aws

用户指南

AWS IAM Identity Center

AWS IAM Identity Center: 用户指南

Table of Contents

IAM Identity Center 是什么？

AWS IAM Identity Center 建议 AWS 服务 用于管理人类用户对 AWS 资源的访问权限。您可以在这一个位置为员工用户（也称为 workforce identities）分配对多个 AWS 账户 和应用程序的一致访问权限。IAM 身份中心不收取额外费用。

借助 IAM Identity Center，您可以创建或连接员工用户，并集中管理他们对所有用户 AWS 账户 和应用程序的访问权限。您可以使用多帐户权限来分配您的员工用户对 AWS 账户的访问权限。您可以使用应用程序分配来为用户分配对托管应用程序和客户 AWS 托管应用程序的访问权限。

> **Note**
>
> 尽管服务名称 AWS Single Sign-On 已停用，但本指南中仍使用单点登录一词来描述允许用户一次登录即可访问多个应用程序和网站的身份验证方案。

IAM Identity Center 功能

IAM Identity Center 包括以下核心功能和特性：

管理员工身份

在中 AWS 构建或操作工作负载的人类用户也称为员工用户或员工身份。Workforce 用户是指您允许在组织和内部业务应用程序 AWS 账户 中访问的员工或承包商。这些个人可能是开发人员，负责构建内部系统和面向客户的系统，也可能是内部数据库系统和应用程序的用户。您可以在 IAM Identity Center 中创建员工用户和群组，也可以连接并同步到您自己的身份源中的一组现有用户和群组，以便在您的所有 AWS 账户 和应用程序中使用。有关更多信息，请参阅 管理您的身份源。

管理 IAM Identity Center 的实例

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， AWS 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 AWS Organizations 管理账户中，可让您通过单点管理整个 AWS 环境中的用户访问权限。

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

管理对多个访问权限 AWS 账户

借助多账户权限，您可以一次性规划和集中实施多个 AWS 账户 账户的权限，而无需手动配置每个账户。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，以控制他们对特定帐户的访问权限。

此可选功能仅适用于组织实例。如果您在环境中使用按账户的 IAM 角色管理，那么两个系统可以共存。如果您想尝试使用多账户权限，可以先在有限的范围实施此系统，然后逐渐将更多环境迁移到此系统。

管理对应用程序的访问

IAM Identity Cente 允许您简化应用程序的访问管理。通过 IAM Identity Center，您可以在 IAM Identity Center 中授予员工用户对应用程序的单点登录访问权限。

AWS 托管应用程序

AWS 提供与 IAM 身份中心集成的应用程序 Amazon Redshift，例如亚马逊托管 Grafana 和 Amazon Monitron。这些应用程序可以使用 IAM Identity Center 实现身份验证、目录服务和可信身份传播。您的用户将受益于一致的单点登录体验，而且由于这些应用程序以共同的视角看待用户、组和组成员身份，用户在与其他人共享应用程序资源时也会具有一致的体验。您可以直接在相关的应用程序控制台中或通过 API 将 AWS 托管应用程序配置为与 IAM Identity Center 配合使用。

客户托管的应用程序

您可以在 IAM Identity Center 授予员工用户对应用程序（支持 SAML 2.0 身份联合验证）的单点登录访问权限。Salesforce 和 Microsoft 365 等许多常用的 SAML 2.0 应用程序都可以与 IAM Identity Center 协同工作，您可以在 IAM Identity Center 控制台的应用程序目录中找到它们。这是一项可选功能，如果您使用此类应用程序，并在 IAM Identity Center 中创建用户和组，或使用 Microsoft Active Directory 域服务作为身份源，该功能会很有帮助。

跨应用程序的可信身份传播

可信身份传播为需要访问 AWS 服务中数据的查询工具和商业智能 (BI) 应用程序的用户提供了简化的单点登录体验。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。用户对 AWS 服务和其他事件的访问记录在服务特定的日志和 CloudTrail 事件中，以便审计员知道用户采取了哪些操作以及用户访问了哪些资源。

