明，请参阅创建、管理和删除权限集。

托管策略和客户 Amazon 托管策略的自定义权限

您可以创建具有自定义权限的权限集，将您在 Amazon Identity and Access Management (IAM) 中拥有的任何托管策略和客户托管策略与内联策略相结合。 Amazon 您还可以纳入权限边界，设置其他策略可授予权限集用户的最大可能权限。

有关如何创建权限集的说明，请参阅创建、管理和删除权限集。

您可以附加到权限集的策略类型

主题

- 内联策略
- Amazon 托管策略
- 客户托管策略
- 权限边界

内联策略

您可以将内联策略附加到权限集。内联策略是格式为 IAM policy 的文本块，您可以将其直接添加到权限集中。创建新权限集时，您可以粘贴策略，也可以使用 IAM Identity Center 控制台中的策略创建工具生成新策略。您还可以使用 Amazon 策略生成器创建 IAM 策略。

当您使用内联策略部署权限集时，IAM Identity Center 会在您分配权限集的 Amazon Web Services 账户 位置创建一个 IAM 策略。当您将权限集分配给帐户时，IAM Identity Center 会创建策略。然后，该策略将附加到您的用户担任 Amazon Web Services 账户 的 IAM 角色。

当您创建内联策略并分配权限集时，IAM Identity Center 会 Amazon Web Services 账户 为您配置您的策略。使用构建权限集时客户托管策略，在分配权限集之前，必须 Amazon Web Services 账户 自己创建策略。

Amazon 托管策略

您可以将Amazon 托管策略附加到您的权限集。 Amazon 托管策略是用于 Amazon 维护的 IAM 策略。相比之下，客户托管策略是您在账户中创建和维护的 IAM 策略。 Amazon 托管策略解决了您的常见的最低权限用例 Amazon Web Services 账户。您可以将 Amazon 托管策略分配为 IAM Identity Center 创建的角色的权限或权限边界。

Amazon 维护工作职能的Amazon 托管策略，这些策略可为您的 Amazon 资源分配特定于作业的访问权限。当您选择对权限集使用预定义权限时，可以添加一项工作职能策略。选择自定义权限时，可以添加多项工作职能策略。

您 Amazon Web Services 账户 还包含大量针对特定策略 Amazon Web Services 服务 和组合的 Amazon 托管 IAM 策略 Amazon Web Services 服务。创建具有自定义权限的权限集时，可以从许多其他 Amazon 托管策略中进行选择，将其分配给您的权限集。

Amazon 每个都填 Amazon Web Services 账户 充 Amazon 托管策略。要部署包含 Amazon 托管策略的权限集，您无需先在中创建策略 Amazon Web Services 账户。使用构建权限集时客户托管策略，在分配权限集之前，必须 Amazon Web Services 账户 自己创建策略。

有关 Amazon 托管策略的更多信息，请参阅 IAM 用户指南中的Amazon 托管策略。

客户托管策略

您可以将客户管理型策略附加到您的权限集。客户管理型策略是您在帐户中创建和维护的 IAM 策略。相比之下，您的账户中Amazon 托管策略是否有 IAM 策略可以 Amazon 维护。您可以将客户管理型策略指定为 IAM Identity Center 所创建角色的权限或权限边界。

使用客户托管策略创建权限集时，必须在 IAM Identity Center 分配权限集的每个 Amazon Web Services 账户 策略中创建具有相同名称和路径的 IAM 策略。如果要指定自定义路径，请确保在每个 Amazon Web Services 账户中指定相同的路径。有关更多信息，请参阅《IAM 用户指南》中的友好名称和路径。IAM Identity Center 将 IAM policy 附加到其在您的 Amazon Web Services 账户中创建的 IAM 角色。最佳做法是在每个您分配权限集的帐户中对策略应用相同的权限。有关更多信息，请参阅在权限集中使用 IAM 策略。

> **Note**
>
> 当客户管理型策略附加到权限集时，策略名称不区分大小写。

有关更多信息，请参阅 IAM 用户指南中的客户管理型策略。

权限边界

您可以将权限边界附加到您的权限集。权限边界是一种 Amazon 托管或客户托管的 IAM 策略，用于设置基于身份的策略可以向 IAM 委托人授予的最大权限。当您应用权限边界时，您的 内联策略、客户托管策略、和 Amazon 托管策略 不能授予任何超出您的权限边界所授予权限的权限。权限边界不授予任何权限，而是让 IAM 忽略边界之外的所有权限。

当您创建以客户管理型策略作为权限边界的权限集时，您必须在 IAM Identity Center 分配您的权限集的每个 Amazon Web Services 账户 中创建一个名称相同的 IAM policy。IAM Identity Center 将 IAM policy 作为权限边界附加到它在您的 Amazon Web Services 账户 中创建的 IAM 角色。

有关更多信息，请参阅 IAM 用户指南 中的 IAM 实体的权限边界。

创建、管理和删除权限集

权限集定义用户和组对某一 Amazon Web Services 账户帐户的访问级别。权限集存储在 IAM Identity Center 中，可以配置给一个或多个 Amazon Web Services 账户。您可以为用户分配多个权限集。有关权限集以及如何在 IAM Identity Center 中使用权限集的更多信息，请参阅 Amazon Web Services 账户使用权限集进行管理。

> **Note**
>
> 您可以在 IAM Identity Center 控制台中按名称搜索和排序权限集。

创建权限集时，请记住以下注意事项：

- 组织实例

  要使用权限集，您将需要使用 IAM Identity Center 的组织实例。有关更多信息，请参阅 IAM Identity Center 的组织和账户实例。
- 以预定义的权限集为起点

  使用使用预定义权限的预定义权限集，您可以从可用策略列表中选择单个 Amazon 托管策略。每项策略都授予对 Amazon 服务和资源的特定级别的访问权限或对常见工作职能的权限。有关每项策略的信息，请参阅针对工作职能的Amazon 管理型策略。收集使用情况数据后，您可以细化权限集，使其更具有限制性。
- 将管理会话的持续时间限制在合理的工作时间段内

  当用户联合到他们 Amazon Web Services 账户 并使用 Amazon Web Services 管理控制台 或 Amazon 命令行界面 (Amazon CLI) 时，IAM Identity Center 会使用权限集上的会话持续时间设置来控制会话的持续时间。当用户会话达到会话持续时间时，他们将退出控制台，并被要求重新登录。作为最佳安全做法，我们建议您设置的会话持续时间长度不要超过执行角色所需的时间。默认情况下，会话持续时间的值为一个小时。可以指定的最大值为 12 小时。有关更多信息，请参阅 将会话持续时间设置为 Amazon Web Services 账户。
- 限制员工用户门户的会话持续时间

  员工用户使用门户会话来选择角色和访问应用程序。默认情况下，“最大会话持续时间” 的值为八小时，该值决定了员工用户在必须重新进行身份验证之前可以登录 Amazon 访问门户的时间长度。可以将最大值指定为 90 天。有关更多信息，请参阅 在 IAM Identity Center 中配置会话持续时间。
- 使用提供最低权限的角色

您创建并分配给用户的每个权限集在 Amazon 访问门户中显示为可用角色。当您以该用户身份登录门户时，请选择与可用于在帐户中执行任务的最严格的权限集相对应的角色，而不是 `AdministratorAccess`。在发送用户邀请之前，请测试您的权限集，验证其是否提供了必要的访问权限。

> **Note**
>
> 您也可以使用 Amazon CloudFormation 创建和分配权限集，并将这些权限集分配给用户。

主题

创建权限集

使用此过程创建使用单个 Amazon 管理型策略的预定义权限集，或者创建使用多达 10 个 Amazon 管理型策略或客户管理型策略和内联策略的自定义权限集。您可以在 IAM 的 服务限额控制台中请求调整 10 个策略的最大数量。您可以在 IAM Identity Center 控制台中创建权限集。

> **Note**
>
> 要使用权限集，您将需要使用 IAM Identity Center 的组织实例。有关更多信息，请参阅 IAM Identity Center 的组织和账户实例。

创建权限集

1. 打开 IAM Identity Center 控制台。
2. 在多帐户权限下，选择权限集。

3. 选择 Create permission set (创建权限集合)。
4. 在选择权限集类型页面的权限集类型下，选择权限集类型。
5. 根据权限集类型，选择一个或多个要用于权限集的策略：

   - 预定义的权限集

     1. 在预先定义的权限集的策略下，从列表选择一项 IAM 工作职能策略或通用权限策略，然后选择下一步。有关更多信息，请参阅 Amazon Identity and Access Management 用户指南 中的工作职能的Amazon 管理型策略 和 Amazon 管理型策略。
     2. 转至步骤 6，完成指定权限集详细信息页面。

   - 自定义权限集

     1. 选择下一步。
     2. 在指定策略和权限边界页面上，选择要应用于新权限集的 IAM 策略类型。默认情况下，您可以将多达 10 个 Amazon 管理型策略和客户管理型策略的任意组合添加到您的权限集中。此限额由 IAM 设置。要提高该限额，请在您要分配权限集的每个 Amazon Web Services 账户的服务限额控制台中请求增加 IAM 限额附加到 IAM 角色的管理型策略。

        - 扩展Amazon 托管策略以添加来自 IAM 的 Amazon 构建和维护策略。有关更多信息，请参阅 Amazon 托管策略。

          a. 在权限集中搜索并选择要应用于用户的 Amazon 管理型策略。

          b. 如果要添加其他类型的策略，请选择其容器并进行选择。选择了所有要应用的策略后，请选择下一步。转至步骤 6，完成指定权限集详细信息页面。

        - 扩展客户管理型策略以添加您构建和维护的 IAM 中的策略。有关更多信息，请参阅 客户托管策略。

          a. 选择附加策略，然后输入要添加到权限集的策略的名称。在要向其分配权限集的每个帐户中，使用您输入的名称创建策略。最佳做法是为每个帐户中的策略分配相同的权限。

          b. 选择附加更多以添加其他策略。

          c. 如果要添加其他类型的策略，请选择其容器并进行选择。选择了所有要应用的策略后，请选择下一步。转至步骤 6，完成指定权限集详细信息页面。

        - 展开内联策略，添加自定义 JSON 格式的策略文本。内联策略与现有的 IAM 资源不对应。要创建内联策略，请在提供的表单中输入自定义策略语言。IAM Identity Center 会将策略添加到它在您的成员帐户中创建的 IAM 资源中。有关更多信息，请参阅 内联策略。

          a. 在交互式编辑器中将所需操作和资源添加到内联策略中。可以使用添加新语句添加其他语句。

b. 如果要添加其他类型的策略，请选择其容器并进行选择。选择了所有要应用的策略后，请选择下一步。转至步骤 6，完成指定权限集详细信息页面。

- 展开权限边界，将 Amazon 托管或客户托管的 IAM 策略添加为权限集中的其他策略可以分配的最大权限。有关更多信息，请参阅 权限边界。

  a. 选择使用权限边界控制最大权限。

  b. 选择 Amazon 管理型策略来设置来自 IAM 的策略，该策略将 Amazon 构建和维护作为您的权限边界。选择客户管理型策略，从 IAM 中设置一个由您构建和维护的策略作为权限边界。

  c. 如果要添加其他类型的策略，请选择其容器并进行选择。选择了所有要应用的策略后，请选择下一步。转至步骤 6，完成指定权限集详细信息页面。

6. 在指定权限集详细信息 页面中，请执行以下操作：

   1. 在权限集名称 下，键入一个名称以在 IAM Identity Center 中标识此权限集。您为此权限集指定的名称作为可用角色出现在 Amazon Web Services 访问门户中。用户登录 Amazon Web Services 访问门户，选择一个 Amazon Web Services 账户，然后选择角色。

      > **Note**
      >
      > 权限集名称在您的 IAM Identity Center 实例中必须唯一。

   2. （可选）您也可以键入描述。描述仅显示在 IAM Identity Center 控制台中，不显示在 Amazon Web Services 访问门户中。

   3. （可选）指定会话持续时间的值。该值确定用户在控制台注销其会话之前可以登录的时间长度。有关更多信息，请参阅 将会话持续时间设置为 Amazon Web Services 账户。

   4. （可选）指定中继状态的值。此值在联合身份验证过程中用于重定向帐户中的用户。有关更多信息，请参阅 设置中继状态以便快速访问 Amazon Web Services 管理控制台。

      > **Note**
      >
      > 中继状态 URL 必须在 Amazon Web Services 管理控制台中。例如：
      > **`https://console.aws.amazon.com/ec2/`**

   5. 展开标签（可选），选择添加标签，然后为密钥和值（可选）指定值。

      有关标签的信息，请参阅 为资源添加标签 Amazon IAM Identity Center。

   6. 选择下一步。

7. 在查看并创建页面上，查看您所做的选择，然后选择创建。
8. 默认情况下，当您创建权限集时，不会配置该权限集（用于任何权限集 Amazon Web Services 账户）。要在中配置权限集 Amazon Web Services 账户，您必须为账户中的用户和群组分配 IAM Identity Center 访问权限，然后将该权限集应用于这些用户和群组。有关更多信息，请参阅 为用户或群组分配访问权限 Amazon Web Services 账户。

查看和更改权限集

您可以使用权限集为用户授予 Amazon Web Services 账户的访问权限。您可以使用 Amazon IAM Identity Center 控制台查看和更改权限集。您可以在 IAM Identity Center 控制台中按名称搜索和排序权限集。有关权限集以及如何在 IAM Identity Center 中使用权限集的更多信息，请参阅 the section called “权限集”。

管理用户对应用程序的访问权限无需使用权限集。

> **Note**
>
> 要使用权限集，您将需要使用 IAM Identity Center 的组织实例。有关更多信息，请参阅 IAM Identity Center 的组织和账户实例。

查看权限集分配

按照此过程在 Amazon IAM Identity Center 控制台中查看已应用的权限集。

All Amazon Web Services 账户 where a permission set is provisioned

要查看某个权限集的所有分配，请执行以下过程：

1. 登录 Amazon Web Services 管理控制台 并打开 Amazon IAM Identity Center 控制台，网址为https://console.aws.amazon.com/singlesignon/。
2. 在多账户权限下，选择权限集。
3. 在权限集页面选择要查看的权限集。
4. 进入所选权限集页面后，在账户选项卡下，您可以查看该权限集所应用的账户。您可以选择某个账户，查看该权限集在该账户中的配置方式。您可以删除策略、编辑策略、将策略附加到权限集。

All permission sets for an Amazon Web Services 账户

要查看某个权限集的所有分配，请执行以下过程：

1. 登录 Amazon Web Services 管理控制台 并打开 Amazon IAM Identity Center 控制台，网址为https://console.aws.amazon.com/singlesignon/。
2. 在多帐户权限下，选择 Amazon Web Services 账户。选择您要查看已配置权限集的账户。
3. 进入选定 Amazon Web Services 账户 页面后，在 “权限集” 选项卡下，您可以查看分配给选定权限的不同权限集 Amazon Web Services 账户。您可以点击权限集的超链接，了解该权限集的详细信息。

All applied permission sets to users and groups

要查看分配给用户或组的所有权限集，请执行以下过程：

1. 登录 Amazon Web Services 管理控制台 并打开 Amazon IAM Identity Center 控制台，网址为https://console.aws.amazon.com/singlesignon/。
2. 在控制面板下选择“用户”或“组”，查看 IAM Identity Center 用户或组。
   a. 进入用户页面后，选择您要查看其已应用权限集的用户。接下来，选择 Amazon Web Services 账户 选项卡，然后选择 Amazon 账户访问区域下的 Amazon Web Services 账户 。您将能够看到所选用户的已应用权限集。 Amazon Web Services 账户
   b. 进入组页面后，选择您要查看其已应用权限集的组。接下来，选择 Amazon Web Services 账户选项卡，然后选择 Amazon Web Services 账户 访问区域下的 Amazon Web Services 账户 。您将能够看到所选群组所应用 Amazon Web Services 账户 的权限集。

更改权限集

按照此过程通过 IAM Identity Center 控制台更改权限集。您可以向用户或组添加或移除权限集。

1. 登录 Amazon Web Services 管理控制台 并打开 Amazon IAM Identity Center 控制台，网址为https://console.aws.amazon.com/singlesignon/。
2. 在多帐户权限下，选择 Amazon Web Services 账户。
3. 在 Amazon Web Services 账户 页面上，将显示您的组织的树视图列表。选择要更改权限集的 Amazon Web Services 账户 的名称。
4. 在 Amazon Web Services 账户概述页面上，从分配的用户和组下选择要更改的权限集的用户名或组名。然后选择更改权限集。

5. 对权限集进行所需更改，然后选择保存更改。
6. 导航至权限集选项卡，选择最近更改的权限集，然后选择更新。
7. 在更新权限页面选择更新。

委派权限集管理

IAM Identity Center 允许您通过创建引用 IAM 身份中心资源的亚马逊资源名称 (ARNs) 的 IAM 策略来委托账户中的权限集和分配的管理。例如，您可以创建策略，使不同的管理员能够在指定帐户中为具有特定标签的权限集管理分配。

> **Note**
>
> 要使用权限集，您将需要使用 IAM Identity Center 的组织实例。有关更多信息，请参阅 IAM Identity Center 的组织和账户实例。

您可以使用下列任一方法创建这些类型的策略。

- （推荐）在 IAM Identity Center 中创建权限集，每个权限集都有不同的策略，并将权限集分配给不同的用户或组。这使您能够管理使用您选择的 IAM Identity Center 身份源登录的用户的管理权限。
- 在 IAM 中创建自定义策略，然后将其附加到您的管理员担任的 IAM 角色。有关角色的信息，请参阅 IAM 角色以获取为其分配的 IAM Identity Center 管理权限。

> **Important**
>
> IAM 身份中心资源区 ARNs 分大小写。

以下内容显示了引用 IAM Identity Center 权限集和帐户资源类型的正确案例。

资源类型	进行筛选	上下文键
PermissionSet	`arn:${Partition}:sso:::permissionSet/${InstanceId}/${PermissionSetId}`	`aws:ResourceTag/${TagKey}`

资源类型	进行筛选	上下文键
Account	`arn:${Partition}:sso:::account/${AccountId}`	不适用

在权限集中使用 IAM 策略

在 创建权限集 中，您学习了如何向权限集添加策略，包括客户管理型策略和权限边界。当您将客户管理型策略和权限添加到权限集时，IAM Identity Center 不会在任何 Amazon Web Services 账户中创建策略。相反，您必须在要分配权限集的每个帐户中提前创建这些策略，并将它们与权限集的名称和路径规范相匹配。当您将权限集分配给组织 Amazon Web Services 账户 中的时，IAM Identity Center 会创建一个 Amazon Identity and Access Management (IAM) 角色并将您的 IAM 策略附加到该角色。

注意事项

- 要使用权限集，您将需要使用 IAM Identity Center 的组织实例。有关更多信息，请参阅 IAM Identity Center 的组织和账户实例。
- 在使用 IAM policy 分配权限集之前，您必须准备好您的成员帐户。成员账户中的 IAM 策略名称必须与管理账户中的策略名称相符。如果您的成员帐户中不存在权限集，IAM Identity Center 将无法分配权限集。

> **Note**
>
> 当客户管理型策略附加到权限集时，策略名称不区分大小写。

- 策略授予的权限不必在账户之间完全匹配。

将 IAM 策略分配给权限集

1. 在您要分配权限集的每个 Amazon Web Services 账户 位置中创建一个 IAM 策略。
2. 向 IAM policy 分配权限。您可以在不同的帐户中分配不同的权限。为了获得一致的体验，请在每个策略中配置和维护相同的权限。您可以使用自动化资源，例如 Amazon CloudFormation StackSets 在每个成员账户中创建具有相同名称和权限的 IAM 策略的副本。有关的更多信息 CloudFormation StackSets，请参阅《Amazon CloudFormation 用户指南》 Amazon CloudFormation StackSets中的 “使用”。

3. 在您的管理帐户中创建权限集，并在客户管理型策略或权限边界下添加您的 IAM policy。有关如何创建权限集的更多详细信息，请参阅 创建权限集。
4. 添加您准备的所有内联策略、 Amazon 管理型策略或其他 IAM policy。
5. 创建并分配您的权限集。

在 IAM Identity Center 中移除权限集

您可以在 IAM Identity Center 控制台中从 IAM Identity Center 用户和组移除权限集。您也可以从 Amazon Web Services 账户移除权限集。有关权限集以及如何在 IAM Identity Center 中使用权限集的更多信息，请参阅 Amazon Web Services 账户 使用权限集进行管理。

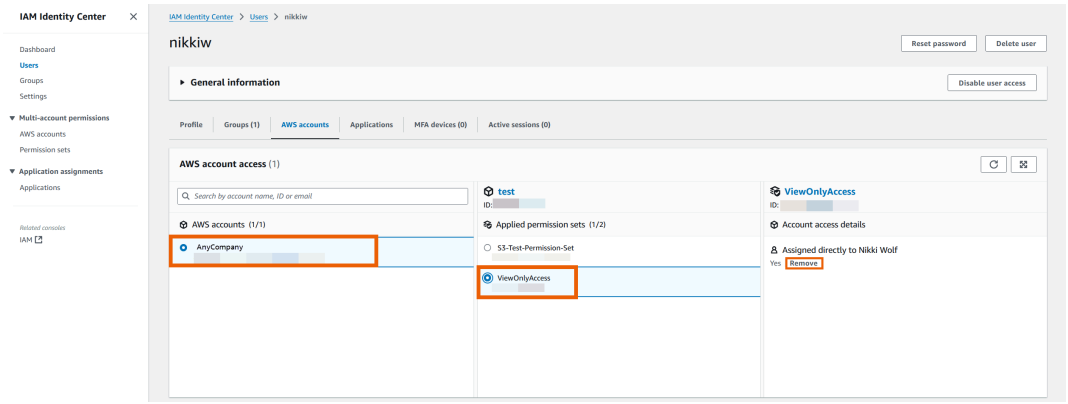
> **Note**
>
> 要使用权限集，您将需要使用 IAM Identity Center 的组织实例。有关更多信息，请参阅 IAM Identity Center 的组织和账户实例。

Remove permission set from a user

从用户移除权限集

使用此过程通过 IAM Identity Center 控制台从用户移除权限集。

1. 登录 Amazon Web Services 管理控制台 并打开 Amazon IAM Identity Center 控制台，网址为https://console.aws.amazon.com/singlesignon/。
2. 在 IAM Identity Center 下，选择用户。
3. 选择您要移除其权限集的用户名。
4. 在用户详情页面，选择 Amazon Web Services 账户选项卡。在 Amazon Web Services 账户访问下，选择您的 Amazon Web Services 账户。
5. 右侧面板将显示所选用户的已应用权限。选择您要移除的权限集。在账户访问详情下，选择移除。
6. 系统将弹出对话框，询问您是否要移除该权限集。选择移除。

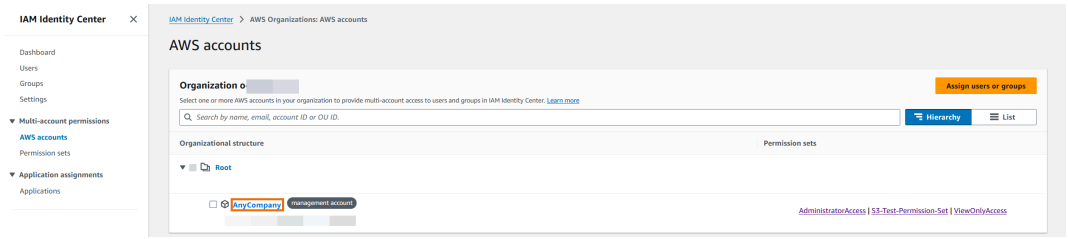


Remove permission set from a group

从组移除权限集

使用此过程通过 IAM Identity Center 控制台从组移除权限集。

1. 登录 Amazon Web Services 管理控制台 并打开 Amazon IAM Identity Center 控制台，网址为https://console.aws.amazon.com/singlesignon/。
2. 在多账户权限下，选择 Amazon Web Services 账户。选择指向您管理账户的链接。



3. 在已分配用户和组选项卡下，选择您要移除其权限集的组，然后选择修改权限集。
4. 在更改权限集页面上，清除您要移除的权限集，然后选择保存更改。

Remove permission set from an Amazon Web Services 账户

使用此过程通过 IAM Identity Center 控制台从 Amazon Web Services 账户 移除权限集。

1. 登录 Amazon Web Services 管理控制台 并打开 Amazon IAM Identity Center 控制台，网址为https://console.aws.amazon.com/singlesignon/。
2. 在多账户权限下，选择 Amazon Web Services 账户。选择要 Amazon Web Services 账户 从中移除权限集的名称。

3. 在 Amazon Web Services 账户的概述页面上，选择权限集选项卡。选择您要移除的权限集。然后选择移除。
4. 在移除权限集对话框中，确认选择了正确的权限集，输入 **Delete** 以确认移除，然后选择移除访问权限。

在 IAM Identity Center 中删除权限集

在从 IAM Identity Center 删除权限集之前，您应将其从使用该权限集的所有 Amazon Web Services 账户 中移除。要查看现有用户和组的访问权限，请参阅查看和更改权限集。

注意事项

- 要使用权限集，您将需要使用 IAM Identity Center 的组织实例。有关更多信息，请参阅 IAM Identity Center 的组织和账户实例。
- 如果要撤销活跃权限集会话，请参阅the section called “结束员工用户的活跃会话”。
- 在删除用户或组之前，应先从这些用户或组中移除权限集和应用程序分配。否则，IAM Identity Center 中将会存在未分配且未使用的权限集和应用程序。

使用以下步骤删除一个或多个权限集，这样组织 Amazon Web Services 账户 中的任何人就无法再使用这些权限集。

> **Important**
>
> 已分配此权限集的所有用户和群组，无论使用 Amazon Web Services 账户 的是什么，都将无法再登录。要查看现有用户和组的访问权限，请参阅查看和更改权限集。

从中删除权限集 Amazon Web Services 账户

1. 打开 IAM Identity Center 控制台。
2. 在多帐户权限下，选择权限集。
3. 选择要删除的权限集，然后选择 Delete (删除)。
4. 在删除权限集对话框中，输入权限集的名称以确认删除，然后选择删除。该名称区分大小写。

配置权限集属性

在 IAM Identity Center 中，管理员可以通过完成以下配置和管理任务来控制用户访问权限及会话持续时间。

Task	了解详情
管理员可以设置通过 IAM Identity Center 访问 Amazon 资源时用户会话的最大持续时间。	将会话持续时间设置为 Amazon Web Services 账户
管理员可以自定义用户在成功通过 IAM Identity Center 进行身份验证后看到的登录页面。	设置中继状态以便快速访问 Amazon Web Services 管理控制台
确保用户在权限被撤销后无法再访问 Amazon 资源。	使用“拒绝策略”撤销活跃用户权限

将会话持续时间设置为 Amazon Web Services 账户

对于每个 权限集，您可以指定会话持续时间，以控制用户可登录 Amazon Web Services 账户帐户的时间长度。当指定的持续时间过后，用户 Amazon 将退出会话。

创建新权限集时，会话持续时间默认设置为 1 小时（以秒为单位）。最短会话持续时间为 1 小时，最多可设置为 12 小时。IAM Identity Center 会在每个分配的帐户中为每个权限集自动创建 IAM 角色，并将这些角色配置为最长会话持续时间为 12 小时。

当用户联合访问其 Amazon Web Services 账户 控制台或使用 Amazon Command Line Interface (Amazon CLI) 时，IAM Identity Center 会使用权限集上的会话持续时间设置来控制会话的持续时间。默认情况下，IAM Identity Center 为权限集生成的 IAM 角色只能由 IAM Identity Center 用户担任，这可确保强制实施 IAM Identity Center 权限集中指定的会话持续时间。

> **Important**
>
> 作为最佳安全做法，我们建议您设置的会话持续时间长度不要超过执行角色所需的时间。

创建权限集后，您可以对其进行更新以应用新的会话持续时间。使用以下过程修改该权限集的会话持续时间长度。

设置会话持续时间

1. 打开 IAM Identity Center 控制台。
2. 在多帐户权限下，选择权限集。
3. 选择要为其更改会话持续时间的权限集的名称。
4. 在权限集的详细信息页面上，在常规设置 部分标题的右侧，选择编辑。
5. 在编辑常规权限集设置页面上，为会话持续时间选择一个新值。
6. 如果以任何方式配置了权限集 Amazon Web Services 账户，则帐户名称将显示在下面，Amazon Web Services 账户 以便自动重新置备。权限集的会话持续时间值更新后，将重新配置所有使用 Amazon Web Services 账户 该权限集的用户。这意味着此设置的新值将应用于所有使用 Amazon Web Services 账户 该权限集的用户。
7. 选择保存更改。
8. Amazon Web Services 账户 页面顶部会显示一条通知。
   - 如果在一个或多个 Amazon Web Services 账户中配置了权限集，则通知会确认 Amazon Web Services 账户 已成功重新配置，并且更新的权限集已应用于帐户。
   - 如果未在中配置权限集 Amazon Web Services 账户，则通知将确认权限集的设置已更新。

设置中继状态以便快速访问 Amazon Web Services 管理控制台

默认情况下，当用户登录 Amazon Web Services 访问门户，选择账户，然后选择根据分配的权限集 Amazon 创建的角色时，IAM Identity Center 会将用户的浏览器重定向到。 Amazon Web Services 管理控制台您可以通过将中继状态设置为不同的控制台 URL 来更改此行为。

通过设置中继状态，您能够为用户提供对最适合其角色的控制台的快速访问。例如，您可以将中继状态设置为 Amazon EC2 控制台 URL (**`https://console.aws.amazon.com/ec2/`**)，以便在用户选择 Amazon EC2 管理员角色时将用户重定向到该控制台。在重定向到默认 URL 或中继状态 URL 的过程中，IAM Identity Center 会将用户的浏览器路由到用户上次 Amazon Web Services 区域 使用的控制台终端节点。例如，如果用户结束了欧洲地区（斯德哥尔摩）(eu-north-1) 的最后一个控制台会话，则该用户将被重定向到该区域中的 Amazon EC2 控制台。

要配置 IAM Identity Center 以将用户重定向到特定 Amazon Web Services 区域中的控制台，将区域规范包含在 URL 中。例如，要将用户重定向到美国东部（俄亥俄州）(us-east-2) 中的 Amazon EC2 控制台，指定该区域中 Amazon EC2 控制台的 URL (**`https://us-east-2.console.aws.amazon.com/ec2/`**)。如果您在美国西部（俄勒冈州）(us-

west-2) 启用了 IAM Identity Center，并且您希望将用户定向到该区域，指定 **`https://us-west-2.console.aws.amazon.com`**。

配置中继状态

使用以下过程为权限集配置中继状态 URL。

1. 打开 IAM Identity Center 控制台。
2. 在多帐户权限下，选择权限集。
3. 选择要为其设置新中继状态 URL 的权限集的名称。
4. 在权限集的详细信息页面上，在常规设置 部分标题的右侧，选择编辑。
5. 在 “编辑常规权限集设置” 页面的 “中继状态” 下，键入任何 Amazon 服务的控制台 URL。例如：

   `https://console.aws.amazon.com/ec2/`

   > **Note**
   >
   > 中继状态 URL 必须在 Amazon Web Services 管理控制台中。

6. 如果以任何方式配置了权限集 Amazon Web Services 账户，则帐户名称将显示在下面，Amazon Web Services 账户 以便自动重新置备。权限集的中继状态 URL 更新后，所有使用 Amazon Web Services 账户 该权限集的用户都将重新置备。这意味着此设置的新值将应用于所有使用 Amazon Web Services 账户 该权限集的用户。
7. 选择保存更改。
8. 在 Amazon 组织页面的顶部会显示一条通知。

   - 如果在一个或多个 Amazon Web Services 账户中配置了权限集，则通知会确认 Amazon Web Services 账户 已成功重新配置，并且更新的权限集已应用于帐户。
   - 如果权限集未在 Amazon Web Services 账户中配置，则通知会确认权限集的设置已更新。

> **Note**
>
> 您可以使用 Amazon API、 Amazon SDK 或 Amazon Command Line Interface(Amazon CLI) 自动执行此过程。有关更多信息，请参阅:
>
> - IAM Identity Center API 参考中的 `CreatePermissionSet` 或 `UpdatePermissionSet` 操作

- Amazon CLI 命令参考的 sso-admin 部分中的 `create-permission-set` 或 `update-permission-set` 命令。

使用“拒绝策略”撤销活跃用户权限

当 IAM Identity Center 用户正在使用权限集 Amazon Web Services 账户 时，您可能需要撤销该用户的访问权限。事先为未指定用户实施“拒绝策略”，可以取消其使用其活跃 IAM 角色会话的权限；然后在需要时可以更新“拒绝策略”，指定要阻止其访问权限的用户。本主题旨在介绍如何创建“拒绝策略”以及部署策略的注意事项。

准备撤销由权限集创建的活跃 IAM 角色会话

您可以通过使用“服务控制策略”对特定用户应用“全部拒绝”策略，以此阻止用户使用他们正活跃使用的 IAM 角色执行操作。您还可以在自己更改密码之前阻止用户使用任何权限集，这样可以移除活跃滥用被盗凭证的恶意行为者。如需大范围拒绝访问并阻止用户重新进入权限集或访问其他权限集，也可移除所有用户访问权限，停止活跃的 Amazon Web Services 访问门户会话，并禁用用户登录。请参阅the section called “结束员工用户的活跃会话”，了解如何将“拒绝策略”与其他操作结合使用，从而扩大访问权限的撤销范围。

拒绝策略

您可以使用“拒绝策略”，其条件与 IAM Identity Center 身份存储中的用户 `UserID` 匹配，以此阻止用户使用他们正活跃使用的 IAM 角色执行进一步的操作。使用此策略可以避免对部署“拒绝策略”时可能使用相同权限集的其他用户造成影响。此策略将占位符用户 ID *`Add user ID here`* 用于您将通过要撤销访问权限的用户 ID 进行更新的 `"identitystore:userId"`。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "*"
            ],
            "Resource": "*",
            "Condition": {
```

```
                "StringEquals": {
                    "identitystore:userId": "Add user ID here"
                }
            }
        }
    ]
}
```

虽然可以使用其他条件键（例如“aws:userId”），但“identitystore:userId”是确定的，因为这是与某个人员有关的全局唯一值。在条件中使用“aws:userId”可能会受到从身份源同步用户属性的方式影响，并且如果用户的用户名或电子邮件地址发生变化，则可能会发生变化。

在 IAM Identity Center 控制台中，您可以通过导航到用户、按用户名搜索用户、展开一般信息部分并复制用户 ID 来查找用户 identitystore:userId。在搜索用户 ID 时，停止用户的 Amazon Web Services 访问门户会话并禁用他们在同一部分的登录访问权限也很方便。您可以通过查询身份存储来获取用户的用户 ID，从而自动创建拒绝策略 APIs。

部署“拒绝策略”

您可以使用无效的占位符用户 ID（例如）*Add user ID here*，使用附加到 Amazon Web Services 账户 用户可能有权访问的服务控制策略 (SCP) 提前部署拒绝策略。推荐使用此方法，因为操作简单、见效快。使用“拒绝策略”撤销用户的访问权限时，您需要编辑该策略，将占位符用户 ID 替换为要撤销其访问权限之人的用户 ID。这可以防止用户使用您附加 SCP 的各个账户中设置的任何权限集执行任何操作。即使用户使用活跃的 Amazon Web Services 访问门户会话导航到不同账户并代入不同角色，也无法进行操作。当 SCP 完全屏蔽了用户的访问权限后，您可以根据需要禁用他们的登录、撤消分配和停止 Amazon Web Services 访问门户会话的功能。

除了使用之外 SCPs，您还可以将 “拒绝” 策略包含在权限集的内联策略和用户可以访问的权限集使用的客户托管策略中。

如果必须撤销多人的访问权限，则可在条件块中使用值列表，例如：

```
        "Condition": {
                "StringEquals": {
                    "identitystore:userId": [" user1 userId", "user2 userId"...]
                    }
    }
```

> **Important**
>
> 无论采用何种方法，均须采取任何其他纠正措施，并在策略中保留用户的用户 ID 至少 12 小时。之后，用户代入的任何角色都将过期，然后您可以将其用户 ID 从“拒绝策略”中移除。

在资源策略、Amazon EKS 集群配置映射和 Amazon KMS 密钥策略中引用权限集

当您为 Amazon 账户分配权限集时，IAM Identity Center 会创建一个名称以开头的角色`AWSReservedSSO_`。

角色的完整名称和 Amazon 资源名称（ARN）使用以下格式：

Name	进行筛选
`AWSReservedSSO_` *`permission-set-name_unique-suffix`*	`arn:aws:iam::` *`aws-account-ID`*`:role/aws-reserved/sso.amazonaws.com/` *`aws-region`* `/AWSReservedSSO_` *`permission-set-name_unique-suffix`*

如果您在 IAM 身份中心中的身份源托管在 us-east-1 中，则 ARN 中没有。*`aws-region`*角色的完整名称和 ARN 使用以下格式：

Name	进行筛选
`AWSReservedSSO_` *`permission-set-name_unique-suffix`*	`arn:aws:iam::` *`aws-account-ID`* `:role/aws-reserved/sso.amazonaws.com/AWSReservedSSO_` *`permission-set-name_unique-suffix`*

例如，如果您创建了向数据库管理员授予 Amazon 账户访问权限的权限集，则会使用以下名称和 ARN 创建相应的角色：

Name	进行筛选
AWSReservedSSO_DatabaseAdministrator_1234567890abcdef	arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_1234567890abcdef

如果您删除 Amazon 账户中对该权限集的所有分配，则 IAM Identity Center 创建的相应角色也会被删除。如果您稍后对同一权限集进行新分配，IAM Identity Center 会为该权限集创建一个新角色。新角色的名称和 ARN 包含不同的唯一后缀。在此示例中，唯一后缀是 abcdef0123456789。

Name	进行筛选
AWSReservedSSO_DatabaseAdministrator_ **abcdef0123456789**	arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_ **abcdef0123456789**

角色的新名称和 ARN 的后缀更改将导致任何引用原始名称和 ARN 的策略出现，从而中断使用 out-of-date相应权限集的个人的访问权限。例如，如果在以下配置中引用原始 ARN，则角色 ARN 的更改将中断权限集用户的访问：

- 如使用 `aws-auth ConfigMap` 访问集群，则在 Amazon Elastic Kubernetes Service（Amazon EKS）集群的 `aws-auth ConfigMap` 文件中。
- 在 Amazon Key Management Service (Amazon KMS) 密钥的基于资源的策略中。该政策也被称为密钥政策。

> **Note**
>
> 建议使用 Amazon EKS 访问条目管理对 Amazon EKS 集群的访问权限。这样您就可以使用 IAM 权限管理有权访问 Amazon EKS 集群的主体。通过使用 Amazon EKS 访问条目，您无需

联系 Amazon Web Services 支持即可使用具有 Amazon EKS 权限的 IAM 主体重新获得对集群的访问权限。

尽管您可以更新大多数 Amazon 服务的基于资源的策略，以便为与权限集相对应的角色引用新 ARN，但您必须拥有在 IAM for Amazon EKS 中创建的备用角色， Amazon KMS 并且如果 ARN 发生变化。对于 Amazon EKS，备份 IAM 角色必须存在于 `aws-auth ConfigMap` 中。因为 Amazon KMS，它必须存在于您的密钥策略中。如果您没有有权更新`aws-auth ConfigMap`或 Amazon KMS 密钥策略的备用 IAM 角色，请联系 Amazon Web Services 支持 以重新获得对这些资源的访问权限。

避免访问中断的建议

为了避免因与权限集对应的角色的 ARN 更改而导致访问中断，我们建议您执行以下操作。

- 维护至少一项权限集分配。

  在包含您在 Amazon EKS 中引用的角色、中的`aws-auth ConfigMap`关键策略或其他 Amazon Web Services 服务基于资源的策略的 Amazon 账户中 Amazon KMS保留此分配。

  例如，如果您创建`EKSAccess`权限集并从 Amazon 账户中引用相应角色 ARN`111122223333`，则将管理组永久分配给该账户中的权限集。由于分配是永久性的，IAM Identity Center 不会删除相应的角色，从而消除了重命名风险。管理组将始终具有访问权限，而无需担心权限升级的风险。
- 对于使用**`aws-auth ConfigMap`**和的 Amazon EKS 集群 Amazon KMS：包括在 IAM 中创建的角色。

  如果您在 for Amazon EKS 集群中 ARNs `aws-auth ConfigMap`为权限集引用角色，或者在 Amazon KMS 密钥策略中为密钥引用角色，我们建议您至少包括一个在 IAM 中创建的角色。该角色必须允许您访问 Amazon EKS 集群或管理 Amazon KMS 密钥策略。权限集必须能够承担此角色。这样，如果权限集的角色 ARN 发生更改，则可以在或密钥策略中更新对 ARN 的`aws-auth ConfigMap`引用。 Amazon KMS 下一部分提供了如何为 IAM 中创建的角色创建信任策略的示例。该角色只能由 `AdministratorAccess` 权限集承担。

自定义信任策略示例

以下是自定义信任策略的示例，该策略提供 `AdministratorAccess` 权限集，可以访问在 IAM 中创建的角色。该策略的关键要素包括：

- 此信任策略的 “委托人” 元素指定了 Amazon 账户委托人。在此策略中， Amazon 账户中111122223333拥有sts:AssumeRole权限的委托人可以代入在 IAM 中创建的角色。
- 此信任策略的 Condition element 指定了可以担任在 IAM 中创建的角色的主体的附加要求。在此策略中，具有以下角色 ARN 的权限集可以担任该角色。

```
arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/
AWSReservedSSO_AdministratorAccess_*"
```

> **Note**
>
> Condition 元素包括 ArnLike 条件运算符，并在权限集角色 ARN 末尾使用通配符，而不是唯一的后缀。这意味着，即使权限集的角色 ARN 发生更改，策略也允许权限集代入在 IAM 中创建的角色。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnLike": {
          "aws:PrincipalArn": "arn:aws:iam::111122223333:role/aws-reserved/
sso.amazonaws.com/eu-west-2/AWSReservedSSO_AdministratorAccess_*"
        }
      }
    }
  ]
}
```

如果意外删除并重新创建了权限集或对该权限集的所有分配，则在此类策略中包含您在 IAM 中创建的角色将为您提供对您的 Amazon EKS 集群或其他 Amazon 资源的紧急访问权限。 Amazon KMS keys

基于属性的访问控制

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。您可以使用 IAM Identity Center Amazon Web Services 账户 使用来自任何 IAM Identity Center 身份源的用户属性来管理对多个 Amazon 资源的访问权限。在中 Amazon，这些属性称为标签。在中使用用户属性作为标签 Amazon 可以帮助您简化在中创建细粒度权限的过程， Amazon 并确保您的员工只能访问带有匹配标签的 Amazon 资源。

例如，您可以将来自两个不同团队的开发人员 Bob 和 Sally 分配到 IAM Identity Center 中的相同权限集，然后选择团队名称属性进行访问控制。当 Bob 和 Sally 登录他们时 Amazon Web Services 账户，IAM Identity Center 会在 Amazon 会话中发送他们的团队名称属性，因此，只有当他们的团队名称属性与 Amazon 项目资源上的团队名称标签匹配时，Bob 和 Sally 才能访问项目资源。如果 Bob 将来转到 Sally 的团队，您只需在公司目录中更新他的团队名称属性即可修改他的访问权限。当 Bob 下次登录时，他将自动获得对新团队的项目资源的访问权限，而不需要在 Amazon中更新任何权限。

此方法还有助于减少您需要在 IAM Identity Center 中创建和管理的不同权限的数量，因为与相同权限集关联的用户现在可以根据其属性拥有唯一权限。您可以在 IAM Identity Center 权限集和基于资源的策略中使用这些用户属性对 Amazon 资源实施 ABAC 并大规模简化权限管理。

优势

以下是在 IAM Identity Center 使用 ABAC 的其他好处。

- ABAC 需要更少的权限集 – 由于您不必为不同的工作职能创建不同的策略，因此您创建的权限集更少。这降低了权限管理的复杂性。
- 使用 ABAC，团队可以快速变化和成长 – 当资源在创建时被适当标记时，系统会根据属性自动授予新资源的权限。
- 通过 ABAC 使用公司目录中的员工属性 – 您可以使用 IAM Identity Center 中配置的任何身份源中的现有员工属性在 Amazon中做出访问控制决策。
- 跟踪谁在访问资源 — 安全管理员可以通过查看中的用户属性来跟踪中的用户活动， Amazon CloudTrail 从而轻松确定会话的身份 Amazon。

有关使用 IAM Identity Center 控制台如何配置 ABAC 的信息，请参阅 访问控制属性。有关如何使用 IAM 身份中心启用和配置 ABAC 的信息 APIs，请参阅 I AM 身份中心 API 参考指南CreateInstanceAccessControlAttributeConfiguration中的。

主题

- 清单： Amazon 使用 IAM 身份中心配置 ABAC

- 访问控制属性

清单： Amazon 使用 IAM 身份中心配置 ABAC

此清单包括准备您的 Amazon 资源和设置 IAM Identity Center 以进行 ABAC 访问所需的配置任务。按顺序完成此清单中的任务。当参考链接将您带到某个主题时，请返回到该主题，以便您可以继续执行此清单中的其余任务。