AWS 为您的用户提供门户访问权限

AWS 访问门户是一个简单的 Web 门户，可让您的用户无缝访问他们分配的所有应用程序 AWS 账户 和应用程序。

IAM Identity Center 重命名

2022 年 7 月 26 日，AWS 单点登录更名为。 AWS IAM Identity Center对于现有客户，下表旨在描述因重命名而在本指南中更新的一些更常见的术语更改。

旧术语	当前术语
AWS SSO 用户或 SSO 用户	员工用户或用户
AWS SSO 用户门户或用户门户	AWS 访问门户
AWS 集成 SSO 的应用程序	AWS 托管应用程序
AWS SSO 目录	Identity Center 目录
AWS SSO 存储或 AWS SSO 身份存储	IAM Identity Center 使用的身份存储

下表描述了因此次重命名而发生的适用用户、开发人员和 API 参考指南名称更改。

旧指南	当前指南
AWS 单点登录用户指南	IAM Identity Center 用户指南
AWS 单点登录 SCIM 实施开发人员指南	IAM Identity Center SCIM 实施开发人员指南
AWS 单点登录 API 参考指南	IAM Identity Center API 参考
AWS 单点登录身份存储 API 参考指南	身份存储 API 参考
AWS 单点登录 OIDC API 参考指南	IAM Identity Center OIDC API 参考
AWS 单点登录门户 API 参考指南	IAM Identity Center 门户 API 参考

旧命名空间保持不变

出于向后兼容目的，`sso` 和 `identitystore` API 命名空间以及以下相关命名空间保持不变。

- CLI 命令
  - aws configure sso
  - identitystore
  - sso
  - sso-admin
  - sso-oidc
- 包含 AWSSSO 和 AWSIdentitySync 前缀的托管策略
- 包含 sso 和 identitystore 的服务端点
- 包含 AWS::SSO 前缀的 AWS CloudFormation 资源
- 包含 AWSServiceRoleForSSO 的服务相关角色
- 包含 sso 和 singlesignon 的控制台 URL
- 包含 singlesignon 的文档 URL

启用 AWS IAM Identity Center

完成以下步骤登录 AWS Management Console 并启用 IAM Identity Center 的组织实例。

1. 请执行以下任一操作，登录 AWS Management Console。
   - AWS （root 用户）新手 — 选择 R oot 用户并输入您的 AWS 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 AWS （IAM 证书）— 使用具有管理权限的 IAM 凭证登录。
2. 打开 IAM Identity Center 控制台。
3. 在启用 IAM Identity Center 下，选择与 AWS Organizations一起启用。
4. （可选）添加要与此组织实例关联的标签。
5. （可选）配置委托管理。

> **Note**
>
> 如果您正在使用多账户环境，我们建议您配置委托管理。通过委托管理，您可以限制AWS Organizations中需要访问管理账户的人数。有关更多信息，请参阅委派管理。

> **Important**
>
> 创建 IAM Identity Center 账户实例的功能默认已启用。IAM Identity Center 账户实例包含的功能是组织实例可用功能的一部分。您可以使用服务控制策略，控制用户是否可以访问此功能。

是否需要更新防火墙和网关？

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)）来过滤对特定 AWS 域或 URL 端点的访问，则必须将以下域或 URL 端点添加到您的网络内容过滤解决方案许可名单中。这样您就可以访问您的 AWS 访问门户。

- *[Directory ID or alias]*.awsapps.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]*.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com

将域名和 URL 端点列入许可名单的注意事项

了解 AWS 访问门户之外的域名许可名单的影响。

- 要从您的访问 AWS 账户门户 AWS 访问 AWS Management Console、和 IAM Identity Center 控制台，您必须将其他域列入许可名单。有关 AWS Management Console 域名列表，请参阅《AWS Management Console 入门指南》中的疑难解答。
- 要从您的访问门户 AWS 访问 AWS 托管应用程序，您必须将其各自的域列入许可名单。有关指导，请参阅相应的服务文档。
- 这些许可名单涵盖 AWS 服务。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。