步骤	Task	参考
1	查看如何为所有 Amazon 资源添加标签。要在 IAM Identity Center 中实施 ABAC，您首先需要向要实施 ABAC 的所有 Amazon 资源添加标签。	• 为资源添加标签 Amazon
2	查看如何使用身份存储中的关联用户身份和属性在 IAM Identity Center 中配置您的身份源。IAM 身份中心允许您在中使用 ABAC 的任何支持的 IAM 身份中心身份源的用户属性。 Amazon	• 管理您的身份源
3	根据以下标准，确定要使用哪些属性来做出访问控制决策，然后将其发送到 IAM I Amazon dentity Center。	• 开始使用
	• 如果您使用外部身份提供者（IdP），请决定是要使用从 IdP 传递的属性还是从 IAM Identity Center 中选择属性。	• 使用外部身份提供者作为身份源时选择属性
	• 如果您选择让 IdP 发送属性，请将 IdP 配置为在 SAML 断言中传输属性。请参阅特定 IdP 教程中的 `Optional` 部分。	• IAM Identity Center 身份源教程
	• 如果您使用 IdP 作为身份源并选择在 IAM Identity Center 中选择属性，请研究如何配置 SCIM 以便属性值来自您的 IdP。如果您无法将 SCIM 与 IdP 一起使用，则使用 IAM Identity Center 控制台用户页面添加用户及其属性。	• 使用 SCIM 从外部身份提供者预置用户和组 • 支持的外部身份提供商属性
	• 如果您使用 Active Directory 或 IAM Identity Center 作为身份源，或者使用 IdP 并选择在 IAM Identity	• 使用 IAM Identity Center 作为身份源时选择属性

步骤	Task	参考
	Center 中选择属性，则查看您可以配置的可用属性。然后立即跳至步骤 4，开始使用 IAM Identity Center 控制台配置您的 ABAC 属性。	• 在 Amazon Managed Microsoft AD 用作身份来源时选择属性 • IAM Identity Center 与 Microsoft AD 之间的默认映射
4	使用 IAM Identity Center 控制台中的访问控制属性页面选择要用于 ABAC 的属性。在此页面中，您可以从步骤 2 中配置的身份源中选择访问控制属性。在您的身份及其属性进入 IAM Identity Center 后，您必须创建键值对（映射），这些键值对将传递给您以 Amazon Web Services 账户 用于访问控制决策。	• 启用并配置访问控制属性
5	在权限集中创建自定义权限策略，并使用访问控制属性创建 ABAC 规则，以便用户只能访问具有匹配标签的资源。您在步骤 4 中配置的用户属性将用作 Amazon 中的标签来做出访问控制决策。您可以使用 `aws:PrincipalTag/key` 条件引用权限策略中的访问控制属性。	• 在 IAM Identity Center 中为 ABAC 创建权限策略
6	在您的各种权限集中 Amazon Web Services 账户，将用户分配给您在步骤 5 中创建的权限集。这样做可以确保当他们联合账户并访问 Amazon 资源时，他们只能根据匹配的标签获得访问权限。	• 为用户或群组分配访问权限 Amazon Web Services 账户

完成这些步骤后，联合 Amazon Web Services 账户 使用单点登录的用户将根据匹配的属性访问其 Amazon 资源。

访问控制属性

访问控制属性是 IAM Identity Center 控制台中的页面名称，您可以在其中选择要在策略中使用的用户属性来控制对资源的访问。您可以 Amazon 根据用户身份源中的现有属性将用户分配给中的工作负载。

例如，假设您想要根据部门名称分配对 S3 桶的访问权限。在访问控制属性页面上，您可以选择部门用户属性以与基于属性的访问权限控制（ABAC）结合使用。然后，您可以在 IAM Identity Center 权限集中编写一个策略，仅当部门属性与您分配给 S3 桶的部门标签匹配时才授予用户访问权限。IAM Identity Center 将用户的部门属性传递给正在访问的帐户。然后，该属性用于根据策略确定访问。当 IAM Identity Center 将这些属性传递给账户时，它们将作为会话标签发送，您可以使用所有相关 Amazon IAM 策略类型中的`aws:PrincipalTag/`*`tag-key`*条件密钥来引用这些标签。有关 ABAC 的更多信息，请参阅基于属性的访问控制。

开始使用

如何开始配置访问控制属性取决于您使用的身份源。无论您选择哪种身份源，在选择属性后，您都需要创建或编辑权限集策略。这些策略必须授予用户身份访问 Amazon 资源的权限。

使用 IAM Identity Center 作为身份源时选择属性

当您将 IAM Identity Center 配置为身份源时，您首先添加用户并配置其属性。接下来，导航到访问控制的属性页面，然后选择要在策略中使用的属性。最后，导航到 Amazon Web Services 账户 页面以创建或编辑权限集以使用 ABAC 的属性。

在 Amazon Managed Microsoft AD 用作身份来源时选择属性

当您将 IAM 身份中心配置 Amazon Managed Microsoft AD 为身份源时，首先要将 Active Directory 中的一组属性映射到 IAM Identity Center 中的用户属性。接下来，导航到访问控制的属性页面。然后，根据从 Active Directory 映射的现有 SSO 属性集选择要在 ABAC 配置中使用的属性。最后，作者使用权限集中的访问控制属性来编写 ABAC 规则，以授予用户身份对 Amazon 资源的访问权限。有关 IAM Identity Center 中用户属性与 Amazon Managed Microsoft AD 目录中用户属性的默认映射列表，请参阅IAM Identity Center 与 Microsoft AD 之间的默认映射。

使用外部身份提供者作为身份源时选择属性

当您使用外部身份提供者（IdP）作为身份源配置 IAM Identity Center 时，有两种方法可以使用 ABAC 的属性。

- 在 IAM 身份中心控制台中配置属性映射。您可以在 IAM Identity Center 控制台的访问控制属性页面上将 IAM 身份中心目录中的属性映射到会话标签。您在此处选择的属性值源自 Identity Center 目录，用于替换通过 SAML 断言来自 IdP 的任何匹配属性的值。根据您是否使用 SCIM，请考虑以下事项：
  - 如果使用 SCIM，IdP 会自动将属性值同步到 IAM Identity Center。然后，您可以在 “访问控制的属性” 页面上选择这些同步属性，将其用作会话标记。

  - 如果您不使用 SCIM，则必须手动添加用户并设置其属性，就像使用 IAM Identity Center 作为身份源一样。接下来，导航到访问控制的属性页面，然后选择要在策略中使用的属性。
- 通过 SAML 断言传递来自 IdP 的属性。您可以将 IdP 配置为通过 SAML 断言将属性作为会话标签发送。为此，请将您的 IdP 配置为发送 SAML 断言，并将属性名称设置为`https://aws.amazon.com/SAML/Attributes/AccessControl:`*`TagKey`*，替换为要填*`TagKey`*充的会话标签密钥。IAM Identity Center 将来自 IdP 的属性名称和值传递给策略评估。

  对于通过外部 IdP 的 SAML 断言传入的属性，无需在 “访问控制的属性” 页面上配置 ABAC 属性映射。但是，如果您在 “访问控制的属性” 页面上为同一属性配置 ABAC 映射，则身份中心目录中的映射优先，并替换您的 IdP 在 SAML 断言中发送的值。

  > **Note**
  >
  > SAML 断言中的属性在访问控制属性页面上对您不可见。您必须提前了解这些属性，并在编写策略时将它们添加到访问控制规则中。如果您决定信任外部 IdPs 的属性，那么当用户联合到 Amazon Web Services 账户时，这些属性将始终被传递。有关如何在 IdP 中配置进行访问控制的用户属性以通过 SAML 断言发送的信息，请参阅 IdP IAM Identity Center 身份源教程。

有关 IAM Identity Center 中的用户属性与外部用户属性的支持属性的完整列表 IdPs，请参阅支持的外部身份提供商属性。

要开始在 IAM Identity Center 中使用 ABAC，请参阅以下主题。

主题

- 启用并配置访问控制属性
- 在 IAM Identity Center 中为 ABAC 创建权限策略

启用并配置访问控制属性

要使用基于属性的访问权限控制（ABAC），您必须首先在 IAM Identity Center 控制台的设置页面或 IAM Identity Center API 中启用它。无论使用何种身份源，您都可以从身份存储中配置用户属性，用于基于属性的访问控制（ABAC）。在控制台中，您可通过导航至设置页面的访问控制属性选项卡完成此配置。如果您使用外部身份提供者（IdP）作为身份源，还可以选择通过 SAML 断言接收来自外部 IdP 的属性。在此情况下，您需要配置外部 IdP 以发送所需属性。如果 SAML 断言中的某个属性在

IAM Identity Center 中也被定义为 ABAC 属性，则 IAM Identity Center 会在用户登录 Amazon Web Services 账户时，将其身份存储中的该属性值作为会话标签发送。

> **Note**
>
> 您无法从 IAM Identity Center 控制台的访问控制属性页面查看外部 IdP 配置和发送的属性。如果您在来自外部 IdP 的 SAML 断言中传递访问控制属性，则当用户进行联合身份验证时，这些属性将直接发送到 Amazon Web Services 账户 。这些属性在 IAM Identity Center 中不可用于映射。

主题

启用访问控制属性

使用以下过程可使用 IAM Identity Center 控制台启用访问属性 (ABAC) 控制功能。

> **Note**
>
> 如果您有现有权限集且计划在 IAM Identity Center 实例中启用 ABAC，则额外的安全限制要求您首先拥有 `iam:UpdateAssumeRolePolicy` 策略。如果您没有在帐户中创建任何权限集，则不需要这些额外的安全限制。
>
> 如果您的 IAM Identity Center 实例是在 2020 年 12 月之前创建的，并且您计划在其中启用 ABAC，则无论您的账户中是否创建了权限集，都必须将`iam:UpdateAssumeRolePolicy`策略与 IAM Identity Center 管理角色相关联。

启用访问控制的属性

1. 打开 IAM Identity Center 控制台。
2. 选择 设置
3. 在设置页面上，找到访问控制属性 框，然后选择启用。继续执行下一个步骤以对其进行配置。

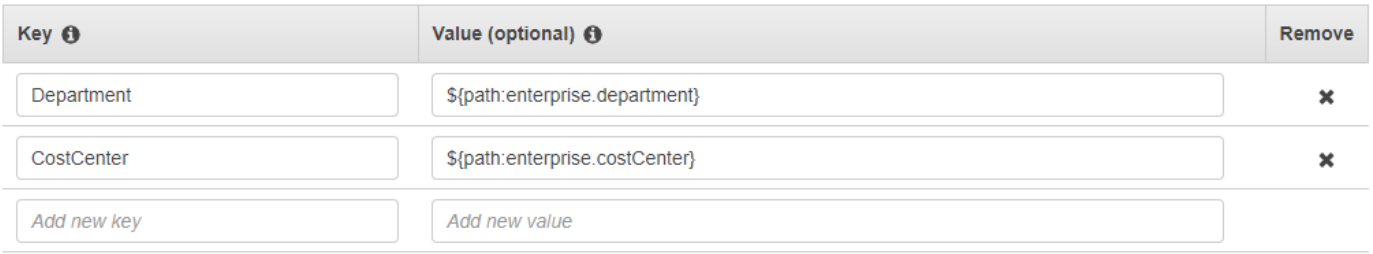
选择访问控制属性

按照以下过程为 ABAC 配置设置 ABAC 配置属性。

> **Note**
>
> 仅当您想要映射 IAM Identity Center 目录中的属性以用作会话标签时，此过程才适用。如果您通过 SAML 断言传递来自外部身份提供商 (IdP) 的属性，则无需在此处配置属性映射。有关更多信息，请参阅 使用外部身份提供者作为身份源时选择属性。在 Identity Center 目录映射中设置的值会覆盖 SAML 断言中设置的值。

使用 IAM Identity Center 控制台选择您的属性

1. 打开 IAM Identity Center 控制台。
2. 选择 设置
3. 在设置页面上，选择访问控制的属性选项卡，然后选择管理属性。
4. 在访问控制的属性页面上，选择添加属性并输入键和值的详细信息。在这里，您可以将来自您的身份源的属性映射到 IAM Identity Center 作为会话标签传递的属性。



密钥表示您为该属性提供的名称，以便在策略中使用。这可以是任意名称，但您需要在为访问控制编写的策略中指定该确切名称。例如，假设您使用Okta（外部 IdP）作为身份源，并且需要将组织的成本中心数据作为会话标签传递。在 Key 中，您可以输入与密钥名称类似CostCenter的匹配名称。需要注意的是，无论您在此处选择哪个名称，它都必须与您的 `aws:PrincipalTag ###`（即 `"ec2:ResourceTag/CostCenter": "${aws:PrincipalTag/CostCenter}"`）中的名称完全相同。

> **Note**
>
> 对您的密钥使用单值属性，例如 **`Manager`**。IAM Identity Center 不支持 ABAC 的多值属性，例如 **`Manager, IT Systems`**。

值表示来自您配置的身份源的属性内容。您可以在此处输入在 IAM Identity Center 与外部身份提供者目录之间的属性映射 中列出的相应身份源表中的任何值。例如，使用上述示例中提供的上下文，您可以查看受支持的 IdP 属性列表，并确定受支持属性的最接近匹配项是 **${path:enterprise.costCenter}**，然后输入在值字段中。请参阅上面提供的屏幕截图以供参考。请注意，除非您使用通过 SAML 断言传递属性的选项，否则不能使用 ABAC 列表之外的外部 IdP 属性值。

5. 选择保存更改。

现在您已经配置了访问控制属性的映射，接下来需要完成 ABAC 配置过程。为此，请创建您的 ABAC 规则并将其添加到您的权限集 and/or 基于资源的策略中。这是必需的，这样您才能向用户身份授予对 Amazon 资源的访问权限。有关更多信息，请参阅 在 IAM Identity Center 中为 ABAC 创建权限策略。

禁用访问控制属性

使用以下过程禁用 ABAC 功能并删除所有已配置的属性映射。

禁用访问控制的属性

1. 打开 IAM Identity Center 控制台。
2. 选择设置。
3. 在设置页面上，选择访问控制的属性选项卡，然后选择管理属性。
4. 在管理访问控制属性页面，选择禁用。
5. 在禁用访问控制属性对话框中，查看相关信息，准备就绪后输入 **DISABLE**，然后选择确认。

> **Important**
>
> 此步骤将删除所有属性，并停止在联合登录 Amazon Web Services 账户 时使用属性进行访问控制，无论外部身份源提供者的 SAML 断言中是否包含任何属性。

在 IAM Identity Center 中为 ABAC 创建权限策略

您可以创建权限策略，根据配置的属性值确定谁可以访问您的 Amazon 资源。当您启用 ABAC 并指定属性时，IAM Identity Center 会将经过身份验证的用户的属性值传递到 IAM，以便在策略评估中使用。

aws:PrincipalTag 条件键

您可以使用权限集中的访问控制属性，并使用 aws:PrincipalTag 条件密钥创建访问控制规则。例如，在以下策略中，您可以使用各自的成本中心标记组织中的所有资源。您还可以使用单个权限集来授予开发人员访问其成本中心资源的权限。现在，每当开发人员使用单点登录及其成本中心属性对账号进行联合身份验证时，他们只能访问各自成本中心中的资源。随着团队向其项目添加更多开发人员和资源，您只需使用正确的成本中心标记资源即可。然后，当开发人员联合进入 Amazon Web Services 账户时，您可以在会 Amazon 话中传递成本中心信息。因此，当组织向成本中心添加新资源和开发人员时，开发人员可以管理与其成本中心一致的资源，而无需任何权限更新。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/CostCenter": "${aws:PrincipalTag/
CostCenter}"
                }
            }
        }
    ]
}
```

当用户 Amazon Web Services 账户 通过 IAM 身份中心联合身份中心时，配置的访问控制属性将作为会话标签传递。您可以使用`aws:PrincipalTag/tag-key`条件键在策略中引用这些会话标签。所有相关的 Amazon IAM 策略类型都支持此条件密钥，您可以在其中使用条件，包括基于身份的策略、基于资源的策略、权限边界、服务控制策略 (SCPs) 和 VPC 终端节点策略。这使您能够根据整个 Amazon 环境中的用户属性做出精细的访问控制决策。

有关更多信息，请参阅 IAM 用户指南中的aws:PrincipalTag和 EC2：根据匹配的主体和资源标签启动或停止实例。

如果策略的条件中包含无效属性，则策略条件将失败并且访问将被拒绝。有关更多信息，请参阅 当用户尝试使用外部身份提供者登录时显示错误信息“出现意外错误”。

了解 IAM Identity Center 中的服务相关角色

服务相关角色是预定义的 IAM 权限，以允许 IAM Identity Center 委派和强制执行哪些用户对您在 Amazon Organizations中的组织内的特定 Amazon Web Services 账户 帐户拥有单点登录访问权限。该服务通过在其组织 Amazon Web Services 账户 内的每个组织中配置一个与服务相关的角色来实现此功能。然后，该服务允许其他 Amazon 服务（例如 IAM Identity Center）利用这些角色来执行与服务相关的任务。有关更多信息，请参阅 Amazon Organizations 和服务相关角色。

当您启用 IAM Identity Center 时，IAM Identity Center 在 Amazon Organizations中的组织内的所有帐户中创建服务相关角色。IAM Identity Center 还会在随后添加到您的组织的每个帐户中创建相同的服务相关角色。此角色允许 IAM Identity Center 代表您访问每个帐户的资源。有关更多信息，请参阅 配置对的访问权限 Amazon Web Services 账户。

在每个角色中创建的服务相关角色 Amazon Web Services 账户 都被命名`AWSServiceRoleForSSO`。有关更多信息，请参阅 使用 IAM Identity Center 的服务相关角色。

> **注意**
>
> - 如果您登录了 Amazon Organizations 管理账户，则该账户将使用您当前登录的角色而不是与服务相关的角色。这可以防止权限升级。
> - 当 IAM Identity Center 在 Amazon Organizations 管理账户中执行任何 IAM 操作时，所有操作都将使用 IAM 委托人的证书进行。这样，登录 CloudTrail 即可查看谁在管理账户中进行了所有权限更改。

设置和使用 Amazon Web Services 访问门户

Amazon Web Services 访问门户通过 IAM 身份中心将您的员工 Amazon Web Services 账户 与云应用程序连接起来。管理员配置门户并管理用户访问权限，而最终用户只需登录一次即可无缝访问其所有授权资源。

Amazon Web Services 访问门户提供对以下内容的单点登录访问权限：

- Amazon Web Services 账户 在你的组织中。
- Amazon 托管应用程序，例如 Amazon Quick 和 Kiro。
- 云应用程序，例如 Office 365、Concur、Salesforce 等。

当用户登录门户时，他们会发现他们无需额外登录即可访问的 Amazon Web Services 账户 和应用程序。

Amazon Web Services 访问门户网站入门

对于管理员：

您需要对您的组织实例或 IAM Identity Center 账户实例具有管理权限，才能配置 Amazon Web Services 访问门户并管理用户访问权限。

1. （可选）自定义 Amazon Web Services 访问门户 URL。
2. 为用户分配对 Amazon Web Services 账户 和应用程序的访问权限。分配的 Amazon 资源显示在门户中。

对于最终用户：

您的管理员必须已完成 Amazon Web Services 访问门户的设置并向您提供了门户 URL 和登录凭证。

1. 从管理员处获取您的门户 URL（通常为 `https://your-company.awsapps.com/start`）。
2. 使用管理员提供的凭证登录。
3. 在您的门户中访问您的资源。

配置 Amazon Web Services 访问门户

作为管理员，您可以自定义 Amazon Web Services 访问门户以满足组织的需求，并确保用户可以轻松访问其授权资源。

您可以配置的内容

Amazon Web Services 访问门户激活：设置访问门户的初始用户 Amazon Web Services 访问权限，包括用户凭据激活和首次登录流程。

自定义 Amazon Web Services 访问门户 URL（可选）：将组织的 Amazon Web Services 访问门户 URL 从默认格式 (`d-xxxxxxxxxx.awsapps.com/start`) 个性化为更易于识别的子域 (`your-company.awsapps.com/start`)。

开始前的准备工作

确保您对 IAM Identity Center 具有管理访问权限，验证 IAM Identity Center 是否设置为组织实例或账户实例，并规划您的自定义子域名（这是一次性配置，以后无法更改）。

配置完成后，用户可以使用自定义 URL Amazon Web Services 访问门户，并按照您为组织建立的激活流程进行操作。

主题

- 为首次使用 IAM 身份中心的用户激活 Amazon Web Services 访问门户
- 自定义 Amazon Web Services 访问门户 URL
- 确认用户可以登录 Amazon Web Services 访问门户

为首次使用 IAM 身份中心的用户激活 Amazon Web Services 访问门户

如果这是您第一次尝试登录 Amazon Web Services 访问门户，请查看您的电子邮件以获取有关如何激活用户凭据的说明。

要激活您的用户凭证

1. 根据您从公司收到的电子邮件，选择以下方法之一来激活您的用户凭证，以便您可以开始使用 Amazon Web Services 访问门户。

a. 如果收到主题为邀请加入 Amazon IAM Identity Center 的电子邮件，请打开邮件并选择接受邀请。在新用户注册页面上，输入并确认密码，然后选择设置新密码。您每次登录门户时都将使用该密码。

b. 如果您收到一封来自公司 IT 支持或 IT 管理员的电子邮件，请按照他们提供的说明来激活您的用户凭证。

2. 通过提供新密码激活用户凭证后，Amazon Web Services 访问门户会自动为您登录。如果没有发生这种情况，您可以按照 登录 Amazon Web Services 访问门户 中提供的说明手动登录 Amazon Web Services 访问门户。

自定义 Amazon Web Services 访问门户 URL

默认情况下，您可以使用遵循以下格式的 URL Amazon Web Services 访问访问门户：`start.home.awsapps.cn/directory/d-xxxxxxxxxx`。您可以按如下方式自定义 URL：`start.home.awsapps.com.cn/directory/your_subdomain`。

> **Important**
>
> 如果您更改了 Amazon Web Services 访问门户 URL，则以后将无法对其进行编辑。

自定义您的网址

1. 打开 Amazon IAM Identity Center 控制台，网址为https://console.aws.amazon.com/singlesignon/。
2. 在 IAM Identity Center 控制台中，选择导航窗格中的控制面板，然后找到设置摘要部分。
3. 选择 Amazon Web Services 访问门户 URL 下方的自定义按钮。

> **Note**
>
> 如果未显示自定义按钮，则表示 Amazon Web Services 访问门户已被自定义。自定义 Amazon Web Services 访问门户 URL 是一次性操作，无法撤消。

4. 输入所需的子域名并选择保存。

现在，您可以使用自定义 URL 通过 Amazon Web Services 访问门户登录 Amazon 控制台。

确认用户可以登录 Amazon Web Services 访问门户

以下步骤可让 IAM 身份中心管理员确认 IAM Identity Center 用户可以登录 Amazon Web Services 访问门户并访问 Amazon Web Services 账户。

登录 Amazon Web Services 访问门户

1. 请执行以下任一操作，登录 Amazon Web Services 管理控制台。
   - Amazon （root 用户）新手 — 选择 R oot 用户并输入您的 Amazon Web Services 账户 电子邮件地址，以账户所有者身份登录。在下一页上，输入您的密码。
   - 已在使用 Amazon （IAM 证书）— 使用您的 IAM 证书登录并选择管理员角色。
2. 打开 IAM Identity Center 控制台。
3. 在导航窗格中，选择控制面板。
4. 在 “控制面板” 页面的 “设置摘要” 下，选择 Amazon Web Services 访问门户 URL。
5. 使用以下方式之一登录：
   - 如果您使用 Active Directory 或外部身份提供者（IdP）作为身份源，请使用 Active Directory 或 IdP 用户的凭证登录。
   - 如果您使用默认的 Identity Center 目录作为身份源，请使用您在创建用户时指定的用户名和为该用户指定的新密码登录。
6. 在 “帐户” 选项卡中，找到您的 Amazon Web Services 账户 并将其展开。
7. 将显示可供您使用的角色。例如，如果您同时分配了AdministratorAccess权限集和账单权限集，则这些角色将显示在 Amazon Web Services 访问门户中。选择要用于会话的 IAM 角色名称。
8. 如果您被重定向到 Amazon 管理控制台，则成功完成了对管理控制台的访问权限的设置 Amazon Web Services 账户。

> **Note**
>
> 如果您没有看到任何列出的 Amazon Web Services 账户，则很可能是尚未为该用户分配该账户的权限集。有关为用户分配权限集的说明，请参阅 为用户或群组分配访问权限 Amazon Web Services 账户。

既然您已确认可以使用 IAM Identity Center 凭证登录，请切换到用于登录的浏览器， Amazon Web Services 管理控制台 然后使用根用户或 IAM 用户证书注销。

> **Important**
>
> 我们强烈建议您在登录 Amazon Web Services 访问门户时使用 IAM Identity Center 管理用户的证书来执行管理任务，而不是使用 IAM 用户或根用户证书。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。要允许其他用户访问您的帐户和应用程序以及管理 IAM Identity Center，请仅通过 IAM Identity Center 创建和分配权限集。

使用 Amazon Web Services 访问门户

您可以通过选择门户中的 Amazon Web Services 账户 或应用程序选项卡来启动多个应用程序。Amazon Web Services 访问门户中存在应用程序图标意味着贵公司的管理员已授予您访问这些 Amazon Web Services 账户 或应用程序的权限。这也意味着您可以从访问门户 Amazon Web Services 访问所有这些账户或应用程序，而无需其他登录提示。

如何使用 Amazon Web Services 访问门户

要使用 Amazon Web Services 访问门户，请执行以下操作：

1. 从管理员处获取您的门户 URL（通常类似于 `https://your-company.awsapps.com/start`）。
2. 使用管理员提供的凭证登录。
3. 在门户中选择您想要访问的账户和应用程序。

您的管理员根据您的角色与权限控制您在门户中看到的内容。在这些情况下，请联系您的管理员请求额外访问权限：

- 您看不到需要访问的 Amazon Web Services 账户 或应用程序。
- 您拥有的对给定账户或应用程序的访问权限不是您所期望的。

主题

- 注册设备进行 MFA
- 查看和结束活跃会话

登录 Amazon Web Services 访问门户

Amazon Web Services 访问门户为 IAM Identity Center 用户提供通过门户网站对其分配的所有应用程序 Amazon Web Services 账户 和应用程序的单点登录访问权限。以下内容概述了如何登录 Amazon Web Services 访问门户、登录提示以及如何注销 Amazon Web Services 访问门户。

先决条件

需要启用 IAM 身份中心才能使用 Amazon Web Services 访问门户。有关更多信息，请参阅 启用 IAM Identity Center。

> **Note**
>
> 登录后， Amazon Web Services 访问门户会话的默认持续时间为 8 小时。请注意，管理员可以更改此会话的持续时间。

登录 Amazon Web Services 访问门户

登录 Amazon Web Services 访问门户

1. 在浏览器窗口中，粘贴提供给您的登录 URL，然后选择 Enter。URL 类似于 `d-xxxxxxxxxx.awsapps.com/start` 或 *`your_subdomain`*`.awsapps.com/start`。建议您现在创建此门户链接的书签，以便今后可以快速访问。
2. 使用您的标准公司登录凭证登录。

   > **Note**
   >
   > 如果管理员向您发送了包含一次性密码 (OTP) 的电子邮件，而且这是您首次登录，请输入该密码。登录后，您必须创建新密码以备用于后续登录。

   如果系统提示输入验证码，请检查您的电子邮件，然后复制验证码并将其粘贴到登录页面中。

> **Note**
>
> 验证码通常通过电子邮件发送，但送达方式可能有所不同。有关详细信息，请咨询您的管理员。

3. 登录后，您可以访问门户中显示的任何 Amazon Web Services 账户 和应用程序。

受信任设备

当您从登录页面选择选项这是受信任的设备时，IAM Identity Center 会将以后从该设备进行的所有登录视为已授权。这意味着，只要您使用的是可信设备，IAM Identity Center 就不会提供输入 MFA 代码的选项。但是，也有一些例外情况，包括使用新浏览器登录或您的设备获得未知 IP 地址时。

Amazon Web Services 访问门户的登录提示

以下是一些可帮助您管理 Amazon Web Services 访问门户体验的提示。

- 有时，您可能需要注销并重新登录 Amazon Web Services 访问门户。这对于访问管理员最近分配给您的新应用程序可能必要。但这不是必需的，因为所有新应用程序每小时都会刷新。
- 登录 Amazon Web Services 访问门户时，您可以通过选择应用程序的图标来打开该门户中列出的任何应用程序。使用完应用程序后，您可以关闭应用程序或退出 Amazon Web Services 访问门户。关闭应用程序只是从应用程序注销。您从 Amazon Web Services 访问门户打开的任何其他应用程序都将保持打开和运行状态。
- 您必须先退出 Amazon Web Services 访问门户，然后才能以其他用户身份登录。从门户注销会从浏览器会话中完全删除您的凭证。
- 登录 Amazon Web Services 访问门户后，即可切换到角色。切换角色会暂时保留您原来的用户权限，并为您提供分配给该角色的权限。 有关更多信息，请参阅切换到角色（控制台）。

退出 Amazon Web Services 访问门户

从门户注销时，您的凭证将从浏览器会话中完全删除。有关更多信息，请参阅Amazon 登录指南中的退出 Amazon Web Services 访问门户。

要退出 Amazon Web Services 访问门户

- 在 Amazon Web Services 访问门户中，从导航栏中选择注销。

> **Note**
>
> 如果您想以其他用户身份登录，则必须先退出 Amazon Web Services 访问门户。

重置您的 Amazon Web Services 访问门户用户密码

Amazon Web Services 访问门户为 IAM Identity Center 用户提供通过门户网站对其所有分配的 Amazon 账户和云应用程序的单点登录访问权限。 Amazon Web Services 访问门户不同于 Amazon Web Services 管理控制台，后者是一组用于管理 Amazon 资源的服务控制台。

使用此过程重置 Amazon Web Services 访问门户的 IAM Identity Center 用户密码。在Amazon 登录 用户指南中了解有关用户类型的更多信息。

注意事项

Amazon Web Services 访问门户的重置密码功能仅适用于使用 Identity Center 目录或Amazon Managed Microsoft AD作为其身份源的身份中心实例的用户。如果用户已连接到外部身份提供者或 AD Connector，则必须通过外部身份提供者或连接的 Active Directory 完成用户密码重置。

- 如果身份源是 IAM Identity Center 目录，请参阅在 IAM Identity Center 中管理身份时的密码要求。
- 如果身份源是 Amazon Managed Microsoft AD，请参阅在 Amazon Managed Microsoft AD中重置密码时密码要求。

重置 Amazon Web Services 访问门户的密码

1. 打开 Web 浏览器，进入 Amazon Web Services 访问门户的登录页面。

   如果您没有 Amazon Web Services 访问门户 URL，请查看您的电子邮件。您应该已经收到加入 Amazon IAM Identity Center 的电子邮件邀请，其中包括 Amazon Web Services 访问门户的特定登录 URL。或者，您的管理员可能直接向您提供了一次性密码和 Amazon Web Services 访问门户 URL。如果您找不到此信息，请让您的管理员将其发送给您。

   有关登录 Amazon Web Services 访问门户的更多信息，请参阅《Amazon 登录 用户指南》中的登录 Amazon Web Services 访问门户。
2. 输入您的用户名，然后选择下一步。
3. 在密码下，选择忘记密码。

验证您的用户名并输入所提供图像的字符，以确认您不是机器人。然后选择下一步。如果无法输入字符，您可能需要禁用广告拦截软件。

4. 将显示一条消息，确认已发送重置密码电子邮件。选择继续。
5. 您将收到一封来自 no-reply@signin.aws 的电子邮件，主题为请求重置密码。在您的电子邮件中，选择重置密码。
6. 在重置密码页面上，验证您的用户名，为 Amazon Web Services 访问门户指定新密码，然后选择设置新密码。
7. 您将收到一封来自 no-reply@signin.aws 的电子邮件，主题行密码已更新。

> **Note**
>
> 管理员可以通过向您发送一封包含重置密码说明的电子邮件来重置您的密码，或者生成一次性密码并与您共享。如果您是管理员，请参阅 重置最终用户的 IAM Identity Center 用户密码。

获取 Amazon CLI 或的 IAM Identity Center 用户证书 Amazon SDKs

您可以使用 Amazon Command Line Interface 或带有 IAM Identity Center 用户证书的 Amazon 软件开发套件 (SDKs)，以编程方式访问 Amazon 服务。本主题介绍如何在 IAM Identity Center 中获取用户的临时凭证。

Amazon Web Services 访问门户为 IAM Identity Center 用户提供了对其应用程序 Amazon Web Services 账户 和云应用程序的单点登录访问权限。作为 IAM Identity Center 用户登录 Amazon Web Services 访问门户后，您可以获得临时证书。然后，您可以使用 Amazon CLI 或中的证书（也称为 IAM Identity Center 用户证书）Amazon SDKs 来访问中的资源 Amazon Web Services 账户。

如果您使用 Amazon CLI 以编程方式访问 Amazon 服务，则可以使用本主题中的过程启动对的 Amazon CLI访问。有关信息 Amazon CLI，请参阅《Amazon Command Line Interface 用户指南》。

如果您使用以编程方式访问 Amazon 服务，则按照本主题中的步骤还可以直接为建立身份验证。Amazon SDKs Amazon SDKs有关信息 Amazon SDKs，请参阅Amazon SDKs 和工具参考指南。

> **Note**
>
> IAM Identity Center 中的用户与 IAM 用户不同。IAM 用户将获得 Amazon 资源的长期证书。IAM Identity Center 中的用户被授予临时凭证。我们建议您使用临时证书作为访问您的证书的最佳安全实践， Amazon Web Services 账户 因为这些证书是在您每次登录时生成的。

先决条件

要获取 IAM Identity Center 用户的临时凭证，您需要以下内容：

- IAM Identity Center 用户——您将以该用户身份登录 Amazon Web Services 访问门户。您或您的管理员可能会创建此用户。有关如何启用 IAM Identity Center 和创建 IAM Identity Center 用户的信息，请参阅 开始使用 IAM Identity Center。
- 用户访问权限 Amazon Web Services 账户— 要向 IAM Identity Center 用户授予检索其临时证书的权限，您或管理员必须将 IAM Identity Center 用户分配给权限集。权限集存储在 IAM Identity Center 中，定义 IAM Identity Center 用户对 Amazon Web Services 账户的访问级别。如果您的管理员为您创建了 IAM Identity Center 用户，请要求他们为您添加此访问权限。有关更多信息，请参阅 为用户或群组分配访问权限 Amazon Web Services 账户。
- Amazon CLI 已安装-要使用临时证书，必须安装 Amazon CLI。有关说明，请参阅 Amazon CLI 用户指南中的安装或更新最新版本的 Amazon CLI。

注意事项

在完成为 IAM Identity Center 用户获取临时凭证的步骤之前，请记住以下注意事项：

- IAM Identity Center 创建 IAM 角色——当您将 IAM Identity Center 中的用户分配给权限集时，IAM Identity Center 从权限集中创建相应的 IAM 角色。权限集创建的 IAM 角色与通过以下 Amazon Identity and Access Management 方式创建的 IAM 角色不同：
  - IAM Identity Center 拥有并保护由权限集创建的角色。只有 IAM Identity Center 可以修改这些角色。
  - 只有 IAM Identity Center 中的用户才能承担与其分配的权限集相对应的角色。您无法将权限集访问权限分配给 IAM 用户、IAM 联合用户或服务帐户。
  - 您无法修改这些角色的角色信任策略以允许访问 IAM Identity Center 外部的主体。

  有关如何获取您在 IAM 中创建的角色的临时凭证的信息，请参阅 Amazon Identity and Access Management 用户指南中的使用临时安全凭证 Amazon CLI。

- 您可以为权限集设置会话持续时间 — 登录 Amazon Web Services 访问门户后，分配给您的 IAM Identity Center 用户的权限集将显示为可用角色。IAM Identity Center 为此角色创建一个单独的会话。此会话可能为 1 到 12 小时，具体取决于为权限集配置的会话持续时间。默认会话持续时间为一小时。有关更多信息，请参阅 将会话持续时间设置为 Amazon Web Services 账户。

获取和刷新临时凭证

您可以自动或手动获取和刷新 IAM Identity Center 用户的临时凭证。

主题

自动刷新凭证（推荐）

自动刷新凭证使用 Open ID Connect（OIDC）设备代码授权标准。该方法是使用 Amazon CLI中的 `aws configure sso` 命令直接发起访问。您可以使用此命令自动访问与您为任何 Amazon Web Services 账户分配的任何权限集关联的任何角色。

要访问为您的 IAM Identity Center 用户创建的角色，`aws configure sso`请运行命令，然后 Amazon CLI 从浏览器窗口对其进行授权。只要您的 Amazon Web Services 访问门户会话处于活动状态， Amazon CLI 就会自动检索临时证书并自动刷新证书。

有关详细信息，请参阅 Amazon Command Line Interface 用户指南中的 `aws configure sso wizard` 配置您的配置文件。

获取可自动刷新的临时凭证

1. 使用管理员提供的特定登录 URL 登录 Amazon Web Services 访问门户。如果您创建了 IAM Identity Center 用户，则会 Amazon 发送一封包含您的登录 URL 的电子邮件邀请。有关更多信息，请参阅《登录用户指南》中的Amazon 登录 Amazon Web Services 访问门户。
2. 在 “帐户” 选项卡中，找到要 Amazon Web Services 账户 从中检索凭据的。当您选择帐户时，会显示与该帐户关联的帐户名称、帐户 ID 和电子邮件地址。

> **Note**
>
> 如果您没有看到列出的任何 Amazon Web Services 账户，则可能尚未为该账户分配权限集。在这种情况下，请联系您的管理员并要求他们为您添加此访问权限。有关更多信息，请参阅 为用户或群组分配访问权限 Amazon Web Services 账户。

3. 在帐户名称下方，分配给您的 IAM Identity Center 用户的权限集显示为可用角色。例如，如果您的 IAM Identity Center 用户被分配到该账户的PowerUserAccess权限集，则该角色在 Amazon Web Services 访问门户中显示为PowerUserAccess。
4. 根据角色名称旁边的选项，选择访问密钥图标或选择命令行或编程访问。
5. 在 “获取凭据” 对话框中，选择 macOS 和 Linux、Windows 或 PowerShell，具体取决于您安装的操作系统。 Amazon CLI
6. 在 Amazon IAM Identity Center 凭证（推荐）下，将显示您的 `SSO Start URL` 和 `SSO Region`。将启用 IAM Identity Center 的配置文件和 `sso-session` 配置为 Amazon CLI需要这些值。要完成此配置，请按照 Amazon Command Line Interface 用户指南中的使用 `aws configure sso wizard` 配置您的配置文件中的说明进行操作。

根据 Amazon CLI 需要继续使用， Amazon Web Services 账户 直到证书过期。

手动凭证刷新

您可以使用手动凭据刷新方法来获取与特定 Amazon Web Services 账户中的特定权限集关联的角色的临时凭证。为此，您可以复制并粘贴临时凭证所需的命令。使用此方法，您必须手动刷新临时凭证。

在临时证书到期之前，您可以运行 Amazon CLI 命令。

获取您手动刷新的凭证

1. 使用管理员提供的特定登录 URL 登录 Amazon Web Services 访问门户。如果您创建了 IAM Identity Center 用户，则会 Amazon 发送一封包含您的登录 URL 的电子邮件邀请。有关更多信息，请参阅《登录用户指南》中的Amazon 登录 Amazon Web Services 访问门户。
2. 在账户选项卡中，找到您要 Amazon Web Services 账户 从中检索访问凭证的，然后将其展开以显示 IAM 角色名称（例如管理员）。根据 IAM 角色名称旁边的选项，选择访问密钥图标或选择命令行或编程访问。

> **Note**
>
> 如果您没有看到列出的任何 Amazon Web Services 账户，则可能尚未为该账户分配权限集。在这种情况下，请联系您的管理员并要求他们为您添加此访问权限。有关更多信息，请参阅 为用户或群组分配访问权限 Amazon Web Services 账户。

3. 在 “获取凭据” 对话框中，选择 macOS 和 Linux PowerShell、Windows 或，具体取决于您安装的操作系统。 Amazon CLI
4. 选择以下任一选项：

   - 选项 1：设置 Amazon 环境变量

     选择此选项可覆盖所有凭证设置，包括 `credentials` 文件和 `config` 文件中的任何设置。有关更多信息，请参阅 Amazon CLI 用户指南中的环境变量配置 Amazon CLI。

     要使用此选项，请将命令复制到剪贴板，将命令粘贴到 Amazon CLI 终端窗口，然后按 Enter 键设置所需的环境变量。

   - 选项 2：在您的 Amazon 凭证文件中添加个人资料

     选择此选项可使用不同的凭证集运行命令。

     要使用此选项，请将命令复制到剪贴板，然后将命令粘贴到共享 Amazon `credentials`文件中以设置新的命名配置文件。有关更多信息，请参阅《工具参考指南》和《工具参考指南》中的共享配置Amazon SDKs 和凭据文件。要使用此凭证，请在 Amazon CLI 命令中指定该`--profile`选项。这会影响使用相同凭证文件的所有环境。

   - 选项 3：在 Amazon 服务客户端中使用个人值

     选择此选项可从 Amazon 服务客户端访问 Amazon 资源。有关更多信息，请参阅用于在Amazon上进行构建的工具。

     要使用此选项，请将值复制到剪贴板，将这些值粘贴到代码中，然后将其分配给适合您的 SDK 的相应变量。有关更多信息，请参阅特定 SDK API 的文档。

创建指向 Amazon Web Services 管理控制台 目的地的快捷链接

在 Amazon Web Services 访问门户中创建的快捷方式链接将 IAM Identity Center 用户带到具有特定权限集和特定权限集的特定目的地 Amazon Web Services 账户。 Amazon Web Services 管理控制台

快捷方式链接可以为自己和协作者节省时间。您无需通过多个页面（包括 Amazon Web Services 访问门户）导航到所需的目标 URL Amazon Web Services 管理控制台 （例如，Amazon S3 存储桶实例页面），而是可以使用快捷链接自动到达同一个目的地。

快捷方式链接目标选项

快捷方式链接有三个目标选项，此处按优先级列出：

- （可选）快捷方式链接中 Amazon Web Services 管理控制台 指定的任何目标 URL。例如，Amazon S3 存储桶实例页面。
- （可选）管理员为相关权限集配置的中继状态 URL。有关设置中继状态的更多信息，请参阅设置中继状态以便快速访问 Amazon Web Services 管理控制台。
- Amazon Web Services 管理控制台 家。未指定目标时的默认目标。

> **Note**
>
> 只有当您通过 IAM Identity Center 进行身份验证并且为 Amazon 账户和目标 URL 分配了必要的权限集时，才能成功自动导航到目的地。

Amazon Web Services 访问门户包含一个 “创建快捷方式” 按钮，可帮助您创建可共享的快捷方式链接。如果打算指定目标 URL（上一个列表中的第一个选项），则可以将该 URL 复制到剪贴板进行共享。

在 Amazon Web Services 访问门户中创建快捷方式链接

1. 登录 Amazon Web Services 访问门户后，选择 “帐户” 选项卡，然后选择 “创建快捷方式” 按钮。
2. 在对话框中：
   a. Amazon Web Services 账户 使用账户 ID 或账户名选择。键入时，下拉菜单会显示您可以访问的匹配帐户 IDs 和名称。您只能选择自己有权访问的账户。
   b. （可选）从下拉列表中选择 IAM 角色。这些是分配给选定账户的权限集。如果您省略选择角色，则在使用快捷方式链接时，系统会提示用户为所选账户选择一个分配给他们的角色。

> **Note**
>
> 您无法通过快捷方式链接授予新的访问权限。快捷方式链接仅适用于已分配给用户的权限集。如果用户没有为账户和目标 URL 分配的必要权限集，则会被拒绝访问。

c. （可选）输入 Amazon Web Services 访问门户的目标 URL。如果您省略输入 URL，则在使用快捷方式链接时，将根据前面提到的快捷方式链接目标选项自动确定目标。

d. 根据输入内容，快捷方式链接会在对话框底部生成。选择复制 URL 按钮。现在，您可以使用复制的快捷方式链接创建书签，也可以与具有相同权限集或其他足够权限集以访问同一个账户的协作者共享书签。

使用 URL 编码构造安全的 Amazon Web Services 管理控制台 快捷方式链接

URL 的所有参数值，包括账户 ID、权限集名称和目标 URL，都必须经过 URL 编码。

快捷链接使用以下路径扩展了 Amazon Web Services 访问门户 URL：

```
/#/console?
account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination
```

中国区域的完整 URL 遵循以下模式：

IPv4 端点：

```
https://start.[region].home.awsapps.cn/directory/[directory_id_or_alias]/
#/console?
account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination
```

双栈端点