现在，您可以配置 IAM Identity Center。启用 IAM Identity Center 后，它会自动配置 IAM Identity Center 目录作为您的默认身份源，这是开始使用 IAM Identity Center 的最快方法。有关说明，请参阅使用默认 IAM Identity Center 目录配置用户访问权限。

如果您想进一步了解 IAM Identity Center 如何与 Organizations、身份源和 IAM 角色配合使用，请参阅以下主题。

主题

- 先决条件和注意事项
- 在 IAM 身份中心确认您的身份来源

先决条件和注意事项

以下主题提供有关设置 IAM Identity Center 先决条件和其他注意事项的信息。

选择的注意事项 AWS 区域

您可以根据自己的选择在单个实例中启用 IAM Identity C AWS 区域 enter 实例。选择区域需要根据您的用例和公司政策评估您的优先级。从您的 IAM Identity Center 访问 AWS 账户 和云应用程序不取决于此选择；但是，对 AWS 托管应用程序的访问权限以及是否能够 AWS Managed Microsoft AD 用作身份源可能取决于此选择。有关 AWS IAM 身份中心支持的区域列表， AWS 一般参考 请参阅中的 IAM 身份中心终端节点和配额。

选择的关键注意事项 AWS 区域.

- 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 AWS 访问门户和 AWS 托管应用程序（例如亚马逊 SageMaker Studio）的延迟将更低。
- AWS 托管应用程序的可用性 — AWS 托管应用程序（例如 Amazon SageMaker）只能在其支持的应用程序中 AWS 区域 运行。在您要与之配合使用的 AWS 托管应用程序支持的区域中启用 IAM 身份中心。许多 AWS 托管应用程序也只能在您启用 IAM Identity Center 的同一区域运行。
- 数字主权 — 数字主权法规或公司政策可能强制使用特定内容 AWS 区域。请咨询贵公司的法律部门。
- 身份来源 — 如果您使用 AWS Managed Microsoft AD 或 AD Connector 作为身份源，则其主区域必须与您启用 IAM 身份中心时所在的区域相匹配。 AWS 区域
- 默认情况下禁用区域 — AWS 最初 AWS 账户 默认启用所有新区域 AWS 区域 以供在中使用，这会自动允许您的用户在任何区域创建资源。现在，当 AWS 添加新区域时，默认情况下，所有账户都将禁用该区域。如果您在默认禁用的区域部署 IAM Identity Center，则必须在您想要管理 IAM Identity Center 访问权限的所有账户中启用该区域。即使您不打算在该区域的这些账户中创建任何资源，这也是必需的。

  您可以为组织中的当前账户启用区域，并且必须对稍后可能添加的新账户重复此操作。有关说明，请参阅 AWS Organizations 用户指南中的在组织中启用或禁用区域。为避免重复这些额外步骤，您可以选择在默认启用的区域部署您的 IAM 身份中心。作为参考，以下区域默认处于启用状态：

  - 美国东部（俄亥俄）
  - 美国东部（弗吉尼亚州北部）
  - US West（Oregon）
  - 美国西部（北加利福尼亚）

- 欧洲地区（巴黎）
- South America（São Paulo）
- 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）

- 跨区域呼叫 — 在某些区域，IAM Identity Center 可能会调用其他区域的 Amazon 简单电子邮件服务发送电子邮件。在这些跨区域调用中，IAM Identity Center 会将某些用户属性发送到另一个区域。有关 区域的更多信息，请参阅AWS IAM Identity Center 地区可用性。

切换 AWS 区域

您只能通过删除当前实例并在另一个区域创建新实例来切换 IAM 身份中心区域。如果您已经使用现有实例启用了 AWS 托管应用程序，则应先将其删除，然后再删除 IAM Identity Center。您必须在新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 API 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。您可能还需要通过新实例的管理控制台重新创建一些 IAM Identity Center 配置。有关删除 IAM 身份中心的说明，请参阅删除您的 IAM Identity Center 配置。

IAM 身份中心创建的 IAM 角色配额

IAM Identity Center 通过创建 IAM 角色，向用户提供资源访问权限。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 AWS 访问门户或代入该角色。 AWS 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。