```
https://[identity_center_instance_id].portal.[region].app.amazonwebservices.com.
#/console?
account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination
```

以下是一个快捷方式链接示例，使用 S3FullAccess 权限集让用户登录 123456789012 账户，并将他们引导至 S3 控制台主页：

- IPv4 端点：https://start.cn-north-1.home.awsapps.cn/directory/example/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.amazonaws.cn%2Fs3%2Fhome

- 双栈端点：`https://ssoins-1234567890abcdef.portal.cn-north-1.app.amazonwebservices.com.cn/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.amazonaws.cn%2Fs3%2Fhome`

注册设备进行 MFA

对于 Identity Center 目录中的用户，请在 Amazon Web Services 访问门户中使用以下过程来注册新设备以进行多重身份验证（MFA）。

> **Important**
>
> 目前，外部身份提供者不支持 IAM Identity Center 中的 MFA。

开始前的准备工作

我们建议您先将适当的身份验证器应用程序下载到您的设备上，然后再开始执行此过程中的步骤。有关可以在 MFA 设备上使用的应用程序的列表，请参阅 虚拟身份验证器应用程序。

注册您的设备

注册您的设备，以便在 MFA 上使用

1. 登录您的 Amazon Web Services 访问门户。有关更多信息，请参阅 登录 Amazon Web Services 访问门户。
2. 在页面右上角附近，选择 MFA 设备。
3. 在多重身份验证 (MFA) 设备页面上，选择注册设备。

   > **Note**
   >
   > 如果注册 MFA 设备选项显示为灰色，请联系您的管理员以获取注册设备的帮助。

4. 在注册 MFA 设备页面上，选择以下 MFA 设备类型之一，然后按照说明进行操作：

   - 身份验证器应用程序
     1. 在设置身份验证器应用程序页面上，您可能会注意到新 MFA 设备的配置信息，包括 QR 代码图形。该图表示可在不支持 QR 码的设备上手动输入的密钥。

2. 使用物理 MFA 设备，执行以下操作：

   a. 打开兼容的 MFA 身份验证器应用程序。有关可以在 MFA 设备上使用的经过测试的应用程序的列表，请参阅 虚拟身份验证器应用程序。如果 MFA 应用支持多个帐户（多个 MFA 设备），请选择创建新帐户（新的 MFA 设备）的选项。

   b. 确定 MFA 应用程序是否支持 QR 码，然后在设置身份验证器应用程序页面上执行以下操作之一：

      i. 选择显示 QR 代码，然后使用该应用程序扫描 QR 代码。例如，您可选择摄像头图标或选择类似于 Scan code（扫描代码）的选项，然后使用装置的摄像头扫描此代码。

      ii. 选择显示密钥，然后将该密钥输入到您的 MFA 应用程序中。

> **Important**
>
> 当您为 IAM Identity Center 配置 MFA 设备时，我们建议您将 QR 码或密钥的副本保存在安全的位置。如果您丢失手机或必须重新安装 MFA 身份验证器应用程序，这会有所帮助。如果出现上述任一情况，您可以快速重新配置应用程序，使其使用相同的 MFA 配置。

3. 在设置身份验证器应用程序页面的身份验证器代码下，输入当前显示在物理 MFA 设备上的一次性密码。

> **Important**
>
> 生成代码之后立即提交您的请求。如果您生成代码，然后等待太长时间才提交请求，则 MFA 设备已成功与您的用户关联，但 MFA 设备不同步。这是因为基于时间的一次性密码（TOTP）很快会过期。如果发生这种情况，您可以再次同步设备。

4. 选择分配 MFA。MFA 设备现在可以开始生成一次性密码，现在可以与之配合使用了。Amazon

- 安全密钥或内置身份验证器

1. 在注册用户的安全密钥页面上，按照浏览器或平台提供的说明进行操作。

> **Note**
>
> 体验会因浏览器或平台而异。成功注册设备后，您可以将友好的显示名称与新注册的设备关联起来。要更改名称，请选择重命名，输入新名称，然后选择保存。

查看和结束活跃会话

您可以使用 Amazon Web Services 访问门户查看活动会话列表，并在需要时结束一个或多个会话。

使用 Amazon Web Services 访问门户结束活动会话

1. 登录您的 Amazon Web Services 访问门户。有关更多信息，请参阅 登录 Amazon Web Services 访问门户。
2. 在页面右上角附近，选择安全。
3. 在安全页面上，活跃会话旁边的括号中的数字表示您有多少个活跃会话。选择要结束的每个会话旁边的复选框，然后选择结束会话。

   > **Tip**
   >
   > 对于用户后台会话，您可以通过使用该会话的作业的 Amazon 资源名称（ARN）来搜索会话。在会话类型列表中，选择用户后台会话，然后在搜索框中输入作业 ARN。

   您只能结束已加载的活跃会话。如果您有许多会话，请选择加载更多活跃会话，以显示其他会话。
4. 选择要结束的每个会话旁边的复选框，然后选择结束会话。
5. 此时会出现一个对话框，确认您正在结束活跃会话。查看信息，如果要继续，请键入 `confirm`，然后选择结束会话。
6. 您将返回到活跃会话列表。此时会出现绿色通知消息，表示所选会话已成功结束。

跨多个 IAM 身份中心使用 Amazon Web Services 区域

本主题说明了如何 Amazon IAM Identity Center 跨多个使用 Amazon Web Services 区域。了解如何在服务中断期间将您的实例复制到其他区域、管理员工访问权限和会话、部署应用程序以及在服务中断期间维护账户访问权限。

启用 IAM Identity Center 的组织实例时，您可以选择一个 Amazon Web Services 区域 （主区域）。如果此实例满足某些先决条件， Amazon Web Services 区域 则可以将其复制到其他实例。IAM Identity Center 会自动将工作人员身份、权限集、用户和群组分配、会话和其他元数据从主要区域复制到选定的其他区域。

多区域支持的好处

将 IAM Identity Cen Amazon Web Services 区域 ter 复制到其他服务器有两个主要好处：

- 提高了 Amazon Web Services 账户 访问弹性 — 即使 IAM Identity Amazon Web Services 账户 Center 实例在其主要区域遇到服务中断，您的员工也可以访问他们的。这适用于在中断之前预置权限的访问权限。
- 提高了为 Amazon 托管应用程序选择部署区域的灵活性 — 您可以在首选区域部署 Amazon 托管应用程序，以满足应用程序数据驻留要求并通过靠近用户来提高性能。部署在其他地区的应用程序可在本地访问复制的员工身份，以实现最佳性能和可靠性。

先决条件和注意事项

在复制 IAM 身份中心实例之前，请确保满足以下要求：

- 实例类型-您的 IAM 身份中心实例必须是组织实例。账户实例不提供多区域支持。
- 身份来源-您的 IAM 身份中心实例必须连接到外部身份提供商 (IdP)，例如。Okta多区域支持不适用于使用 A ctive Directory 或身份中心目录作为身份源的实例。
- Amazon 区域-多区域支持适用于您的Amazon Web Services 账户默认启用的商业区域。目前不支持选择加入区域。
- 用于静态加密的 KMS 密钥类型-您的 IAM Identity Center 实例必须使用多区域客户托管 KMS 密钥进行配置。KMS 密钥必须与 IAM 身份中心位于同一个 Amazon 账户中。有关更多信息，请参阅 在中实现客户托管的 KMS 密钥 Amazon IAM Identity Center。
- Amazon 托管应用程序兼容性-访问中的应用程序表the section called “可与 IAM Identity Center 搭配使用的应用程序”，确认以下两个应用程序要求：

  - 您的组织正在使用的所有 Amazon 托管应用程序都必须支持使用客户托管 KMS 密钥配置的 IAM 身份中心。
  - 您要在其他区域部署的 Amazon 托管应用程序必须支持此类部署。
- 外部 IdP 兼容性-要充分利用多区域支持，外部 IdP 必须支持多断言消费者服务 (ACS)。 URLs这是 Okta、、Microsoft Entra ID、 PingFederate和 IdPs JumpCloud等支持的 SAML 功能。 PingOne

  如果您使用不支持多个 ACS 的 IdP（例如） URLsGoogle Workspace，我们建议您与您的 IdP 供应商合作以启用此功能。有关在不使用多个 ACS 的情况下可用的选项 URLs，请参见the section called “使用没有多个 ACS 的 Amazon 托管应用程序 URLs”和the section called “Amazon Web Services 账户 无需多个 ACS 即可实现访问弹性 URLs”。

选择其他区域

在默认启用的商业区域中选择其他区域时，请考虑以下因素：

- 合规性要求-如果出于合规性原因，您需要运行访问仅限于特定区域的数据集的 Amazon 托管应用程序，请选择数据集所在的区域。
- 性能优化-如果数据驻留不是一个因素，请选择离您的应用程序用户最近的区域来优化他们的体验。
- 应用程序支持-验证您所选的地区是否提供所需的 Amazon 应用程序。
- Amazon Web Services 账户 访问弹性 — 为了连续访问 Amazon Web Services 账户 s，请选择一个地理位置远离您的 IAM Identity Center 实例主区域的区域。

> **Note**
>
> IAM Identity Center 的数量有配额 Amazon Web Services 区域。有关更多信息，请参阅 the section called “其他配额”。

将 IAM 身份中心复制到其他区域

如果您的环境满足先决条件，例如使用多区域客户托管的 KMS 密钥配置 IAM Identity Center，请完成以下步骤将您的 IAM Identity Center 实例复制到其他区域。在这些步骤期间和之后，您的主要区域将继续正常运行。

步骤 1：在其他区域创建副本密钥

在将 IAM Identity Center 复制到某个区域之前，您必须先在该区域创建客户托管 KMS 密钥的副本密钥，然后将副本密钥配置为 IAM Identity Center 操作所需的权限。有关创建多区域副本密钥的说明，请参阅创建多区域副本密钥。

KMS 密钥权限的推荐方法是从主密钥复制密钥策略，该策略授予的权限与已在主区域中为 IAM Identity Center 建立的权限相同。或者，您可以定义特定于区域的密钥策略，但这种方法会增加跨区域管理权限的复杂性，并且将来更新策略时可能需要额外的协调。

> **Note**
>
> Amazon KMS 不会在您的多区域 KMS 密钥所在区域之间同步您的 KMS 密钥策略。要在 KMS 密钥区域之间保持 KMS 密钥策略同步，您需要在每个区域中单独应用更改。

步骤 2：在 IAM 身份中心添加区域

在 IAM Identity Center 中添加区域会触发 IAM 身份中心数据自动复制到该区域。复制是异步的，具有最终一致性。以下选项卡提供了在 Amazon Web Services 管理控制台 和中执行此操作的说明 Amazon CLI。

Console

添加区域

1. 打开 IAM Identity Center 控制台。
2. 在导航窗格中，选择设置。
3. 选择管理选项卡。
4. 在 IAM 身份中心的区域部分，选择添加区域。
5. 在 “Amazon Web Services 区域 可供复制” 部分中，选择您的首选 Amazon Web Services 区域。如果该区域未出现在列表中，则该区域不可复制，因为 KMS 密钥尚未在列表中复制。有关更多信息，请参阅 the section called “实施客户自主管理型 KMS 密钥”。
6. 选择添加区域。
7. 在 IAM 身份中心的区域部分，监控区域状态。根据需要使用刷新按钮（圆形箭头）检查最新的区域状态。复制完成后，继续执行步骤 2。

Amazon CLI

添加区域

```
aws sso-admin add-region \
    --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \
    --region-name eu-west-1
```

查看当前区域状态

```
aws sso-admin describe-region \
    --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \
    --region-name eu-west-1
```

当区域状态为 “活动” 时，您可以继续执行步骤 2。

初始复制到其他区域的持续时间取决于您的 IAM Identity Center 实例中的数据量。在大多数情况下，后续的增量更改将在几秒钟内复制。

步骤 3：更新外部 IdP 设置

按照外部 IdP 中的教程身份源教程进行以下步骤：

步骤 3.a：将断言使用者服务 (ACS) URLs 添加到您的外部 IdP

此步骤允许直接登录到其他每个区域，并且是允许登录部署在这些区域中的 Amazon 托管应用程序以及通过这些区域访问所必需 Amazon Web Services 账户的。要了解在哪里可以找到 ACS URLs，请参阅主端点和附加端点中的 ACS 端点 Amazon Web Services 区域。

步骤 3.b（可选）：在外部 IdP 门户中 Amazon Web Services 访问门户 提供

Amazon Web Services 访问门户 在外部 IdP 门户中将其他区域中的作为书签应用程序提供。书签应用程序仅包含指向所需目的地的链接 (URL)，类似于浏览器书签。 Amazon Web Services 访问门户 URLs 在 IAM 身份中心区域部分选择查看全部，即可 Amazon Web Services 访问门户 URLs在控制台中找到。有关更多信息，请参阅 the section called “Amazon Web Services 访问主服务器和其他服务器中的门户终端节点 Amazon Web Services 区域”。

IAM Identity Center 在其他每个区域都支持 IDP 发起的 SAML SSO，但外部 IdPs通常仅使用一个 ACS URL 即可支持这一点。为了保持连续性，我们建议保留主区域的 ACS URL 用于 IDP 发起的 SAML SSO，并依靠书签应用程序和浏览器书签来访问其他区域。

步骤 4：确认防火墙和网关允许列表

在防火墙或网关中查看您的域名许可名单，并根据记录的允许列表对其进行更新。

第 5 步：向您的用户提供信息

向您的用户提供有关新设置的信息，包括附加区域 Amazon Web Services 访问门户 的 URL 以及如何使用其他区域。请查看以下章节以了解相关详细信息：

- the section called “通过其他地区访问员工”
- the section called “故障转移到其他区域进行 Amazon Web Services 账户 访问”
- the section called “跨多个部署和管理应用程序 Amazon Web Services 区域”

除了添加第一个区域之外，区域会发生变化

您可以添加和移除其他区域。除非删除整个 IAM 身份中心实例，否则无法移除主要区域。有关移除区域的更多信息，请参阅the section called “从 IAM 身份中心移除区域”。

您不能将其他区域提升为主区域，也不能将主要区域降级为额外区域。

复制了哪些数据？

IAM 身份中心复制以下数据：

数据	复制源和目标
员工身份（用户、群组、群组成员资格）	从主要区域到其他区域
权限集及其对用户和组的分配	从主要区域到其他区域
配置（例如外部 IdP SAML 设置）	从主要区域到其他区域
应用程序元数据以及对用户和群组的应用程序分配	从应用程序连接的 IAM 身份中心区域到其他已启用的区域
值得信赖的代币发行商	从主要区域到其他区域

数据	复制源和目标
会话	从会话的原始区域到其他已启用的区域

> **Note**
>
> IAM 身份中心不会复制存储在 Amazon 托管应用程序中的数据。此外，它不会改变应用程序部署的区域覆盖范围。例如，如果您的 IAM 身份中心实例位于美国东部（弗吉尼亚北部），并且您在同一地区部署了 Amazon Redshift，则将 IAM 身份中心复制到美国西部（俄勒冈）不会影响 Amazon Redshift 的部署区域及其存储的数据。

注意事项：

- 已启用区域的全球资源标识符-用户、群组、权限集和其他资源在已启用的区域中具有相同的标识符。
- 复制不会影响已配置的 IAM 角色-从任何已启用的区域登录账户期间，将使用从权限集分配中配置的现有 IAM 角色。

通过其他地区访问员工

本节介绍当您在多个区域启用 IAM Identity Amazon Web Services 账户 Center 后，您的员工如何访问、和应用程序。 Amazon Web Services 访问门户

“ Amazon Web Services 访问门户 在其他区域” 中 Amazon Web Services 账户显示您的员工可以访问的和应用程序，其方式与在主要区域中相同。您的员工可以通过直接链接到区域门户终端节点（例如`https://ssoins-111111h2222j33pp.eu-west-1.portal.amazonaws.com`）或通过您在外部 IdP 中设置的书签应用程序登录其他区域。 Amazon Web Services 访问门户

您可以使用其他区域中的 Amazon Web Services 访问门户 终端节点来授予以 IAM 身份中心用户身份访问的权限。 Amazon CLI APIs 此功能的工作方式与在主区域中的工作方式相同。但是，不会在已启用的区域之间复制 CLI 授权。因此，您必须在每个区域单独授权 CLI。

跨多个用户会话 Amazon Web Services 区域

IAM Identity Center 将用户会话从原始区域复制到其他已启用的区域。一个区域中的会话撤消和注销也会复制到其他区域。

IAM 身份中心管理员撤销会话

IAM 身份中心管理员可以撤消其他区域的用户会话。由于会话是跨区域复制的，因此在正常情况下，撤消单个区域中的会话并让 IAM Identity Center 将更改复制到其他已启用的区域即可。如果 IAM Identity Center 的主区域出现中断，管理员可以在其他区域执行此操作。

Amazon Web Services 访问门户 主端点和其他端点 Amazon Web Services 区域

如果您需要在已启用区域的 Amazon Web Services 访问门户 URLs 中查找，请按照以下步骤操作：

1. 打开 IAM Identity Center 控制台。
2. 在导航窗格中，选择设置。
3. 选择管理选项卡。
4. 在 IAM 身份中心区域部分，选择查看所有 Amazon 访问门户 URLs。

下表指定了 IAM Identity Center 实例的主区域和其他区域的 Amazon Web Services 访问门户 终端节点。

Amazon Web Services 访问门户 endpoint	主 区域	其他区域	网址模式和示例
IPv4 仅限经典 [1]	是	否	图案：`https://[Identity Store ID].awsapps.com/start` 示例：`https://d-12345678.awsapps.com/start`
IPv4 仅限自定义别名 [1]	是（可选）	否	图案：`https://[custom alias].awsapps.com/start` 示例：`https://mycompany.awsapps.com/start`
IPv4 仅有备选方案 [2]	支持	是	图案：`https://[Identity Center instance ID].`

Amazon Web Services 访问门户 endpoint	主 区域	其他区域	网址模式和示例
			[Region].portal.amazonaws.com 示例：https://ssoins-111111h2222j33pp.eu-west-1.portal.amazonaws.com
双栈 2	支持	是	图案：https://*[Identity Center instance ID]*.portal.*[Region]*.app.aws 示例：https://ssoins-111111h2222j33pp.portal.eu-west-1.app.aws

[1] 在其他区域，不支持自定义别名，awsapps.com父域名不可用。

[2] IPv4 仅限替代方案，双栈门户端点的网址/start中没有尾随字符。

主端点和附加端点中的断言消费者服务 (ACS) 端点 Amazon Web Services 区域

如果您需要查找 ACS URLs 或将其作为 SAML 元数据的一部分下载，请按照以下步骤操作：

1. 打开 IAM Identity Center 控制台。
2. 在导航窗格中，选择设置。
3. 选择 “身份来源” 选项卡。
4. 在 “操作” 下拉菜单中，选择 “管理身份验证”。
5. 服务提供商元数据部分显示每个已启用区域的 Amazon Web Services 访问门户 和 ACS URL。IPv4-only 和 dual-stack 显示 URLs 在单独的选项卡上。如果您的 IdP 支持上传 SAML 元数据文件，则可以选择下载元数据文件来下载所有 ACS 的 SAML 元数据文件。 URLs如果您的 IdP 不支持上传元数据文件，或者您更喜欢单独添加 ACS，则可以 URLs 从控制台的表格中 URLs 单独复

制，或者选择查看 ACS， URLs然后选择全部复制。 URLs保留已为主区域配置的 ACS URL，以确保服务提供商启动的 SAML 从主区域进行单点登录仍能正常运行。

下表指定了 IAM Identity Center 实例的主区域和其他区域的 SAML 断言消费者服务 (ACS) 终端节点：

ACS 端点	主 区域	其他区域	网址模式和示例
IPv4 只有	支持	是	图案：https://*[Region]*.signin.aws/platform/saml/acs/ *[Tenant ID]* 示例： https://us-west-2.signin.aws/platform/saml/acs/1111111111111111-aaee-ffff-dddd-11111111111
IPv4 仅限备选*	是	否	图案：https://*[Region]*.signin.aws.amazon.com/platform/saml/acs/ *[Tenant ID]* 示例： https://us-west-2.signin.aws.amazon.com/platform/saml/acs/1111111111111111-aaee-ffff-dddd-11111111111
双堆栈	支持	是	图案：https://*[Region]*.sso.signin.aws/platform/saml/acs/*[Tenant ID]* 示例： https://us-west-2.sso.signin.aws/platform/saml/acs/1111111111111111-aaee-ffff-dddd-11111111111

* 对于 2026 年 2 月之前启用的实例，请保留此终端节点，因为服务提供商发起的 SAML 单点登录到主区域需要它。IAM Identity Center 不会将此终端节点用于在 2026 年 2 月或之后启用的实例。

使用没有多个 ACS 的 Amazon 托管应用程序 URLs

一些外部身份提供商 (IdPs) URLs 在其 IAM Identity Center 应用程序中不支持多重断言消费者服务 (ACS)。多 URLs 个 ACS 是一项 SAML 功能，需要在多区域 IAM 身份中心中直接登录特定区域。

例如，如果您通过应用程序链接启动 Amazon 托管应用程序，则系统会通过该应用程序连接的 IAM 身份中心区域触发登录。但是，如果未在外部 IdP 中配置该区域的 ACS URL，则登录将失败。

要解决此问题，请与您的 IdP 供应商合作，启用对多个 ACS 的支持。 URLs同时，您仍然可以在其他区域使用 Amazon 托管应用程序。首先，登录在外部 IdP 中配置 ACS URL 的区域（默认为主区域）。在 IAM Identity Center 中激活会话后，您可以从任何已启用区域的 Amazon Web Services 访问门户或通过应用程序链接启动应用程序。

故障转移到其他区域进行 Amazon Web Services 账户 访问

中详细介绍了通过 IAM 身份中心进行 Amazon Web Services 账户 访问的主题Amazon Web Services 账户 访问。本节提供了有关在主区域服务 Amazon Web Services 区域 中断时保持多个区域 Amazon Web Services 账户 访问权限的更多详细信息。

如果您的 IAM Identity Center 实例在主区域中遇到中断（例如，主区域的 Amazon Web Services 访问门户不可用），则您的员工可以切换到其他区域以继续访问 Amazon Web Services 账户和未受影响的应用程序。有关更多信息，请参阅 the section called “通过其他地区访问员工”。

我们建议您在中完成设置后，立即将其他地区的 Amazon Web Services 访问门户 终端节点和外部 IdP 设置（例如其他地区的书签应用程序）传达给员工。the section called “将 IAM 身份中心复制到其他区域”这将使他们能够在需要时为故障转移到其他区域做好准备。

同样，我们建议 Amazon CLI 用户为其拥有的主区域的每个配置文件创建Amazon CLI 其他区域的配置文件。然后，如果主区域出现服务中断，他们可以切换到该配置文件。

> **Note**
>
> 访问 Amazon Web Services 账户的连续性还取决于外部 IdP 的运行状况以及在服务中断之前配置和复制的权限（例如权限集分配和群组成员资格）。我们建议您的组织还设置漏洞访问权限，以便在外部 IdP 服务中Amazon 断时保持对一小部分特权用户的 Amazon 访问权限。紧急访问是避免使用 IAM 用户的类似选项，但它也取决于外部 IdP。

Amazon Web Services 账户 无需多个 ACS 即可实现访问弹性 URLs

一些外部身份提供商 (IdPs) URLs 在其 IAM Identity Center 应用程序中不支持多重断言消费者服务 (ACS)。多 URLs 个 ACS 是一项 SAML 功能，需要在多区域 IAM 身份中心中直接登录特定区域。

要让您的用户能够 Amazon Web Services 账户 通过多个 IAM 身份中心区域访问他们的区域，您必须在外部 IdP URLs 中配置相应的区域 ACS。但是，如果外部 IdP 在其 IAM 身份中心应用程序中仅支持单个 ACS URL，则用户可以直接登录单个 IAM 身份中心区域。

要解决此问题，请与您的 IdP 供应商合作，启用对多个 ACS 的支持。 URLs同时，您可以使用其他区域作为访问的备份 Amazon Web Services 账户。

如果主区域发生 IAM 身份中心服务中断，则必须使用其他区域的 ACS URL 更新外部 IdP 中的 ACS 网址。更新后，您的用户可以使用外部 IdP 门户中的现有 IAM Identity Center 应用程序或通过您与他们共享的直接链接 Amazon Web Services 访问其他区域的访问门户。

我们建议您定期测试此设置，以确保它在需要时起作用，并将此故障转移过程传达给您的组织。

> **Note**
>
> 在此设置 Amazon Web Services 账户 中使用其他区域进行访问时，您的用户可能无法访问连接到主区域的 Amazon 托管应用程序。因此，我们建议仅将其作为维持访问权限的临时措施 Amazon Web Services 账户。

跨多个 Amazon 区域部署和管理应用程序

中详细介绍了通过 IAM 身份中心访问应用程序的主题应用程序访问。本节提供了与跨多个应用程序的部署和管理相关的更多详细信息 Amazon Web Services 区域。

跨多个 Amazon 托管应用程序部署和管理托管应用程序 Amazon Web Services 区域

使用单区域 IAM Identity Center 实例，您可以在与您的实例相同的区域部署 Amazon 托管应用程序。某些应用程序（例如 Amazon Q Business）支持与 IAM 身份中心的跨区域连接，如果有感兴趣的应用程序，则可以将其部署到 IAM 身份中心的区域之外。但是，跨区域调用可能会导致应用程序性能降低，而且大多数 Amazon 托管应用程序不支持这种类型的连接。

多区域 IAM Identity Center 实例允许您在任何已启用的区域部署 Amazon 托管应用程序，并连接到同一区域的 IAM 身份中心（“区域本地连接”）。所有集成的 Amazon 托管应用程序都支持在主区域进行

部署。要确认哪些 Amazon 托管应用程序支持在 IAM Identity Center 的其他区域进行部署，请参阅中的应用程序表the section called “可与 IAM Identity Center 搭配使用的应用程序”。无论如何， Amazon 托管应用程序必须在您要部署的区域中可用。

通过与 IAM Identity Center 的区域本地连接， Amazon 托管应用程序可以访问同一区域的员工身份，以获得最佳性能和可靠性。只要满足先决条件，我们建议在部署 Amazon 托管应用程序时选择区域本地连接。

要在 IAM Identity Center 的其他区域部署 Amazon 托管应用程序，请通过应用程序控制台或 API 在该区域开始部署，方法与在主区域部署相同。

注意事项：

- 如果您尚未将 IAM Identity Center 复制到该区域，我们建议您先执行此操作，以便可以立即完成应用程序部署。
- Amazon 如果您已将 IAM Identity Center 复制到该区域，则在许多情况下，托管应用程序会自动建立区域本地连接。
- 如果 Amazon 托管应用程序提供到 IAM Identity Center 的跨区域连接，我们建议您选择区域本地连接，前提是满足先决条件。
- 如果应用程序不支持在其他区域部署，则可以在主区域部署该应用程序，前提是该应用程序在那里可用。

> **Important**
>
> 如果您的 IAM Identity Center 实例是多区域的，则无论应用程序部署区域如何，您的组织使用的所有 Amazon 托管应用程序都必须支持使用客户管理的 KMS 密钥配置的 IAM Identity Center。在部署应用程序the section called “可与 IAM Identity Center 搭配使用的应用程序”之前和在您的 IAM 身份中心配置客户托管的 KMS 密钥之前，请在中确认这一点。

应用程序的管理区域

使用区域本地连接在 IAM Identity Center 的其他区域部署 Amazon 托管应用程序后，您可以管理该应用程序及其对同一区域的用户和群组的分配。IAM Identity Center 复制应用程序元数据，包括分配给其他启用区域的用户和群组，以便您的员工可以从任何已启用的区域启动应用程序。

如果您的 Amazon 托管应用程序使用与 IAM Identity Center 的跨区域连接，则可以在连接区域中通过 IAM Identity Center 控制台和 API 管理应用程序详细信息，例如名称和描述，以及向用户和群组分配的应用程序。无论连接类型如何，您都可以在其部署区域中通过其控制台管理应用程序。

可信身份传播

在您的 IAM Identity Center 实例的任何已启用区域中，您可以将可信身份传播与支持可信身份传播的 Amazon 托管应用程序结合使用。

所有相互传播身份上下文的应用程序都必须位于同一个区域。

应用程序对其连接的 IAM 身份中心区域的依赖性

每个 Amazon 托管应用程序在部署期间都连接到特定的 IAM 身份中心区域。然后，即使您的 IAM 身份中心已在多个区域启用，应用程序也会依赖该区域进行用户登录。如果您的 IAM Identity Center 在该区域遇到中断，则用户可能无法访问连接到该地区的 Amazon 托管应用程序。

跨多个部署和管理客户托管的应用程序 Amazon Web Services 区域

IAM 身份中心支持 SAML 和 OAuth2 客户托管的应用程序。您可以选择在您的 IAM Identity Center 实例的任何已启用区域中创建它们。创建应用程序后，您可以管理该应用程序及其对同一区域的用户和群组的分配。

从 IAM 身份中心移除区域

要从您的 IAM 身份中心实例中移除其他区域，请按照以下步骤操作：

步骤 1：更新外部 IdP 配置

您可以选择从外部 IdP 中删除该区域的 ACS URL，也可以保留该网址，以备日后再次添加此区域时使用。我们建议您移除或隐藏您可能在该地区为创建 Amazon Web Services 访问门户 的书签应用程序。

步骤 2：移除该区域

Console

添加区域

1. 打开 IAM Identity Center 控制台。
2. 在导航窗格中，选择设置。
3. 选择管理选项卡。

4. 在 IAM 身份中心区域部分，选择您要删除的其他区域。
5. 选择移除 。
6. 在通过选择移除区域确认删除之前，请注意可能无法访问在此 IAM 身份中心区域中创建的应用程序的警告。如果您不确定自己是否有此类应用程序，请在导航窗格中选择 “应用程序”，然后在 “创建自” 列中确认每个 Amazon 托管应用程序和客户托管应用程序的连接区域。

   > **Note**
   >
   > 即使您无法访问这些应用程序，您也可能会因为部署仍连接到已删除区域的 Amazon 托管应用程序而继续产生费用。为防止这种情况，您需要先通过应用程序控制台或 API 移除这些 Amazon 托管应用程序部署，然后再在 IAM Identity Center 中移除该区域。如果您已经移除了 IAM 身份中心区域，则可以通过重新添加该区域来恢复对应用程序的访问权限。

7. 在 IAM 身份中心的区域部分，监控区域状态。根据需要使用刷新按钮（圆形箭头）查看最新的区域状态。移除该区域后，该区域将不再出现在区域列表中。

Amazon CLI

移除区域

```
aws sso-admin remove-region \
    --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \
    --region-name eu-west-1
```

查看当前区域状态

```
aws sso-admin describe-region \
    --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \
    --region-name eu-west-1
```

移除该区域后，请继续执行步骤 2。

步骤 3：删除副本密钥

您可以选择从该区域移除副本密钥，以避免产生 KMS 存储费用。有关更多信息，请参阅删除密 Amazon KMS 钥。

> **Important**
>
> 确保仅删除此特定区域中的副本密钥。其他 IAM 身份中心区域继续依赖其他已启用区域中的 KMS 密钥进行正常操作。

其他 Amazon 区域 APIs 支持 IAM 身份中心服务

API	其他区域的功能
身份中心 API	支持： • 应用程序管理 read/write 操作 • 实例读取操作 不支持： • 除应用程序相关之外的任何写入操作 • 权限集和账户分配读取操作
Identity Store API	读取操作
OIDC API	支持所有操作
访问门户 API	支持所有操作
SCIM API	不支持任何操作

Amazon CloudTrail 主区域和其他区域的 IAM 身份中心事件

在中 Amazon CloudTrail，您可以审计 IAM Identity Center 用户和管理员对所有启用的 IAM 身份中心实例执行 Amazon Web Services 区域 的操作。 Amazon CloudTrail 事件在操作发生的区域中发出并记录下来。有关更多信息，请参阅 the section called “日志记录和监控”。

IAM 身份中心用例在主要区域和其他区域的可用性

功能	区域可用性
带有用户门户的员工名录	
用户访问 Amazon Web Services 访问门户 包括门户登录和全球会话（所有区域都需要一次登录）	所有已启用的区域
显示所有已分配的账户	所有已启用的区域
显示所有已分配的应用程序（无论应用程序是在何处创建的）	所有已启用的区域
在 Amazon 控制台中或通过 Identity Store 读取用户、群组和成员资格的访问权限 APIs	所有已启用的区域
撤消用户会话	所有已启用的区域
通过 SCIM API 或 Identity Store API 自动同步来自外部身份来源（例如外部 IdP）的用户和群组	仅限主要区域
使用 SCIM 配置自动身份配置	仅限主要区域
使用外部 IdP 配置 SAML SSO	仅限主要区域-在所有已启用的区域中通过控制台进行读取权限
Create/update/delete通过控制台或 Identity Stor APIs e 对用户、群组和群组成员资格进行操作。	主要区域：通过 Identity Store API 可用，但在使用 SCIM API 进行配置时，IAM Identity Center 控制台会被屏蔽（ disable/enable 用户访问和删除用户除外，它们始终可用）。其他区域：不可用
多账户访问权限	
通过 Amazon Web Services 访问门户、 Amazon CLI 和快捷方式链接访问分配的帐户	所有已启用的区域

功能	区域可用性
在控制台中管理多账户权限集及其分配 APIs（包括临时提升的访问权限）	仅限主要区域
访问应用程序和 Amazon 服务	
通过应用程序控制台部署 Amazon 托管应用程序 APIs	所有已启用的区域-视应用程序的区域可用性以及对在其他区域部署的支持而定
通过 Identity Center 控制台创建客户托管的应用程序，然后 APIs	所有已启用的区域
在控制台中管理应用程序元数据和分配 APIs	应用程序的连接的 IAM 身份中心区域
从 Amazon Web Services 访问门户 或直接通过应用程序链接或书签启动应用程序	所有已启用的区域
Amazon EC2 实例的 SSO	所有已启用的区域
可信身份传播	
创建可信令牌颁发机构	仅限主要区域
使用 Amazon 托管应用程序进行可信身份传播	所有已启用的区域-相互传播身份上下文的应用程序必须位于同一区域
其他管理功能	
所有其他管理功能，例如区域管理、KMS 密钥管理、实例管理和会话管理（会话撤销除外）	仅限主要区域-某些数据的读取权限适用于所有已启用的区域（不包括权限集分配）

弹性设计和区域行为

IAM 身份中心服务是完全托管的，使用高度可用和持久的 Amazon 服务，例如 Amazon S3 和 Amazon EC2。为了确保可用区中断时的可用性，IAM Identity Center 跨多个可用区运行。您可以将您的 IAM Identity Center 实例复制到其他区域，以便在发生区域中断时使用已配置的权限保持账户访问权限。有关更多信息，请参阅 跨多个 IAM 身份中心使用 Amazon Web Services 区域。

您可以在 Amazon Organizations 管理账户中启用 IAM 身份中心。这是 IAM Identity Center 在您的 Amazon Web Services 账户所有角色中配置、取消配置和更新角色所必需的。启用 IAM Identity Center 时 Amazon Web Services 区域 ，它会部署到当前选定的区域，即 “主区域”。如果您想部署到特定区域 Amazon Web Services 区域，请在启用 IAM 身份中心之前更改区域选择，因为启用 IAM 身份中心后无法更改主要区域。

IAM Identity Center 仅支持主区域的大多数管理功能。这包括与外部身份提供商的连接、用户和组的同步，以及为用户和组创建和分配权限集。相比之下，应用程序及其分配的管理必须在创建应用程序的 IAM 身份中心区域进行。

> **Note**
>
> 即使您的 IAM 身份中心已复制到其他区域，我们也建议您设置Amazon 漏洞访问权限。这可以帮助您在外部 IdP 服务中断等事件期间保持一小部分特权用户的 Amazon 访问权限。紧急访问是使用来自外部 IdP 而不是 IAM 用户的身份的另一种选择；但是，它不能防止外部 IdP 中断。

尽管 IAM Identity Center 确定来自您启用服务的区域的访问权限，但 Amazon Web Services 账户 是全局的。这意味着，用户登录 IAM 身份中心后，当他们 Amazon Web Services 账户 通过 IAM 身份中心访问时，他们可以在任何区域进行操作。但是，大多数 Amazon 托管应用程序（例如 SageMaker Amazon AI）都必须安装在您的 IAM 身份中心实例的某个区域，用户才能对这些应用程序进行身份验证和分配访问权限。有关在 IAM Identity Center 中使用应用程序时的区域限制的信息，请参阅该应用程序的文档和the section called “跨多个 Amazon 托管应用程序部署和管理托管应用程序 Amazon Web Services 区域”。

您还可以使用 IAM Identity Center 对基于 SAML 的客户托管应用程序进行身份验证和授权，这些应用程序可通过公共 URL 访问，无论应用程序是在哪个平台或云上构建的。

我们不建议使用IAM Identity Center 的账户实例作为实现弹性的手段，因为它们不支持 Amazon 账户访问权限，而且它们会创建第二个与您的组织实例无关的隔离控制点。

为可用性而生

下表提供了 IAM Identity Center 旨在在单个 Amazon 区域中实现的可用性。这些值并不代表服务水平协议或保证，而是提供对设计目标的洞察。可用性百分比指的是对数据或功能的访问情况，而不是指持久性（例如，数据的长期保留）。

服务组件	可用性设计目标
数据面板（包括登录）	99.95%
控制面板	99.90%

设置紧急访问权限 Amazon Web Services 管理控制台

IAM Identity Center 基于高度可用的 Amazon 基础设施构建，并使用可用区架构来消除单点故障。为了在万一发生 IAM Identity Center 或 Amazon Web Services 区域 中断时提供额外的保护，我们建议您设置一个可用于提供临时访问权限的配置 Amazon Web Services 管理控制台。

Amazon 使您能够：

- 将您的第三方 IdP 连接到 IAM Identity Center。
- 使用基于 SAML 2.0 的联合身份验证将您的第三方 IdP 连接到个人 Amazon Web Services 账户 。

如果您使用 IAM Identity Center，则可以使用这些功能来创建以下部分中所述的紧急访问配置。此配置使您能够使用 IAM 身份中心作为 Amazon Web Services 账户 访问机制。如果 IAM Identity Center 中断，您的紧急操作用户可以使用与访问其账户相同的证书， Amazon Web Services 管理控制台 通过直接联合身份验证登录。当 IAM Identity Center 不可用，但 IAM 数据面板和外部身份提供商 (IdP) 可用时，此配置有效。如果您不想依赖外部 IdP，可以考虑设置Amazon 漏洞访问权限

> **Important**
>
> 我们建议您在发生中断之前部署此配置，因为如果您创建所需 IAM 角色的访问也被中断，您将无法创建该配置。此外，请定期测试此配置，以确保您的团队了解在 IAM Identity Center 中断时该怎么做。

主题

紧急访问配置汇总

配置紧急访问需要完成以下任务：

1. 在 Amazon Organizations中的组织中创建一个紧急操作帐户。该账户会成为紧急行动账户。
2. 使用基于 SAML 2.0 的联合身份验证将您的 IdP 连接到紧急操作帐户。
3. 在紧急操作帐户中，为第三方身份提供商联合身份验证创建角色。此外，在每个工作负载帐户中创建紧急操作角色，并具有所需的权限。
4. 为您在紧急操作帐户中创建的 IAM 角色委派对工作负载帐户的访问权限。要授权访问您的紧急行动账户，请在您的 IdP 中创建一个没有成员的紧急行动组。
5. 通过在 IdP 中创建启用 SAML 2.0 联合身份验证访问 Amazon Web Services 管理控制台 的规则，使 IdP 中的紧急操作组能够使用紧急操作角色。

在正常操作期间，没有人可以访问紧急操作帐户，因为 IdP 中的紧急操作组没有成员。如果 IAM Identity Center 中断，请使用您的 IdP 将受信任的用户添加到 IdP 中的紧急操作组。然后，这些用户可以登录到您的 IdP，导航到 Amazon Web Services 管理控制台，并在紧急行动账户中担任紧急行动角色。从那里，这些用户可以将角色切换到需要执行操作工作的工作负载帐户中的紧急访问角色。

如何设计关键操作角色

通过这种设计，您可以配置一个通过 IAM 进行联合的单 Amazon Web Services 账户 个，以便用户可以扮演关键操作角色。关键操作角色具有信任策略，使用户能够在工作负载帐户中担任相应的角色。工作负载帐户中的角色提供用户执行基本工作所需的权限。

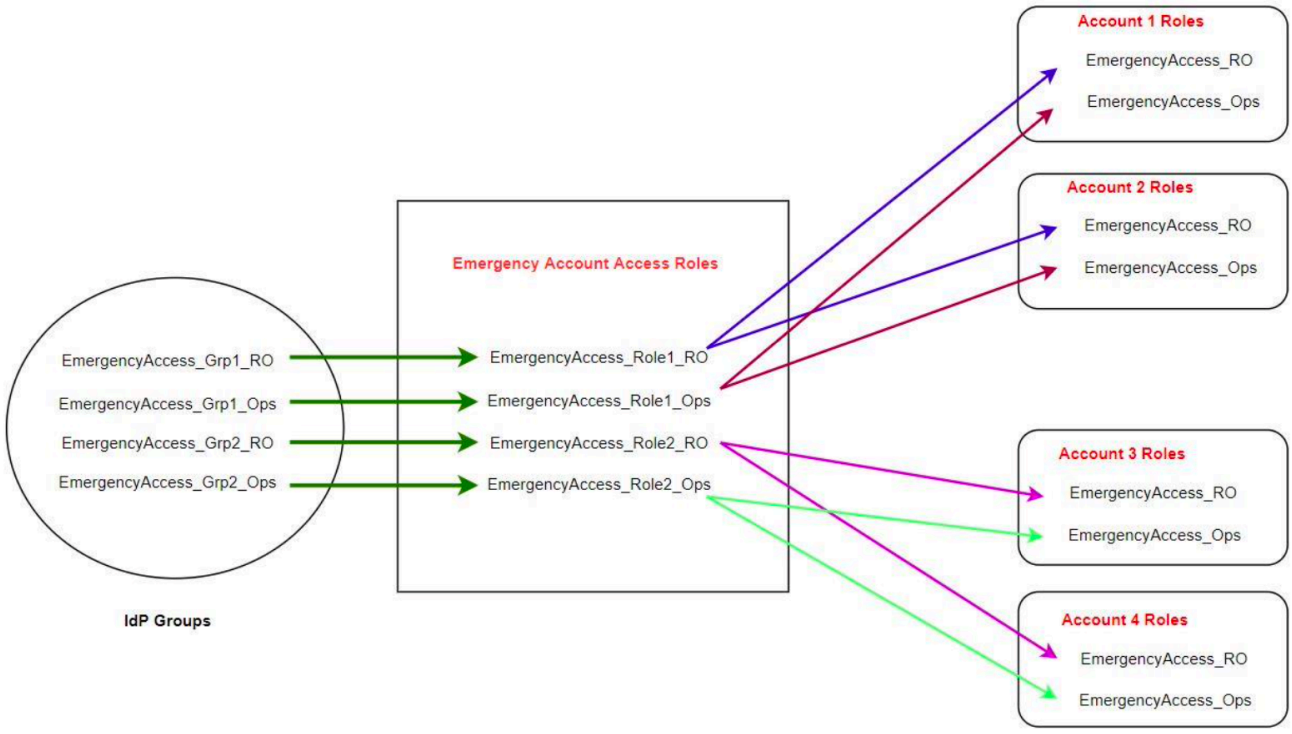
如何规划您的访问模型

在配置紧急访问之前，请为访问模型的工作方式制定计划。使用以下过程来创建此计划。

1. 确定 Amazon Web Services 账户 在 IAM Identity Center 中断期间，哪些地方需要紧急操作员访问。例如，您的生产帐户可能是必需的，但您的开发和测试帐户可能不是必需的。
2. 对于该帐户集合，确定您的帐户中需要的特定关键角色。在这些帐户中，在定义角色可以做什么时保持一致。这简化了您在紧急访问帐户中创建跨帐户角色的工作。我们建议您从这些帐户中的两个不同角色开始：只读 (RO) 和操作 (Ops)。如果需要，您可以创建更多角色并将这些角色映射到设置中更独特的紧急访问用户组。
3. 在 IdP 中识别并创建紧急访问组。组成员是您向其委派紧急访问角色访问权限的用户。
4. 定义这些组可以在紧急访问帐户中承担哪些角色。为此，请在 IdP 中定义规则，以生成列出该组可以访问的角色的声明。然后，这些组可以承担您在紧急访问帐户中的“只读”或“操作”角色。通过这些角色，他们可以在您的工作负载帐户中担任相应的角色。

如何设计紧急角色、帐户和组映射

下图显示如何将紧急访问组映射到紧急访问帐户中的角色。该图还显示了跨帐户角色信任关系，这些关系使紧急访问帐户角色能够访问工作负载帐户中的相应角色。我们建议您的应急计划设计使用这些映射作为起点。



如何创建紧急访问配置

使用以下映射表创建紧急访问配置。此表反映了一个计划，其中包括工作负载帐户中的两个角色：只读 (RO) 和操作 (Ops) 以及相应的信任策略和权限策略。信任策略使紧急访问帐户角色能够访问各个工作负载帐户角色。各个工作负载帐户角色还具有关于角色可以在帐户中执行的操作的权限策略。权限策略可以是 Amazon 管理型策略或客户管理型策略。

帐户	要创建的角色	信任策略	权限策略
Account 1	Emergency Access_RO	Emergency Access_Role1_RO	arn:aws:iam::aws:policy/ReadOnlyAccess
Account 1	Emergency Access_Ops	Emergency Access_Role1_Ops	arn:aws:iam::aws:policy/job-function/SystemAdministrator
Account 2	Emergency Access_RO	Emergency Access_Role2_RO	arn: aws: iam:: aws: policy/ ReadOnlyAccess

帐户	要创建的角色	信任策略	权限策略
Account 2	Emergency Access_Ops	Emergency Access_Role2_Ops	arn:aws:iam::aws:policy/job-function/SystemAdministrator
紧急访问帐户	Emergency Access_Role1_RO Emergency Access_Role1_Ops Emergency Access_Role2_RO Emergency Access_Role2_Ops	IdP	AssumeRole 用于账户中的角色资源

在此映射计划中，紧急访问帐户包含两个只读角色和两个操作角色。这些角色信任您的 IdP，通过在断言中传递角色名称来验证和授权您选择的组访问角色。工作负载 Account 1 和 Account 2 中有对应的只读和操作角色。对于工作负载帐户 1，`EmergencyAccess_RO` 角色信任驻留在紧急访问帐户中的 `EmergencyAccess_Role1_RO` 角色。该表指定了工作负载帐户只读和操作角色与相应的紧急访问角色之间的类似信任模式。

应急准备工作

要准备紧急访问配置，我们建议您在紧急情况发生之前执行以下任务。

1. 在您的 IdP 中设置直接 IAM 联合身份验证应用程序。如果您使用 Okta 或其他外部设备 IdPs 作为身份源，请参阅在 Okta 中一次性设置直接 IAM 联合身份验证应用程序。如果您使用 Active Directory 作为身份源，请参阅一次性设置直接 IAM 联合应用程序 ADFS。
2. 在事件期间可以访问的紧急访问帐户中创建 IdP 连接。
3. 如上面的映射表中所述，在紧急访问帐户中创建紧急访问角色。
4. 在每个工作负载帐户中创建具有信任和权限策略的临时操作角色。
5. 在 IdP 中创建临时操作组。组名称将取决于临时操作角色的名称。
6. 测试直接 IAM 联合身份验证。
7. 禁用 IdP 中的 IdP 联合身份验证应用程序以防止经常使用。

紧急故障转移流程

当 IAM Identity Center 实例不可用并且您决定必须提供对 Amazon 管理控制台的紧急访问权限时，我们建议您执行以下故障转移流程。

1. IdP 管理员在您的 IdP 中启用直接 IAM 联合身份验证应用程序。
2. 用户通过现有机制请求访问临时操作组，例如电子邮件请求、Slack 通道或其他形式的通信。
3. 添加到紧急访问组的用户登录 IdP，选择紧急访问帐户，然后用户选择要在紧急访问帐户中使用的角色。通过这些角色，他们可以在与紧急帐户角色具有跨帐户信任的相应工作负载帐户中担任角色。

恢复正常运营

查看 He Amazon alth Das hboard 以确认 IAM 身份中心服务的运行状况何时恢复。要恢复正常操作，请执行以下步骤。

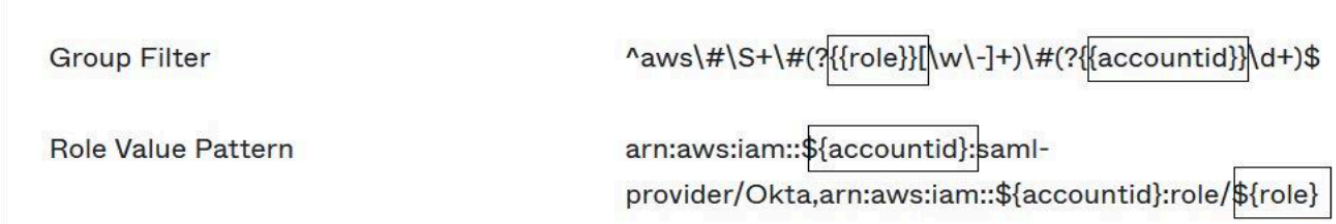
1. 当 IAM Identity Center 服务的状态图标指示该服务运行正常后，登录 IAM Identity Center。
2. 如果您可以成功登录 IAM Identity Center，请告知紧急访问用户 IAM Identity Center 可用。指示这些用户注销并使用 Amazon Web Services 访问门户重新登录 IAM Identity Center。
3. 所有紧急访问用户注销后，在 IdP 中禁用 IdP 联合身份验证应用程序。我们建议您在下班后执行此任务。
4. 从 IdP 中的紧急访问组中删除所有用户。

您的紧急访问角色基础设施仍作为备份访问计划保留，但现已禁用。

在 Okta 中一次性设置直接 IAM 联合身份验证应用程序

1. 以具有管理权限的用户身份登录您的 Okta 帐户。
2. 在 Okta 管理控制台中的应用程序下，选择应用程序。
3. 选择浏览应用程序目录。搜索并选择 Amazon 帐户联合身份验证。然后选择添加集成。
4. 按照如何为 Amazon 账户联合配置 SAML 2.0 中的步骤设置直接 IAM 联合 Amazon 。为了处理区域故障情况，在配置登录终端节点时，我们建议您为所有运营区域同时启用非区域终端节点和多个区域终端节点，以提高联邦弹性。在为此紧急访问配置 ACS URL 时，我们建议您使用不同于您的 IAM 身份中心所在区域的区域终端节点。有关区域终端节点列表，请参阅Amazon 一般参考中的登录终端节点。

5. 在登录选项选项卡上，选择 SAML 2.0 并输入组筛选条件和角色值模式设置。用户目录的组名称取决于您配置的筛选条件。



   在上图中，role 变量适用于您的紧急访问帐户中的紧急操作角色。例如，如果您在中创建EmergencyAccess_Role1_RO角色（如映射表中所述） Amazon Web Services 账户 123456789012，并且您的群组筛选器设置配置如上图所示，则您的群组名称应为aws#EmergencyAccess_Role1_RO#123456789012。

6. 在您的目录（例如，Active Directory 中的目录）中，创建紧急访问组并指定目录名称（例如，aws#EmergencyAccess_Role1_RO#123456789012）。使用现有的预置机制将您的用户分配到该组。

7. 在紧急访问帐户中，配置自定义信任策略，该策略提供在中断期间承担紧急访问角色所需的权限。以下是附加到 EmergencyAccess_Role1_RO 角色的自定义信任策略的示例语句。示例请参见如何设计紧急角色、帐户和组映射 下图中的紧急帐户。将示例 SAML 提供商 ARN 替换为您在紧急访问账户中创建的正确提供商 ARN。将示例中的区域终端节点替换为您选择的区域。

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
      {
         "Effect":"Allow",
         "Principal":{
            "Federated":"arn:aws:iam::123456789012:saml-provider/[SAML
 PROVIDER NAME]"
         },
         "Action":[
            "sts:AssumeRoleWithSAML",
            "sts:TagSession"
         ],
         "Condition":{
            "StringEquals":{
               "SAML:aud": [
```

```
                        "https://signin.aws.amazon.com/saml",
                        "https://us-west-2.signin.aws.amazon.com/saml",
                        "https://us-west-1.signin.aws.amazon.com/saml",
                        "https://us-east-2.signin.aws.amazon.com/saml"
                    ]
                }
            }
        },
        {
            "Effect":"Allow",
            "Principal":{
            "Federated":"arn:aws:iam::123456789012:saml-provider/Okta"
            },
            "Action":"sts:SetSourceIdentity"
         }
    ]
}
```

8. 以下是附加到 EmergencyAccess_Role1_RO 角色的权限策略的示例语句。示例请参见 如何设计紧急角色、帐户和组映射 下图中的紧急帐户。

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": [
                "arn:aws:iam::111122223333:role/EmergencyAccess_RO",
                "arn:aws:iam::444455556666:role/EmergencyAccess_RO"
            ]
        }
    ]
}
```

9. 在工作负载帐户上，配置自定义信任策略。以下是附加到 EmergencyAccess_RO 角色的信任策略的示例语句。在本例中，帐户 123456789012 是紧急访问帐户。有关说明，请参阅 如何设计紧急角色、帐户和组映射 下图表中的工作负载帐户。

JSON

```
{
    "Version":"2012-10-17",
    "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::123456789012:root"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

> **Note**
>
> 大多数都 IdPs 允许您在需要之前停用应用程序集成。我们建议您在 IdP 中保持直接 IAM 联合身份验证应用程序处于停用状态，直到需要紧急访问为止。

一次性设置直接 IAM 联合应用程序 ADFS

本指南介绍了一次性设置过程，用于配置直接 IAM 联合身份验证，ADFS以便在 IAM Identity Center 不可用 Amazon Web Services 账户 时启用紧急访问权限。

先决条件

如果您计划ADFS使用 Amazon 托管 Microsoft AD 进行配置，我们建议您首先配置多区域复制，然后在其他区域而不是主区域中继续执行以下步骤，以实现弹性。

规划您的活动目录组命名惯例

使用特定的命名模式创建 AD 组，从而实现群组名称和 Amazon IAM 角色之间的自动匹配。

群组命名格式：`AWS-<AccountNumber>-<RoleName>`

示例请参见 如何设计紧急角色、帐户和组映射 下图中的紧急帐户。当用户被分配到该组时，他们被授予对账户中EmergencyAccess_Role1_RO角色的访问权限123456789012。如果用户与多个群组关联，他们会看到可用角色列表， Amazon Web Services 账户 并可以选择要扮演的角色。

Amazon 配置

完整的设置包括紧急访问帐户和工作负载帐户中的配置。有关整体设置的说明，请参见如何设计紧急角色、帐户和组映射。

1. 创建 SAML 身份提供商
2. 创建紧急访问角色
3. 配置工作负载帐户角色

创建 SAML 身份提供商

在紧急访问账户中，按照在 IAM 中创建 SAML 身份提供商中的步骤在 IAM 中创建 SAML 身份提供商。从您的ADFS服务器下载所需的元数据：

```
https://<yourADFSserverFQDN>/FederationMetadata/2007-06/
FederationMetadata.xml
```

创建紧急访问角色

使用 SAML 2.0 Federation 作为可信实体类型，在紧急账户中@@ 创建紧急访问角色。选择您在上一步中创建的 SAML 2.0 提供商。

注意事项：

- 包括您运营的所有区域 — 选择您拥有活跃工作负载的每个区域，以确保联合在区域中断期间保持可用。
- 即使您在单个区域中运营，也至少配置一个额外的区域终端节点，例如，如果您仅在其中操作us-east-1，则添加us-west-2为辅助终端节点。即使没有任何工作负载，您也可以将 IdP 故障转移到 us-west-2 SAML 登录终端节点并仍然可以访问您的us-east-1资源。us-west-2
- 同时启用非区域终端节点和区域终端节点 — 尽管非区域终端节点 (https://signin.aws.amazon.com/saml) 高度可用，但它托管在单个终端节点中 Amazon Web Services 区域us-east-1，而区域端点 (https://<region>.signin.aws.amazon.com/saml) 则通过减少对单个全球终端节点的依赖来提高弹性。

配置信任策略

有关具有多个登录区域终端节点的信任策略示例，请参阅。在 Okta 中一次性设置直接 IAM 联合身份验证应用程序将示例区域终端节点和 SAML 提供商替换为您的终端节点和 SAML ARNs 提供商。

配置权限策略

有关附加到在 Okta 中一次性设置直接 IAM 联合身份验证应用程序紧急访问角色的权限策略示例，请参阅。

配置工作负载帐户角色

对于工作负载账户角色，请配置自定义信任策略，允许紧急访问账户中的紧急访问角色代入这些角色。请参阅信任策略示例，其中账户123456789012是紧急访问账户。在 Okta 中一次性设置直接 IAM 联合身份验证应用程序

活动目录配置

以下步骤描述了如何配置 Active Directory 以及如何ADFS进行紧急访问。

1. 创建群组
2. 创建信赖方
3. 创建索赔规则

创建群组

根据前面描述的命名惯例在 Active Directory 中创建紧急群组（例如，`AWS-123456789012-EmergencyAccess_Role1_R0`）。通过现有的配置机制将用户分配到这些群组。

创建信赖方

ADFS联合需要信赖方配置。依赖方是 Amazon Security Token Service (Amazon STS)，它将身份验证外包给ADFS身份提供者。

1. 在ADFS管理控制台中，使用操作菜单并选择添加信赖方信任。添加信赖方时选择 “声明感知”。
2. 对于联合元数据，请在 IAM 控制台上输入身份提供商元数据信息中的元数据 URL。例如：

   ```
   https://signin.aws.amazon.com/static/saml/SAMLSPXXXXXX/saml-metadata.xml
   ```
3. 设置信赖方的显示名称（例如，Amazon 账户访问权限），然后选择下一步。
4. 选择您想要允许谁进行访问 Amazon。您可以选择特定的群组并定义诸如 MFA 之类的要求。
5. 在 “完成” 页上选择 “关闭” 以完成 “添加信赖方信任向导”。 Amazon 现在已配置为信赖方。

创建索赔规则

ADFS使用索赔规则语言在索赔提供者和依赖方之间发出和转换索赔。您需要创建四条声明规则：NameId、RoleSessionName、“获取广告组” 和 “ Amazon 访问角色”。

右键单击信赖方，然后选择 “编辑索赔发放政策”。选择添加规则以添加规则。

1NameId.

a. 选择 “转换传入的声明”，然后选择 “下一步”。

b. 使用以下设置：

- 声明规则名称：NameId
- 收到的索赔类型：Windows Account Name
- 发出的索赔类型：Name ID
- 传出姓名 ID 格式：Persistent Identifier
- 传递所有索赔值：已选中

c. 选择确定。

2。 RoleSessionName

a. 选择添加规则。

b. 在 “声明规则模板” 列表中，选择 “将 LDAP 属性作为声明发送”。

c. 使用以下设置：

- 声明规则名称：RoleSessionName
- 属性存储：Active Directory
- LDAP 属性：E-Mail-Addresses
- 发出的索赔类型：https://aws.amazon.com/SAML/Attributes/RoleSessionName

d. 选择确定。

3。获取广告组

a. 选择添加规则。

b. 在 “索赔规则模板” 列表中，选择 “使用自定义规则发送索赔”，然后选择 “下一步”。

c. 在 “声明规则名称” 中Get AD Groups，输入，然后在 “自定义规则” 中输入以下内容：

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/
windowsaccountname", Issuer == "AD AUTHORITY"]
=> add(store = "Active Directory", types = ("http://temp/variable"), query =
 ";tokenGroups;{0}", param = c.Value);
```

此自定义规则使用声明规则语言中的脚本，该脚本检索经过身份验证的用户所属的所有群组，并将其置于名http://temp/variable为的临时声明中。

> **Note**
>
> 确保尾部没有空格，以免出现意外结果。

4。角色属性

a. 选择添加规则。

b. 在 “索赔规则模板” 列表中，选择 “使用自定义规则发送索赔”，然后选择 “下一步”。

c. 在 “声明规则名称” 中Roles，输入，然后在 “自定义规则” 中输入以下内容：

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([\d]{12})"]
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =
 RegExReplace(c.Value, "AWS-([\d]{12})-", "arn:aws:iam::$1:saml-provider/
<ADFS>,arn:aws:iam::$1:role/"));
```

此自定义规则使用正则表达式将表单AWS-<Account Number>-<Role Name>中的每个群组成员资格转换为预期的 IAM 角色 ARN 和 IAM 联合提供商 ARN 表单。 Amazon

> **Note**
>
> 在上面的示例规则语言中，ADFS表示在身份提供商设置中给 SAML 身份提供商的 Amazon 逻辑名称。根据您在 IAM 控制台中为身份提供商选择的逻辑名称进行更改。

测试配置

通过在进行身份验证来测试解决方案是否有效。https://<yourADFSserverFQDN>/adfs/ls/IdpInitiatedSignOn.aspx从站点的下拉列表中选择您创建的信赖方的名称。

更新中的默认 SAML 断言端点 ADFS

> **Important**
>
> 在中配置信赖方信任时ADFS，SAML Assertion 端点默认为`https://signin.aws.amazon.com/`它不是全局终端节点，位于中。`us-east-1`我们建议您将默认终端节点修改为不同于 IAM Identity Center 弹性配置的区域终端节点。例如，如果您的 IAM 身份中心部署在中`us-east-1`并且您也在中进行操作`us-west-2`，请将默认 SAML Assertion 使用者终端节点更改为。`https://us-west-2.signin.aws.amazon.com/saml`

1. 在信赖方信任上选择 “属性”，然后转到 “监控” 选项卡。清除 “自动更新信赖方” 复选框。
2. 前往终端节点选项卡，选择您的首选登录端点，然后选择编辑。
3. 选中 “将可信 URL 设置为默认值” 复选框。选择 “确定” 和 “应用” 以使设置生效。

> **Note**
>
> 大多数都 IdPs 允许您在需要之前停用应用程序集成。我们建议您在 IdP 中保持直接 IAM 联合身份验证应用程序处于停用状态，直到需要紧急访问为止。

中的安全性 Amazon IAM Identity Center

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

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

- 云安全 — Amazon 负责保护在 Amazon 云中运行 Amazon 服务的基础架构。 Amazon 还为您提供可以安全使用的服务。 Third-party 作为Amazon 合规计划的一部分，审计师定期测试和验证我们安全的有效性。要了解适用的合规计划 Amazon IAM Identity Center，请参阅按合规计划划分的范围内的Amazon 服务。
- 云端安全-您的责任由您使用的 Amazon 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

本文档可帮助您了解如何在使用 IAM Identity Center 时应用责任共担模型。以下主题向您展示如何配置 IAM Identity Center 以满足您的安全性和合规性目标。您还将学习如何使用其他 Amazon 服务来帮助您监控和保护您的 IAM Identity Center 资源。

主题

IAM Identity Center 身份和访问管理

访问 IAM Identity Center 需要 Amazon 可用于对您的请求进行身份验证的证书。这些证书必须具有访问 Amazon 资源（例如 Amazon 托管应用程序）的权限。

Amazon Web Services 访问门户的身份验证由您连接到 IAM Identity Center 的目录控制。但是，Amazon Web Services 访问门户内部可供用户访问的权限由两个因素决定： Amazon Web Services 账户

1. 谁被分配了 IAM 身份中心控制台 Amazon Web Services 账户 中用户的访问权限。有关更多信息，请参阅 单点登录访问权限 Amazon Web Services 账户。
2. 在 IAM Identity Center 控制台中向用户授予了什么权限级别，以允许其适当访问这些 Amazon Web Services 账户。有关更多信息，请参阅 创建、管理和删除权限集。

以下各节说明了您作为管理员如何控制对 IAM Identity Center 控制台的访问权限，或者如何委派管理访问权限来执行 IAM Identity Center 控制台中的日常任务。

- 身份验证
- 访问控制

身份验证

了解如何 Amazon 使用 IAM 身份进行访问。

访问控制

您可以使用有效的凭证来对自己的请求进行身份验证，但您还必须拥有权限才能创建或访问 IAM Identity Center 资源。例如，您必须拥有权限才能创建 IAM Identity Center 连接目录。

> **Note**
>
> 如果您的 IAM Identity Center 实例配置了客户自主管理型 KMS 密钥，则 IAM Identity Center 管理员和其他需要访问该 KMS 密钥的人员将需要额外权限。请参考在中实现客户托管的 KMS 密钥 Amazon IAM Identity Center。

下面几节介绍如何管理 IAM Identity Center 的权限。我们建议您先阅读概述。

- 管理 IAM Identity Center 资源的访问权限概述
- Identity-based IAM 身份中心的策略示例
- Resource-based IAM 身份中心 IAM 身份中心的策略示例
- 使用 IAM Identity Center 的服务相关角色

管理 IAM Identity Center 资源的访问权限概述

每个 Amazon 资源都归人所有 Amazon Web Services 账户，创建或访问资源的权限受权限策略的约束。为了提供访问权限，帐户管理员可以向 IAM 身份（即用户、组和角色）添加权限。某些服务（例如 Amazon Lambda）还支持向资源添加权限。

> **Note**
>
> 帐户管理员（或管理员用户）是具有管理员权限的用户。有关更多信息，请参阅 IAM 用户指南中的 IAM 最佳实践。

主题

IAM Identity Center 资源和操作

在 IAM Identity Center 中，主要资源是应用程序实例、配置文件和权限集。

了解资源所有权

资源所有者 Amazon Web Services 账户 是创建资源的人。也就是说，资源所有者是 Amazon Web Services 账户 对创建资源的请求进行身份验证的委托人实体（账户、用户或 IAM 角色）。以下示例说明了它的工作原理：

- 如果 Amazon Web Services 账户根用户 创建了 IAM Identity Center 资源，例如应用程序实例或权限集， Amazon Web Services 账户 则您就是该资源的所有者。
- 如果您在 Amazon 账户中创建用户并向该用户授予创建 IAM Identity Center 资源的权限，则该用户随后可以创建 IAM Identity Center 资源。但是，该用户所属的您的 Amazon 账户拥有这些资源。
- 如果您在 Amazon 账户中创建具有创建 IAM Identity Center 资源的权限的 IAM 角色，则任何能够代入该角色的人都可以创建 IAM 身份中心资源。该角色所属的 Amazon Web Services 账户拥有 IAM Identity Center 资源。

管理对 资源的访问

权限策略规定谁可以访问哪些内容。下一节介绍创建权限策略时的可用选项。

> **Note**
>
> 本节讨论如何在 IAM Identity Center 范围内使用 IAM。这里不提供有关 IAM 服务的详细信息。有关完整的 IAM 文档，请参阅 IAM 用户指南中的什么是 IAM？。有关 IAM 策略语法和说明的信息，请参阅 IAM 用户指南中的 Amazon IAM 策略参考。

附加到 IAM 身份的策略称作基于身份的策略 (IAM policy)。附加到资源的策略称作基于资源的 策略。IAM Identity Center 只支持基于身份的策略 (IAM 策略)。

主题

- Identity-based 策略（IAM 策略）
- Resource-based 政策

Identity-based 策略（IAM 策略）

您可以向 IAM 身份添加权限。例如，您可以执行以下操作：

- 将@@ 权限策略附加到您的用户或群组 Amazon Web Services 账户 — 账户管理员可以使用与特定用户关联的权限策略向该用户授予添加 IAM Identity Center 资源（例如新应用程序）的权限。
- 向角色附加权限策略（授予跨帐户权限）– 您可以向 IAM 角色附加基于身份的权限策略，以授予跨帐户的权限。

  有关使用 IAM 委派权限的更多信息，请参阅 IAM 用户指南中的访问权限管理。

以下权限策略对用户授予权限以运行以 `List` 开头的所有操作。这些操作显示了有关 IAM Identity Center 资源（如应用程序实例或权限集合）的信息。请注意，`Resource` 元素中的通配符 (*) 表示可对该帐户拥有的所有 IAM Identity Center 资源执行操作。

JSON

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

```
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"sso:List*",
         "Resource":"*"
      }
   ]
}
```

有关对 IAM Identity Center 使用基于身份的策略的更多信息，请参阅 Identity-based IAM 身份中心的策略示例。有关用户、组、角色和权限的更多信息，请参阅 IAM 用户指南中的身份（用户、组和角色）。

Resource-based 政策

其他服务（如 Amazon S3）还支持基于资源的权限策略。例如，您可以将策略附加到 S3 存储桶以管理对该存储桶的访问权限。IAM Identity Center 不支持基于资源的策略。

指定策略元素：操作、效果、资源和主体

对于每种 IAM Identity Center 资源（请参阅 IAM Identity Center 资源和操作），该服务都定义了一组 API 操作。为授予这些 API 操作的权限，IAM Identity Center 定义了一组您可以在策略中指定的操作。请注意，执行某项 API 操作可能需要执行多个操作的权限。

以下是基本的策略元素：

- 资源：在策略中，您可以使用 Amazon 资源名称（ARN）标识策略应用到的资源。
- 操作：您可以使用操作关键字标识要允许或拒绝的资源操作。例如，`sso:DescribePermissionsPolicies` 权限允许执行 IAM Identity Center `DescribePermissionsPolicies` 操作的用户权限。
- 效果：您可以指定当用户请求特定操作（可以是允许或拒绝）时的效果。如果没有显式授予 (允许) 对资源的访问权限，则隐式拒绝访问。您也可显式拒绝对资源的访问，这样可确保用户无法访问该资源，即使有其他策略授予了访问权限的情况下也是如此。
- 主体：在基于身份的策略（IAM 策略）中，附加了策略的用户是隐式主体。对于基于资源的策略，您可以指定要接收权限的用户、帐户、服务或其他实体（仅适用于基于资源的策略）。IAM Identity Center 不支持基于资源的策略。

有关 IAM 策略语法和描述的更多信息，请参阅 IAM 用户指南中的 Amazon IAM 策略参考。

在策略中指定条件

当您授予权限时，可使用访问策略语言来指定规定策略生效的条件。例如，您可能希望策略仅在特定日期后应用。有关使用策略语言指定条件的更多信息，请参阅《IAM 用户指南》中的条件。

要表示条件，您可以使用预定义的条件键。没有特定于 IAM Identity Center 的条件键。但是，您可以根据需要使用一些 Amazon 条件键。有关 Amazon 密钥的完整列表，请参阅 IAM 用户指南中的可用全局条件密钥。

Identity-based IAM 身份中心的策略示例

本主题提供了 IAM 策略示例，您可以创建这些策略来授予用户和角色管理 IAM Identity Center 的权限。

> **Important**
>
> 我们建议您首先阅读以下介绍性主题，这些主题讲解了管理 IAM Identity Center 资源访问的基本概念和选项。有关更多信息，请参阅 管理 IAM Identity Center 资源的访问权限概述。

本主题的各个部分涵盖以下内容：

- 自定义策略示例
- 使用 IAM Identity Center 控制台所需的权限

自定义策略示例

本部分提供了需要自定义 IAM policy 的常见用例示例。这些示例策略是基于身份的策略，不指定主体元素。这是因为使用基于身份的策略时，您无需指定获得权限的主体。相反，您将策略附加到主体。向 IAM 角色附加基于身份的权限策略后，该角色的信任策略中标识的主体将获取权限。您可以在 IAM 中创建基于身份的策略并将其附加到用户、 and/or 群组和角色。当您在 IAM Identity Center 中创建权限集时，您还可以将这些策略应用于 IAM Identity Center 用户。

> **Note**
>
> 在为您的环境创建策略时使用这些示例，并确保在生产环境中部署这些策略之前测试正面（“授予访问”）和负面（“拒绝访问”）测试用例。有关测试 IAM 策略的更多信息，请参阅 IAM 用户指南中的使用 IAM policy simulator 测试 IAM 策略。

主题

示例 1：允许用户查看 IAM Identity Center

以下权限策略向用户授予只读权限，以便他们可以查看 IAM Identity Center 中配置的所有设置和目录信息。

> **Note**
>
> 本策略仅供参考。在生产环境中，我们建议您使用 IAM Identity Center 的`ViewOnlyAccess` Amazon 托管策略。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ds:DescribeDirectories",
                "ds:DescribeTrusts",
                "iam:ListPolicies",
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:ListAccountsForParent",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListOrganizationalUnitsForParent",
                "sso:ListManagedPoliciesInPermissionSet",
```

```
                "sso:ListPermissionSetsProvisionedToAccount",
                "sso:ListAccountAssignments",
                "sso:ListAccountsForProvisionedPermissionSet",
                "sso:ListPermissionSets",
                "sso:DescribePermissionSet",
                "sso:GetInlinePolicyForPermissionSet",
                "sso-directory:DescribeDirectory",
                "sso-directory:SearchUsers",
                "sso-directory:SearchGroups"
            ],
            "Resource": "*"
        }
    ]
}
```

示例 2：允许用户管理以下权限 Amazon Web Services 账户 在 IAM 身份中心中

以下权限策略授予允许用户为您的 Amazon Web Services 账户创建、管理和部署权限集的权限。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:AttachManagedPolicyToPermissionSet",
                "sso:CreateAccountAssignment",
                "sso:CreatePermissionSet",
                "sso:DeleteAccountAssignment",
                "sso:DeleteInlinePolicyFromPermissionSet",
                "sso:DeletePermissionSet",
                "sso:DetachManagedPolicyFromPermissionSet",
                "sso:ProvisionPermissionSet",
                "sso:PutInlinePolicyToPermissionSet",
                "sso:UpdatePermissionSet"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMListPermissions",
```

```
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles",
                "iam:ListPolicies"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AccessToSSOProvisionedRoles",
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:GetRole",
                "iam:ListAttachedRolePolicies",
                "iam:ListRolePolicies",
                "iam:PutRolePolicy",
                "iam:UpdateRole",
                "iam:UpdateRoleDescription"
            ],
            "Resource": "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetSAMLProvider"
            ],
            "Resource": "arn:aws:iam::*:saml-provider/AWSSSO_*_DO_NOT_DELETE"
        }
    ]
}
```

> **Note**
>
> 和”"Sid": "AccessToSSOProvisionedRoles" 部分下列出的"Sid": "IAMListPermissions"其他权限仅用于使用户能够在 Amazon Organizations 管理账户中创建任务。在某些情况下，您可能还需要添加 iam:UpdateSAMLProvider 到这些部分。

示例 3：允许用户管理 IAM Identity Center 中的应用程序

以下权限策略授予权限以允许用户查看和配置 IAM Identity Center 中的应用程序，包括 IAM Identity Center 目录中预集成的 SaaS 应用程序。

> **Note**
>
> 管理应用程序的用户和组分配需要以下策略示例中使用的 `sso:AssociateProfile` 操作。它还允许用户使用现有权限集向 Amazon Web Services 账户 其分配用户和组。如果用户必须在 IAM Identity Center 中管理 Amazon Web Services 账户 访问权限，并且需要管理权限集所需的权限，请参阅示例 2：允许用户管理以下权限 Amazon Web Services 账户 在 IAM 身份中心中。

截至 2020 年 10 月，其中许多操作只能通过 Amazon 控制台进行。此示例策略包括“读取”操作，例如列表、获取和搜索，这些操作与本例中控制台的无错误操作相关。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:AssociateProfile",
                "sso:CreateApplicationInstance",
                "sso:ImportApplicationInstanceServiceProviderMetadata",
                "sso:DeleteApplicationInstance",
                "sso:DeleteProfile",
                "sso:DisassociateProfile",
                "sso:GetApplicationTemplate",
                "sso:UpdateApplicationInstanceServiceProviderConfiguration",
                "sso:UpdateApplicationInstanceDisplayData",
                "sso:DeleteManagedApplicationInstance",
                "sso:UpdateApplicationInstanceStatus",
                "sso:GetManagedApplicationInstance",
                "sso:UpdateManagedApplicationInstanceStatus",
                "sso:CreateManagedApplicationInstance",
                "sso:UpdateApplicationInstanceSecurityConfiguration",
                "sso:UpdateApplicationInstanceResponseConfiguration",
```

```
                "sso:GetApplicationInstance",
                "sso:CreateApplicationInstanceCertificate",
                "sso:UpdateApplicationInstanceResponseSchemaConfiguration",
                "sso:UpdateApplicationInstanceActiveCertificate",
                "sso:DeleteApplicationInstanceCertificate",
                "sso:ListApplicationInstanceCertificates",
                "sso:ListApplicationTemplates",
                "sso:ListApplications",
                "sso:ListApplicationInstances",
                "sso:ListDirectoryAssociations",
                "sso:ListProfiles",
                "sso:ListProfileAssociations",
                "sso:ListInstances",
                "sso:GetProfile",
                "sso:GetSSOStatus",
                "sso:GetSsoConfiguration",
                "sso-directory:DescribeDirectory",
                "sso-directory:DescribeUsers",
                "sso-directory:ListMembersInGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

示例 4：允许用户管理 Identity Center 目录中的用户和组

以下权限策略授予权限以允许用户在 IAM Identity Center 中创建、查看、修改和删除用户和组。

在某些情况下，对 IAM Identity Center 中的用户和组的直接修改受到限制。例如，当选择 Active Directory 或启用了自动预置的外部身份提供商作为身份源时。

JSON

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

```
                "sso-directory:ListGroupsForUser",
                "sso-directory:DisableUser",
                "sso-directory:EnableUser",
                "sso-directory:SearchGroups",
                "sso-directory:DeleteGroup",
                "sso-directory:AddMemberToGroup",
                "sso-directory:DescribeDirectory",
                "sso-directory:UpdateUser",
                "sso-directory:ListMembersInGroup",
                "sso-directory:CreateUser",
                "sso-directory:DescribeGroups",
                "sso-directory:SearchUsers",
                "sso:ListDirectoryAssociations",
                "sso-directory:RemoveMemberFromGroup",
                "sso-directory:DeleteUser",
                "sso-directory:DescribeUsers",
                "sso-directory:UpdateGroup",
                "sso-directory:CreateGroup"
            ],
            "Resource": "*"
        }
    ]
}
```

使用 IAM Identity Center 控制台所需的权限

为了使用户能够正确使用 IAM Identity Center 控制台，需要额外的权限。如果创建的 IAM 策略比所需的最低权限更严格，则控制台将无法按使用该策略的用户的预期运行。以下示例列出了确保 IAM Identity Center 控制台中无错误操作可能需要的权限集。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:DescribeAccountAssignmentCreationStatus",
                "sso:DescribeAccountAssignmentDeletionStatus",
                "sso:DescribePermissionSet",
```

```
                "sso:DescribePermissionSetProvisioningStatus",
                "sso:DescribeRegisteredRegions",
                "sso:GetApplicationInstance",
                "sso:GetApplicationTemplate",
                "sso:GetInlinePolicyForPermissionSet",
                "sso:GetManagedApplicationInstance",
                "sso:GetMfaDeviceManagementForDirectory",
                "sso:GetPermissionSet",
                "sso:GetProfile",
                "sso:GetSharedSsoConfiguration",
                "sso:GetSsoConfiguration",
                "sso:GetSSOStatus",
                "sso:GetTrust",
                "sso:ListAccountAssignmentCreationStatus",
                "sso:ListAccountAssignmentDeletionStatus",
                "sso:ListAccountAssignments",
                "sso:ListAccountsForProvisionedPermissionSet",
                "sso:ListApplicationInstanceCertificates",
                "sso:ListApplicationInstances",
                "sso:ListApplications",
                "sso:ListApplicationTemplates",
                "sso:ListDirectoryAssociations",
                "sso:ListInstances",
                "sso:ListManagedPoliciesInPermissionSet",
                "sso:ListPermissionSetProvisioningStatus",
                "sso:ListPermissionSets",
                "sso:ListPermissionSetsProvisionedToAccount",
                "sso:ListProfileAssociations",
                "sso:ListProfiles",
                "sso:ListTagsForResource",
                "sso-directory:DescribeDirectory",
                "sso-directory:DescribeGroups",
                "sso-directory:DescribeUsers",
                "sso-directory:ListGroupsForUser",
                "sso-directory:ListMembersInGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Resource-based IAM 身份中心 IAM 身份中心的策略示例

所有与 IAM Identity Center 集成且使用 OAuth 2.0 的应用程序都需要配置基于资源的策略。该应用程序可以由客户管理或 Amazon 管理。所需的基于资源的策略称为应用程序策略（或ActorPolicy在 API 中），它定义了哪些 IAM 委托人有权调用 IAM 身份验证方法 API 操作，例如。CreateTokenWithIAMIAM 身份验证方法允许 IAM 委托人（例如 IAM 角色或 Amazon 服务）通过在 /token? 上出示 IAM 证书来请求或管理访问令牌，从而向 IAM 身份中心 OIDC 服务进行身份验证 aws_iam=t 端点。

应用程序策略管控令牌颁发操作（CreateTokenWithIAM）。该政策还管理仅限许可的操作，这些操作仅供 Amazon 托管应用程序用于验证令牌 (IntrospectTokenWithIAM) 和撤消令牌 ()。RevokeTokenWithIAM对于客户自主管理型应用程序，您可以通过指定哪些 IAM 主体有权调用 CreateTokenWithIAM 来配置此策略。当授权主体调用此 API 操作时，将获取该应用程序的访问令牌和刷新令牌。

如果您使用 IAM Identity Center 控制台为可信身份传播设置客户自主管理型应用程序，请参阅设置客户自主管理型 OAuth 2.0 应用程序中的步骤 4，了解应用程序策略的配置方法。有关策略示例，请参阅本主题后面的 示例策略：允许 IAM 角色创建访问令牌和刷新令牌。

政策要求

策略必须满足以下要求：

- 策略必须包含设置为“2012-10-17”的 Version 元素。
- 必须包含至少一个 Statement 元素。
- 每个策略 Statement 必须包含以下元素：Effect、Principal、Action 和 Resource。

策略元素

该策略必须包含以下元素：

版本

指定策略文档版本。将版本设置为 2012-10-17（最新版本）。

语句

包含策略 Statements。策略必须包含至少一个 Statement。

每个策略 Statement 包含以下元素。

效果

（必需）确定是允许还是拒绝该策略语句中的权限。有效值为 `Allow` 或 `Deny`。

Principal

（必需）主题是获取策略语句中指定的权限的身份。您可以指定 IAM 角色或 Amazon 服务主体。

处理建议

（必需）允许或拒绝的 IAM Identity Center OIDC 服务 API 操作。有效操作包括：

- `sso-oauth:CreateTokenWithIAM`：此操作与 `CreateTokenWithIAM`API 操作相对应，授予使用任何 IAM 实体（例如 Amazon 服务角色或用户）进行身份验证的授权客户端应用程序创建和返回访问和刷新令牌的权限。这些令牌可能包含已定义的作用域，用于指定 `read:profile` 或 `write:data` 等权限。
- `sso-oauth:IntrospectTokenWithIAM` [仅限权限]：授予权限验证并检索活跃的 OAuth 2.0 访问令牌和刷新令牌的相关信息，包括其关联的作用域和权限。此权限仅供 Amazon 托管应用程序使用，未记录在 IAM 身份中心 OIDC API 参考中。
- `RevokeTokenWithIAM` [仅限权限]：授予权限撤销 OAuth 2.0 访问令牌和刷新令牌，使其在正常过期前失效。此权限仅供 Amazon 托管应用程序使用，未记录在 IAM 身份中心 OIDC API 参考中。

资源

（必需）在此策略中 `Resource` 元素的值为 `"*"`，表示“此应用程序”。

有关 Amazon 策略语法的更多信息，请参阅 Amazon IAM 用户指南中的 IAM 策略参考。

示例策略：允许 IAM 角色创建访问令牌和刷新令牌

以下权限策略授予工作负载所扮演的 IAM 角色 `ExampleAppClientRole` 创建并返回访问令牌及刷新令牌的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRoleToCreateTokens",
            "Effect": "Allow",
            "Principal": {
```