如果您已经在中配置了 IAM 角色 AWS 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 角色限额的账户预置权限集时，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 服务在账户中创建的角色，它们来自向账户分配权限集。

IAM 身份中心和 AWS Organizations

AWS 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，您将选择是否启用该服务 AWS Organizations。当你建立组织时，建立 AWS 账户 该组织的用户将成为该组织的管理帐户。此时， AWS 账户 的根用户将是组织管理账户的所有者。 AWS 账户 您邀请加入组织的所有其他成员均为成员帐户。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 AWS 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，请参阅管理 IAM Identity Center 的组织实例和账户实例。

如果您已经设置 AWS Organizations 并打算将 IAM Identity Center 添加到您的组织，请确保所有 AWS 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《AWS Organizations 用户指南》中的启用企业中的所有功能。

要启用 IAM Identit AWS Management Console y Center，您必须以拥有 AWS 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。使用 AWS Organizations 成员账户的管理证书登录时，您无法启用 IAM Identity Center。有关更多信息，请参阅《AWS Organizations 用户指南》中的创建和管理 AWS 组织。

在 IAM 身份中心确认您的身份来源

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。

确认身份源

1. 前往控制面板
2. 在优化 IAM Identity Center 部分，选择确认身份源按钮。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

   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。如果您尚未使用其他外部身份提供商，您可以开始创建用户和组，并为其分配对 AWS 账户 和应用程序的访问权限级别。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 AWS Directory Service 或中的自管理 AWS 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。AWS Directory Service 有关更多信息，请参阅连接到 Microsoft AD 目录。

   > **Note**
   >
   > IAM Identity Center 不支持基于 SAMBA4 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，请参阅入门教程。

> **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。外部不支持使用 IAM 身份中心中的 MFA。 IdPs有关更多信息，请参阅提示用户完成 MFA。

您选择的身份源决定 IAM Identity Center 在何处搜索需要单点登录访问的用户和组。确认或更改身份源后，您将创建或指定用户，并为其分配对 AWS 账户的管理权限。

> **Important**
>
> 如果您已经在管理 Active Directory 或外部身份提供者（IdP）中的用户和组，我们建议您在启用 IAM Identity Center 并选择您的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 AWS 账户 和应用程序的单点登录访问权限。有关更多信息，请参阅更改身份来源的注意事项。

配置身份源后，您可以查找用户或群组，向他们授予对云应用程序或两者的单点登录访问权限。 AWS 账户

入门教程

每个组织只能有一个身份源，因此花时间测试每个身份源的功能非常重要。

在本节中，您可以选择以下教程之一，设置 IAM Identity Center 使用您首选的身份源，创建管理用户，并配置权限集以授予用户访问资源的权限。

在开始这些教程之前，请启用 IAM 身份中心。有关更多信息，请参阅 启用 AWS IAM Identity Center。

主题

- 使用默认 IAM Identity Center 目录配置用户访问权限
- 使用 Active Directory 作为身份源
- Setting up SCIM provisioning between CyberArk and IAM Identity Center
- 通过 Google Workspace 和 IAM Identity Center 配置 SAML 和 SCIM
- 使用 IAM Identity Center 与 JumpCloud 目录平台连接
- 通过 Microsoft Entra ID 和 IAM Identity Center 配置 SAML 和 SCIM
- 通过 Okta 和 IAM Identity Center 配置 SAML 和 SCIM
- 在 OneLogin 和 IAM Identity Center 之间设置 SCIM 预置
- 将 Ping Identity 产品与 IAM Identity Center 结合使用

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 AWS Directory Service for Microsoft Active DirectoryMicrosoft 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，并设置和测试用户访问权限。在此方案中，您将在 IAM Identity Center 管理所有用户和组。用户通过 AWS 访问门户登录。本教程适用于刚接触 IAM AWS 或一直在使用 IAM 管理用户和群组的用户。在接下来的步骤中，您将创建以下内容：

- 名为 *Nikki Wolf* 的管理用户
- 名为 *Admin team* 的组
- 名为的权限集 *AdminAccess*

要验证所有内容是否正确创建，您需要登录并设置管理员用户的密码。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。