```
                "AWS": "arn:aws:iam::111122223333:role/ExampleAppClientRole"
            },
            "Action": "sso-oauth:CreateTokenWithIAM",
            "Resource": "*"
        }
    ]
}
```

Amazon IAM 身份中心的托管策略

要创建 IAM 客户管理型策略以仅向您的团队提供他们所需的权限，需要时间和专业知识。要快速入门，您可以使用 Amazon 托管策略。这些策略涵盖常见使用案例，可在您的 Amazon Web Services 账户中使用。有关 Amazon 托管式策略的更多信息，请参阅《IAM 用户指南》中的 Amazon 托管式策略。

Amazon 服务维护和更新 Amazon 托管策略。您无法更改 Amazon 托管策略中的权限。服务偶尔会向 Amazon 托管式策略添加额外权限以支持新特征。此类更新会影响附加策略的所有身份（用户、组和角色）。当启动新特征或新操作可用时，服务最有可能会更新 Amazon 托管式策略。服务不会从 Amazon 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 Amazon 支持跨多个服务的工作职能的托管策略。例如，ReadOnlyAccess Amazon 托管策略提供对所有 Amazon 服务和资源的只读访问权限。当服务启动一项新功能时， Amazon 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 Amazon 管理型策略。

新命名空间 `identitystore-auth` 下提供了允许您列出和删除用户会话的新操作。此命名空间中的任何其他操作权限都将在此页面上更新。创建自定义 IAM 策略时，请避免在 `identitystore-auth` 后使用 `*`，因为这适用于当前或将来命名空间中存在的所有操作。

Amazon 托管策略： AWSSSOMasterAccountAdministrator

`AWSSSOMasterAccountAdministrator` 策略向主体提供所需的管理操作。该政策适用于担任 Amazon IAM Identity Center 管理员工作角色的委托人。随着时间的推移，所提供的操作列表将会更新，以匹配 IAM Identity Center 的现有功能以及管理员所需的操作。

您可以将 `AWSSSOMasterAccountAdministrator` 策略附加到 IAM 身份。
将`AWSSSOMasterAccountAdministrator`策略附加到身份时，即授予管理 Amazon IAM Identity Center 权限。拥有此政策的委托人可以在 Amazon Organizations 管理账户和所有成员账户中访问 IAM Identity Center。该主体可以完全管理所有 IAM Identity Center 操作，包括创建 IAM Identity Center 实例、用户、权限集和分配的能力。委托人还可以在整个 Amazon 组织成员账户中实例化这些分配，

并在 Amazon Directory Service 托管目录和 IAM Identity Center 之间建立连接。随着新管理功能的发布，帐户管理员将自动获得这些权限。

该策略还包括使用客户托管密钥进行加密的 IAM Identity Center 实例所需的 Amazon Key Management Service 权限。

权限分组

此策略根据提供的权限集分为多个语句。

- `AWSSSOMasterAccountAdministrator`——允许 IAM Identity Center 将命名为 `AWSServiceRoleforSSO` 的服务角色传递给 IAM Identity Center，以便稍后可以代入该角色并代表他们执行操作。当个人或应用程序尝试启用 IAM Identity Center 时，这是必要的。有关更多信息，请参阅 配置对的访问权限 Amazon Web Services 账户。
- `AWSSSOMemberAccountAdministrator`— 允许 IAM Identity Center 在多账户 Amazon 环境中执行账户管理员操作。有关更多信息，请参阅 Amazon 托管策略：AWSSSOMemberAccountAdministrator。
- `AWSSSOManageDelegatedAdministrator`——允许 IAM Identity Center 为您的组织注册和取消注册委派管理员。
- `AllowKMSKeyUseViaService`和 `AllowKMSKeyDiscovery` — 允许对 IAM 身份中心实例使用的客户托管密钥进行 Amazon Key Management Service 操作。

要查看此策略的权限，请参阅Amazon 托管策略参考AWSSSOMasterAccountAdministrator中的。

有关此策略的其他信息

首次启用 IAM Identity Center 时，IAM Identity Center 服务会在 Amazon Organizations 管理账户（以前称为主账户）中创建一个服务关联角色，这样 IAM Identity Center 就可以管理您账户中的资源。所需的操作包括 `iam:CreateServiceLinkedRole` 和 `iam:PassRole`。

Amazon 托管策略： AWSSSOMemberAccountAdministrator

`AWSSSOMemberAccountAdministrator` 策略向主体提供所需的管理操作。该策略适用于执行 IAM Identity Center 管理员工作角色的主体。随着时间的推移，所提供的操作列表将会更新，以匹配 IAM Identity Center 的现有功能以及管理员所需的操作。

您可以将 `AWSSSOMemberAccountAdministrator` 策略附加到 IAM 身份。
将`AWSSSOMemberAccountAdministrator`策略附加到身份时，即授予管理 Amazon IAM Identity Center 权限。拥有此政策的委托人可以在 Amazon Organizations 管理账户和所有成员账户中访问

IAM Identity Center。该主体可以完全管理所有 IAM Identity Center 操作，包括创建用户、权限集和分配的能力。委托人还可以在整个 Amazon 组织成员账户中实例化这些分配，并在 Amazon Directory Service 托管目录和 IAM Identity Center 之间建立连接。随着新管理功能的发布，帐户管理员自动获得这些权限。

该策略还包括使用客户托管密钥进行加密的 IAM Identity Center 实例所需的 Amazon Key Management Service 权限。

要查看此策略的权限，请参阅Amazon 托管策略参考AWSSSOMemberAccountAdministrator中的。

有关此策略的其他信息

IAM Identity Center 管理员管理其 Identity Center 目录存储（sso 目录）中的用户、组和密码。帐户管理员角色包括以下操作的权限：

- `"sso:*"`
- `"sso-directory:*"`

IAM Identity Center 管理员需要对以下 Amazon Directory Service 操作的有限权限才能执行日常任务。

- `"ds:DescribeTrusts"`
- `"ds:UnauthorizeApplication"`
- `"ds:DescribeDirectories"`
- `"ds:AuthorizeApplication"`
- `“ds:CreateAlias”`

这些权限允许 IAM Identity Center 管理员识别现有目录并管理应用程序，以便可以将它们配置为与 IAM Identity Center 一起使用。有关每个操作的更多信息，请参阅 Amazon Directory Service API 权限：操作、资源和条件参考。

IAM Identity Center 使用 IAM 策略向 IAM Identity Center 用户授予权限。IAM Identity Center 管理员创建权限集并向其附加策略。IAM Identity Center 管理员必须有权列出现有策略，以便他们可以选择将哪些策略与他们正在创建或更新的权限集一起使用。要设置安全和功能权限，IAM Identity Center 管理员必须有权运行 IAM Access Analyzer 策略验证。

- `"iam:ListPolicies"`
- `"access-analyzer:ValidatePolicy"`

IAM Identity Center 管理员需要有限访问以下 Amazon Organizations 操作才能执行日常任务：

- `"organizations:EnableAWSServiceAccess"`
- `"organizations:ListRoots"`
- `"organizations:ListAccounts"`
- `"organizations:ListOrganizationalUnitsForParent"`
- `"organizations:ListAccountsForParent"`
- `"organizations:DescribeOrganization"`
- `"organizations:ListChildren"`
- `"organizations:DescribeAccount"`
- `"organizations:ListParents"`
- `"organizations:ListDelegatedAdministrators"`
- `"organizations:RegisterDelegatedAdministrator"`
- `"organizations:DeregisterDelegatedAdministrator"`

这些权限使 IAM Identity Center 管理员能够使用组织资源（帐户）来执行基本 IAM Identity Center 管理任务，如下所示：

- 识别属于组织的管理帐户
- 识别属于组织的成员帐户
- 为账户启用 Amazon 服务访问权限
- 设置和管理委派管理员

有关通过 IAM Identity Center 使用委派管理员的更多信息，请参阅 委派管理。有关如何将这些权限用于的更多信息 Amazon Organizations，请参阅与其他 Amazon 服务 Amazon Organizations 一起使用。

Amazon 托管策略： AWSSSODirectoryAdministrator

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

此策略授予对 IAM Identity Center 用户和组的管理权限。附加此策略的主体可以对 IAM Identity Center 用户和组进行任何更新。该策略还包括使用客户托管密钥进行加密的 IAM Identity Center 实例所需的 Amazon Key Management Service 权限。

该策略包含以下权限：

- IAM Identity Center 目录 - 对 IAM Identity Center 目录操作的完全管理访问权限。
- 身份存储 - 对身份存储操作和身份验证的完全管理访问权限。
- IAM Identity Center - 列出目录关联的权限。
- Amazon Key Management Service - 对 IAM Identity Center 实例使用的客户自主管理型密钥执行解密、描述密钥和生成数据密钥的权限。

要查看此策略的权限，请参阅Amazon 托管策略参考AWSSSODirectoryAdministrator中的。

Amazon 托管策略： AWSSSOReadOnly

您可以将 `AWSSSOReadOnly` 策略附加到 IAM 身份。

此策略授予只读权限，允许用户查看 IAM Identity Center 中的信息。附加此策略的主体无法直接查看 IAM Identity Center 用户或组。附加此策略的主体无法在 IAM Identity Center 中进行任何更新。例如，具有这些权限的主体可以查看 IAM Identity Center 设置，但无法更改任何设置值。

该策略还包括使用客户托管密钥进行加密的 IAM Identity Center 实例所需的 Amazon Key Management Service 权限。

要查看此策略的权限，请参阅Amazon 托管策略参考AWSSSOReadOnly中的。

Amazon 托管策略： AWSSSODirectoryReadOnly

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

此策略授予只读权限，允许用户查看 IAM Identity Center 中的用户和组。附加此策略的主体无法查看 IAM Identity Center 分配、权限集、应用程序或设置。附加此策略的主体无法在 IAM Identity Center 中进行任何更新。例如，具有这些权限的主体可以查看 IAM Identity Center 用户，但他们无法更改任何用户属性或分配 MFA 设备。

该策略还包括使用客户托管密钥进行加密的 IAM Identity Center 实例所需的 Amazon Key Management Service 权限。

要查看此策略的权限，请参阅Amazon 托管策略参考AWSSSODirectoryReadOnly中的。

Amazon 托管策略： AWSIdentitySyncFullAccess

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

附加此策略的主体拥有完全访问权限，可以创建和删除同步配置文件、将同步配置文件与同步目标关联或更新、创建、列出和删除同步筛选条件以及启动或停止同步。

权限详细信息

要查看此策略的权限，请参阅Amazon 托管策略参考AWSIdentitySyncFullAccess中的。

Amazon 托管策略： AWSIdentitySyncReadOnlyAccess

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

此策略授予只读权限，允许用户查看有关身份同步配置文件、筛选条件和目标设置的信息。附加此策略的主体无法对同步设置进行任何更新。例如，具有这些权限的主体可以查看身份同步设置，但无法更改任何配置文件或筛选条件值。

要查看此策略的权限，请参阅Amazon 托管策略参考AWSIdentitySyncReadOnlyAccess中的。

Amazon 托管策略： AWSSSOServiceRolePolicy

您不可以将 `AWSSSOServiceRolePolicy` 策略附加到 IAM 身份。

此策略附加到服务相关角色，允许 IAM Identity Center 委派和强制执行哪些用户具有单点登录访问权限的特定 Amazon Web Services 账户 用户。 Amazon Organizations启用 IAM 后，将在组织 Amazon Web Services 账户 内的所有区域中创建一个与服务相关的角色。IAM Identity Center 还会在随后添加到您的组织的每个帐户中创建相同的服务相关角色。此角色允许 IAM Identity Center 代表您访问每个账户的资源。 Service-linked 在每个角色中创建的角色 Amazon Web Services 账户 都被命名`AWSServiceRoleForSSO`。有关更多信息，请参阅 使用 IAM Identity Center 的服务相关角色。

Amazon 托管策略： AWSIAMIdentityCenterAllowListForIdentityContext

在 IAM Identity Center 身份上下文中担任角色时， Amazon Security Token Service (Amazon STS) 会自动将`AWSIAMIdentityCenterAllowListForIdentityContext`策略附加到该角色。

此策略提供了当您对在 IAM Identity Center 身份上下文中担任的角色使用可信身份传播时，所允许的操作列表。在此上下文中调用的所有其他操作都将被阻止。身份上下文作为 `ProvidedContext` 传递。

要查看此策略的权限，请参阅Amazon 托管策略参考AWSIAMIdentityCenterAllowListForIdentityContext中的。

Amazon 托管策略： AWSIdentityCenterExternalManagementPolicy

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

此策略提供从外部提供商管理 IAM 身份中心用户的权限。

要查看此策略的权限，请参阅Amazon 托管策略参考AWSIdentityCenterExternalManagementPolicy中的。

IAM 身份中心更新至 Amazon 托管策略

下表描述了自该服务开始跟踪这些更改以来对 IAM Identity Center Amazon 托管策略的更新。有关此页面更改的自动提示，请订阅 IAM Identity Center 文档历史记录页面上的 RSS 源。

更改	描述	日期
AWSIdentityCenterExternalManagementPolicy	更新了托管策略以更改置备租户的 ARN。	2025 年 12 月 5 日
AWSIdentityCenterExternalManagementPolicy	此策略提供从外部提供商管理 IAM 身份中心用户的权限。	2025 年 11 月 21 日
AWSSSOMasterAccountAdministrator, AWSSSOMemberAccountAdministrator, AWSSSOReadOnly, AWSSSODirectoryAdministrator, AWSSSODirectoryReadOnly	更新了托管策略，增加了使用客户托管密钥进行加密的 IAM Identity Center 实例所需的 Amazon KMS 权限。	2025 年 9 月 17 日
AWSSSOServiceRolePolicy	此策略现在包含调用 `identity-sync:DeleteSyncProfile` 的新权限。	2025 年 2 月 11 日
AWSIAMIdentityCenterAllowListForIdentityContext	此策略现在包括`qapps:ListQAppSessionData` 和`qapps:ExportQAppSessionData` 操作，用于支持身份增强控制台会话的 Amazon 托管应用程序的身份增强控制台会话。	2024 年 10 月 2 日

更改	描述	日期
AWSSSOMasterAccountAdministrator	IAM Identity Center 添加了一项新操作来授予 DeleteSyncProfile 权限，允许您使用此策略删除同步配置文件。这是与 DeleteInstance API 关联的操作。	2024 年 9 月 26 日
AWSIAMIdentityCenterAllowListForIdentityContext	此策略现在包括支持身份增强控制台会话的 Amazon 托管应用程序的身份增强控制台会话的`s3:ListCallerAccessGrants` 操作。	2024 年 9 月 4 日
AWSIAMIdentityCenterAllowListForIdentityContext	此策略现在包括支持身份增强控制台会话的`aoss:APIAccessAll` `es:ESHttpHead` `es:ESHttpPost` `es:ESHttpGet` 、`es:ESHttpPatch` 、`es:ESHttpDelete` 、、和`es:ESHttpPut` 操作，用于支持这些会话的 Amazon 托管应用程序的身份增强控制台会话。	2024 年 7 月 12 日

更改	描述	日期
AWSIAMIdentityCenterAllowListForIdentityContext	此策略现在包括qapps:PredictQApp 、、、qapps:ImportDocument 、、qapps:AssociateLibraryItemReview 、qapps:DisassociateLibraryItemReview qapps:GetQAppSession qapps:UpdateQAppSession qapps:GetQAppSessionMetadata qapps:UpdateQAppSessionMetadata 、和qapps:TagResource 操作，用于支持身份增强控制台会话的 Amazon 托管应用程序的身份增强控制台会话。	2024 年 6 月 27 日
AWSIAMIdentityCenterAllowListForIdentityContext	为支持 Amazon EMR 中的可信身份传播，此策略现在包括 elasticmapreduce:AddJobFlowSteps 、elasticmapreduce:DescribeCluster 、elasticmapreduce:CancelSteps 、elasticmapreduce:DescribeStep 和 elasticmapreduce:ListSteps 操作。	2024 年 5 月 17 日

更改	描述	日期
AWSIAMIdentityCenterAllowListForIdentityContext	此策略现在包括qapps:CreateQApp 、、、、、、qapps:PredictProblemStatementFromConversation 、qapps:PredictQAppFromProblemStatement 、、qapps:CopyQApp 、、qapps:GetQApp 、qapps:ListQApps 、、qapps:UpdateQApp 、qapps:DeleteQApp 、、qapps:AssociateQAppWithUser 、、qapps:DisassociateQAppFromUser 、qapps:ImportDocumentToQApp 、、qapps:ImportDocumentToQAppSession 、qapps:CreateLibraryItem 、、qapps:GetLibraryItem 、qapps:UpdateLibraryItem 、、qapps:CreateLibraryItemReview 、、qapps:ListLibraryItems 、qapps:CreateSubscriptionToken 、、qapps:StartQAppSession 、、、、、、、、以	2024 年 4 月 30 日

更改	描述	日期
	及qapps:StopQAppSession 支持这些会话的 Amazon 托管应用程序的身份增强控制台会话。	
AWSSSOMasterAccountAdministrator	此策略现在包括signin:CreateTrustedIdentityPropagationApplicationForConsole 和signin:ListTrustedIdentityPropagationApplicationsForConsole 操作，用于支持身份增强控制台会话的 Amazon 托管应用程序的身份增强控制台会话。	2024 年 4 月 26 日
AWSSSOMemberAccountAdministrator	此策略现在包括signin:CreateTrustedIdentityPropagationApplicationForConsole 和signin:ListTrustedIdentityPropagationApplicationsForConsole 操作，用于支持身份增强控制台会话的 Amazon 托管应用程序的身份增强控制台会话。	2024 年 4 月 26 日

更改	描述	日期
AWSSSOReadOnly	此策略现在包括支持身份增强控制台会话的 Amazon 托管应用程序的身份增强控制台会话的signin:ListTrustedIdentityPropagationApplicationsForConsole 操作。	2024 年 4 月 26 日
AWSIAMIdentityCenterAllowListForIdentityContext	此策略现在包括支持身份增强控制台会话的 Amazon 托管应用程序的身份增强控制台会话的qbusiness:PutFeedback 操作。	2024 年 4 月 26 日
AWSIAMIdentityCenterAllowListForIdentityContext	此策略现在包括q:StartConversation 、、、q:SendMessage 、、q:ListConversations q:GetConversation q:StartTroubleshootingAnalysis q:GetTroubleshootingResults q:StartTroubleshootingResolutionExplanation 、和 q:UpdateTroubleshootingCommandResult 操作，用于支持身份增强控制台会话的 Amazon 托管应用程序的身份增强控制台会话。	2024 年 4 月 24 日

更改	描述	日期
AWSIAMIdentityCenterAllowListForIdentityContext	此策略现在包括支持身份增强控制台会话的 Amazon 托管应用程序的身份增强控制台会话的`sts:SetContext` 操作。	2024 年 4 月 19 日
AWSIAMIdentityCenterAllowListForIdentityContext	此策略现在包括`qbusiness:Chat` 、、`qbusiness:ChatSync` `qbusiness:ListConversations` `qbusiness:ListMessages` 、和`qbusiness:DeleteConversation` 操作，用于支持身份增强控制台会话的 Amazon 托管应用程序的身份增强控制台会话。	2024 年 4 月 11 日
AWSIAMIdentityCenterAllowListForIdentityContext	此策略现在包括 `s3:GetAccessGrantsInstanceForPrefix` 和 `s3:GetDataAccess` 操作。	2023 年 11 月 26 日
AWSIAMIdentityCenterAllowListForIdentityContext	此策略提供了当您对在 IAM Identity Center 身份上下文中担任的角色使用可信身份传播时，所允许的操作列表。	2023 年 11 月 15 日
AWSSSODirectoryReadOnly	此策略现在包括具有新权限的新命名空间 `identitystore-auth` ，以允许用户列出和获取会话。	2023 年 2 月 21 日
AWSSSOServiceRolePolicy	此策略现在允许对管理帐户执行 `UpdateSAMLProvider` 操作。	2022 年 10 月 20 日

更改	描述	日期
AWSSSOMasterAccountAdministrator	此策略现在包括具有新权限的新命名空间 identitystore-auth ，以允许管理员列出和删除用户的会话。	2022 年 10 月 20 日
AWSSSOMemberAccountAdministrator	此策略现在包括具有新权限的新命名空间 identitystore-auth ，以允许管理员列出和删除用户的会话。	2022 年 10 月 20 日
AWSSSODirectoryAdministrator	此策略现在包括具有新权限的新命名空间 identitystore-auth ，以允许管理员列出和删除用户的会话。	2022 年 10 月 20 日
AWSSSOMasterAccountAdministrator	此策略现在包括新的呼ListDelegatedAdministrators 入权限 Amazon Organizations。此策略现在还包括权限 AWSSSOManageDelegatedAdministrator 子集，其中包括调用 RegisterDelegatedAdministrator 和 DeregisterDelegatedAdministrator 的权限。	2022 年 8 月 16 日

更改	描述	日期
AWSSSOMemberAccountAdministrator	此策略现在包括新的呼ListDelegatedAdministrators入权限 Amazon Organizations。此策略现在还包括权限 AWSSSOManageDelegatedAdministrator 子集，其中包括调用 RegisterDelegatedAdministrator 和 DeregisterDelegatedAdministrator 的权限。	2022 年 8 月 16 日
AWSSSOReadOnly	此策略现在包括新的呼ListDelegatedAdministrators入权限 Amazon Organizations。	2022 年 8 月 11 日
AWSSSOServiceRolePolicy	此策略现在包括调用 DeleteRolePermissionsBoundary 和 PutRolePermisionsBoundary 的新权限。	2022 年 7 月 14 日
AWSSSOServiceRolePolicy	此策略现在包含允许调用 Amazon Organizations中的 ListAWSServiceAccessForOrganization and ListDelegatedAdministrators 的新权限。	2022 年 5 月 11 日

更改	描述	日期
AWSSSOMasterAccountAdministrator AWSSSOMemberAccountAdministrator AWSSSOReadOnly	添加 IAM Access Analyzer 权限，允许主体使用策略检查进行验证。	2022 年 4 月 28 日
AWSSSOMasterAccountAdministrator	此策略现在允许所有 IAM Identity Center 身份存储服务操作。 有关 IAM Identity Center 身份存储服务中可用操作的信息，请参阅 IAM Identity Center 身份存储 API 参考。	2022 年 3 月 29 日
AWSSSOMemberAccountAdministrator	此策略现在允许所有 IAM Identity Center 身份存储服务操作。	2022 年 3 月 29 日
AWSSSODirectoryAdministrator	此策略现在允许所有 IAM Identity Center 身份存储服务操作。	2022 年 3 月 29 日
AWSSSODirectoryReadOnly	此策略现在授予对 IAM Identity Center 身份存储服务读取操作的访问权限。需要此访问权限才能从 IAM Identity Center 身份存储服务检索用户和组信息。	2022 年 3 月 29 日
AWSIdentitySyncFullAccess	此策略允许完全访问身份同步权限。	2022 年 3 月 3 日
AWSIdentitySyncReadOnlyAccess	此策略授予只读权限，允许主体查看身份同步设置。	2022 年 3 月 3 日

更改	描述	日期
AWSSSOReadOnly	此策略授予只读权限，允许主体查看 IAM Identity Center 配置设置。	2021 年 8 月 4 日
IAM Identity Center 开始跟踪更改	IAM 身份中心开始跟踪 Amazon 托管策略的更改。	2021 年 8 月 4 日

使用 IAM Identity Center 的服务相关角色

Amazon IAM Identity Center 使用 Amazon 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，直接链接到 IAM Identity Center。它由 IAM Identity Center 预定义，包括该服务代表您调用其他 Amazon 服务所需的所有权限。有关更多信息，请参阅 了解 IAM Identity Center 中的服务相关角色。

服务相关角色使设置 IAM Identity Center 变得更加容易，因为您无需手动添加必要的权限。IAM Identity Center 定义其服务相关角色的权限，除非另有定义，否则只有 IAM Identity Center 可以承担其角色。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他 IAM 实体。

有关支持服务相关角色的其它服务的信息，请参阅使用 IAM 的Amazon 服务并查找Service-Linked 角色列中显示为是的服务。请选择是与查看该服务的服务关联角色文档的链接。

Service-linked IAM 身份中心的角色权限

IAM Identity Center 使用名AWSServiceRoleForSSO为的服务相关角色授予 IAM 身份中心代表您管理 Amazon 资源的权限，包括 IAM 角色、策略和 SAML IdP。

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

- IAM Identity Center（服务前缀：`sso`）

AWSSSOServiceRolePolicy 服务相关角色权限策略允许 IAM Identity Center 对路径 “/aws-reserved/sso .amazonaws.com/” 上且名称前缀为 “awsReservedso_” 的角色完成以下操作：

- `iam:AttachRolePolicy`
- `iam:CreateRole`
- `iam:DeleteRole`

- iam:DeleteRolePermissionsBoundary
- iam:DeleteRolePolicy
- iam:DetachRolePolicy
- iam:GetRole
- iam:ListRolePolicies
- iam:PutRolePolicy
- iam:PutRolePermissionsBoundary
- iam:ListAttachedRolePolicies

AWSSSOServiceRolePolicy 服务相关角色权限策略允许 IAM Identity Center 在名称前缀为“AWSSSO_” 的 SAML 提供商上完成以下操作：

- iam:CreateSAMLProvider
- iam:GetSAMLProvider
- iam:UpdateSAMLProvider
- iam:DeleteSAMLProvider

AWSSSOServiceRolePolicy 服务相关角色权限策略允许 IAM Identity Center 在所有组织上完成以下操作：

- organizations:DescribeAccount
- organizations:DescribeOrganization
- organizations:ListAccounts
- organizations:ListAWSServiceAccessForOrganization
- organizations:ListDelegatedAdministrators

AWSSSOServiceRolePolicy 服务相关角色权限策略允许 IAM Identity Center 在所有 IAM 角色 (*) 上完成以下操作：

- iam:listRoles

AWSSSOServiceRolePolicy 服务相关角色权限策略允许 IAM Identity Center 在 “arn: aws:: iam:: *:-service-.amazonaws 上完成以下操作。role/aws role/sso com/AWSServiceRoleForSSO”:

- `iam:GetServiceLinkedRoleDeletionStatus`
- `iam:DeleteServiceLinkedRole`

AWSSSOServiceRolePolicy 服务相关角色权限策略允许 IAM Identity Center 在 “arn: aws: identity-sync: *: profile/*” 上完成以下操作：

- `identity-sync:DeleteSyncProfile`

有关 AWSSSOServiceRolePolicy 服务相关角色权限策略更新的更多信息，请参阅IAM 身份中心更新至 Amazon 托管策略。

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"IAMRoleProvisioningActions",
         "Effect":"Allow",
         "Action":[
            "iam:AttachRolePolicy",
            "iam:CreateRole",
            "iam:DeleteRolePermissionsBoundary",
            "iam:PutRolePermissionsBoundary",
            "iam:PutRolePolicy",
            "iam:UpdateRole",
            "iam:UpdateRoleDescription",
            "iam:UpdateAssumeRolePolicy"
         ],
         "Resource":[
            "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
         ],
         "Condition":{
            "StringNotEquals":{
               "aws:PrincipalOrgMasterAccountId":"${aws:PrincipalAccount}"
            }
         }
      },
      {
         "Sid":"IAMRoleReadActions",
```

```
         "Effect":"Allow",
         "Action":[
            "iam:GetRole",
            "iam:ListRoles"
         ],
         "Resource":[
            "*"
         ]
      },
      {
         "Sid":"IAMRoleCleanupActions",
         "Effect":"Allow",
         "Action":[
            "iam:DeleteRole",
            "iam:DeleteRolePolicy",
            "iam:DetachRolePolicy",
            "iam:ListRolePolicies",
            "iam:ListAttachedRolePolicies"
         ],
         "Resource":[
            "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
         ]
      },
      {
         "Sid":"IAMSLRCleanupActions",
         "Effect":"Allow",
         "Action":[
            "iam:DeleteServiceLinkedRole",
            "iam:GetServiceLinkedRoleDeletionStatus",
            "iam:DeleteRole",
            "iam:GetRole"
         ],
         "Resource":[
            "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO"
         ]
      },
      {
        "Sid": "IAMSAMLProviderCreationAction",
        "Effect": "Allow",
        "Action": [
          "iam:CreateSAMLProvider"
      ],
      "Resource": [
```

```
            "arn:aws:iam::*:saml-provider/AWSSSO_*"
         ],
        "Condition": {
            "StringNotEquals": {
               "aws:PrincipalOrgMasterAccountId": "${aws:PrincipalAccount}"
             }
          }
        },
        {
          "Sid": "IAMSAMLProviderUpdateAction",
          "Effect": "Allow",
          "Action": [
            "iam:UpdateSAMLProvider"
          ],
          "Resource": [
             "arn:aws:iam::*:saml-provider/AWSSSO_*"
          ]
        },
        {
           "Sid":"IAMSAMLProviderCleanupActions",
           "Effect":"Allow",
           "Action":[
              "iam:DeleteSAMLProvider",
              "iam:GetSAMLProvider"
           ],
           "Resource":[
              "arn:aws:iam::*:saml-provider/AWSSSO_*"
           ]
        },
        {
           "Effect":"Allow",
           "Action":[
              "organizations:DescribeAccount",
              "organizations:DescribeOrganization",
              "organizations:ListAccounts",
              "organizations:ListAWSServiceAccessForOrganization",
              "organizations:ListDelegatedAdministrators"
           ],
           "Resource":[
              "*"
           ]
        },
        {
           "Sid":"AllowUnauthAppForDirectory",
```

```
            "Effect":"Allow",
            "Action":[
               "ds:UnauthorizeApplication"
            ],
            "Resource":[
               "*"
            ]
         },
         {
            "Sid":"AllowDescribeForDirectory",
            "Effect":"Allow",
            "Action":[
               "ds:DescribeDirectories",
               "ds:DescribeTrusts"
            ],
            "Resource":[
               "*"
            ]
         },
         {
            "Sid":"AllowDescribeAndListOperationsOnIdentitySource",
            "Effect":"Allow",
            "Action":[
               "identitystore:DescribeUser",
               "identitystore:DescribeGroup",
               "identitystore:ListGroups",
               "identitystore:ListUsers"
            ],
            "Resource":[
               "*"
            ]
         },
         {
            "Sid":"AllowDeleteSyncProfile",
            "Effect":"Allow",
            "Action":[
               "identity-sync:DeleteSyncProfile"
            ],
            "Resource":[
               "arn:aws:identity-sync:*:*:profile/*"
            ]
         }
      ]
```

```
}
```

您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务关联角色。有关更多信息，请参阅 IAM 用户指南中的Service-linked 角色权限。

为 IAM Identity Center 创建服务相关角色

无需手动创建服务相关角色。启用后，IAM Identity Center 将在 Organizations 中组织内的所有账户中 Amazon 创建一个服务相关角色。IAM Identity Center 还会在随后添加到您的组织的每个帐户中创建相同的服务相关角色。此角色允许 IAM Identity Center 代表您访问每个帐户的资源。

> **注意**
>
> - 如果您登录了 Amazon Organizations 管理账户，则该账户将使用您当前登录的角色而不是与服务相关的角色。这可以防止权限升级。
> - 当 IAM Identity Center 在 Amazon Organizations 管理账户中执行任何 IAM 操作时，所有操作都将使用 IAM 委托人的证书进行。这样，登录 CloudTrail 即可查看谁在管理账户中进行了所有权限更改。

> **Important**
>
> 如果您在 2017 年 12 月 7 日开始支持服务相关角色之前使用 IAM 身份中心服务，那么 IAM Identity Center 会在您的账户中创建该 AWSServiceRoleForSSO 角色。要了解更多信息，请参阅我的 IAM 帐户中出现新角色。

如果您删除了此服务相关角色然后需要再次创建它，可以使用相同的流程在您的帐户中重新创建此角色。

编辑 IAM Identity Center 的服务相关角色

IAM 身份中心不允许您编辑 AWSServiceRoleForSSO 服务相关角色。创建服务关联角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是可以使用 IAM 编辑角色描述。有关更多信息，请参阅《IAM 用户指南》中的编辑服务关联角色。

删除 IAM Identity Center 的服务相关角色

您无需手动删除该 AWSServiceRoleForSSO 角色。从 Amazon 组织中移除后，IAM I Amazon Web Services 账户 dentity Center 会自动清理资源并从中删除服务相关角色。 Amazon Web Services 账户

您还可以使用 IAM 控制台、IAM CLI 或 IAM API 手动删除服务相关角色。为此，必须先手动清除服务相关角色的资源，然后才能手动删除。

> **Note**
>
> 如果在您尝试删除资源时 IAM Identity Center 服务正在使用该角色，则删除可能会失败。如果发生这种情况，请等待几分钟后重试。

删除使用的 IAM 身份中心资源 AWSServiceRoleForSSO

1. 移除用户和群组对的访问权限 Amazon Web Services 账户 适用于有权访问 Amazon Web Services 账户的所有用户和组。
2. 与 Amazon Web Services 账户关联的 在 IAM Identity Center 中移除权限集。

使用 IAM 手动删除服务关联角色

使用 IAM 控制台、IAM CLI 或 IAM API 删除 AWSServiceRoleForSSO 服务相关角色。有关更多信息，请参阅 IAM 用户指南中的删除 Service-Linked 角色。

IAM Identity Center 控制台和 API 授权

现有的 IAM Identity Center 控制台 API 支持双重授权，因此当较新的 API 可用时，您仍可以继续使用现有的 API 操作。如果您现有的 IAM Identity Center 实例是在 2023 年 11 月 15 日和 2020 年 10 月 15 日之前创建的，您可以使用下表确定现在哪些 API 操作可以映射到这些日期之后发布的较新 API 操作。

主题

- 2023 年 11 月之后的 API 操作
- 2020 年 10 月之后的 API 操作

2023 年 11 月之后的 API 操作

只要没有明确拒绝任何操作，2023 年 11 月 15 日之前创建的 IAM Identity Center 实例就会同时支持新旧 API 操作。2023 年 11 月 15 日之后创建的实例使用较新的 API 操作在 IAM Identity Center 控制台中进行授权。

2023 年 11 月 15 日之前使用的控制台操作名称	2023 年 11 月 15 日之后使用的 API 操作
AssociateProfile	CreateApplicationAssignment
CreateManagedApplicationInstance | CreateApplicationInstance	CreateApplication
CreateManagedApplicationInstance	PutApplicationAuthenticationMethod
DeleteApplicationInstance | DeleteManagedApplicationInstance	DeleteApplication
DeleteSSO	DeleteInstance
DisassociateProfile	DeleteApplicationAssignment
GetApplicationTemplate	DescribeApplicationProvider
GetManagedApplicationInstance	DescribeApplication
GetSharedSsoConfiguration	DescribeInstance
ListApplicationInstances	ListApplications
ListApplicationTemplates	ListApplicationProviders
ListDirectoryAssociations	DescribeInstance
ListProfileAssociations	ListApplicationAssignments
UpdateApplicationInstanceDisplayData | UpdateApplicationInstanceStatus | UpdateManagedApplicationInstanceStatus	UpdateApplication

2020 年 10 月之后的 API 操作

只要没有明确拒绝任何操作，2020 年 10 月 15 日之前创建的 IAM Identity Center 实例就会同时支持新旧 API 操作。2020 年 10 月 15 日之后创建的实例使用较新的 API 操作在 IAM Identity Center 控制台中进行授权。

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
AssociateProfile	AssociateProfile	CreateAccountAssignment
AttachManagedPolicy	PutPermissionsPolicy	AttachManagedPolicyToPermissionSet
CreatePermissionSet	CreatePermissionSet	CreatePermissionSet
DeleteApplicationInstanceForAWsAccount	DeleteApplicationInstance | DeleteTrust	DeleteAccountAssignment
DeleteApplicationProfileForAwsAccount	DeleteProfile	DeleteAccountAssignment
DeletePermissionsPolicy	DeletePermissionsPolicy	DeleteInlinePolicyFromPermissionSet
DeletePermissionSet	DeletePermissionSet	DeletePermissionSet
DescribePermissionsPolicies	DescribePermissionsPolicies	ListManagedPoliciesInPermissionSet
DetachManagedPolicy	DeletePermissionsPolicy	DetachManagedPolicyFromPermissionSet
DisassociateProfile	DisassociateProfile	DeleteAccountAssignment
GetApplicationInstanceForAWSAccount	GetApplicationInstance	ListAccountAssignments
GetAWSAccountProfileStatus	GetProfile	ListPermissionSetsProvisionedToAccount

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
GetPermissionSet	GetPermissionSet	DescribePermissionSet
GetPermissionsPolicy	GetPermissionsPolicy	GetInlinePolicyForPermissionSet
ListAccountsWithProvisionedPermissionSet	ListApplicationInstances | GetApplicationInstance	ListAccountsForProvisionedPermissionSet
ListAWSAccountProfiles	ListProfiles | GetProfile	ListPermissionSetsProvisionedToAccount
ListPermissionSets	ListPermissionSets	ListPermissionSets
ListProfileAssociations	ListProfileAssociations	ListAccountAssignments
ProvisionApplicationInstanceForAWSAccount	GetApplicationInstance | CreateApplicationInstance	CreateAccountAssignment
ProvisionApplicationProfileForAWSAccountInstance	GetProfile | CreateProfile | UpdateProfile	CreateAccountAssignment
ProvisionSAMLProvider	GetTrust | CreateTrust | UpdateTrust	CreateAccountAssignment
PutPermissionsPolicy	PutPermissionsPolicy	PutInlinePolicyToPermissionSet
UpdatePermissionSet	UpdatePermissionSet	UpdatePermissionSet

Amazon STS IAM 身份中心的条件上下文密钥

当委托人向其提出请求时 Amazon，会将请求信息 Amazon 收集到请求上下文中，该上下文用于评估和批准请求。您可以使用 JSON 策略的 `Condition` 元素将请求上下文中的键与您在策略中指定的键值进行比较。请求信息由不同的来源提供，包括提出请求的委托人、资源、请求所针对的以及请求本身的元数据。 Service-specific 条件键定义为与单个 Amazon 服务一起使用。

IAM Identity Center 包含一个 Amazon STS 上下文提供商，允许 Amazon 托管应用程序和第三方应用程序为 IAM Identity Center 定义的条件键添加值。这些键包含在 IAM 角色中。密钥值是在应用程序向传递令牌时设置的 Amazon STS。应用程序通过以下任一方式获取传递给 Amazon STS 它的令牌：

- 使用 IAM Identity Center 进行身份验证的过程中。
- 在与可信令牌发布者交换令牌进行可信身份传播之后。在这种情况下，应用程序会从可信令牌发布者中获取令牌，然后将该令牌交换为 IAM Identity Center 中的令牌。

这些键通常由与可信身份传播集成的应用程序使用。在某些情况下，如果存在键值，则可以使用您创建的 IAM 策略中的这些键来允许或拒绝权限。

例如，您可能想要根据 `UserId` 的值提供对资源的条件访问。此值表示哪个 IAM Identity Center 用户正在使用角色。示例类似于使用 `SourceId`。但是，与 `SourceId` 不同的是，`UserId` 的值表示身份存储中经过验证的特定用户。此值存在于应用程序获取并传递给 Amazon STS的令牌中。并非可以包含任意值的通用字符串。

主题

- identitystore：UserId
- identitystore：IdentityStoreArn
- 身份中心：ApplicationArn
- 身份中心：CredentialId
- 身份中心：InstanceArn

identitystore：UserId

此上下文键是 IAM Identity Center 用户的 `UserId`，该用户是 IAM Identity Center 发布的上下文断言的主体。上下文断言传递给。 Amazon STS您可以使用此键将发出请求所代表的 IAM Identity Center 用户的 `UserId` 与您在策略中指定的用户标识符进行比较。

- 可用性 — 在设置由 IAM Identity Center 发出的上下文断言之后，当使用 Amazon CLI 或 Amazon STS `AssumeRole` API 操作中的任何 Amazon STS `assume-role`命令代入角色时，此密钥将包含在请求上下文中。
- 数据类型-字符串
- 值类型 — Single-valued

identitystore：IdentityStoreArn

此上下文键是附加到发布上下文断言的 IAM Identity Center 实例的身份存储的 ARN，也是可供您在其中查找 `identitystore:UserID` 的属性的身份存储。您可以在策略中使用此键确定 `identitystore:UserID` 是否来自预期的身份存储 ARN。

- 可用性 — 在设置由 IAM Identity Center 发出的上下文断言之后，当使用 Amazon CLI 或 Amazon STS `AssumeRole` API 操作中的任何 Amazon STS `assume-role`命令代入角色时，此密钥将包含在请求上下文中。
- 数据类型 – Arn、字符串
- 值类型 — Single-valued

身份中心：ApplicationArn

此上下文键是 IAM Identity Center 向其发布上下文断言的应用程序的 ARN。您可以在策略中使用此键确定 `identitycenter:ApplicationArn` 是否来自预期的应用程序。使用此键有助于防止意外应用程序访问 IAM 角色。

- 可用性-此密钥包含在 Amazon STS `AssumeRole` API 操作的请求上下文中。该请求上下文包含 IAM Identity Center 发布的上下文断言。
- 数据类型 – Arn、字符串
- 值类型 — Single-valued

身份中心：CredentialId

此上下文键是身份增强型角色凭证的随机 ID，仅用于记录。由于此键值不可预测，建议不要将其用于策略中的上下文断言。

- 可用性-此密钥包含在 Amazon STS `AssumeRole` API 操作的请求上下文中。该请求上下文包含 IAM Identity Center 发布的上下文断言。
- 数据类型-字符串
- 值类型 — Single-valued

身份中心：InstanceArn

此上下文键是为 `identitystore:UserID` 发布上下文断言的 IAM Identity Center 实例的 ARN。您可以使用此键确定 `identitystore:UserID` 和上下文断言是否来自预期的 IAM Identity Center 实例的 ARN。

- 可用性-此密钥包含在 Amazon STS `AssumeRole` API 操作的请求上下文中。该请求上下文包含 IAM Identity Center 发布的上下文断言。
- 数据类型 – Arn、字符串
- 值类型 — Single-valued

IAM Identity Center 中的日志记录和监控

最佳实践是对组织进行监控，确保对所做的更改进行记录。监控可帮助您调查任何意外变更，并回滚不需要的变更。IAM Identity Center 目前支持两项 Amazon 服务，可帮助您监控您的组织及其内部发生的活动： Amazon CloudTrail 和 Amazon EventBridge。

主题

- 使用记录 IAM 身份中心 API 调用 Amazon CloudTrail
- 使用记录 IAM 身份中心 SCIM API 调用 Amazon CloudTrail
- 将应用程序组件与 Amazon 连接起来 EventBridge
- 记录可配置 AD 同步错误

使用记录 IAM 身份中心 API 调用 Amazon CloudTrail

Amazon IAM Identity Center 与一项服务集成 Amazon CloudTrail，该服务提供用户、角色或 Amazon 服务在 IAM Identity Center 中采取的操作的记录。 CloudTrail 将 IAM 身份中心的 API 调用捕获为事件。捕获的调用包括来自 IAM Identity Center 控制台的调用和对 IAM Identity Center API 操作的代码调用。如果您创建跟踪，则可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括 IAM 身份中心的事件。如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的 “事件历史记录” 中查看最新的事件。使用收集的信息 CloudTrail，您可以确定向 IAM Identity Center 发出的请求、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。

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

下表汇总了 IAM I CloudTrail dentity Center 的事件、其 CloudTrail 事件源和匹配的 API。有关 API 的更多信息，请参阅 IAM Identity Center API 参考。

> **Note**
>
> 作 Sign-in为 IAM Identity Center 用户登录时还会 Amazon 发出另外一组 CloudTrail 事件（称为）。 Amazon 这些事件没有对应的公开 API，因此未在 API 参考中列出。

CloudTrail 事件	公有 API	说明	CloudTrail 事件源
IAM Identity Center	IAM Identity Center	IAM Identity Center API 支持管理权限集、应用程序、可信令牌颁发者、账户和应用程序分配、IAM Identity Center 实例及标签。	`sso.amazonaws.com`
身份存储	身份存储	身份存储 API 支持管理企业用户和组的生命周期，以及用户的组成员身份。此外，还支持管理用户的多重身份验证（MFA）设备。	`sso-directory.amazonaws.com` ，`identitystore.amazonaws.com`
OIDC	OIDC	OIDC API 支持可信身份传播，以及以已通过身份验证的 IAM 身份中心用户身份登录 Amazon CLI 和 IDE 工具包。	`sso.amazonaws.com` ，`sso-oauth.amazonaws.com`
Amazon Web Services 访问门户	Amazon Web Services 访问门户	Amazon Web Services 访问门户 API 支持 Amazon Web Services 访问	`sso.amazonaws.com`

CloudTrail 事件	公有 API	说明	CloudTrail 事件源
		门户的操作，支持用户通过获取账户凭证 Amazon CLI。	
SCIM	SCIM	SCIM API 支持通过 SCIM 协议配置用户、组和组成员身份。请参阅使用记录 IAM 身份中心 SCIM API 调用 Amazon CloudTrail了解更多信息。	identitystore-scim.amazonaws.com
Amazon 登录	没有公有 API	Amazon 为进入 IAM 身份中心的用户身份验证和联合身份验证流程发出 Sign-in CloudTrail 事件。	signin.amazon.com

主题

- CloudTrail IAM 身份中心的用例
- IAM 身份中心信息位于 CloudTrail

CloudTrail IAM 身份中心的用例

IAM Identity Center 发出 CloudTrail 的事件对于各种用例来说可能很有价值。Organizations 可以使用这些事件日志来监控和审核用户在其 Amazon 环境中的访问和活动。这有助于合规使用案例，因为日志会记录谁在何时访问了哪些资源的详细信息。您还可以使用这些 CloudTrail 数据进行事件调查，从而使团队能够分析用户行为并跟踪可疑行为。此外，事件历史记录可支持故障排除，让您清晰了解用户权限和配置随时间的变更情况。

以下部分介绍了支撑审计、事件调查和故障排除等工作流程的基础使用案例。

在 IAM 身份中心用户发起 CloudTrail 的事件中识别用户

IAM Identity Center 会发出两个 CloudTrail 字段，使您能够识别 CloudTrail事件背后的 IAM 身份中心用户，例如登录 IAM 身份中心或 Amazon CLI使用 Amazon Web Services 访问门户，包括管理 MFA 设备：

- `userId` - 来自 IAM Identity Center 实例身份存储的唯一且不可变的用户标识符。
- `identityStoreArn` - 包含该用户的身份存储的 Amazon 资源名称（ARN）。

`userID`和`identityStoreArn`字段显示在嵌套在`onBehalfOf`元素内的`userIdentity`元素中，如以下示例 CloudTrail事件日志所示。此事件日志展示了 `userIdentity` 类型为“`IdentityCenterUser`”的事件中的这两个字段。您还可以在已认证 IAM Identity Center 用户的事件中找到这些字段，此类事件的 `userIdentity` 类型为“Unknown”。您的工作流程应支持这两种类型值。

```
"userIdentity":{
  "type":"IdentityCenterUser",
  "accountId":"111122223333",
  "onBehalfOf": {
    "userId": "544894e8-80c1-707f-60e3-3ba6510dfac1",
    "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
    },
    "credentialId" : "90e292de-5eb8-446e-9602-90f7c45044f7"
  }
```

> **Tip**
>
> 我们建议您使用`userId`和`identityStoreArn`来识别 IAM Identity Center CloudTrail 事件背后的用户。`userIdentity` 元素下的 `userName` 和 `principalId` 字段已不再提供。如果您的工作流程（例如审计或事件响应）依赖于访问 `username`，则您有两个选择：
>
> - 按照 登录事件 CloudTrail 中的用户名 中的说明，从 IAM Identity Center 目录中获取用户名。
> - `UserName`获取 IAM 身份中心在`additionalEventData` Sign-in元素下发布的。此选项不需要访问 IAM Identity Center 目录。有关更多信息，请参阅 登录事件 CloudTrail 中的用户名。

要检索用户的详细信息，包括 username 字段，您需要使用用户 ID 和身份存储 ID 作为参数来查询身份存储。您可以通过 DescribeUser API 请求或通过 CLI 执行此操作。示例 CLI 命令如下。如果您的 IAM Identity Center 实例位于 CLI 默认区域，可省略 region 参数。

```
aws identitystore describe-user \
--identity-store-id  d-1234567890 \
--user-id  544894e8-80c1-707f-60e3-3ba6510dfac1 \
--region your-region-id
```

要确定前面示例中 CLI 命令的身份存储 ID 值，您可以从 identityStoreArn 值中提取身份存储 ID。在示例 ARN arn:aws:identitystore::111122223333:identitystore/d-1234567890 中，身份存储 ID 为 d-1234567890。或者，您可以通过导航至 IAM Identity Center 控制台设置区域的身份存储选项卡查找身份存储 ID。

如果您正在自动化 IAM Identity Center 目录中的用户查询，建议您估算用户查询频率，并考虑 IAM Identity Center 对身份存储 API 的限流阈值。缓存已获取的用户属性有助于您控制查询频率在限流阈值内。

关联同一用户会话内的用户事件

登录事件中发出的AuthWorkflowID字段允许在 IAM Identity Center 用户会话开始之前跟踪与登录序列相关的所有 CloudTrail 事件。

对于 Amazon Web Services 访问门户内部的用户操作，该credentialId值设置为用于请求操作的 IAM Identity Center 用户会话的 ID。您可以使用此值来识别在 Amazon Web Services 访问门户中同一个经过身份验证的 IAM Identity Center 用户会话中启动 CloudTrail 的事件。

> **Note**
>
> 您无法使用 credentialId 将登录事件与后续事件（如 Amazon Web Services 访问门户的使用）相关联。登录事件中输出的 credentialId 字段值仅供内部使用，建议您不要依赖该值。对于通过 OIDC 调用的 Amazon Web Services 访问门户事件，其输出的 credentialId 字段值等于访问令牌 ID。

在 IAM 身份中心用户发起的事件中识别用户 CloudTrail 后台会话详细信息

以下 CloudTrail 事件捕获了 OAuth 2.0 令牌交换的过程，在该过程中，将代表用户交互式会话的现有访问令牌 (thesubjectToken) 交换为刷新令牌 (the)。requestedTokenType刷新令牌允许用户发起的任何长时间运行的作业在用户退出登录后，仍以该用户的权限继续运行。

对于 IAM Identity Cent er 用户后台会话，该 CloudTrail 事件包括元素resource中名为的附加requestParameters元素。resource 参数包含在后台运行的作业的 Amazon 资源名称（ARN）。此元素仅存在于 CloudTrail 事件记录中，不包含在 IAM Identity Center CreateTokenWithIAMAPI 或 SDK 响应中。

```
{
  "clientId": "EXAMPLE-CLIENT-ID",
  "grantType": "urn:ietf:params:oauth:grant-type:token-exchange",
  "code": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "redirectUri": "https://example.com/callback",
  "assertion": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "subjectToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "subjectTokenType": "urn:ietf:params:oauth:token-type:access_token",
  "requestedTokenType": "urn:ietf:params:oauth:token-type:refresh_token",
  "resource": "arn:aws:sagemaker:us-west-2:123456789012:training-job/my-job"
}
```

在 IAM Identity Center 与外部目录之间关联用户

IAM Identity Center 提供两个用户属性，可用于将其目录中的用户与外部目录（例如 Microsoft Active Directory 和 Okta Universal Directory）中的同一用户相关联。

- externalId - IAM Identity Center 用户的外部标识符。建议您将此标识符映射到外部目录中不可变的用户标识符。请注意，IAM Identity Center 不会在中发出此值。 CloudTrail
- username - 客户提供的值，用户通常使用该值登录。该值可能会变更（例如通过 SCIM 更新）。请注意，当身份源为时 Amazon Directory Service，IAM Identity Center 发出的用户名与您为进行身份验证而输入的用户名 CloudTrail 相匹配。该用户名无需与 IAM Identity Center 目录中的用户名完全一致。

  如果您有权访问 CloudTrail 事件但没有 IAM Identity Center 目录的访问权限，则可以使用登录时additionalEventData元素下方显示的用户名。有关 additionalEventData 中用户名的更多详情，请参阅 登录事件 CloudTrail 中的用户名。

当身份源为 Amazon Directory Service时，这两个用户属性与外部目录中对应用户属性的映射关系在 IAM Identity Center 中定义。有关信息，请参阅 IAM Identity Center 与外部身份提供者目录之间的属性映射。 IdPs 在外部，使用 SCIM 的用户有自己的映射。即使您使用 IAM Identity Center 目录作为身份源，也可以使用 externalId 属性将安全主体与您的外部目录进行交叉引用。