如果您尚未启用 IAM Identity Center，请参阅 启用 AWS IAM Identity Center。

开始前的准备工作：

请执行以下任一操作，登录 AWS Management Console。

- AWS （root 用户）新手 — 以账户所有者的身份登录，方法是选择 AWS 账户 root 用户并输入您的 AWS 账户 电子邮件地址。在下一页上，输入您的密码。
- 已在使用 AWS （IAM 证书）— 使用具有管理权限的 IAM 凭证登录。

打开 IAM Identity Center 控制台。

步骤 1：添加用户

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

     创建用户时，请选择易于记忆的用户名。用户必须记住用户名才能登录 AWS 访问门户，您此后无法更改该用户名。
   - 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）。

     此选项向用户发送一封来自 Amazon Web Services 的电子邮件，其主题行是 “邀请加入 IAM 身份中心”（ AWS 单点登录的继任者）。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。

3. 选择下一步。此时将出现将用户添加到组页面。我们将创建一个组来分配管理权限，而不是将其直接授予 *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

4. 在组区域，选择刷新按钮。*Admin team* 组将显示在列表中。

   选中 “*#####*” 旁边的复选框，然后选择 “下一步”。

5. 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 *Admin team* 组添加管理权限，以便 *Nikki* 有权访问资源。

步骤 2：添加管理权限

1. 在 IAM Identity Center 导航窗格的多账户权限下，选择 AWS 账户。
2. 在 AWS 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。选中您的管理帐户对应的复选框，然后选择分配用户或群组。
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，选择您创建的 *Admin team* 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。

iii. 对于“步骤 3：查看并创建”，请验证权限集类型是否使用 AWS 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。选中该权限集的复选框，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“*###” ##*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 AWS 账户 正在配置中。等待该过程完成。

您将返回到该 AWS 账户 页面。系统会显示一条通知消息，告知您 AWS 账户 已重新配置您的权限集，并且已应用更新的权限集。

> **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，您将使用 *Nikki ####### AWS ############## Nikki* 的访问权限。现在，注销控制台。

步骤 3：测试用户访问权限

现在，*Nikki Wolf* 已成为您组织中的用户，可以登录并根据权限集访问其有权访问的资源。要验证用户配置是否正确，在下一步中，您将使用 *Nikki* 的凭证登录，并为其设置密码。在步骤 1 中添加用

户 *Nikki Wolf* 时，您选择让 *Nikki* 接收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**
   >
   > 该电子邮件还包含 *Nikki* 的用户名以及用于登录组织的 AWS 访问门户 URL。记录这些信息，以供将来使用。

   您将转到新用户注册页面，您可以在其中设置 *Nikki* 的密码。
2. 设置 *Nikki* 的密码后，您将转到登录页面。输入 *nikkiw*，选择下一步，然后输入 *Nikki #*密码，选择登录。
3. AWS 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， AWS 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可供您使用的管理方法，即角色密钥或访问密钥。

   - 例如，角色 ***AdministratorAccess***-打开 AWS Console Home。
   - 访问密钥-提供可用于 AWS CLI 或和 AWS 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 AWS CLI 或 AWS 软件开发工具包的 IAM Identity Center 用户证书。
4. 选择 “角色” 链接以登录 AWS Console Home。

您已登录并导航到该 AWS 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 AWS 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 AWS 访问门户后，门户中显示的项目仅限于分配给他们的 AWS 账户、角色和应用程序。

> **Important**
>
> 我们建议您对用户启用多重身份验证 (MFA)。有关更多信息，请参阅 Identity Center 用户的多重身份验证。

使用 Active Directory 作为身份源

如果您正在使用 AWS Directory Service 管理 AWS Managed Microsoft AD 目录中的用户，或正在管理 Active Directory (AD) 自托管式目录中的用户，您可以更改 IAM Identity Center 的身份源，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 AWS Managed Microsoft AD，则必须在设置 AWS Managed Microsoft AD 目录的同一 AWS 区域 中启用 IAM Identity Center。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。此外，请注意，AWS 访问门户使用与该目录相同的访问 URL。
- 使用驻留在管理账户中的 Active Directory：

  您必须在 AWS Directory Service 中设置现有 AD Connector 或 AWS Managed Microsoft AD 目录，并且该目录必须位于您的 AWS Organizations 管理账户内。一次只能在 AWS 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 AWS Managed Microsoft AD。有关更多信息，请参阅：
  - 将目录连接 AWS Managed Microsoft AD 到 IAM 身份中心
  - 将 Active Directory 中的自托管式目录连接到 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 Identity Center 委派管理员，并使用 Active Directory 作为您的 IAM Identity Center 身份源，则可以使用现有 AD Connector 或在驻留于委派管理员账户内的 AWS 目录中设置的 AWS Managed Microsoft AD 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**
>
> 强烈建议您启用多重验证，这是最佳安全实践。如果您计划连接 Active Directory 中的 AWS Managed Microsoft AD 目录或自托管式目录，但未将 RADIUS MFA 与 AWS Directory Service 搭配使用，请在 IAM Identity Center 中启用 MFA。

AWS Managed Microsoft AD

1. 请查看 连接到 Microsoft AD 目录 中的指南。
2. 按照 将目录连接 AWS 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 中的自托管式目录

1. 请查看 连接到 Microsoft AD 目录 中的指南。
2. 按照 将 Active Directory 中的自托管式目录连接到 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. 在已添加用户和群组下，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账户的管理访问权限。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。您可以使用 IAM Identity Center SCIM 终端节点和访问令牌在 CyberArk 中配置此连接。配置 SCIM 同步时，您将在 CyberArk 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 CyberArk 之间的预期属性匹配。

本指南基于截至 2021 年 8 月的 CyberArk。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。

> **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：

- CyberArk 订阅或免费试用。报名参加免费试用访问 CyberArk。
- 支持 IAM Identity Center 的账户（免费）。有关更多信息，请参阅启用 IAM Identity Center。
- 从您的 CyberArk 账户到 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 AWS 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 终端节点和访问令牌信息。
4. 在入站自动预置对话框中，复制以下选项的每个值。稍后在 IdP 中配置预置时，您需要粘贴这些内容。
   a. SCIM 端点
   b. 访问令牌
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 终端节点值。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。确保删除 URL 末尾的尾部正斜杠。
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账户并可以在 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 AWS 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 AWS 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 Google Workspace 和 IAM Identity Center 配置 SAML 和 SCIM

如果您的组织正在使用，Google Workspace您可以将您的用户和群组从 IAM Identity Center 集成 Google Workspace到 IAM Identity Center 中，通过将您的 IAM Identity Center 身份源从默认 IAM Identity Center 身份源更改为 AWS Google Workspace

Google Workspace 的用户信息通过跨域身份管理系统 (SCIM) v2.0 协议同步到 IAM Identity Center。您可以在 Google Workspace 中使用 IAM Identity Center 的 SCIM 端点和 IAM Identity Center 持有者令牌来配置此连接。配置 SCIM 同步时，您将创建从 Google Workspace 中的用户属性到 IAM Identity Center 中的命名属性的映射。此映射在 IAM Identity Center 和 Google Workspace 之间匹配预期的用户属性。为此，您需要将 Google Workspace 设置为 IAM 身份提供商和 IAM Identity Center 身份提供商。

目标

本教程中的步骤有助于指导您在Google Workspace和 AWS之间建立 SAML 连接。稍后，您将使用 SCIM 从 Google Workspace 同步用户。要验证所有配置是否正确，完成配置步骤后，您将以Google Workspace用户身份登录并验证对 AWS 资源的访问权限。请注意，本教程基于一个小型 Google Workspace 目录测试环境。其中不包括组和组织单位等目录结构。

> **Note**
>
> 要注册 Google Workspace 的免费试用，请访问 Google's 网站上的 Google Workspace。如果您尚未启用 IAM Identity Center，请参阅 启用 AWS IAM Identity Center。