以下部分说明如何根据用户的 username 和 externalId 查找 IAM Identity Center 用户。

通过用户名和 externalId 查看 IAM Identity Center 用户

对于已知用户名，您可先通过 GetUserId API 请求获取对应的 userId，再发起 DescribeUser API 请求，从 IAM Identity Center 目录中获取用户属性（如前例所示）。以下示例展示如何从身份存储中获取特定用户名对应的 userId。如果您的 IAM Identity Center 实例位于 CLI 默认区域，可省略 region 参数。

```
aws identitystore get-user-id \
    --identity-store d-9876543210 \
    --alternate-identifier '{
      "UniqueAttribute": {
      "AttributePath": "username",
      "AttributeValue": "anyuser@example.com"
        }
          }' \
    --region your-region-id
```

同理，如果已知 externalId，也可使用相同机制查询。将前例中的属性路径更新为 externalId，并将属性值设置为您要查询的具体 externalId。

在 Microsoft Active Directory（AD）中查看用户的安全标识符（SID）与 externalId

在某些情况下，IAM Identity Center 会在 CloudTrail 事件principalId字段中发出用户的 SID，例如 Amazon Web Services 访问门户和 OIDC API 发出的事件。此类场景正逐步淘汰。如果需从 AD 中获取唯一用户标识符，建议您的工作流程使用 AD 属性 objectguid。您可在 IAM Identity Center 目录的 externalId 属性中找到该值。但是，如果您的工作流程需要使用 SID，请从 AD 中检索该值，因为它无法通过 IAM Identity Center API 获得。

关联同一用户会话内的用户事件 介绍了如何使用 externalId 和 username 字段将 IAM Identity Center 用户与外部目录中的对应用户相关联。默认情况下，IAM Identity Center 将 externalId 映射到 AD 中的 objectguid 属性，此映射关系为固定配置。IAM Identity Center 允许管理员灵活配置 username 的映射关系，而非默认映射到 AD 中的 userprincipalname。

您可在 IAM Identity Center 控制台中查看这些映射关系。导航到设置的身份源选项卡，然后在操作菜单中选择管理同步。在管理同步部分，选择查看属性映射按钮。

虽然您可以使用 IAM Identity Center 中可用的任何唯一 AD 用户标识符在 AD 中查找用户，但我们建议您在查询中使用 objectguid，因为它是一个不可变的标识符。以下示例展示了如何使用 Powershell 查询 Microsoft AD，以使用用户的 objectguid 值 16809ecc-7225-4c20-ad98-30094aefdbca 来检索用户。该查询的成功响应将包含用户的 SID。

```
Install-WindowsFeature -Name  RSAT-AD-PowerShell

  Get-ADUser `
  -Filter {objectGUID -eq  [GUID]::Parse("16809ecc-7225-4c20-ad98-30094aefdbca")} `
  -Properties *
```

IAM 身份中心信息位于 CloudTrail

CloudTrail 在您创建账户 Amazon Web Services 账户 时已在您的账户上启用。当 IAM Identity Center 中发生活动时，该活动会与其他 Amazon 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在中查看、搜索和下载最近发生的事件 Amazon Web Services 账户。有关更多信息，请参阅使用事件历史查看 CloudTrail 事件。

> **Note**
>
> 有关 CloudTrail 事件中用户识别和对用户操作的跟踪如何演变的更多信息，请参阅Amazon 安全博客中的 IAM Identity Center CloudTrail 事件的重要更改。

要持续记录您的事件 Amazon Web Services 账户，包括 IAM Identity Center 的事件，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。预设情况下，在控制台中创建跟踪时，此跟踪应用于所有 Amazon 区域。跟踪记录 Amazon 分区中所有区域的事件，并将日志文件传送到您指定的 Amazon S3 存储桶。此外，您可以配置其他 Amazon 服务，以进一步分析 CloudTrail 日志中收集的事件数据并对其采取行动。有关更多信息，请参阅《Amazon CloudTrail 用户指南》中的以下主题：

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

在您的中启用 CloudTrail 日志记录后 Amazon Web Services 账户，将在日志文件中跟踪对 IAM Identity Center 操作进行的 API 调用。IAM 身份中心记录与其他 Amazon 服务记录一起写入日志文件。 CloudTrail 根据时间段和文件大小决定何时创建和写入新文件。

CloudTrail 支持的 IAM 身份中心 API 的事件

以下部分提供有关与 IAM 身份中心支持的以下 API 相关 CloudTrail 的事件的信息：

- IAM Identity Center API
- Identity Store API
- OIDC API
- Amazon Web Services 访问门户 API
- SCIM API

CloudTrail IAM 身份中心 API 操作的事件

以下列表包含公共 IAM Identity Center 操作通过`sso.amazonaws.com`事件源发出的事件。CloudTrail 有关公共 IAM Identity Center API 操作的更多信息，请参阅《IAM Identity Center API 参考》。

您可能会在 CloudTrail 控制台所依赖的 IAM Identity Center 控制台 API 操作中找到其他事件。有关这些控制台 API 的更多信息，请参阅《服务授权参考》。

- AttachCustomerManagedPolicyReferenceToPermissionSet
- AttachManagedPolicyToPermissionSet
- CreateAccountAssignment
- CreateApplication
- CreateApplicationAssignment
- CreateInstance
- CreateInstanceAccessControlAttributeConfiguration
- CreatePermissionSet
- CreateTrustedTokenIssuer
- DeleteAccountAssignment
- DeleteApplication

- DeleteApplicationAccessScope
- DeleteApplicationAssignment
- DeleteApplicationAuthenticationMethod
- DeleteApplicationGrant
- DeleteInlinePolicyFromPermissionSet
- DeleteInstance
- DeleteInstanceAccessControlAttributeConfiguration
- DeletePermissionsBoundaryFromPermissionSet
- DeletePermissionSet
- DeleteTrustedTokenIssuer
- DescribeAccountAssignmentCreationStatus
- DescribeAccountAssignmentDeletionStatus
- DescribeApplication
- DescribeApplicationAssignment
- DescribeApplicationProvider
-

DescribeInstance

- DescribeInstanceAccessControlAttributeConfiguration
- DescribePermissionSet
- DescribePermissionSetProvisioningStatus
- DescribeTrustedTokenIssuer
- DetachCustomerManagedPolicyReferenceFromPermissionSet
- DetachManagedPolicyFromPermissionSet
- GetApplicationAccessScope
- GetApplicationAssignmentConfiguration
- GetApplicationAuthenticationMethod
- GetApplicationGrant
- GetInlinePolicyForPermissionSet
- GetPermissionsBoundaryForPermissionSet
- ListAccountAssignmentCreationStatus
- ListAccountAssignmentDeletionStatus
- ListAccountAssignments

- ListAccountAssignmentsForPrincipal
- ListAccountsForProvisionedPermissionSet
- ListApplicationAccessScopes
- ListApplicationAssignments
- ListApplicationAssignmentsForPrincipal
- ListApplicationAuthenticationMethods
- ListApplicationGrants
- ListApplicationProviders
- ListApplications
- ListCustomerManagedPolicyReferencesInPermissionSet
- ListInstances
- ListManagedPoliciesInPermissionSet
- ListPermissionSetProvisioningStatus
- ListPermissionSets
- ListPermissionSetsProvisionedToAccount
- ListTagsForResource

- ListTrustedTokenIssuers
- ProvisionPermissionSet
- PutApplicationAccessScope
- PutApplicationAssignmentConfiguration
- PutApplicationAuthenticationMethod
- PutApplicationGrant
- PutInlinePolicyToPermissionSet
- PutPermissionsBoundaryToPermissionSet
- TagResource
- UntagResource
- UpdateApplication
- UpdateInstance
- UpdateInstanceAccessControlAttributeConfiguration
- UpdatePermissionSet
- UpdateTrustedTokenIssuer

CloudTrail 身份存储 API 操作的事件

以下列表包含公共 Id CloudTrail entity Store 操作随`identitystore.amazonaws.com`事件源一起发出的事件。有关公共 Identity Store API 操作的更多信息，请参阅《Identity Store API 参考》。

您可能会在 CloudTrail 带有事件源的 Identity Store 控制台 API 操作中找到其他`sso-directory.amazonaws.com`事件。这些 API 支持控制台和 Amazon Web Services 访问门户。如果您需要检测特定操作（例如将成员添加到组）的发生，我们建议您同时考虑公共和控制台 API 操作。有关这些控制台 API 的更多信息，请参阅《服务授权参考》。

- CreateGroup
- CreateGroupMembership
- CreateUser
- DeleteGroup
- DeleteGroupMembership
- DeleteUser
- DescribeGroup
- DescribeGroupMembership
- DescribeUser
- GetGroupId
- GetGroupMembershipId
- GetUserId
- IsMemberInGroups
- ListGroupMemberships
- ListGroupMembershipsForMember
- ListGroups
- ListUsers
- UpdateGroup
- UpdateUser

CloudTrail OIDC API 操作的事件

以下列表包含公共 OIDC 操作发出 CloudTrail 的事件。有关公共 OIDC API 操作的更多信息，请参阅《OIDC API 参考》。

- CreateToken（事件源 sso.amazonaws.com）
- CreateTokenWithIAM（事件源 sso-oauth.amazonaws.com）

CloudTrail 的事件 Amazon Web Services 访问门户 API 操作

以下列表包含 Amazon Web Services 访问门户 API 操作随sso.amazonaws.com事件源一起发出的事件。 CloudTrail 公共 API 中标明不可用的 API 操作支持 Amazon Web Services 访问门户的操作。使用 Amazon CLI 可能会导致发布公共 Amazon Web Services 访问门户 API 操作和公共 API 中不可用的操作 CloudTrail 的事件。有关公共 Amazon Web Services 访问门户 API 操作的更多信息，请参阅Amazon Web Services 访问门户 API 参考。

- Authenticate（在公共 API 中不可用。 提供 Amazon Web Services 访问门户的登录信息。）
- Federate（公开 API 中不可用。提供应用程序的联合身份验证功能。）
- ListAccountRoles
- ListAccounts
- ListApplications（在公共 API 中不可用。 为用户提供分配的资源以显示在 Amazon Web Services 访问门户中。）
- ListProfilesForApplication（在公共 API 中不可用。 提供应用程序元数据以显示在 Amazon Web Services 访问门户中。）
- GetRoleCredentials
- Logout

CloudTrail SCIM API 操作的事件

有关公开 SCIM API 操作的信息，请参阅《Amazon Web Services 访问门户 API 参考》。

IAM 身份中心 CloudTrail 活动中的身份信息

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

- 请求是使用根用户还是 Amazon Identity and Access Management (IAM) 用户证书发出。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 Amazon 服务发出。
- 请求是否由 IAM Identity Center 用户发起。如果是，则 CloudTrail 事件中的userId和identityStoreArn字段可用来识别发起请求的 IAM Identity Center 用户。有关更多信息，请参阅 在 IAM 身份中心用户发起 CloudTrail 的事件中识别用户。

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

> **Note**
>
> 目前，IAM Identity Center 不会为用户使用 O IDC API 登录 Amazon 托管网络应用程序（例如 Amazon A SageMaker I Studio）发出 CloudTrail 事件。这些 Web 应用程序是更广泛的 the section called “Amazon 托管应用程序” 集合的子集，该集合还包括非 Web 应用程序，例如 Amazon Athena SQL 和 Amazon S3 访问权限管控。

了解 IAM 身份中心 CloudTrail 的事件

跟踪是一种配置，可用于将事件传送到您指定的 Amazon S3 存储桶。事件代表来自任何来源的单个请求，包括有关请求的操作、操作的日期和时间、请求参数等的信息。 CloudTrail 事件不是公共 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序出现。在《CloudTrail 用户指南》中了解 CloudTrail 记录的内容。

此示例演示了一个 CloudTrail 日志条目，用于捕获与 IAM 身份中心交互的 IAM 用户 (samadams) 执行的`DescribePermissionsPolicies`操作：

```
{
   "Records":[
      {
         "eventVersion":"1.05",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDAJAIENLMexample",
            "arn":"arn:aws:iam::08966example:user/samadams",
            "accountId":"111122223333",
            "accessKeyId":"AKIAIIJM2K4example",
            "userName":"samadams"
         },
         "eventTime":"2017-11-29T22:39:43Z",
         "eventSource":"sso.amazonaws.com",
         "eventName":"DescribePermissionsPolicies",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"203.0.113.0",
         "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
         "requestParameters":{
            "permissionSetId":"ps-79a0dde74b95ed05"
         },
```

```
         "responseElements":null,
         "requestID":"319ac6a1-d556-11e7-a34f-69a333106015",
         "eventID":"a93a952b-13dd-4ae5-a156-d3ad6220b071",
         "readOnly":true,
         "resources":[

         ],
         "eventType":"AwsApiCall",
         "recipientAccountId":"111122223333"
      }
   ]
}
```

此示例演示了一个 CloudTrail 日志条目，用于捕获 IAM Identity Center 用户在 Amazon Web Services 访问门户中执行的`ListApplications`操作：

```
{
   "Records":[
      {
         "eventVersion":"1.05",
         "userIdentity":{
            "type":"IdentityCenterUser",
            "accountId":"111122223333",
            "onBehalfOf": {
              "userId": "94d00cd8-e9e6-4810-b177-b08e84775435",
              "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
            },
            "credentialId" : "cdee2490-82ed-43b3-96ee-b75fbf0b97a5"
         },
         "eventTime":"2017-11-29T18:48:28Z",
         "eventSource":"sso.amazonaws.com",
         "eventName":"ListApplications",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"203.0.113.0",
         "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
         "requestParameters":null,
         "responseElements":null,
         "requestID":"de6c0435-ce4b-49c7-9bcc-bc5ed631ce04",
         "eventID":"e6e1f3df-9528-4c6d-a877-6b2b895d1f91",
         "eventType":"AwsApiCall",
         "recipientAccountId":"111122223333"
```

```
      }
   ]
}
```

此示例演示了一个 CloudTrail 日志条目，用于捕获通过 IAM Identity Center OIDC 服务进行身份验证的 IAM 身份中心用户执行的`CreateToken`操作：

```
{
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IdentityCenterUser",
        "accountId": "111122223333",
        "onBehalfOf": {
          "userId": "94d00cd8-e9e6-4810-b177-b08e84775435",
          "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
        },
        "credentialId" : "cdee2490-82ed-43b3-96ee-b75fbf0b97a5"
      },
      "eventTime": "2020-06-16T01:31:15Z",
      "eventSource": "sso.amazonaws.com",
      "eventName": "CreateToken",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "203.0.113.0",
      "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
      "requestParameters": {
        "clientId": "clientid1234example",
        "clientSecret": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "grantType": "urn:ietf:params:oauth:grant-type:device_code",
        "deviceCode": "devicecode1234example"
      },
      "responseElements": {
        "accessToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "tokenType": "Bearer",
        "expiresIn": 28800,
        "refreshToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "idToken": "HIDDEN_DUE_TO_SECURITY_REASONS"
      },
      "eventID": "09a6e1a9-50e5-45c0-9f08-e6ef5089b262",
      "readOnly": false,
      "resources": [
        {
```

```
            "accountId": "111122223333",
            "type": "IdentityStoreId",
            "ARN": "d-1234567890"
          }
        ],
        "eventType": "AwsApiCall",
        "recipientAccountId": "111122223333"
}
```

了解 IAM Identity Center 登录事件

Amazon CloudTrail 记录所有 IAM Identity Center 身份源的成功和失败登录事件。IAM Identity Center 和 Active Directory（AD Connector 和 Amazon Managed Microsoft AD）来源的身份除了该特定凭证验证请求的状态外，还包括每次提示用户解决特定凭证问题或因素时捕获的其他登录事件。只有在用户完成所有必需的凭证质询后，用户才会登录，这将导致记录 `UserAuthentication` 事件。

下表记录了每个 IAM Identity Center 登录 CloudTrail 事件的名称、其目的以及对不同身份源的适用性。

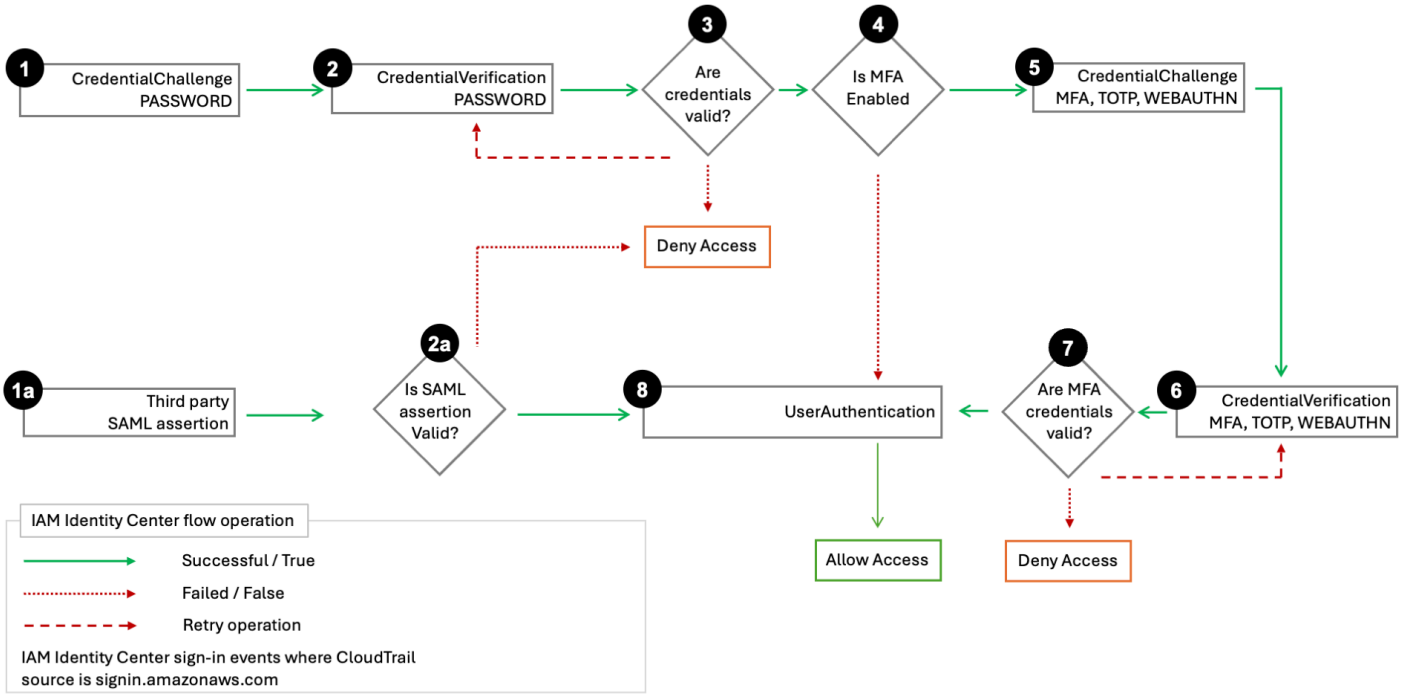
事件名称	活动目的	身份源适用性
`CredentialChallenge`	用于通知 IAM Identity Center 已请求用户解决特定的凭证质询并指定所需的 `CredentialType`（例如 PASSWORD 或 TOTP）。	原生 IAM 身份中心用户、AD Connector 和 Amazon Managed Microsoft AD
`CredentialVerification`	用于通知用户已尝试解决特定 `CredentialChallenge` 请求并指定该凭证是成功还是失败。	原生 IAM 身份中心用户、AD Connector 和 Amazon Managed Microsoft AD
`UserAuthentication`	用于通知用户面临的所有身份验证要求均已成功完成并且用户已成功登录。用户未能成功完成所需的凭证质询将导致不记录任何 *`UserAuthentication`* 事件。	所有身份源

下表捕获了特定登录事件中包含的其他有用 CloudTrail 事件数据字段。

字段	活动目的	Sign-in 事件适用性	示例值
AuthWorkflowID	用于关联整个登录序列中发出的所有事件。对于每次用户登录，IAM Identity Center 可能会发出多个事件。	CredentialChallenge，CredentialVerification，UserAuthentication	“AuthWorkflowID”：“9de74b32-8362-4a01-a524-de21df59fd83”
CredentialType	用于指定受到询问的凭证或因素。UserAuthentication 事件将包括在用户登录序列中成功验证的所有 CredentialType 值。	CredentialChallenge，CredentialVerification，UserAuthentication	CredentialType“: “密码” 或” “: “密码，TOTP”（可能的值包括：密码、TOTP、WEBAUTHN、EXTERNAL_IDP、RESYNC_TOTP、EMAIL_OTP、EMAIL_OTP）CredentialType
DeviceEnrollmentRequired	用于指定用户需要在登录期间注册 MFA 设备，并且用户已成功完成该请求。	UserAuthentication	“DeviceEnrollmentRequired“: “没错”
LoginTo	用于指定成功登录序列后的重定向位置。	UserAuthentication	"LoginTo": "https://mydirectory.awsapps.com/start/....."

CloudTrail IAM 身份中心登录流程中的事件

下图描述了登录流程和 Sign-in发出 CloudTrail 的事件。



该图显示了一个密码登录流程和一个联合登录流程。

密码登录流程（包括步骤 1–8）展示了用户名和密码登录过程中的步骤。IAM Identity Center 将 `userIdentity.additionalEventData.CredentialType` 设置为“PASSWORD”，并执行凭据质询-响应周期，必要时进行重试。

步骤数量取决于登录类型和多重身份验证（MFA）的启用状态。初始过程会导致三到五个 CloudTrail 事件，并以成功身份验证的序列`UserAuthentication`结束。密码身份验证尝试失败会导致其他 CloudTrail 事件，因为 IAM Identity Center 会重新发布`CredentialChallenge`常规身份验证或 MFA（如果启用）身份验证。

密码登录流程还包括使用 `CreateUser` API 调用新创建的 IAM Identity Center 用户使用一次性密码（OTP）登录的场景。此场景中的凭证类型是“EMAIL_OTP”。

联合登录流程（包括步骤 1a, 2a 和 8）展示了联合身份验证过程中的主要步骤，其中身份提供者提供 SAML 断言，由 IAM Identity Center 进行验证，如果成功，则产生 `UserAuthentication`。IAM Identity Center 不会调用步骤 3 – 7 中的内部 MFA 身份验证序列，因为外部联合身份提供者负责所有用户凭证身份验证。

登录事件 CloudTrail 中的用户名

IAM Identity Center 在每次 IAM Identity Center 用户成功登录时，在 additionalEventData 元素下发出 UserName 字段一次。以下列表描述了范围内的两种登录事件，以及这些事件发生的条件。当用户登录时，只有一个条件可能为真。

- CredentialChallenge
  - 何时CredentialType为 “PASSWORD” — 适用于使用 Amazon Directory Service 或进行密码身份验证 IAM Identity Center 目录。
  - Wh CredentialType e EMAIL_OTP n 为 “” — 仅适用于CreateUser通过 API 调用创建的用户首次尝试登录，并且该用户收到一次性密码即可使用该密码登录一次的情况。 IAM Identity Center 目录
- UserAuthentication
  - 当 CredentialType 为“EXTERNAL_IDP”时 - 适用于使用外部 IdP 进行的身份验证。

成功认证的 UserName 值如下：

- 当身份源是外部 IdP 时，该值等于传入 SAML 断言中的 nameID 值。该值等于 IAM Identity Center 目录中的 UserName 字段。
- 当身份源为时 IAM Identity Center 目录，发出的值等于该目录中的UserName字段。
- 当身份源为时 Amazon Directory Service，发出的值等于用户在身份验证期间输入的用户名。例如，拥有用户名的用户可以使用anyuser@company.com、或进行身份验证 anyuseranyuser@company.com，在每种情况下company.com/anyuser，输入的值都将 CloudTrail 分别发出。

错误用户名尝试的安全屏蔽

HIDDEN_DUE_TO_SECURITY_REASONS当记录的事件是由于用户名输入不正确导致的控制台登录失败时，该UserName字段包含字符串。 CloudTrail 在这种情况下，不会记录内容，因为文本可能包含敏感信息，如以下示例所述：

- 用户不小心在用户名称字段中键入了密码。
- 用户意外键入了个人电子邮件账户的账户名称、银行登录标识符或某个其他私有 ID。

> **Tip**
>
> 我们建议您使用userId和identityStoreArn来识别 IAM Identity Center CloudTrail 事件背后的用户。如果您需要使用 userName 字段，可以使用每次成功登录时在 additionalEventData 元素下发出的 userName。

有关如何使用 UserName 字段的更多信息，请参阅 关联同一用户会话内的用户事件。

IAM Identity Center 登录场景的示例事件

以下示例说明了在各种 Amazon 登录场景中生成的典型 CloudTrail 事件序列。这些示例作为参考模式，可帮助您解释身份验证日志、识别安全问题并验证您的身份验证策略是否正常运行。

主题

- 仅使用密码身份验证时的成功登录
- 通过外部身份提供商进行身份验证时成功登录
- 使用密码和基于时间的一次性密码（TOTP）验证器应用程序进行身份验证时的成功登录
- 使用密码进行身份验证并需要强制 MFA 注册时成功登录
- 由于密码身份验证不正确导致的登录失败

仅使用密码身份验证时的成功登录

以下事件序列捕获了仅密码成功登录的示例。

CredentialChallenge（密码）

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
```

```
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "eventTime":"2020-12-07T20:33:58Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "UserName":"bobsmith@example.com",
      "CredentialType":"PASSWORD"
   },
   "requestID":"5be44ffb-6946-4f47-acaf-1adebd4afead",
   "eventID":"27ea7725-c1fd-4355-bdba-d0e628e0e604",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```

成功 CredentialVerification（密码）

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
```

```
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "CredentialType":"PASSWORD"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"c49640f6-0c8a-43d3-a6e0-900e3bb188d4",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```

成功 UserAuthentication（仅限密码）

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
```

```
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?
state=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
BshlIc5OBAA6ftz73M6LsfLWDlfOxviO2K3wet946lC30f_iWdilx-
zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7TqziOLiBLBUSx
east-1",
      "CredentialType":"PASSWORD"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"e959a95a-2b33-478d-906c-4fe303e8a9f1",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```


通过外部身份提供商进行身份验证时成功登录

以下事件序列捕获了使用外部身份提供商通过 SAML 协议进行身份验证时成功登录的示例。

成功 UserAuthentication（外部身份提供商）


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
```

```
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?
state=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
BshlIc5OBAA6ftz73M6LsfLWDlfOxviO2K3wet946lC30f_iWdilx-
zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7TqziOLiBLBUSx
east-1",
      "CredentialType":"EXTERNAL_IDP",
      "UserName":"bobsmith@example.com"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"e959a95a-2b33-478d-906c-4fe303e8a9f1",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```


使用密码和基于时间的一次性密码（TOTP）验证器应用程序进行身份验证时的成功登录

以下事件序列捕获了一个示例，其中登录期间需要多重身份验证，并且用户使用密码和 TOTP 身份验证器应用成功登录。

CredentialChallenge （密码）


```
{
```

```
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "eventTime":"2020-12-08T20:40:13Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"PASSWORD",
      "UserName":"bobsmith@example.com"
   },
   "requestID":"e454ea66-1027-4d00-9912-09c0589649e1",
   "eventID":"d89cc0b5-a23a-4b88-843a-89329aeaef2e",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```


成功 CredentialVerification（密码）


```
{
   "eventVersion":"1.08",
```

```
   "userIdentity":{
      "type":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "eventTime":"2020-12-08T20:40:20Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"PASSWORD"
   },
   "requestID":"92c4ac90-0d9b-452d-95d5-728487612f5e",
   "eventID":"4533fd49-6669-4d0b-b272-a0b2139309a8",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```

CredentialChallenge（TOTP）

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"IdentityCenterUser",
```

```
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "eventTime":"2020-12-08T20:40:20Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"TOTP"
   },
   "requestID":"92c4ac90-0d9b-452d-95d5-728487612f5e",
   "eventID":"29202f08-f240-40cc-b789-c0cea8a27847",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```

成功 CredentialVerification (TOTP)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
```

```
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "eventTime":"2020-12-08T20:40:27Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"TOTP"
   },
   "requestID":"c40a691f-eeb1-4352-b286-5e909f96f318",
   "eventID":"e889ff1d-fcaf-454f-805d-7132cf2362a4",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```

成功 UserAuthentication（密码 + TOTP）

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
```

```
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "eventTime":"2020-12-08T20:40:27Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?state
\u003dQVlBQmVLeFhWeDRmZFJmMmxHcWYwdzhZck5RQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
\u0026auth_code
\u003d11Fir1mCVJ-4Y5UY6RI10UCXvRePCHd6195xvYg1rwo1Pj7B-7UGIGlYUUVe31Nkzd7ihxKn6DMdnFfO01O8qc3RF
Sx-pjBXKG_jUcvBk_UILdGytV4o1u97h42B-
TA_6uwdmJiw1dcCz_Rv44d_BS0PkulW-5LVJy1oeP1H0FPPMeheyuk5Uy48d5of9-c\u0026wdc_csrf_token
\u003dNMlui44guoVnxRd0qu2tYJIdyyFPX6SDRNTspIScfMM0AgFbho1nvvCaxPTghHbgHCRIXdffFtzH0sL1ow419Bobn
\u0026organization\u003dd-9067230c03\u0026region\u003dus-east-1",
      "CredentialType":"PASSWORD,TOTP"
   },
   "requestID":"c40a691f-eeb1-4352-b286-5e909f96f318",
   "eventID":"7a8c8725-db2f-488d-a43e-788dc6c73a4a",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```


使用密码进行身份验证并需要强制 MFA 注册时成功登录

以下事件序列展示了一次成功的密码身份验证，其中要求用户在完成登录过程之前注册并成功完成多重身份验证（MFA）。

CredentialChallenge（密码）


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "eventTime":"2020-12-09T01:24:02Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "CredentialType":"PASSWORD",
      "UserName":"bobsmith@example.com"
   },
   "requestID":"321f4b13-42b5-4005-a0f7-826cad26d159",
   "eventID":"8c707b0f-e45a-4a9c-bee2-ff68638d2f1b",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```


成功 CredentialVerification（密码）

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "eventTime":"2020-12-09T01:24:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "CredentialType":"PASSWORD"
   },
   "requestID":"12b57efa-0a92-4479-91a3-5b6641817c21",
   "eventID":"783b0c89-7142-4942-8b84-6ee0de1b992e",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```


成功 UserAuthentication（需要密码 + MFA 注册）


```
{
   "eventVersion":"1.08",
```

```
   "userIdentity":{
      "type":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "eventTime":"2020-12-09T01:24:14Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?state
\u003dQVlBQmVGQ3VqdHF5aW9CUDdrNXRTVTJUaWNnQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
\u0026auth_code
\u003d11eZ80S_maUsZ7ABETjeQhyWfvIHYz52rgR28sYAKN1oEk2G07czrwzXvE9HLlN2K9De8LyBEV83SFeDQfrWpkwXf
FJyJqkoGrt_w6rm_MpAn0uyrVq8udY EgU3fhOL3QWvWiquYnDPMyPmmy_qkZgR9rz__BI
\u0026wdc_csrf_token
\u003dJih9U62o5LQDtYLNqCK8a6xj0gJg5BRWq2tbl75y8vAmwZhAqrgrgbxXat2M646UZGp93krw7WYQdHIgi5OYI9QSc
\u003dd-9067230c03\u0026region\u003dus-east-1",
      "CredentialType":"PASSWORD",
      "DeviceEnrollmentRequired":"true"
   },
   "requestID":"74d24604-a365-4237-8c4a-350795494b92",
   "eventID":"a15bf257-7f37-46c0-b67c-fea5fa6166be",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
```

```
}
```

由于密码身份验证不正确导致的登录失败

以下事件序列展示了一次身份验证尝试，其中用户成功输入了用户名但在密码验证步骤失败，导致登录不成功。

CredentialChallenge（密码）

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
   },
   "eventTime":"2020-12-08T18:56:15Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"adbf67c4-8188-4e2b-8527-fe539e328fa7",
      "CredentialType":"PASSWORD",
      "UserName":"bobsmith@example.com"
   },
   "requestID":"f54848ea-b1aa-402f-bf0d-a54561a2ffcc",
   "eventID":"d96f1d6c-dbd9-4a0b-9a45-6a2b66078c78",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```

失败 CredentialVerification （ 密码 ）


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
   },
   "eventTime":"2020-12-08T18:56:21Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"adbf67c4-8188-4e2b-8527-fe539e328fa7",
      "CredentialType":"PASSWORD"
   },
   "requestID":"04528c82-a678-4a1f-a56d-ea2c6445a72a",
   "eventID":"9160fe06-fc2a-474f-9b78-000ee067a09d",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Failure"
   }
}
```


使用记录 IAM 身份中心 SCIM API 调用 Amazon CloudTrail

IAM Identity Center SCIM 与 Amazon CloudTrail一项服务集成，该服务提供用户、角色或角色所采取的操作的 Amazon Web Services 服务记录。 CloudTrail 将 SCIM 的 API 调用捕获为事件。使用收集的信息 CloudTrail，您可以确定有关所请求操作的信息、操作的日期和时间、请求参数等。要了解更多信息 CloudTrail，请参阅Amazon CloudTrail 用户指南。

> **Note**
>
> CloudTrail 在您创建账户 Amazon Web Services 账户 时已在您的账户上启用。但是，如果您的访问令牌是在 2024 年 9 月之前创建的，则可能需要轮换访问令牌才能看到来自 SCIM 的事件。
> 有关更多信息，请参阅 轮换访问令牌。

SCIM 支持将以下操作记录为事件： CloudTrail

- CreateGroup
- CreateUser
- DeleteGroup
- DeleteUser
- GetGroup
- GetSchema
- GetUser
- ListGroups
- ListResourceTypes
- ListSchemas
- ListUsers
- PatchGroup
- PatchUser
- PutUser
- ServiceProviderConfig

示例 CloudTrail 事件

以下示例演示了使用 IAM Identity Center 进行 SCIM 操作期间生成的典型 CloudTrail 事件日志。这些示例显示了成功操作和常见错误场景的事件的结构和内容，可帮助您了解在排除 SCIM 配置问题时如何解释 CloudTrail 日志。

成功的 **CreateUser** 操作

此 CloudTrail 事件显示通过 SCIM API 成功执行的`CreateUser`操作。该事件捕获了请求参数（敏感信息已脱敏）和响应元素，包括新创建用户的 ID。此类事件在身份提供者通过 SCIM 协议成功向 IAM Identity Center 配置新用户时生成。


```
{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "WebIdentityUser",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "CreateUser",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "requestParameters": {
    "httpBody": {
      "displayName": "HIDDEN_DUE_TO_SECURITY_REASONS",
      "schemas" : [
        "urn:ietf:params:scim:schemas:core:2.0:User"
      ],
      "name": {
        "familyName": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "givenName": "HIDDEN_DUE_TO_SECURITY_REASONS"
      },
      "active": true,
      "userName": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "tenantId": "xxxx"
  },
  "responseElements": {
    "meta" : {
      "created" : "Oct 10, 2024, 1:23:45 PM",
      "lastModified" : "Oct 10, 2024, 1:23:45 PM",
      "resourceType" : "User"
    },
    "displayName" : "HIDDEN_DUE_TO_SECURITY_REASONS",
    "schemas" : [
      "urn:ietf:params:scim:schemas:core:2.0:User"
```

```
    ],
    "name": {
      "familyName": "HIDDEN_DUE_TO_SECURITY_REASONS",
      "givenName": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "active": true,
    "id" : "c4488478-a0e1-700e-3d75-96c6bb641596",
    "userName": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "requestID": "xxxx",
  "eventID": "xxxx",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
  }
}
```

失败的 **PatchGroup** 操作：缺少必需的路径属性

此 CloudTrail 事件显示了导致错误消息`ValidationException`的失败`PatchGroup`操作`"Missing path in PATCH request"`。发生此错误是因为 PATCH 操作需要一个路径属性来指定要修改哪个组属性，但该属性在请求中缺失。

```
{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "PatchGroup",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "errorCode": "ValidationException",
  "errorMessage": "Missing path in PATCH request",
  "requestParameters": {
```

```
    "httpBody": {
      "operations": [
        {
          "op": "REMOVE",
          "value": "HIDDEN_DUE_TO_SECURITY_REASONS"
        }
      ],
      "schemas": [
        "HIDDEN_DUE_TO_SECURITY_REASONS"
      ]
    },
    "tenantId": "xxxx",
    "id": "xxxx"
  },
  "responseElements": null,
  "requestID": "xxxx",
  "eventID": "xxxx",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
  }
}
```

失败的 **CreateGroup** 操作：组名已存在

此 CloudTrail 事件显示了导致错误消息ConflictException的失败CreateGroup操作"Duplicate GroupDisplayName"。当尝试创建显示名在 IAM Identity Center 中已存在的组时，会发生此错误。身份提供者必须使用唯一的组名，或者更新现有组而不是创建新组。

```
{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "CreateGroup",
```

```
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "errorCode": "ConflictException",
  "errorMessage": "Duplicate GroupDisplayName",
  "requestParameters": {
    "httpBody": {
      "displayName": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "tenantId": "xxxx"
  },
  "responseElements": null,
  "requestID": "xxxx",
  "eventID": "xxxx",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
  }
}
```


失败的 **PatchUser** 操作：不支持多个电子邮件地址

此 CloudTrail 事件显示了导致错误消息`ValidationException`的失败`PatchUser`操作`"List attribute emails exceeds allowed limit of 1"`。当尝试为用户分配多个电子邮件地址时会发生此错误，因为 IAM Identity Center 每个用户仅支持一个电子邮件地址。身份提供者必须配置 SCIM 映射，以便为每个用户仅发送一个电子邮件地址。


```
{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "PatchUser",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",
```

```
  "userAgent": "Go-http-client/2.0",
  "errorCode": "ValidationException",
  "errorMessage": "List attribute emails exceeds allowed limit of 1",
  "requestParameters": {
    "httpBody": {
      "operations": [
        {
          "op": "REPLACE",
          "path": "emails",
          "value": "HIDDEN_DUE_TO_SECURITY_REASONS"
        }
      ],
      "schemas": [
        "HIDDEN_DUE_TO_SECURITY_REASONS"
      ]
    },
    "tenantId": "xxxx",
    "id": "xxxx"
  },
  "responseElements": null,
  "requestID": "xxxx",
  "eventID": "xxxx",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
  }
}
```


IAM Identity Center 中常见的 SCIM API 验证错误

在 IAM Identity Center 中使用 SCIM API 时，通常会在 CloudTrail 事件中出现以下验证错误消息。这些验证错误通常发生在用户和组配置操作期间。

有关解决这些错误和正确配置 SCIM 配置的详细指南，请参阅此 Amazon Web Services re:Post 文章。

- List attribute email exceeds allowed limit of 1
- List attribute addresses allowed limit of 1

- 1 validation errors detected: Value at '*name.familyName*' failed to satisfy constraint: Member must satisfy regular expression pattern: [\\p{L}\\p{M}\\p{S}\\p{N}\\p{P}\\t\\n\\r]+
- 2 validation errors detected: Value at 'name.familyName' failed to satisfy constraint: Member must have length greater than or equal to 1; Value at 'name.familyName' failed to satisfy constraint: Member must satisfy regular expression pattern: [\\p{L}\\p{M}\\p{S}\\p{N}\\p{P}\\t\\n\\r]+
- 检测到 2 个验证错误：'urn: ietf: params: scim: schemas: extension: enterprise: 2.0: User.manager.value '处的值未能满足约束：成员的长度必须大于或等于 1；'urn: ietf: params: scim:schemas: extension: enterprise: 2.0:User.manager.value' 处的值无法满足约束：成员必须满足正则表达式模式：[\\ p {L}\ p {M}\\ p {S}\\ p {N}\\ p {P}\\ t\\ n\\ r] +”，
- 来自的 JSON RequestBody
- Invalid Filter format

将应用程序组件与 Amazon 连接起来 EventBridge

您可以将 IAM Identity Center 与 A mazon 集成， EventBridge以引发启动管理通知的事件，或者调用自动工作流程以响应 CloudTrail 事件中记录的特定 IAM 身份中心操作。

例如，您可以配置EventBridge 规则来检测用户何时删除应用程序或 IAM Identity Center 何时创建新群组。根据您的使用案例，您可以将这些事件路由到 Amazon SNS 主题以通知管理员或使用 Amazon LambdaStep Fun ctions 或其他EventBridge-supported 服务调用额外的自动化。

记录可配置 AD 同步错误

您可以启用可配置 Active Directory（AD）同步配置的日志记录功能，用以接收包含同步过程中可能发生的错误相关信息的日志。利用这些日志，您可以监控可配置 AD 同步是否存在问题，在有问题时采取措施。您可以将日志发送到亚马逊 CloudWatch 日志组、亚马逊简单存储服务 (Amazon S3) Service 存储桶或支持跨账户传输的亚马逊数据 Firehose，Amazon S3 存储桶和 Firehose 支持跨账户传输。

有关限制、权限和公开日志的更多信息，请参阅从中 Amazon Web Services 服务启用日志记录。

> **Note**
>
> 您需要为日志记录支付费用。有关更多信息，请参阅 Amazon CloudWatch 定价页面上的销售日志。

启用可配置 AD 同步错误日志

1. 登录到 IAM Identity Center 控制台。
2. 选择设置。
3. 在设置页面上，选择身份源选项卡，从中选择操作，然后选择管理日记。
4. 选择添加日志传输和以下某个目标类型。
   a. 选择 “收到 Amazon CloudWatch 日志”。再选择或输入目标日志组。
   b. 选择到 Amazon S3。再选择或输入目标存储桶。
   c. 选择到 Firehose。再选择或输入目标传输流。
5. 选择提交。

禁用可配置 AD 同步错误日志

1. 登录到 IAM Identity Center 控制台。
2. 选择设置。
3. 在设置页面上，选择身份源选项卡，从中选择操作，然后选择管理日记。
4. 为要删除的目标选择删除。
5. 选择提交。

可配置 AD 同步错误日志字段

请参阅如下列表，了解可能的错误日志字段。

`sync_profile_name`

同步配置文件的名称。

`error_code`

表示发生了哪种错误类型的错误代码。

`error_message`

包含有关所发生错误的详细信息的一条消息。

`sync_source`

同步源是指要从中同步实体的位置。对 IAM Identity Center 而言，这是指由 Amazon Directory Service管理的 Active Directory（AD）。同步源包含受影响目录的域和 ARN。

`sync_target`

同步目标是指要保存实体的目标位置。对 IAM Identity Center 而言，这是指身份存储。同步目标包含受影响的身份存储 ARN。

`source_entity_id`

导致错误的实体的唯一标识符。对 IAM Identity Center 而言，这是指实体的 SID。

`source_entity_type`

导致错误的实体类型。该值可以是 `USER` 或 `GROUP`。

`eventTimestamp`

错误出现的时间戳。

可配置 AD 同步错误日志示例

示例 1：AD 目录密码过期的错误日志

```
{
    "sync_profile_name": "EXAMPLE-PROFILE-NAME",
    "error" : {
        "error_code": "InvalidDirectoryCredentials",
        "error_message": "The password for your AD directory has expired. Please reset
 the password to allow Identity Sync to access the directory."
    },
    "sync_source": {
        "arn": "arn:aws:ds:us-east-1:123456789:directory/d-123456",
        "domain": "EXAMPLE.com"
    },
    "eventTimestamp": "1683355579981"
}
```

示例 2：用户的用户名不唯一的错误日志

```
{
```

```
    "sync_profile_name": "EXAMPLE-PROFILE-NAME",
    "error" : {
        "error_code": "ConflictError",
        "error_message": "The source entity has a username conflict with the sync
 target. Please verify that the source identity has a unique username in the target."
    },
    "sync_source": {
        "arn": "arn:aws:ds:us-east-1:111122223333:directory/d-123456",
        "domain": "EXAMPLE.com"
    },
    "sync_target": {
        "arn": "arn:aws:identitystore::111122223333:identitystore/d-123456"
    },
    "source_entity_id": "SID-1234",
    "source_entity_type": "USER",
    "eventTimestamp": "1683355579981"
}
```

IAM Identity Center 的合规性验证

Third-party 审计师评估 Amazon Web Services 服务 诸如此类的安全性和合规性 Amazon IAM Identity Center ，将其作为多个合 Amazon 规计划的一部分。

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

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

您在使用 Amazon Web Services 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。有关您在使用时的合规责任的更多信息 Amazon Web Services 服务 ，请参阅Amazon 安全文档。

支持的合规性标准

IAM Identity Center 已经过以下标准的审核，并且有资格用作您需要获得合规性认证的解决方案的一部分。

Amazon 已扩大其《健康保险流通与责任法案》(HIPAA) 合规计划，将IAM Identity Center列为符合 HIP AA资格的服务。

Amazon 为想要详细了解如何处理和存储健康信息的客户提供了一HIPAA-focused 份白皮书。 Amazon Web Services 服务 有关更多信息，请参阅 HIPAA 合规性。

信息安全注册评估员计划 (IRAP) 使澳大利亚政府客户能够确保适当的合规控制措施到位，并确定适当的责任模型，以满足澳大利亚网络安全中心 (ISM) 编制的澳大利亚政府信息安全手册 (ISM) 的要求。有关更多信息，请参阅 IRAP 资源。

IAM Identity Center 已通过支付卡行业 (PCI) 数据安全标准 (DSS) 版本 3.2 一级服务提供商的合规性认证。

使用 Amazon 产品和服务存储、处理或传输持卡人数据的客户可以在 IAM Identity Center 中使用以下身份源来管理自己的 PCI DSS 合规性认证：

- Active Directory
- 外部身份提供商

IAM Identity Center 身份源当前不符合 PCI DSS。

有关 PCI DSS 的更多信息，包括如何申请 PCI Compliance Package 的副本，请参阅 Amazon PCI DSS 第 1 级。

系统和组织控制 (SOC) 报告是独立的第三方检查报告，展示 IAM Identity Center 如何实现关键合规性控制和目标。这些报告可帮助您和您的审计员了解控制措施如何支持运营和合规性。SOC 报告分为三种类型：

- Amazon SOC 1 报告——使用 Ar ti Amazon fact 下载
- Amazon SOC 2：安全、可用性和机密性报告——使用 Ar ti Amazon fact 下载
- Amazon SOC 3：安全性、可用性和机密性报告

IAM 身份中心属于 Amazon SOC 1、SOC 2 和 SOC 3 报告的范围。有关更多信息，请参阅 SOC 合规性。

IAM Identity Center 的弹性

Amazon 全球基础设施是围绕 Amazon 区域和可用区构建的。 Amazon 区域提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络相连。利用可用区，您可以设计和操作在可用区之间无中断地自动实现失效转移的应用程序和数据库。与传统的单个或多个数据中心基础架构相比，可用区具有更高的可用性、容错性和可扩展性。

有关 Amazon 区域和可用区的更多信息，请参阅Amazon 全球基础设施。

要了解有关 Amazon IAM Identity Center 弹性的更多信息，请参阅弹性设计和区域行为。

IAM Identity Center 的基础设施安全

作为一项托管服务 Amazon IAM Identity Center ，受 Amazon 全球网络安全的保护。有关 Amazon 安全服务以及如何 Amazon 保护基础设施的信息，请参阅Amazon 云安全。要使用基础设施安全的最佳实践来设计您的 Amazon 环境，请参阅 S Amazon ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 Amazon 已发布的 API 调用通过网络访问 IAM 身份中心。客户端必须支持以下内容：

- 传输层安全性协议（TLS）。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密 (PFS) 的密码套件，例如 DHE（短暂的）或 ECDHE（椭圆曲线短暂的 Diffie-Hellman）。 Diffie-Hellman大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

IAM Identity Center 中的数据保护

责任 Amazon 共担模型适用于 Amazon IAM 身份中心的数据保护。如本模型所述 Amazon ，负责保护运行所有 Amazon 云的全球基础架构。您负责维护对托管在此基础结构上的内容的控制。您还负责所用 Amazon 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 Amazon Security Blog 上的 Amazon Shared Responsibility Model and GDPR 博客文章。

我们建议您通过以下方式保护您的数据：

- 在 IAM Identity Center 中启用多重身份验证（MFA）。
- 使用 TLS 与 Amazon 资源通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 Amazon CloudTrail。有关使用 CloudTrail 跟踪捕获 Amazon 活动的信息，请参阅《Amazon CloudTrail 用户指南》中的使用跟 CloudTrail 踪。
- 使用 Amazon 加密解决方案以及 Amazon 服务中的所有默认安全控制。

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 Amazon IAM Identity Center、 Amazon CLI API 或使用其他 Amazon 服务时 Amazon SDKs。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诊断日志。

传输中加密

IAM Identity Center 使用传输层安全性协议（TLS）1.2 或 TLS 1.3 加密协议自动加密所有网络间数据，从而保护往返服务的过程中的传输中数据。使用 IAM 进行身份验证并发送到 IAM 身份中心 APIs、身份存储 API 或 OIDC API 的直接 HTTPS 请求使用签Amazon 名版本 4 算法进行签名，以建立安全连接。

数据隐私

借助 IAM Identity Center，您保留对组织数据的控制权。您存储在 IAM Identity Center 中的用户和群组身份与其他 Amazon 服务（例如Amazon 托管应用程序）共享，前提是您使用 IAM Identity Center 启用这些身份，并且这些服务需要这些服务。

有关更多信息，请参阅 Amazon 数据隐私常见问题解答。

数据留存

IAM Identity Center 会存储您的数据，例如用户和组身份以及元数据，直到您从服务中删除它们。当您删除 IAM Identity Center 实例时，其中包含的数据也会被删除。

静态加密

IAM Identity Center 使用以下密钥类型提供加密以保护静态数据：

- Amazon 拥有的密钥 （默认密钥类型）— IAM Identity Center 默认使用这些密钥来自动加密您的数据。您无法查看、管理、审核其使用情况，也无法将 Amazon 拥有的密钥用于其他目的。IAM Identity Center 完全处理密钥管理以保护您的数据安全，您无需采取任何操作。有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的 Amazon 拥有密钥。
- 客户自主管理型密钥 - 在 IAM Identity Center 的组织实例中，您可以选择对称客户自主管理型密钥来对您的员工身份数据（例如用户和组属性）进行静态加密。您创建、拥有并管理这些加密密钥。由于您可以完全控制这层加密，因此可以执行以下任务：
  - 制定和维护密钥策略，将密钥的访问权限限制为只有需要访问权限的 IAM 委托人，例如 IAM Identity Center Amazon Organizations 及其管理员。Amazon 托管应用程序
  - 制定并维护用于密钥访问（包括跨账户访问）的 IAM 策略
  - 启用和禁用密钥策略
  - 轮换加密材料
  - 审计需要密钥访问权限的数据访问
  - 添加 标签
  - 创建密钥别名
  - 安排密钥删除

要了解如何在 IAM Identity Center 中实施客户自主管理型 KMS 密钥，请参阅 在中实现客户托管的 KMS 密钥 Amazon IAM Identity Center。有关客户自主管理型密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的客户自主管理型密钥。

> **Note**
>
> IAM Identity Center 使用 Amazon 自有的 KMS 密钥自动启用静态加密，从而免费保护客户数据。但是，使用客户管理的密钥需要 Amazon KMS 付费。有关定价的更多信息，请参阅 Amazon Key Management Service 定价。

实施客户自主管理型密钥的注意事项：

- 专用密钥：我们建议为每个 IAM Identity Center 实例创建一个新的专用客户自主管理型 KMS 密钥，而不是重用现有密钥。这种方法可以更清晰地分离职责，简化访问控制管理，并使安全审计更直接。拥有专用密钥还可以通过将密钥更改的影响限制在单个 IAM Identity Center 实例来降低风险。
- 在多个实例中使用 IAM 身份中心 Amazon Web Services 区域：如果您计划将您的 IAM 身份中心实例复制到其他实例 Amazon Web Services 区域，则需要使用客户托管的 KMS 密钥进行静态加密。多区域 IAM 身份中心不支持默认 Amazon 拥有的 KMS 密钥类型。有关更多信息，请参阅 跨多个 IAM 身份中心使用 Amazon Web Services 区域。

> **Note**
>
> IAM Identity Center 在加密您的员工身份数据时使用信封加密。您的 KMS 密钥充当包装密钥的角色，用于加密实际用于加密数据的数据密钥。

有关 Amazon KMS 的更多信息，请参阅什么是 Amazon 密钥管理服务？

IAM Identity Center 加密上下文

加密上下文是一组可选的非秘密密钥值对，其中包含有关数据的其他上下文信息。 Amazon KMS 使用加密上下文作为其他经过身份验证的数据来支持经过身份验证的加密。当您在加密数据的请求中包含加密上下文时，会将加密上下文 Amazon KMS 绑定到加密数据。要解密数据，您必须在请求中包含相同的加密上下文。有关加密上下文的更多信息，请参阅《Amazon KMS 开发人员指南》。

IAM Identity Center 使用以下内容中的加密上下文密钥：aws: sso: instance-arn、aws: identitystore: identitystore-arn 和。 tenant-key-id例如，以下加密上下文可能出现在 Amazon KMS I AM Identity Center API 调用的 API 操作中。

```
"encryptionContext": {
    "tenant-key-id": "ssoins-1234567890abcdef",
    "aws:sso:instance-arn": "arn:aws:sso:::instance/ssoins-1234567890abcdef"
}
```

以下加密上下文可能会出现在身份存储 Amazon KMS API 调用的 API 操作中。

```
"encryptionContext": {
    "tenant-key-id": "12345678-1234-1234-1234-123456789012",
    "aws:identitystore:identitystore-arn":
 "arn:aws:identitystore::123456789012:identitystore/d-1234567890"
}
```

使用加密上下文控制对客户托管密钥的访问

您可以使用密钥策略和 IAM 策略中的加密上下文作为条件来控制对您的对称客户托管密钥的访问。高级 KMS 密钥策略语句 中的一些密钥策略模板包含此类条件，以确保密钥仅与特定的 IAM Identity Center 实例一起使用。

监控 IAM Identity Center 的加密密钥

当您将客户托管的 KMS 密钥与 IAM 身份中心实例一起使用时，您可以使用Amazon CloudTrail或 Amazon CloudWatch Logs 来跟踪 IAM 身份中心发送到的请求 Amazon KMS。中列出了 IAM 身份中心调用的 KMS API 操作步骤 2：准备 KMS 密钥策略语句。 CloudTrail 这些 API 操作的事件包含加密上下文，这使您可以监控 IAM Identity Center 实例调用的 Amazon KMS API 操作，以访问由您的客户托管密钥加密的数据。

Amazon KMS API 操作 CloudTrail 事件中的加密上下文示例：

```
{
"requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "encryptionContext": {
            "aws:sso:instance-arn": "arn:aws:sso:::instance/ssoins-xxxxxxxxxxxxxxxx",
            "tenant-key-id": "ssoins-xxxxxxxxxxxxxxxx"
        }
    }
}
```

Amazon 托管应用程序对 IAM Identity Center 身份属性的存储、加密和删除

您部署的某些 Amazon 托管应用程序（例如 S Amazon ystems Manager 和 Amazon CodeCatalyst）会将来自 IAM 身份中心的特定用户和群组属性存储在自己的数据存储中。 Amazon IAM Identity Center在 IAM Identity Center 中使用客户托管 KMS 密钥进行静态加密不会扩展到存储在 Amazon 托管应用程序中的 IAM Identity Center 用户和群组属性。 Amazon 托管应用程序对其存储的数据支持不同的加密方法。最后，当您在 IAM Identity Center 中删除用户和群组属性时，这些 Amazon 托管应用

程序可能会在删除这些信息后继续将其存储在 IAM Identity Center 中。有关存储在应用程序中的数据的加密和安全性，请参阅 Amazon 托管应用程序的用户指南。

在中实现客户托管的 KMS 密钥 Amazon IAM Identity Center

客户管理的密 Amazon 钥是您创建、拥有和管理的密钥管理服务密钥。要在 Amazon IAM Identity Center 中实施客户托管的 KMS 密钥进行静态加密，请执行以下步骤：

> **Important**
>
> 某些 Amazon 托管应用程序不能与配置了客户托管 KMS 密钥的 Amazon IAM 身份中心一起使用。请参阅Amazon 可与 IAM 身份中心配合使用的托管应用程序。

1. 步骤 1：确定组织的使用案例 - 要正确定义 KMS 密钥的使用权限，您需要确定整个组织的相关使用案例。KMS 密钥权限由 KMS 密钥策略语句和基于身份的策略组成，它们协同工作以允许适当的 IAM 主体为其特定使用案例使用 KMS 密钥。
2. 步骤 2：准备 KMS 密钥策略语句 - 根据步骤 1 中确定的使用案例选择相关的 KMS 密钥策略语句模板，并填写必需的标识符和 IAM 主体名称。从基线 KMS 密钥策略语句开始，如果您的安全策略要求，请按照高级 KMS 密钥策略语句中的描述对其进行细化。
3. 步骤 3：创建客户自主管理型 KMS 密钥-在 KMS 中创建符合 IAM 身份中心要求的 Amazon KMS 密钥，并将步骤 2 中准备的 KMS 密钥策略声明添加到 KMS 密钥策略中。
4. 步骤 4：为 KMS 密钥的跨账户使用配置 IAM 策略 - 根据步骤 1 中确定的使用案例选择相关的 IAM 策略语句模板，并通过填写密钥 ARN 来准备使用它们。然后，通过将准备好的 IAM 策略语句添加到主体的 IAM 策略中，允许每个特定使用案例的 IAM 主体跨账户使用 KMS 密钥。
5. 步骤 5：在 IAM Identity Center 中配置 KMS 密钥 - 在您的 IAM Identity Center 实例中启用客户自主管理型 KMS 密钥，以将其用于静态加密。

步骤 1：确定组织的使用案例

在创建和配置客户自主管理型 KMS 密钥之前，请确定您的使用案例并准备所需的 KMS 密钥权限。有关 KMS 密钥策略的更多信息，请参阅《Amazon KMS 开发人员指南》。

调用 IAM 身份中心服务的 IAM 委托人 APIs 需要权限。例如，可以通过权限集策略授权授权管理员使用这些 APIs 权限。当使用客户托管密钥配置 IAM 身份中心时，IAM 委托人还必须有权通过 IAM 身份中心服务 APIs使用 KMS API。您在两个地方定义这些 KMS API 权限：KMS 密钥策略和与 IAM 主体关联的 IAM 策略中。

KMS 密钥权限包括如下：

1. 您在 步骤 3：创建客户自主管理型 KMS 密钥 中创建 KMS 密钥时在密钥上指定的 KMS 密钥策略语句。
2. 您在 步骤 4：为 KMS 密钥的跨账户使用配置 IAM 策略 中创建 KMS 密钥后为 IAM 主体指定的 IAM 策略语句。

下表指定了相关使用案例以及需要使用您的 KMS 密钥权限的 IAM 主体。

使用案例	需要使用 KMS 密钥权限的 IAM 主体	必需/可选
Amazon IAM 身份中心的使用	• Amazon IAM 身份中心的管理员 • IAM Identity Center 服务及相关的 Identity Store 服务	必需
在 IAM 身份中心使用 Amazon 托管应用程序	• Amazon 托管应用程序的管理员 • Amazon 托管应用程序 • Amazon 托管应用程序代入调用 IAM 身份中心服务的@@ 服务角色 APIs	可选
在启用 Amazon Control Tower 的 Amazon IAM 身份中心实例上使用	• Amazon Control Tower 管理员	可选
通过 IA Amazon M 身份中心对 Amazon EC2 实例进行单点登录	• 授权对 Amazon EC2 实例执行 SSO 的 IAM 委托人	可选
使用 IAM 委托人调用 IAM Identity Center 服务的任何其他 APIs 用例，例如客户托管的应用程序、权限集配置工作流程或 Amazon Lambda 函数	• 这些工作流程用于调用 IAM 身份中心服务的 IAM 委托人 APIs	可选

> **Note**
>
> 表中列出的多个 IAM 委托人需要 Amazon KMS API 权限。但是，为了保护您在 IAM 身份中心中的用户和群组数据，只有 IAM 身份中心和身份存储服务可以直接调用 Amazon KMS API。

步骤 2：准备 KMS 密钥策略语句

从开始，基准 KMS 密钥策略然后为您的组织进行自定义。如果您需要基于安全要求的更具体策略，可以使用 高级 KMS 密钥策略语句 中的示例修改策略语句。有关此决策的指导，请参阅 选择基线与高级 KMS 密钥策略语句的注意事项。

1. 将基准策略复制到编辑器，然后在 KMS 密钥策略声明中插入所需的标识符和 IAM 委托人名称。有关查找引用标识符值的帮助，请参阅 在哪里可以找到所需的标识符。
2. 如果您的安全要求有此要求，请使用中的示例完善策略声明高级 KMS 密钥策略语句。

> **Important**
>
> 修改已由 IAM Identity Center 使用的密钥的 KMS 密钥策略时请务必谨慎。虽然 IAM Identity Center 在您初始配置 KMS 密钥时会验证加密和解密权限，但它无法验证后续的策略更改。无意中移除必要的权限可能会中断您的 IAM Identity Center 的正常运行。有关排查 IAM Identity Center 中客户自主管理型密钥相关常见错误的指导，请参阅 对客户管理的密钥进行故障排除 Amazon IAM Identity Center。

> **Note**
>
> IAM Identity Center 及其关联的 Identity Store 需要服务级权限才能使用您的客户自主管理型 KMS 密钥。此要求扩展到 APIs 使用服务证书调用 IAM Identity Center 服务的 Amazon 托管应用程序。对于通过 APIs 正向访问会话调用 IAM Identity Center 服务的其他用例，只有发起方 IAM 委托人（例如管理员）需要 KMS 密钥权限。值得注意的是，使用 Amazon 访问门户和 Amazon 托管应用程序的最终用户不需要直接的 KMS 密钥权限，因为这些权限是通过相应的服务授予的。

步骤 3：创建客户自主管理型 KMS 密钥

您可以使用 Amazon 管理控制台或 KMS 创建客户托管 Amazon 密钥 APIs。在创建密钥时，将您在步骤 2 中准备的 KMS 密钥策略语句添加到 KMS 密钥策略中。有关详细说明，包括关于默认 KMS 密钥策略的指南，请参阅《Amazon Key Management Service 开发人员指南》。

密钥必须满足以下要求：

- KMS 密钥必须与 IAM 身份中心实例位于同一 Amazon 区域

- 您可以选择多区域密钥或单区域密钥。但是，如果您计划同时使用 IAM Identity Center， Amazon Web Services 区域 则必须创建多区域 KMS 密钥。您无法将单区域 KMS 密钥转换为多区域 KMS 密钥，因此除非您对使用单区域 KMS 密钥有特殊要求，否则我们建议您从多区域 KMS 密钥开始。
- KMS 密钥必须是配置为“加密和解密”用途的对称密钥
- KMS 密钥必须与 IAM Identity Center 的组织实例位于同一个 Amazon Organizations 管理账户中

> **Note**
>
> 如果您计划将此 KMS 密钥复制到要复制您的 IAM 身份中心的区域，我们建议您先完成本节中的设置，然后按照中的指导进行操作 the section called “将 IAM 身份中心复制到其他区域”

步骤 4：为 KMS 密钥的跨账户使用配置 IAM 策略

使用其他 Amazon 账户的 IAM 身份中心服务的 APIs 任何 IAM 委托人（例如 IAM Identity Center 委托管理员）还需要一份允许通过这些账户使用 KMS 密钥的 IAM 政策声明 APIs。

对于在步骤 1 中确定的每个使用案例：

1. 在“基线 KMS 密钥和 IAM 策略语句”中找到相关的 IAM 策略语句模板。
2. 将模板复制到编辑器中，并填写密钥 ARN（在步骤 3 中创建 KMS 密钥后，此 ARN 现已可用）。有关查找密钥 ARN 值的帮助，请参阅 在哪里可以找到所需的标识符。
3. 在中 Amazon Web Services 管理控制台，找到与用例关联的 IAM 委托人的 IAM 策略。此策略的位置因使用案例和授予访问权限的方式而异。
   - 对于在 IAM 中直接授予的访问权限，您可以找到 IAM 主体，例如 IAM 控制台中的 IAM 角色。
   - 对于通过 IAM Identity Center 授予的访问权限，您可以在 IAM Identity Center 控制台中找到相关的权限集。
4. 将特定于使用案例的 IAM 策略语句添加到 IAM 角色并保存更改。

> **Note**
>
> 此处所述的 IAM 策略是基于身份的策略。虽然此类策略可以附加到 IAM 用户、组和角色，但我们建议尽可能使用 IAM 角色。有关 IAM 角色与 IAM 用户的更多信息，请参阅 IAM 用户指南。

某些 Amazon 托管应用程序中的其他配置

某些 Amazon 托管应用程序要求您配置服务角色以允许应用程序使用 IAM Identity Center 服务 APIs。如果您的组织将 Amazon 托管应用程序与 IAM Identity Center 配合使用，请为每个已部署的应用程序完成以下步骤：

1. 查看应用程序的用户指南，确认权限是否已更新，以包含将该应用程序与 IAM Identity Center 一起使用时所需的 KMS 密钥相关权限。
2. 如果是，请按照应用程序用户指南中的说明更新权限，以避免中断应用程序的操作。

> **Note**
>
> 如果您不确定 Amazon 托管应用程序是否使用这些权限，我们建议您查看所有已部署的 Amazon 托管应用程序的用户指南。对于每个需要此配置的应用程序，您只需执行一次此配置。

步骤 5：在 IAM Identity Center 中配置 KMS 密钥

> **Important**
>
> 在执行此步骤之前：
>
> - 确认您的 Amazon 托管应用程序与客户托管的 KMS 密钥兼容。有关兼容应用程序的列表，请参阅可与 IAM Identity Center 一起使用的Amazon 托管应用程序。如果您有不兼容的应用程序，请勿继续。
> - 配置使用 KMS 密钥所需的必要权限。如果没有适当的权限，此步骤可能会失败或中断 IAM Identity Center 管理、 Amazon 托管应用程序的使用以及其他需要 KMS 密钥权限的使用案例。有关更多信息，请参阅 步骤 1：确定组织的使用案例。
> - 确保 Amazon 托管应用程序和使用 IAM 角色调用 IAM 身份中心服务的 APIs 客户托管应用程序的权限也允许通过 IAM 身份中心服务使用 KMS 密钥 APIs。某些 Amazon 托管应用程序要求您配置权限（例如服务角色）才能使用这些权限 APIs。请参阅每个已部署的 Amazon 托管应用程序的用户指南，以确认是否需要添加特定的 KMS 密钥权限。

在启用新的 IAM Identity Center 组织实例时指定 KMS 密钥

在启用新的 IAM Identity Center 组织实例时，您可以在设置过程中指定客户自主管理型 KMS 密钥。这可确保实例从一开始就使用您的密钥进行静态加密。开始之前，请参阅 客户自主管理型 KMS 密钥和高级 KMS 密钥策略的注意事项。

1. 在启用 IAM Identity Center 页面上，展开静态加密部分。
2. 选择管理加密。
3. 选择客户自主管理型密钥。
4. 对于 KMS 密钥，请执行以下操作之一：
   a. 选择从您的 KMS 密钥中选择，然后从下拉列表中选择您创建的密钥。
   b. 选择输入 KMS 密钥 ARN，然后输入密钥的完整 ARN。
5. 选择保存。
6. 选择启用，以完成设置。

有关更多信息，请参阅启用 IAM Identity Center。

更改现有 IAM Identity Center 组织实例的密钥配置

您可以随时将客户自主管理型 KMS 密钥更改为另一个密钥，或切换到 Amazon 拥有密钥。

Console

更改 KMS 密钥配置

1. 打开 IAM 身份中心控制台，网址为 https://console.aws.amazon.com/singlesignon/。
2. 在导航窗格中，选择设置。
3. 选择其他设置选项卡。
4. 选择管理加密。
5. 选择下列选项之一：
   a. 客户自主管理型密钥 - 从下拉列表中选择不同的客户自主管理型密钥，或输入新的密钥 ARN。
   b. Amazon 拥有的密钥-切换到默认的加密选项。
6. 选择保存。

Amazon CLI

将现有 IAM Identity Center 组织实例更改为使用 KMS 客户自主管理型密钥

```
aws sso-admin update-instance \
    --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \
    --encryption-configuration \
        KeyType=CUSTOMER_MANAGED_KEY,KmsKeyArn=arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

将现有 IAM Identity Center 组织实例更改为使用 Amazon 拥有的密钥

```
aws sso-admin update-instance \
    --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \
    --encryption-configuration KeyType=AWS_OWNED_KMS_KEY
```

客户自主管理型密钥注意事项

- 更新用于 IAM Identity Center 操作的 KMS 密钥配置不会影响 IAM Identity Center 中的活动用户会话。 APIs 在此过程中，您可以继续使用 Amazon 访问门户、IAM 身份中心控制台和 IAM 身份中心服务。
- 当切换到新的 KMS 密钥时，IAM Identity Center 会验证其是否可以成功使用该密钥进行加密和解密。如果您在设置密钥策略或 IAM 策略时出错，控制台将显示说明性错误消息，并且将继续使用先前的 KMS 密钥。
- 默认的年度 KMS 密钥轮换将自动进行。您可以参阅《Amazon KMS 开发人员指南》以获取有关密钥轮换、监控 Amazon KMS 密钥和控制密钥删除访问权限等主题的信息。

Important

如果您的 IAM Identity Center 实例正在使用的客户自主管理型 KMS 密钥被删除、禁用或因不正确的 KMS 密钥策略而无法访问，您的员工用户和 IAM Identity Center 管理员将无法使用 IAM Identity Center。访问丢失可能是暂时的（可以更正密钥策略）或永久的（已删除的密钥无法恢复），具体取决于情况。我们建议您限制访问关键操作，例如删除或禁用 KMS 密钥。此外，我们建议您的组织设置Amazon 漏洞访问程序，以确保您的特权用户 Amazon 在无法访问 IAM Identity Center 时能够进行访问。

在哪里可以找到所需的标识符

在为客户自主管理型 KMS 密钥配置权限时，您需要特定的 Amazon 资源标识符来完成密钥策略和 IAM 策略语句模板。在 KMS 密钥策略语句中插入所需的标识符（例如，组织 ID）和 IAM 主体名称。

以下是在 Amazon 管理控制台中查找这些标识符的指南。

IAM Identity Center Amazon 资源名称（ARN）和 Identity Store ARN

IAM 身份中心实例是一种具有自己唯一 ARN 的 Amazon 资源，例如 arn: aws: sso::: instance/ssoins-1234567890abcdef。ARN 遵循服务授权参考中 IAM Identity Center 资源类型部分记录的模式。

每个 IAM Identity Center 实例都有一个关联的 Identity Store，用于存储用户和组身份。Identity Store 有一个称为 Identity Store ID 的唯一标识符（例如，d-123456789a）。ARN 遵循服务授权参考中 Identity Store 资源类型部分记录的模式。

您可以在 IAM Identity Center 的“设置”页面上找到 ARN 和 Identity Store ID 值。Identity Store ID 位于“身份源”选项卡中。

Amazon Organizations ID

如果要在密钥策略中指定组织 ID（例如，o-exampleorg1），可以在 IAM Identity Center 和 Organizations 控制台的“设置”页面找到其值。ARN 遵循服务授权参考中 Organizations 资源类型部分记录的模式。

KMS 密钥 ARN

您可以在控制台中找到 KMS 密钥的 ARN。 Amazon KMS 在左侧选择“客户自主管理型密钥”，单击要查找 ARN 的密钥，您将在“常规配置”部分看到它。ARN 遵循《服务授权参考》 Amazon KMS 资源类型部分中记录的模式。

有关中的密钥策略 Amazon KMS 和疑难解答 Amazon KMS 权限的更多信息，请参阅《 Amazon Key Management Service 开发人员指南》。有关 IAM 策略及其 JSON 表示的更多信息，请参阅 IAM 用户指南。

基准 KMS 密钥策略

以下 KMS 密钥策略涵盖了最常见的部署场景：具有委派管理员和托 Amazon 管应用程序（包括 Amazon Control Tower Amazon EC2 实例的 SSO）的 IAM 身份中心实例和自定义工作流程。在为

IAM Identity Center 创建客户托管的 KMS 密钥时，请使用此策略作为起点。如果您需要更精细的访问控制，例如将密钥限制为特定的 IAM Identity Center 实例或应用程序，请参阅高级 KMS 密钥策略语句。请注意，如果使用多区域密钥，则应在所有副本上使用相同的策略，以帮助确保一致的授权。

要使用此策略，请将以下占位符值替换为您自己的占位符值：

- *111122223333*— 您的 Amazon IAM 身份中心实例（ Amazon Organizations 管理账户）的账户 ID。
- *444455556666*— 您的委托管理 Amazon 账户的账户 ID。如果您不使用委托管理，请移除此委托人。

由于 Amazon IAM Identity Center 要求将 KMS 密钥与服务放在同一个 Amazon 账户中，因此以下语句使用`${aws:ResourceOrgID}`和`${aws:ResourceAccount}`变量而不是文字值。如果您愿意，可以将这些变量替换为您的 Amazon 组织 ID 和 Amazon 账户 ID。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowIdentityCenterAdminAccounts",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:root",
          "arn:aws:iam::444455556666:root"
        ]
      },
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Sid": "AllowIdentityCenterAndIdentityStoreToDescribeKey",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "identitystore.amazonaws.com",
          "sso.amazonaws.com"
        ]
      },
      "Action": "kms:DescribeKey",
      "Resource": "*",
```

```
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid": "AllowIdentityCenterAndIdentityStoreToUseKey",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "identitystore.amazonaws.com",
          "sso.amazonaws.com"
        ]
      },
      "Action": [
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "${aws:ResourceAccount}"
        },
        "ForAnyValue:StringEquals": {
          "kms:EncryptionContextKeys": [
            "aws:sso:instance-arn",
            "aws:identitystore:identitystore-arn"
          ]
        }
      }
    },
    {
      "Sid": "AllowOrgPrincipalsViaIdentityCenterAndIdentityStore",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgID": "${aws:ResourceOrgID}"
        },
```

```
        "StringLike": {
          "kms:ViaService": [
            "sso.*.amazonaws.com",
            "identitystore.*.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals": {
          "kms:EncryptionContextKeys": [
            "aws:sso:instance-arn",
            "aws:identitystore:identitystore-arn"
          ]
        }
      }
    },
    {
      "Sid": "AllowManagedApps",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "Bool": {
          "aws:PrincipalIsAWSService": "true"
        },
        "StringEquals": {
          "aws:SourceOrgID": "${aws:ResourceOrgID}"
        },
        "StringLike": {
          "kms:ViaService": [
            "identitystore.*.amazonaws.com",
            "sso.*.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals": {
          "kms:EncryptionContextKeys": [
            "aws:sso:instance-arn",
            "aws:identitystore:identitystore-arn"
          ]
        }
      }
    }
  ]
}
```

本政策包含五项声明。下表描述了每条语句的作用。

语句	用途
AllowIdentityCenterAdminAccounts	向 IAM Identity Center 管理账户和委托管理账户授予完整 KMS 密钥权限。这包括密钥管理操作，例如修改密钥策略和安排密钥删除。如果这些账户中的管理员在基于身份的策略中拥有所需的权限，则可以管理和使用密钥。
AllowIdentityCenterAndIdentityStoreToDescribeKey	允许 IAM 身份中心和身份存储服务委托人检索密钥元数据。这是在不执行加密或解密的情况下验证密钥的服务操作所必需的。该`aws:SourceAccount` 条件有助于确保只有您的 IAM 身份中心实例才能使用您的 KMS 密钥。
AllowIdentityCenterAndIdentityStoreToUseKey	允许 IAM Identity Center 和 Identity Store 服务委托人使用密钥进行加密操作，例如加密、解密和重新加密数据。该`aws:SourceAccount` 条件有助于确保只有您的 IAM 身份中心实例才能使用您的 KMS 密钥。
AllowOrgPrincipalsViaIdentityCenterAndIdentityStore	允许 Amazon 组织中的 IAM 委托人通过 IAM 身份中心和身份存储服务解密数据。这包括使用转发访问会话 (FAS) 与 IAM Identity Cent Amazon er 集成的服务进行交互的应用程序管理员。
AllowManagedApps	允许 Amazon 托管应用程序通过 IAM 身份中心和身份存储解密受您的 KMS 密钥保护的数据。

使用以下 IAM 政策声明步骤 4：为 KMS 密钥的跨账户使用配置 IAM 策略，允许委托的管理员通过 IAM 身份中心服务使用 KMS 密钥 APIs。将示例密钥 ARN 替换为实际的 KMS 密钥 ARN。示例中的通配符区域可容纳多区域 KMS 密钥的所有副本。

对于 IAM Identity Center 管理以外的跨账户用例，例如 Amazon EC2 实例的 SSO 或 Amazon 托管应用程序的管理，请将范围`AllowCrossAccountKMSKeyUse`缩小到`kms:Decrypt`仅限并删除该`AllowListKMSKeyAliases`声明。

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

```
    {
      "Sid": "AllowCrossAccountKMSKeyUse",
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:DescribeKey"
      ],
      "Resource": [
        "arn:aws:kms:*:111122223333:key/mrk-1234abcd-12ab-34cd-56ef-1234567890ab"
      ]
    },
    {
      "Sid": "AllowListKMSKeyAliases",
      "Effect": "Allow",
      "Action": "kms:ListAliases",
      "Resource": "*"
    }
  ]
}
```

高级 KMS 密钥策略语句

使用高级 KMS 密钥策略语句为客户自主管理型 KMS 密钥实施更细粒度的访问控制。这些策略在 基准 KMS 密钥策略 的基础上，通过添加加密上下文条件和特定于服务的限制来构建。在决定是否使用高级 KMS 密钥策略语句之前，请务必查看相关的注意事项。

使用加密上下文限制访问

通过向中的AllowOrgPrincipalsViaIdentityCenterAndIdentityStore和AllowManagedApps语句添加加密上下文条件，您可以将 KMS 密钥的使用限制为特定的 IAM Identity Center 实例基准 KMS 密钥策略。将以下条件与您的特定身份中心实例 ARN 和身份存储 ARN 一起添加。您还可以将相同的加密上下文条件添加到为 KMS 密钥跨账户使用而配置的 IAM 策略中。

身份中心

```
"StringEquals": {
    "kms:EncryptionContext:aws:sso:instance-arn":
 "arn:aws:sso:::instance/ssoins-1234567890abcdef"
```

```
}
```

Identity Store

```
"StringEquals": {
    "kms:EncryptionContext:aws:identitystore:identitystore-arn":
 "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
}
```

如果您在查找这些标识符时需要帮助，请参阅在哪里可以找到所需的标识符。

> **Note**
>
> 您只能将客户自主管理型 KMS 密钥与 IAM Identity Center 的组织实例一起使用。客户托管的密钥必须位于 Amazon 组织的管理账户中，这有助于确保该密钥用于单个 IAM Identity Center 实例。但是，加密上下文机制为单实例使用提供了独立的技术保障。您还可以在用于 Identity Center 和 Identity Store 服务主体的 KMS 密钥策略语句中使用 `aws:SourceArn` 条件键。

实施加密上下文条件的注意事项

在实施加密上下文条件之前，请查看这些要求：

- DescribeKey 行动。加密上下文不能应用于 “kms:DescribeKey” 操作，IAM Identity Center 管理员可以使用该操作。配置 KMS 密钥策略时，请排除此特定操作的加密上下文，以确保 IAM Identity Center 实例的正常运行。
- 新实例设置。如果您正在使用客户自主管理型 KMS 密钥启用新的 IAM Identity Center 实例，请参阅客户自主管理型 KMS 密钥和高级 KMS 密钥策略的注意事项。
- 身份源更改。将身份源更改为 Active Directory 或从 Active Directory 更改时，需要特别注意加密上下文。请参阅更改身份源的注意事项。

策略模板

根据您的安全要求从这些高级策略模板中选择。在细粒度访问控制与其引入的管理开销之间取得平衡。

此处涵盖的主题：

- 用于特定 IAM Identity Center 实例只读使用的 KMS 策略语句。本节展示了使用加密上下文对 IAM Identity Center 进行只读访问。
- 完善了用于 Amazon 托管应用程序的 KMS 密钥策略声明。 本节演示如何使用加密上下文和应用程序信息（例如应用程序服务主体、应用程序 ARN 和 Amazon 账户 ID）完善 Amazon 托管应用程序的 KMS 密钥策略。

用于特定 IAM Identity Center 实例只读使用的 KMS 策略语句

此策略允许安全审计员和其他仅需要对 IAM Identity Center 进行读取访问的人员使用 KMS 密钥。

要使用此策略：

1. 将示例只读管理员 IAM 主体替换为您的实际管理员 IAM 主体
2. 将示例 IAM Identity Center 实例 ARN 替换为您的实际实例 ARN
3. 将示例 Identity Store ARN 替换为您的实际 Identity Store ARN
4. 如果使用委托管理，请参阅 步骤 4：为 KMS 密钥的跨账户使用配置 IAM 策略

如果您需要帮助来查找这些标识符的值，请参阅在哪里可以找到所需的标识符。

使用您的值更新模板后，返回到 步骤 2：准备 KMS 密钥策略语句，以根据需要准备其他 KMS 密钥策略语句。

单独的 “ kms:解密” 操作并不能限制只读操作的访问权限。IAM 策略必须对 IAM 身份中心服务强制执行只读访问权限 APIs。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowReadOnlyAccessToIdentityCenterAPI",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyAdminRole"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
```

```
          "kms:EncryptionContext:aws:sso:instance-arn":
 "arn:aws:sso:::instance/ssoins-1234567890abcdef"
        }
      }
    },
    {
      "Sid": "AllowReadOnlyAccessToIdentityStoreAPI",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyAdminRole"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn":
 "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
        }
      }
    }
  ]
}
```

完善了用于 Amazon 托管应用程序的 KMS 密钥策略声明

这些策略模板可以更精细地控制哪些 Amazon 托管应用程序可以使用您的 KMS 密钥。

> **Note**
>
> 某些 Amazon 托管应用程序不能与配置了客户托管 KMS 密钥的 IAM 身份中心一起使用。请参阅可与 IAM Identity Center 搭配使用的Amazon 托管应用程序。

基准 KMS 密钥策略允许来自同一 Amazon 组织中任何账户的任何 Amazon 托管应用程序使用 KMS 密钥。使用这些精细化策略通过以下方式限制访问：

- 应用程序服务主体
- 应用程序实例 ARNs
- Amazon account IDs
- 特定 IAM Identity Center 实例的加密上下文

> **Note**
>
> 服务主体是服务的唯一标识符，通常格式为 servicename.amazonaws.com（例如，亚马逊 EMR 的 elasticmapreduce.amazonaws.com）。 Amazon

按账户限制

此 KMS 密钥策略声明模板允许特定 Amazon 账户中的 Amazon 托管应用程序通过特定的 IAM Identity Center 实例使用 KMS 密钥。

要使用此策略：

1. 将示例服务主体替换为您的实际应用程序服务主体
2. 将示例账户 IDs 替换为部署 Amazon 托管应用程序 IDs 的实际账户
3. 将示例 Identity Store ARN 替换为您的实际 Identity Store ARN
4. 将示例 IAM Identity Center 实例 ARN 替换为您的实际实例 ARN

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowServiceInSpecificAccountsToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "Service": "myapp.amazonaws.com"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": [
            "111122223333",
            "444455556666"
          ]
        },
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/
ssoins-1234567890abcdef"
```

```
        },
        "Bool": {
          "aws:PrincipalIsAWSService": "true"
        }
      }
    },
    {
      "Sid": "AllowServiceInSpecificAccountsToUseTheKMSKeyViaIdentityStore",
      "Effect": "Allow",
      "Principal": {
        "Service": "myapp.amazonaws.com"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": [
            "111122223333",
            "444455556666"
          ]
        },
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn":
 "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
        },
        "Bool": {
          "aws:PrincipalIsAWSService": "true"
        }
      }
    }
  ]
}
```

按应用程序实例限制

此 KMS 密钥策略声明模板允许特定的 Amazon 托管应用程序实例通过特定的 IAM Identity Center 实例使用 KMS 密钥。

要使用此策略：

1. 将示例服务主体替换为您的实际应用程序服务主体
2. 将示例应用程序 ARN 替换为您的实际应用程序实例 ARN

3. 将示例 Identity Store ARN 替换为您的实际 Identity Store ARN

4. 将示例 IAM Identity Center 实例 ARN 替换为您的实际实例 ARN

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSpecificAppInstanceToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "Service": "myapp.amazonaws.com"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceARN": "arn:aws:myapp:us-east-1:111122223333:application/my-
application"
        },
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/
ssoins-1234567890abcdef"
        },
        "Bool": {
          "aws:PrincipalIsAWSService": "true"
        }
      }
    },
    {
      "Sid": "AllowSpecificAppInstanceToUseTheKMSKeyViaIdentityStore",
      "Effect": "Allow",
      "Principal": {
        "Service": "myapp.amazonaws.com"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceARN": "arn:aws:myapp:us-east-1:111122223333:application/my-
application"
        },
```

```
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn":
 "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
        },
        "Bool": {
          "aws:PrincipalIsAWSService": "true"
        }
      }
    }
  ]
}
```

客户自主管理型 KMS 密钥和高级 KMS 密钥策略的注意事项

在 IAM Identity Center 中实施客户自主管理型 KMS 密钥时，请考虑这些影响加密配置的设置、安全性和持续维护的因素。

选择基线与高级 KMS 密钥策略语句的注意事项

在决定是否使用 高级 KMS 密钥策略语句 使 KMS 密钥权限更具体时，请考虑管理开销和组织的安全需求。更具体的策略语句提供了对谁可以使用密钥以及用于什么目的的更细粒度控制；但是，随着 IAM Identity Center 配置的发展，它们需要持续维护。例如，如果您将 KMS 密钥的使用限制在特定的 Amazon 托管应用程序部署，则每当您的组织想要部署或取消部署应用程序时，都需要更新密钥策略。限制较少的策略可减少管理负担，但可能会授予比安全要求更广泛的权限。

使用客户自主管理型 KMS 密钥启用新 IAM Identity Center 实例的注意事项

如果您使用 高级 KMS 密钥策略语句 中描述的加密上下文将 KMS 密钥的使用限制为特定的 IAM Identity Center 实例，则此处注意事项适用。

使用客户托管的 KMS 密钥启用新的 IAM 身份中心实例时，IAM 身份中心和身份存储 ARNs 要等到设置后才可用。您有以下选项：

- 暂时使用通用 ARN 模式，然后在实例启用 ARNs 后将其替换为完整模式。请记住根据需要在 StringEquals 和 StringLike运算符之间切换。
  - 对于 IAM Identity Center SPN：“arn:${Partition}:sso:::instance/*”。
  - 对于 Identity Store SPN：“arn:${Partition}:identitystore::${Account}:identitystore/*”。
- 临时在 ARN 中使用 "purpose:KEY_CONFIGURATION"。这仅适用于实例启用，并且必须替换为实际 ARN，您的 IAM Identity Center 实例才能正常运行。这种方法的优点是您不会忘记在实例启用后替换它。

- 对于 IAM Identity Center SPN，使用："arn:${Partition}:sso:::instance/purpose:KEY_CONFIGURATION"
- 对于 Identity Store SPN，使用："arn:${Partition}:identitystore::${Account}:identitystore/purpose:KEY_CONFIGURATION"

> **Important**
>
> 不要将此配置应用于已在现有 IAM Identity Center 实例中使用的 KMS 密钥，因为这可能会中断其正常操作。

- 在实例启用之前，从 KMS 密钥策略中省略加密上下文条件。

为资源添加标签 Amazon IAM Identity Center

标签是一种自定义属性标签，您可以将其添加到 Amazon 资源中，以便于识别、组织和搜索资源。每个 标签具有两个部分：

- 标签键（例如，`CostCenter`、`Environment` 或 `Project`）。标签键最大长度可为 128 个字符，且不区分大小写。
- 标签值（例如，`111122223333` 或 `Production`）。标签值的最大长度可为 256 个字符，与标签键一样区分大小写。可以将标签的值设为空的字符串，但是不能将其设为空值。省略标签值与使用空字符串效果相同。

标签可帮助您识别和整理 Amazon 资源。许多 Amazon 服务都支持标记，因此您可以为来自不同服务的资源分配相同的标签，以表明这些资源是相关的。例如，您可以将相同的标签分配给 IAM Identity Center 实例中的特定权限集。有关标记策略的更多信息，请参阅Amazon Web Services 一般参考 指南中的标记 Amazon 资源和标记最佳实践。

除了使用标签识别、组织和跟踪您的 Amazon 资源外，您还可以使用 IAM 策略中的标签来帮助控制谁可以查看您的资源并与之交互。要了解有关使用标签控制访问权限的更多信息，请参阅 IAM 用户指南中的使用标签控制对 Amazon 资源的访问权限。例如，您可以允许用户更新 IAM Identity Center 权限集，但前提是 IAM Identity Center 权限集具有带有该用户名称值的 `owner` 标签。

您只能将标签应用于权限集。您不能将标签应用于 IAM Identity Center 在中创建的相应角色 Amazon Web Services 账户。您可以使用 IAM 身份中心控制台 Amazon CLI 或 IAM 身份中心 APIs 为权限集添加、编辑或删除标签。

以下部分提供有关 IAM Identity Center 标签的更多信息。

主题

标签限制

以下基本限制适用于 IAM Identity Center 资源上的标签：

- 您可以分配给资源的最大标签数量为 50。
- 最大键长度为 128 个 Unicode 字符。
- 最大值长度为 256 个 Unicode 字符。
- 标签键和值的有效字符为：

  a-z、A-Z、0-9、空格和以下字符：_ 。 : / = + - 和 @
- 键和值区分大小写。
- 请不要使用 `aws:` 作为键的前缀；它保留为供 Amazon 使用

使用 IAM Identity Center 控制台管理标签

您可以使用 IAM Identity Center 控制台添加、编辑和删除与您的实例或权限集关联的标签。

要管理 IAM Identity Center 控制台的权限集标签

1. 打开 IAM Identity Center 控制台。
2. 选择权限集。
3. 选择包含您要管理的标签的权限集的名称。
4. 在权限选项卡上的标签下，执行以下操作之一，然后继续执行下一步：
   a. 如果已为此权限集分配标签，请选择编辑标签。
   b. 如果没有标签分配给此权限集，请选择添加标签。
5. 对于每个新标签，在键和值（可选）列中键入值。在完成后，选择保存更改。

要删除标签，请在要删除的标签旁边的删除列中选择 X。

要管理 IAM Identity Center 实例的标签

1. 打开 IAM Identity Center 控制台。
2. 选择设置。
3. 选择标签选项卡。
4. 对于每个标签，在键和值（可选）字段中键入值。完成后，选择添加新标签按钮。

要移除标签，请选择要移除的标签旁的移除按钮。

Amazon CLI 例子

Amazon CLI 提供了可用于管理分配给权限集的标签的命令。

分配标签

使用以下命令将标签分配给您的权限集。

Example **`tag-resource`** 权限集命令

使用 `sso` 命令集中的 `tag-resource` 将标签分配给权限集：

```
$ aws sso-admin tag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tags Stage=Test
```

此命令包含以下参数：

- `instance-arn`——将在其下运行操作的 IAM Identity Center 实例的 Amazon 资源名称 (ARN)。
- `resource-arn`——具有要列出的标签的资源的 ARN。
- `tags` – 标签的键值对。

要一次分配多个标签，请以逗号分隔的列表形式指定它们：

```
$ aws sso-admin tag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tags Stage=Test,CostCenter=80432,Owner=SysEng
```

查看标签

使用以下命令查看您已分配给权限集的标签。

Example **`list-tags-for-resource`** 权限集命令

使用 `sso` 命令集中的 `list-tags-for-resource` 查看分配给权限集的标签：

```
$ aws sso-admin list-tags-for-resource --resource-arn sso-resource-arn
```

移除标签

使用以下命令从权限集中删除标签。

Example **`untag-resource`** 权限集命令

通过在 `sso` 命令集中使用 `untag-resource` 从权限集中删除标签：

```
$ aws sso-admin untag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tag-keys Stage CostCenter Owner
```

对于 `--tag-keys` 参数，指定一个或多个标签键，但不包含标签值。

创建权限集时应用标签

在创建权限集时使用以下命令分配标签。

Example **`create-permission-set`** 命令以及标签

使用 `create-permission-set` 命令创建权限集时，可以通过 `--tags` 参数指定标签：

```
$ aws sso-admin create-permission-set \
> --instance-arn sso-instance-arn \
> --name permission=set-name \
> --tags Stage=Test,CostCenter=80432,Owner=SysEng
```

使用 IAM Identity Center API 管理标签

使用以下 API 操作来分配、查看和删除权限集或 IAM Identity Center 实例的标签。

- TagResource
- ListTagsForResource
- UntagResource
- CreatePermissionSet
- CreateInstance

将 Amazon CLI 与 IAM 身份中心集成

Amazon 命令行界面 (CLI) 第 2 版与 IAM 身份中心的集成简化了登录过程。开发人员可以使用通常用于登录 IAM Identity Center 的 Active Directory 或 IAM 身份中心凭证直接登录，并访问分配给他们的账户和角色。 Amazon CLI 例如，管理员将 IAM Identity Center 配置为使用 Active Directory 进行身份验证后，开发人员可以使用其 Active Directory 凭证 Amazon CLI 直接登录。

Amazon 与 IAM 身份中心的 CLI 集成具有以下好处：

- 通过使用 Amazon Directory Service将 IAM Identity Center 连接到其 Active Directory，企业可以让其开发人员使用来自 IAM Identity Center 或 Active Directory 的凭证进行登录。
- 开发人员可以从 CLI 登录以加快访问速度。
- 开发人员可以列出他们已分配访问权限的帐户和角色并在它们之间进行切换。
- 开发人员可以在 CLI 配置中自动生成和保存命名角色配置文件，并在 CLI 中引用它们以在所需的帐户和角色中运行命令。
- CLI 自动管理短期凭证，因此开发人员可以不间断地安全地启动并停留在 CLI 中，并运行长时间运行的脚本。

如何将 Amazon CLI 与 IAM 身份中心集成

要使用 Amazon CLI 与 IAM 身份中心的集成，请下载、安装和配置 Amazon Command Line Interface 版本 2。有关如何下载并 Amazon CLI 与 IAM 身份中心集成的详细步骤，请参阅Amazon Command Line Interface 用户指南中的配置 Amazon CLI 以使用 IAM 身份中心。

Amazon Web Services 管理控制台 私有访问注意事项

如果您的组织使用 Amazon Web Services 管理控制台 私有访问功能，则应考虑您的用户将如何登录 IAM Identity Center。

VPC 终端节点策略限制了对管理控制台的登录，这会阻止您的用户登录 Amazon Web Services 账户 他们无权访问。有关更多信息，请参阅《Amazon Web Services 管理控制台 Getting Started Guide》中的 Amazon Web Services 管理控制台 Private Access。

VPC 端点阻止登录 IAM Identity Center

请务必注意，使用 VPC 端点会阻止登录 IAM Identity Center。当用户已经通过 VPC 端点登录到管理控制台时，就会发生这种情况。为确保可以继续登录 IAM Identity Center，用户必须使用公共端点而不是 VPC 端点登录 Amazon 。

IAM Identity Center 中的配额和限制

下表描述了 IAM Identity Center 内的配额。配额增加请求必须来自管理帐户或委托管理员帐户。要增加配额，请参阅请求增加配额。

> **Note**
>
> 如果您拥有超过 50,000 个用户、10,000 个群组或 500 个权限集，我们建议您使用 Amazon CLI 和 APIs 管理 IAM 身份中心。有关 CLI 的更多信息，请参阅 将 Amazon CLI 与 IAM 身份中心集成。有关更多信息 APIs，请参阅欢迎来到 IAM 身份中心 API 参考。

应用程序配额

资源	默认配额	能否增加
服务提供商 SAML 证书的文件大小（采用 PEM 格式）	2KB	否
SAML 断言限制	50000 个字符	否
上传到 IAM Identity Center 的 IdP 证书的文件大小限制	2500 (UTF-8) 个字符	否
每个应用程序的访问范围	25	否

Amazon Web Services 账户 配额

资源	默认配额	能否增加
IAM Identity Center 中允许的权限集合数	3500	是
每组允许的已配置权限集数量 Amazon Web Services 账户	500	是

资源	默认配额	能否增加
每个权限集合中的内联策略数	1	否
每个权限集的 Amazon 托管策略和客户托管策略数量	25 [1]	否
每个权限集合中内联策略的最大大小	32,768 字节。 每个权限集的内联策略中非空格字符的最大大小为 10,240 字节。	否
中可以同时更新的 IAM 角色（权限集）的数量 Amazon Web Services 账户	1	否

[1]Amazon Identity and Access Management (IAM) 为每个角色设置 10 个托管策略的配额。要利用此配额，请在 Service Quotas 控制台中为每个要部署权限集 Amazon Web Services 账户 的地方申请增加附加到 IAM 角色的 IAM 配额托管策略。

> **Note**
>
> Amazon Web Services 账户 使用权限集进行管理 Amazon Web Services 账户 作为 IAM 角色进行配置，或者在中使用现有 IAM 角色 Amazon Web Services 账户，因此遵守 IAM 配额。有关与 IAM 角色关联的配额的更多信息，请参阅 IAM 和 STS 配额。

Active Directory 配额

资源	默认配额	能否增加
您可以一次拥有的连接目录数量	1	否

IAM Identity Center 身份存储配额

资源	默认配额	能否增加
IAM Identity Center 中支持的用户数	200000	是
IAM Identity Center 中支持的组数	100000	是
可用于评估用户权限的唯一组数量	1000	否

IAM Identity Center 节流限制

资源	默认配额
IAM 身份中心 APIs	IAM Iden APIs tity Center 的集体限制为每秒 20 笔交易 (TPS)。为了便于阅读 APIs，您可以打开支持案例以请求提高限制。CreateAccountAssignment写入 API 的未完成异步调用限制为 15 个。不能提高此限制。
身份存储 APIs	Ident@@ ity Store APIs 对每个 API 的限制为每秒 20 笔交易 (TPS)。此限制适用于每个身份存储实例。您可以提交支持案例，请求提高限额。
SCIM APIs	SCIM APIs 对每个 API 的写入 APIs 限制为每秒 25 个事务 (TPS)，读取限制为 40 TPS。 APIs 这些限制适用于每个身份存储实例。您可以提交支持案例，请求提高限额。 每个 Identity Store 中的每个成员资格操作`CreateGroup` 或`PatchGroup` 调用都算作一次交易，以达到每个身份存储区单独的成员资格操作限制限制。

如果您的 IAM Identity Center 实例以多个方式启用 Amazon Web Services 区域，则限制限制同样适用于每个已启用的区域。例如，您将在每个启用区域的身份存储 APIs 上限为 20 TPS。有关其他区域提供哪些 API 操作的更多信息，请参阅相应的表格。

OIDC 服务请求配额

资源	默认值（每秒请求数）	能否增加
从远程地址请求速率以注册公共 OAuth 客户端 适用于：RegisterClient	20	是
来自向 OIDC 服务注册的公共客户端的请求速率 适用于：CreateToken，StartDeviceAuthorization	80	是
来自向同一 IAM Identity Center 实例注册的所有公共客户端的请求速率 适用于：CreateToken	250	是
通过令牌交换和刷新令牌授权，向在 IAM 身份中心实例中注册的 IAM 身份中心应用程序请求费率。 适用于：CreateTokenWithIAM	80	是
使用 JWT Bearer 授权方式，来自向同一 IAM Identity Center 实例注册的所有 IAM Identity Center 应用程序的令牌生成速率	10	联系 Supp Amazon ort

资源	默认值（每秒请求数）	能否增加
适用于：CreateTokenWithIAM		

如果您的 IAM Identity Center 实例以多个方式启用 Amazon Web Services 区域，则上述请求费率同样适用于每个已启用的区域。例如，如果您允许从远程地址注册公共 OAuth 客户端的请求速率为每秒 20 个请求，则每个启用的区域都可以使用此吞吐量。有关其他区域提供哪些 API 操作的更多信息，请参阅相应的表格。

其他配额

资源	默认配额	能否增加
可以配置的 Amazon Web Services 账户 或应用程序总数 ***	3000	是
每个账户的 IAM Identity Center 实例总数	1	否
可信令牌发布者总数	10	否
可以分配给每个 Amazon Web Services 账户权限集或应用程序的组总数	100	否
为单个 IAM 身份中心实例 Amazon Web Services 区域 启用的总数	3	是

* 例如，您可能配置了 2750 个账户和 250 个应用程序，总共有 3000 个账户和应用程序。

** ProvisionPermissionSet API 操作使用 ALL_PROVISIONED_ACCOUNTS 选项时，最多可向 3500 个 Amazon Web Services 账户预置权限集。如果需向超过 3500 个 Amazon Web Services 账户预置权限集，可使用带有 Amazon_ACCOUNT 选项的 ProvisionPermissionSet API 操作（单次向

一个 Amazon Web Services 账户预置权限集）。您最多可以同时调用 `ProvisionPermissionSet` 三次。

排查 IAM Identity Center 问题

以下内容可帮您排查在设置或使用 IAM Identity Center 控制台时可能会遇到的一些常见问题。

创建 IAM Identity Center 账户实例时出现的问题

创建 IAM Identity Center 账户实例时可能会遇到一些限制。如果您无法通过 IAM Identity Center 控制台创建账户实例，或者无法通过支持的 Amazon 托管应用程序的设置体验来创建账户实例，请验证以下用例：

- Amazon Web Services 区域 Amazon Web Services 账户 在您尝试创建账户实例时查看其他。每个 Amazon Web Services 账户仅限创建一个 IAM Identity Center 实例。要启用该应用程序，请切换到 Amazon Web Services 区域 带有 IAM 身份中心实例的，或者切换到没有 IAM 身份中心实例的账户。
- 如果组织在 2023 年 9 月 14 日之前启用了 IAM Identity Center，管理员可能需要选择启用账户实例创建功能。请与您的管理员合作，在管理账户中通过 IAM Identity Center 控制台启用账户实例创建功能。
- 您的管理员可能创建了服务控制策略，以限制 IAM Identity Center 账户实例的创建。请与您的管理员合作，将您的账户添加到允许列表中。

尝试查看已预先配置为与 IAM Identity Center 结合使用的云应用程序列表时收到错误消息

当您的策略允许`sso:ListApplications`但不允许其他 IAM 身份中心时，就会发生以下错误 APIs。请更新策略，以解决此错误。

该`ListApplications`权限授权多个 APIs：

- `ListApplications` API。
- 一个与 IAM Identity Center 控制台中使用的 `ListApplicationProviders` API 类似的内部 API。

为了帮助解决重复问题，此内部 API 现在也会授权使用 `ListApplicationProviders` 操作。要允许公共 `ListApplications` API，但拒绝内部 API，您的策略必须加入一条声明，用来拒绝 `ListApplicationProviders` 操作：

```
      "Statement": [
    {
         "Effect": "Deny",
         "Action": "sso:ListApplicationProviders",
         "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": "sso:ListApplications",
        "Resource": "<instanceArn>" // (or "*" for all instances)
    }
]
```

要允许内部 API，但拒绝 `ListApplications`，该策略需要仅允许 `ListApplicationProviders`。如果未明确允许，`ListApplications` API 将被拒绝。

```
      "Statement": [
    {
         "Effect": "Allow",
         "Action": "sso:ListApplicationProviders",
         "Resource": "*"
    }
]
```

当您的政策更新后，请联系 Amazon Web Services 支持 以取消此主动措施。

与 IAM Identity Center 创建的 SAML 断言内容有关的问题

当从访问 Amazon Web Services 账户 门户访问 SAML 应用程序时，IAM Identity Center 为 IAM Identity Center 创建和发送的 SAML 断言（包括这些断言中的属性）提供基于 Web 的调试体验。Amazon Web Services 要查看 IAM Identity Center 生成的 SAML 断言的详细信息，请使用以下步骤。

1. 登录 Amazon Web Services 访问门户。
2. 在您登录到门户后，按住 Shift 键，选择相应的应用程序磁贴，然后松开 Shift 键。
3. 检查名为 You are now in administrator mode (您当前处于管理员模式) 的页面上的信息。要保留这些信息以备将来参考，请选择复制 XML，然后将内容粘贴到其他地方。
4. 选择发送至 <应用程序>继续。此选项将断言发送给服务提供商。

> **Note**
>
> 有些浏览器配置和操作系统可能不支持此步骤。已经在 Windows 10 上使用 Firefox、Chrome 和 Edge 浏览器对此步骤进行了测试。

特定用户无法从外部 SCIM 提供商同步到 IAM Identity Center

如果身份提供者（IdP）配置为使用 SCIM 同步将用户预置到 IAM Identity Center，则在用户预置过程中可能会发生同步失败。这可能表明 IdP 中的用户配置与 IAM Identity Center 要求不兼容。发生这种情况时，IAM Identity Center SCIM APIs 将返回错误消息，提供对问题根本原因的见解。您可以在 IdP 的日志或 UI 中找到这些错误消息。您也可以在 Amazon CloudTrail 日志中找到有关预置失败的更多详细信息。

有关 IAM Identity Center SCIM 实现的更多信息，包括用户对象的必要、可选和不支持参数及操作的规范，请参阅《SCIM Developer Guide》中的 IAM Identity Center SCIM Implementation Developer Guide

以下是导致此错误的几个常见原因：

1. IdP 中的用户对象缺少名字（给定）、姓氏（家族）和显示名称。 and/or

   错误消息：“检测到 2 个验证错误：值*'name.givenName'*未能满足约束：成员必须满足正则表达式模式：[\\ p {L}\\ p {M}\\ p {S}\\ p {N}\\ p {N}\\ t\\ n\\ n\\ r] +；*'name.givenName'*无法满足约束条件的值：成员的长度必须大于或等于 1"

   - 解决方案：为用户对象添加名字、姓氏和显示名称。此外，请确保将 IdP 中用户对象的 SCIM 预调配映射配置为发送所有这些属性的非空值。
2. 正在向用户发送单个属性的多个值（也称为“多值属性”）。例如，用户可能在 IdP 中同时指定了工作电话号码和家庭电话号码，或者有多个电子邮件或实际地址，并且您的 IdP 配置为尝试同步该属性的多个或全部值。

   错误消息：“列表属性*emails*超过允许的限制 1”

   - 解决方案选项：

     i. 更新 IdP 中用户对象的 SCIM 预调配映射，仅发送给定属性的单个值。例如，配置仅发送每个用户工作电话号码的映射。

ii. 如果可以安全地从 IdP 中的用户对象移除其他属性，则可以移除其他值，为用户的该属性保留一个或零个值。

iii. 如果中的任何操作都不需要该属性 Amazon，请从 IdP 用户对象的 SCIM 配置映射中移除该属性的映射。

3. 您的 IdP 正在尝试根据多个属性匹配目标（在本例中为 IAM Identity Center）中的用户。由于保证用户名在给定的 IAM Identity Center 实例中是唯一的，因此您只需指定 `username` 作为用于匹配的属性即可。

   - 解决方案：确保您的 IdP 中的 SCIM 配置仅使用单个属性与 IAM Identity Center 中的用户进行匹配。例如，将 IdP 中的 `username` 或 `userPrincipalName` 映射到 SCIM 中用于预调配到 IAM Identity Center 的 `userName` 属性将是正确的，并且足以满足大多数实施的需求。

使用外部身份提供者预置用户或组时出现重复用户或组错误

如果在外部身份提供者（IdP）中预置用户或组时遇到 IAM Identity Center 同步问题，可能是因为外部 IdP 用户或组没有唯一的属性值。您可能会在外部 IdP 中收到以下错误消息：

拒绝创建新的重复资源

您可能会在以下情况下遇到此问题：

- 方案 1
  - 您正在使用外部 IdP 中的自定义非唯一属性，作为 IAM Identity Center 中必须唯一的属性。现有的 IAM Identity Center 用户或组无法与 IdP 同步。
- 方案 2
  - 您尝试创建具有重复属性的用户，但这些属性在 IAM Identity Center 中必须是唯一的。
    - 例如，您创建或拥有一个具有以下属性的 IAM Identity Center 用户：
      - 用户名：Jane Doe
      - 主电子邮件地址：`jane_doe@example.com`
    - 然后，您可以尝试在外部 IdP 中创建另一个具有以下属性的用户：
      - 用户名：Richard Doe
      - 主电子邮件地址：`jane_doe@example.com`
        - 外部 IdP 尝试在 IAM Identity Center 中同步和创建用户。不过，这些操作会失败，因为两个用户的主电子邮件地址的值是重复的，但该地址必须是唯一值。

用户名、主电子邮件地址和 externalID 必须是唯一的，外部 IdP 用户才能成功同步到 IAM Identity Center。同理，组名称必须是唯一的，外部 IdP 组才能成功同步到 IAM Identity Center。

解决方案是审查身份源的属性并确保属性是唯一的。

当用户名采用 UPN 格式时，用户无法登录

根据用户在登录页面上输入用户名的格式，他们可能无法登录 Amazon Web Services 访问门户。在大多数情况下，用户可以使用其普通用户名、下级登录名 (DOMAIN\UserName) 或 UPN 登录名 () 登录用户门户。`UserName@Corp.Example.com`例外情况是，当 IAM Identity Center 使用已启用 MFA 且验证模式已设置为上下文感知或始终开启的连接目录时。在这种情况下，用户必须使用其向下登录名 (DOMAIN\UserName) 登录。有关更多信息，请参阅 Identity Center 目录用户的多重身份验证。有关用于登录 Active Directory 的用户名格式的一般信息，请参阅 Microsoft 文档网站上的用户名格式。

修改 IAM 角色时出现了“无法对受保护的角色执行操作”错误

在查看账户中的 IAM 角色时，您可能会注意到以 “AWSReservedSSO_” 开头的角色名称。这些角色是 IAM Identity Center 服务在帐户中创建的角色，它们来自向帐户分配权限集。尝试从 IAM 控制台中修改这些角色将导致以下错误：

```
'Cannot perform the operation on the protected role 'AWSReservedSSO_RoleName_Here' -
 this role is only modifiable by Amazon'
```

这些角色只能通过 IAM Identity Center 管理员控制台进行修改，该控制台位于的管理账户中 Amazon Organizations。修改完成后，您可以将更改推送到分配的 Amazon 帐户。

目录用户无法重置密码

当目录用户使用 “忘记密码？” 重置密码时 选项在登录 Amazon Web Services 访问门户期间，他们的新密码必须遵守默认密码策略，如中所在 IAM Identity Center 中管理身份时的密码要求述。

如果用户输入了符合策略的密码后收到错误`We couldn't update your password`，请检查是否 Amazon CloudTrail 记录了失败。这可以通过在 “事件历史记录” 控制台中搜索 CloudTrail 或使用以下过滤器来完成：

```
"UpdatePassword"
```

如果消息显示以下内容，则可能需要联系支持人员：

```
"errorCode": "InternalFailure",
      "errorMessage": "An unknown error occurred“
```

另一个可能造成此问题的原因是应用于用户名值的命名惯例。命名惯例必须遵循特定的模式，例如“surname.givenName”。但是，有些用户名可能很长，或者包含特殊字符，这可能会导致 API 调用中丢掉字符，从而导致错误。您可能需要尝试以同样的方式通过测试用户重置密码，以验证是否是这种情况。

如果问题依旧存在，请联系 Amazon 支持中心。

我的用户在权限集中被引用，但无法访问分配的帐户或应用程序

如果您使用跨域身份管理系统 (SCIM) 通过外部身份提供者进行自动预调配，则可能会出现此问题。具体而言，当删除用户或该用户所属的组，然后在身份提供者中使用相同的用户名（对于用户）或名称（对于组）重新创建时，将在 IAM Identity Center 中为新用户或组创建一个新的唯一内部标识符。但是，IAM Identity Center 的权限数据库中仍有对旧标识符的引用，因此用户或组的名称仍显示在用户界面 (UI) 中，但访问失败。这是因为 UI 引用的底层用户或组 ID 已不存在。

在这种情况下，要恢复 Amazon Web Services 账户 访问权限，您可以从最初分配给旧用户或组的 Amazon Web Services 账户访问权限中移除访问权限，然后将访问权限重新分配给该用户或组。这会使用新用户或组的正确标识符更新权限集。同样，要恢复应用程序访问权限，您可以从该应用程序的已分配用户列表中删除该用户或组的访问权限，然后重新添加该用户或组。

您还可以通过在 CloudTrail 日志中搜索引用相关用户或组名称的 SCIM 同步事件来查看是否 Amazon CloudTrail 记录了故障。

我无法从正确配置的应用程序目录中获取我的应用程序

如果您通过 IAM Identity Center 的应用程序目录添加了应用程序，请注意，每一家服务提供商都提供了自己的详细文档。您可以在 IAM Identity Center 控制台中，通过该应用程序的配置选项卡访问这些信息。

如果问题与在服务提供商应用程序与 IAM Identity Center 之间设置信任有关，请务必参阅说明手册中的故障排除步骤。

当用户尝试使用外部身份提供者登录时显示错误信息“出现意外错误”

出现此错误的原因可能有多种，但其中一个常见原因是 SAML 请求中的用户信息与 IAM Identity Center 中的用户信息不匹配。

为了让 IAM Identity Center 用户在使用外部 IdP 作为身份源时成功登录，必须满足以下条件：

- SAML NameID 格式（在您的身份提供者处配置）必须为“电子邮件”
- NameID 值必须是格式正确 (RFC2822) 的字符串 (user@domain.com)
- nameID 值必须与 IAM Identity Center 中现有用户的用户名完全匹配（IAM Identity Center 中的电子邮件地址是否匹配并不重要，因为入站匹配基于用户名）
- SAML 2.0 联合身份验证的 IAM Identity Center 实施仅支持身份提供者与 IAM Identity Center 之间的 SAML 响应中的 1 个断言。它不支持加密的 SAML 断言。
- 如果您的 IAM Identity Center 帐户中启用了 访问控制属性，则以下陈述适用：
  - SAML 请求中映射的属性数量必须不超过 50。
  - SAML 请求不得包含多值属性。
  - SAML 请求不得包含多个具有相同名称的属性。
  - 该属性不得包含结构化的 XML 作为值。
  - 名称格式必须是 SAML 指定的格式，而不是通用格式。

> **Note**
>
> IAM Identity Center 不会通过 SAML 联合身份验证为新用户或组“及时”创建用户或组。这意味着必须在 IAM Identity Center 中手动或通过自动预调配预先创建用户，才能登录 IAM Identity Center。

当您的身份提供者中配置的断言使用者服务 (ACS) 端点与您的 IAM Identity Center 实例提供的 ACS URL 不匹配时，也可能发生此错误。确保这两个值完全匹配。

此外，您可以访问 Amazon CloudTrail 并筛选事件名称 “登录”，从而进一步解决外部身份提供商ExternalIdPDirectory登录失败的问题。

错误信息“无法启用访问控制的属性”

如果启用 ABAC 的用户没有启用 访问控制属性 所需的 `iam:UpdateAssumeRolePolicy` 权限，则可能会发生此错误。

当我尝试为 MFA 注册设备时，我收到“不支持浏览器”消息

WebAuthn 目前支持谷歌浏览器、Mozilla Firefox、Microsoft Edge 和苹果 Safari 网络浏览器以及 Windows 10 和安卓平台。 WebAuthn 支持的某些组成部分可能有所不同，例如跨macOS和iOS浏览器的平台身份验证器支持。如果用户尝试在不支持的浏览器或平台上注册 WebAuthn 设备，他们将看到某些不支持的选项显示为灰色，或者他们会收到一条错误消息，提示不支持所有支持的方法。在这些情况下，请参阅 FIDO2：Web 身份验证 (WebAuthn) 以获取有关 browser/platform 支持的更多信息。有关 WebAuthn IAM 身份中心的更多信息，请参阅FIDO2 身份验证器。

Active Directory“域用户”组无法正确同步到 IAM Identity Center

Active Directory 域用户组是 AD 用户对象的默认“主组”。IAM Identity Cente 无法读取 Active Directory 主组及其成员资格。分配对 IAM Identity Center 资源或应用程序的访问权限时，使用域用户组以外的组（或分配为主组的其他组），以便组成员资格正确反映在 IAM Identity Center 身份存储中。

MFA 无效凭证错误

在用户使用 SCIM 协议将其帐户完全预调配到 IAM Identity Center 之前，如果用户尝试使用外部身份提供者提供的帐户（例如 Okta 或 Microsoft Entra ID）登录 IAM Identity Center，就会发生此错误。将用户帐户预调配到 IAM Identity Center 后，应解决此问题。确认该帐户已预调配到 IAM Identity Center。如果没有，请检查外部身份提供者中的预调配日志。

尝试使用身份验证器应用程序注册或登录时，收到“出现意外错误”消息

基于时间的一次性密码（TOTP）系统（例如，IAM Identity Center 与基于代码的身份验证器应用程序搭配使用的那些系统），依赖客户端和服务器之间的时间同步。确保安装身份验证器应用程序的设备与可靠的时间源正确同步，或者在设备上手动设置时间以匹配可靠的来源，例如 NIST (https://www.time.gov/) 或其他 local/regional 等效设备。

我在尝试登录 IAM Identity Center 时收到“It's not you, it's us”错误

此错误表明 IAM Identity Center 实例或 IAM Identity Center 用作身份源的外部身份提供者（IdP）存在设置问题。建议验证以下各项：

- 验证用于登录的设备上的日期和时间设置。建议允许自动设置日期和时间。若不可行，建议将日期和时间同步到已知的网络时间协议（NTP）服务器。

- 验证上传到 IAM Identity Center 的 IdP 证书与 IdP 提供的证书相同。您可以通过导航到设置，从 IAM Identity Center 控制台查看证书。在身份源选项卡中选择操作，然后选择管理身份验证。如果 IdP 和 IAM Identity Center 证书不匹配，请将新证书导入 IAM Identity Center。
- 确保身份提供者元数据文件中的 NameID 格式如下：
  - `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`
- 如果您使用来自的 AD Connector Amazon Directory Service 作为身份提供商，请验证服务帐号的凭证是否正确且未过期。有关更多信息，请参阅 Update your AD Connector service account credentials in Amazon Directory Service。

我的用户没有收到来自 IAM Identity Center 的电子邮件

IAM Identity Center 服务发送的所有电子邮件都将来自地址 `no-reply@signin.aws` 或 `no-reply@login.awsapps.com`。必须配置电子邮件系统，以便接受来自这些发件人电子邮件地址的电子邮件，而不将其视为垃圾邮件或群发邮件。

错误：您无法delete/modify/remove/assign访问管理账户中配置的权限集

此消息表示该 委派管理 功能已启用，并且只有在 Amazon Organizations中具有管理账户权限的人员才能成功执行您之前尝试的操作。要解决此问题，请以具有这些权限的用户身份登录，并尝试再次执行任务，或者将此任务分配给具有正确权限的人员。有关更多信息，请参阅 注册成员帐户。

错误：未找到会话令牌或会话令牌无效

当客户端（例如 Web 浏览器）或尝试使用服务器端已撤消或 Amazon CLI失效的会话时，可能会发生此错误。 Amazon Toolkit要更正此问题，请返回到客户端应用程序或网站并重试，出现提示时还需要再次登录。这有时可能还需要您取消待处理的请求，例如来自 IDE 的 Amazon Toolkit 待处理连接尝试。

来自可信域的群组成员不会同步到 IAM 身份中心

如果安全组成功同步到 IAM Identity Center，但其来自可信本地域的成员未出现在 IAM Identity Center 中，则可能是该组所在 Amazon Managed Microsoft AD 且包含代表可信域用户的外国安全委托人 (FSPs) 所致。

请尝试以下步骤进行故障排除：

- 直接从可信域同步群组：与其同步包含跨域成员的群组 Amazon Managed Microsoft AD ，不如直接从受信任的本地域创建和同步群组。这种方法之所以奏效，是因为 IAM Identity Center 可以访问源域中的实际用户对象。
- 验证服务账号权限：确保 IAM Identity Center 服务账户对可信域中的用户对象具有所需的权限 ReadProperties 和 ListContents 权限。

对客户管理的密钥进行故障排除 Amazon IAM Identity Center

本主题介绍您在使用时可能遇到的与客户托管密钥相关的常见错误， Amazon IAM Identity Center 并提供了解决这些错误的故障排除步骤。

访问被拒绝：KMS 解密权限问题

错误：“用户 xxxxxxx 无权执行：对与此密文关联的资源进行 kms:解密，因为没有基于身份的策略允许解密操作” kms:

用户或 IAM 主体在其 IAM 策略或 KMS 密钥策略中缺少所需的 `kms:Decrypt` 权限。

使用 Amazon CloudTrail以下方法进行故障排除

1. 在中查找`kms.amazonaws.com`活动 CloudTrail
2. 搜索事件名称 `Decrypt`
3. 查看 `errorCode` 和 `errorMessage` 字段
4. 检查 `userIdentity` 以确认是哪个主体尝试了该操作

要解决此问题，请在该用户或 IAM 主体的 IAM 策略和 KMS 密钥策略中授予其 `kms:Decrypt` 访问权限。有关更多信息，请参阅 在中实现客户托管的 KMS 密钥 Amazon IAM Identity Center。

Amazon 在 IAM 身份中心启用客户托管 KMS 密钥后，托管应用程序登录失败

如果没有身份中心用户可以登录 Amazon 托管应用程序，并且您在 IAM Identity Center 实例中启用了客户托管的 KMS 密钥，请验证 KMS 密钥策略是否授予 Amazon 托管应用程序使用客户托管的 KMS 密钥的权限。有关更多信息，请参阅 基准 KMS 密钥策略。

Amazon 在 IAM Identity Center 中启用客户托管 KMS 密钥后，托管应用程序安装 and/or 用户分配失败

错误：“用户 xxxxxxx 无权执行：对与此密文关联的资源进行 kms:解密，因为没有基于身份的策略允许解密操作” kms:

用户或 IAM 主体在其 IAM 策略或 KMS 密钥策略中缺少所需的 `kms:Decrypt` 权限。

使用 CloudTrail以下方法进行故障排除

1. 搜索事件名称 `Decrypt`
2. 查看 `errorCode` 和 `errorMessage` 字段
3. 检查 `userIdentity` 以确认是哪个主体尝试了该操作

要解决此问题，请在该用户或 IAM 主体的 IAM 策略和 KMS 密钥策略中授予其 `kms:Decrypt` 访问权限。有关更多信息，请参阅 在中实现客户托管的 KMS 密钥 Amazon IAM Identity Center。

KMS 权限问题：使用配置客户托管密钥 Amazon IAM Identity Center

在启用客户自主管理型密钥时，用户或 IAM 主体缺少一个或多个必需的 KMS 权限（`kms:Decrypt`、`kms:Encrypt`、`kms:GenerateDataKey`、`kms:DescribeKey`）。

使用 CloudTrail以下方法进行故障排除

1. 搜索 `Decrypt`、`Encrypt`、`GenerateDataKey` 或 `DescribeKey` 事件
2. 查看 `errorCode` 和 `errorMessage` 字段
3. 检查 `userIdentity` 以确认是哪个主体尝试了该操作

要解决此问题，请在其基于身份的策略或 KMS 密钥策略中向用户或 IAM 主体授予所有必需的 KMS 权限。有关更多信息，请参阅 在中实现客户托管的 KMS 密钥 Amazon IAM Identity Center。

Amazon 在 IAM 身份中心启用客户托管 KMS 密钥后，访问门户登录失败

错误：“错误代码：0001- IdentityCenter 服务访问被阻止。请联系您的 IdentityCenter 管理员了解更多步骤。”

如果用户无法登录 Amazon 访问门户，并且您在 IAM Identity Center 实例中启用了客户托管的 KMS 密钥，请验证 KMS 密钥策略是否向身份中心和身份存储授予了必要的权限。有关更多信息，请参阅 基准 KMS 密钥策略。

中的多区域设置疑难解答 Amazon IAM Identity Center

本主题描述了您在使用时可能遇到的与多区域设置相关的常见错误， Amazon IAM Identity Center 并提供了解决这些错误的故障排除步骤。

我想要将我的 IAM 身份中心实例复制到的区域在 IAM 身份中心控制台中不可用

您必须先在要将 IAM Identity Center 实例复制到的区域中为客户托管的 KMS 密钥创建副本密钥。创建副本密钥后，您将在可供复制的区域列表中看到该区域。有关更多信息，请参阅 the section called “步骤 1：创建副本密钥”。

Amazon 其他区域的托管应用程序登录失败

如果在 IAM Identity Center 中添加区域后，没有一个 IAM Identity Center 用户可以登录其他区域的 Amazon 托管应用程序，请确认您在外部身份提供商中配置了该区域的断言消费者服务 (ACS) URL，如中所the section called “步骤 3：更新外部 IdP 设置”述。此外，请确认您的用户已连接到该区域。

文档历史记录

下表描述了 Amazon IAM Identity Center 文档的重要补充。我们还经常更新文档来处理发送给我们的反馈意见。

- 最新主要文档更新日期：2025 年 10 月 21 日

变更	说明	日期
简化的基准 KMS 密钥策略	将基准 KMS 密钥策略声明合并为一个简化的策略，简化了客户托管的 KMS 密钥的配置，用于静态加密。	2026年4月30日
多区域支持	增加了多区域支持，包括复制到其他区域、在其他区域 Amazon Web Services 账户 访问和使用 Amazon 托管应用程序。	2026 年 2 月 2 日
更新了 Amazon 托管策略	更新了`AWSIdentityCenterExternalManagementPolicy` Amazon 托管策略以更改置备租户的 ARN。	2025 年 12 月 5 日
新的 Amazon 托管策略主题	添加了`AWSIdentityCenterExternalManagementPolicy` Amazon 托管策略的详细信息。	2025 年 11 月 21 日
自动配置审计与协调指南	添加了有关使用 Identity Store 和命令审核和协调 SCIM 自动配置的用户、群组和群组成员资格的指南。 APIs Amazon CLI	2025 年 10 月 17 日

OIDC 服务请求配额	添加了 OIDC 服务请求配额，包括 OAuth 客户端注册、令牌创建和其他 OIDC 操作的速率限制。	2025 年 10 月 13 日
Amazon 托管策略的更新	IAM Identity Center 更新了托管策略`AWSSSOMasterAccountAdministrator` `AWSSSOMemberAccountAdministrator` `AWSSSOReadOnly` `AWSSSODirectoryAdministrator` 、、和，`AWSSSODirectoryReadOnly` 以包含使用客户托管密钥进行加密的 IAM 身份中心实例所需的 Amazon KMS 权限。	2025 年 9 月 17 日
用于静态加密的客户自主管理型密钥	新增支持使用客户自主管理型 KMS 密钥对员工身份数据进行静态数据加密。	2025 年 9 月 17 日
允许令牌创建的基于资源的策略示例	新增了基于资源的策略示例，该策略允许为授权的客户端应用程序创建令牌。	2025 年 9 月 16 日
支持用户后台会话	新增了关于用户后台会话的内容。	2025 年 8 月 11 日
身份增强的控制台会话	更新了身份增强的控制台会话的术语（之前称为身份感知会话）。	2025 年 5 月 12 日
入门重组	重组了入门内容，以提高清晰度和用户体验。	2025 年 5 月 6 日

弃用 IAM Identity Center AD Sync	您无法再使用 IAM Identity Center AD Sync 配置 Active Directory 用户。相反，您可以使用 IAM Identity Center 可配置 AD Sync。	2025 年 4 月 17 日
更新了已验证会话的内容	更新了删除用户会话时 IAM Identity Center 会话持续时间的信息。	2025 年 4 月 2 日
Amazon 托管策略的更新	更新了`AWSSSOServiceRolePolicy` Amazon 托管策略的权限。	2025 年 2 月 11 日
IAM Identity Center 启用工作流改进	更新了启用 IAM Identity Center 组织实例和账户实例的工作流。	2025 年 2 月 11 日
IAM Identity Center 启用更新	更新了启用 IAM Identity Center 组织实例和账户实例的内容和过程。	2024 年 10 月 10 日
Amazon 托管策略的更新	更新了`AWSIAMIdentityCenterAllowListForIdentityContext` Amazon 托管策略的权限。	2024 年 10 月 2 日
Amazon 托管策略的更新	更新了`AWSSSOMasterAccountAdministrator` Amazon 托管策略的权限。	2024 年 9 月 26 日
Amazon 托管策略的更新	更新了`AWSIAMIdentityCenterAllowListForIdentityContext` Amazon 托管策略的权限。	2024 年 9 月 4 日

更新了“什么是 IAM Identity Center？” topic	更新了描述 IAM Identity Center 优势和功能的内容。	2024 年 8 月 19 日
Amazon 托管策略的更新	更新了AWSIAMIdentityCenterAllowListForIdentityContext Amazon 托管策略的权限。	2024 年 7 月 12 日
Amazon 托管策略的更新	更新了AWSIAMIdentityCenterAllowListForIdentityContext Amazon 托管策略的权限。	2024 年 6 月 27 日
Amazon 托管策略的更新	更新了AWSIAMIdentityCenterAllowListForIdentityContext Amazon 托管策略的权限。	2024 年 5 月 17 日
Amazon 托管策略的更新	更新了AWSIAMIdentityCenterAllowListForIdentityContext Amazon 托管策略的权限。	2024 年 4 月 30 日
Amazon 托管策略的更新	更新了AWSSSOMasterAccountAdministrator Amazon 托管策略的权限。	2024 年 4 月 26 日
Amazon 托管策略的更新	更新了AWSSSOMemberAccountAdministrator Amazon 托管策略的权限。	2024 年 4 月 26 日

Amazon 托管策略的更新	更新了AWSSSOReadOnly Amazon 托管策略的权限。	2024 年 4 月 26 日
Amazon 托管策略的更新	更新了AWSIAMIdentityCenterAllowListForIdentityContext Amazon 托管策略的权限。	2024 年 4 月 26 日
Amazon 托管策略的更新	更新了AWSIAMIdentityCenterAllowListForIdentityContext Amazon 托管策略的权限。	2024 年 4 月 24 日
Amazon 托管策略的更新	更新了AWSIAMIdentityCenterAllowListForIdentityContext Amazon 托管策略的权限。	2024 年 4 月 19 日
Amazon 托管策略的更新	更新了AWSIAMIdentityCenterAllowListForIdentityContext Amazon 托管策略的权限。	2024 年 4 月 11 日
Amazon 托管策略的更新	更新了AWSIAMIdentityCenterAllowListForIdentityContext Amazon 托管策略的权限。	2023 年 11 月 26 日
新的 Amazon 托管策略主题	添加了AWSIAMIdentityCenterAllowListForIdentityContext Amazon 托管策略的详细信息。	2023 年 11 月 15 日

增强了开始使用 IAM Identity Center 指南	为开始使用 IAM Identity Center 和创建管理用户添加了新内容	2022 年 9 月 23 日
更新了 Identity Center API 参考中的用户和组	此更新包括对 Identity Center API 参考指南 APIs 中新的 “创建、更新和删除” 的引用。	2022 年 8 月 31 日
Amazon 单点登录 (Amazon SSO) 已重命名为 Amazon IAM 身份中心	Amazon 介绍 Amazon IAM Identity Center。IAM Identity Center 扩展了 Amazon Identity and Access Management (IAM) 的功能，可帮助您集中管理员工用户的账户和应用程序访问权限。IAM Identity Center 的功能包括应用程序分配、多帐户权限和 Amazon 访问门户。	2022 年 7 月 26 日
支持权限集中的权限边界和客户管理型策略	添加了使用带有权限集的 Amazon 托管策略和客户托管 Amazon Identity and Access Management (IAM) 策略的内容。	2022 年 7 月 14 日
支持手动启用的 Amazon 区域	添加了在手动启用的区域中使用 IAM Identity Center 的内容。	2022 年 6 月 15 日
Amazon 托管策略的更新	更新了`AWSSSOServiceRolePolicy` Amazon 托管策略的权限。	2022 年 5 月 11 日
支持委派管理	为委托管理功能添加了内容。	2022 年 5 月 11 日

Amazon 托管策略的更新	更新了AWSSSOMasterAccountAdministrator AWSSSOMemberAccountAdministrator 、和AWSSSOReadOnly Amazon 托管策略的权限。	2022 年 4 月 28 日
支持可配置的 AD 同步	为可配置的 AD 同步功能添加了内容。	2022 年 4 月 14 日
新的 Amazon 托管策略主题	添加了AWSSSOMasterAccountAdministrator Amazon 托管策略的详细信息。	2021 年 8 月 4 日
限额更新	对限额表的调整。	2020 年 12 月 21 日
新的示例策略	添加了新的客户管理型策略示例，并对“所需权限”部分进行了更新。	2020 年 12 月 21 日
支持基于属性的访问权限控制（ABAC）	添加了 ABAC 功能的内容。	2020 年 11 月 24 日
支持 MFA 强制注册	更新要求用户在登录时注册 MFA 设备。	2020 年 11 月 23 日
Support WebAuthn	为新的 WebAuthn 功能添加了内容。	2020 年 11 月 20 日
支持 Ping 身份	添加了可作为支持的外部身份提供者的与 Ping Identity 产品集成的内容。	2020 年 10 月 26 日
Support OneLogin	添加了可作为支持的外部身份提供者的与 OneLogin 集成的内容。	2020 年 7 月 31 日

支持 Okta	添加了可作为支持的外部身份提供者的与 Okta 集成的内容。	2020 年 5 月 28 日
支持外部身份提供者	将参考从目录更改为身份源，添加内容以支持外部身份提供者。	2019 年 11 月 26 日
新的 MFA 设置	删除了两步验证主题，并在其位置添加了新的 MFA 主题。	2019 年 10 月 24 日
添加两步验证的新设置	添加了有关如何为用户启用两步验证的内容。	2019 年 1 月 16 日
Support 支持 Amazon 账户的会话时长	添加了有关如何为 Amazon 账户设置会话持续时间的内容。	2018 年 10 月 30 日
使用 Identity Center 目录的新选项	增加了如何选择 Identity Center 目录或连接到活动目录中的现有目录的内容。	2018 年 10 月 17 日
对应用程序的中继状态和会话持续时间的支持	增加了有关应用程序的中继状态和会话持续时间的内容。	2018 年 10 月 10 日
对新应用程序的其他支持	将 4me, BambooHR, Bonusly, Citrix ShareFile, ClickTime , Convo, Deputy, Deskpro, Dome9, DruvaInSync, Egnyte, Engagedly, Expensify , Freshdesk, IdeaScale, Igloo, Jitbit, Kudos, LiquidFil es, Lucidchart, PurelyHR, Samanage, ScreenSte ps, Sli.do, SmartSheet, Syncplicity, TalentLMS, Trello, UserVoice, Zoho, OpsGenie, DigiCert, WeekDone, ProdPad, 和 UserEcho 添加到应用程序目录中。	2018 年 8 月 3 日

支持多帐户访问管理帐户	增加了有关如何向托管帐户中的用户委派多帐户访问权限的内容。	2018 年 7 月 9 日
对新应用程序的支持	将 DocuSign, Keeper Security, 和 SugarCRM 添加到应用程序目录中。	2018 年 3 月 16 日
获取 CLI 访问的临时凭证	添加了有关如何获取临时证书以运行 Amazon CLI 命令的信息。	2018 年 2 月 22 日
新指南	这是 IAM Identity Center 用户指南的首个版本。	2017 年 12 月 7 日

Amazon 词汇表

有关最新 Amazon 术语，请参阅《Amazon Web Services 词汇表 参考资料》中的Amazon 词汇表。

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。