开始前的准备工作

在 Google Workspace 和 IAM Identity Center 之间配置 SCIM 预置之前，我们建议您首先查看 使用自动预置的注意事项

在开始之前，确认以下事项：

- 必须已为每位 Google Workspace 用户指定名字、姓氏、用户名和显示名称值。
- 每位 Google Workspace 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。对于任何用户，有多个值都将导致无法同步。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。

> **Note**
>
> - 如果用户在 IAM Identity Center 中被禁用，但在 Google Workspace 中仍然处于活动状态，属性仍然会同步。
> - 如果 Identity Center 目录中存在具有相同用户名和电子邮件的现有用户，则将从 Google Workspace 开始使用 SCIM 覆盖并同步该用户。

步骤 1：为创建自定义用户属性 AWS

1. 使用具有超级管理员权限的账户登录 Google 管理控制台。
2. 在左侧导航面板，展开目录，然后选择用户。

3. 在用户列表顶部，选择更多选项，然后选择管理自定义属性。
4. 在页面右上方，选择添加自定义属性。
5. 在添加自定义字段）窗口，填写以下字段：

   a. 在类别中，输入 Amazon。
   b. 在描述中，输入 Amazon 自定义属性。
   c. 在名称中，输入角色。
   d. 在信息类型中，选择文本。
   e. 在可见性中，选择对用户和管理员可见。
   f. 在值的数量中，选择多个值。

   选择 添加。新属性将显示在管理用户属性页面的自定义属性下。

在 Google 管理控制台中保持登录状态，下一步将继续使用该控制台。

步骤 2：下载身份提供商元数据

1. 在 Google 管理控制台的左侧导航面板中，展开安全性，选择身份验证、SAML 应用程序的单点登录服务。根据控制台的布局，您可能需要选择显示更多，以显示导航面板的安全部分。
2. 在 IdP 元数据下，选择下载元数据。文件 GoogleIDPMetadata.xml 会保存到默认下载文件夹。

将 Google 管理控制台保留为打开状态，因为在本教程中，您将多次继续使用该控制台。

第 3 步：在中设置亚马逊 Web Services 应用程序 Google Workspace

Amazon Web Services 应用程序支持自动通过 SCIM 将您的 Google Workspace 用户预置到 IAM Identity Center。

1. 在 Google 管理控制台的左侧导航面板中，展开应用程序，选择 Web 和移动应用程序。
2. 选择添加应用程序，然后选择搜索应用程序。
3. 在搜索框中输入 Amazon Web Services，然后从列表中选择 Amazon Web Services (SAML) 应用程序。
4. 在 Google 身份提供商详细信息页面，您可以选择下载元数据，或复制 SSO URL、实体 ID 和证书。您无需执行这两项操作，因为您在步骤 2 中下载了 IdP 元数据。您可以选择继续。
5. 在服务提供商详细信息页面上，默认配置的 ACS URL 和实体 ID 值，选择继续。 AWS

6. 在属性映射页面的属性下，在 Google Directory 属性下添加以下字段：

   - 选择基本信息，主电子邮件字段，然后在应用程序属性中输入 `https://aws.amazon.com/SAML/Attributes/RoleSessionName`
   - 选择 Amazon，角色字段，然后在应用程序属性中输入 `https://aws.amazon.com/SAML/Attributes/Role`

   > **Note**
   >
   > Amazon，角色是您在本教程的步骤 1 中创建的自定义属性。

7. 选择完成。

步骤 4：更改 IAM 身份中心身份源并设置Google Workspace为 SAML 身份提供商

1. 使用具有管理权限的角色登录 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. 在选择身份来源下，选择外部身份提供程序，然后选择下一步。
5. 将打开配置外部身份提供商页面。要填写此页面，您需要在 Google Workspace 中将 IAM Identity Center 设置为 SAML 应用程序，并从 Google Admin console 中获取信息。请执行以下操作：

   a. 在 Google 管理控制台的左侧导航面板中，展开应用程序，选择 Web 和移动应用程序。

   b. 选择添加应用程序，然后选择添加自定义 SAML 应用程序。

   c. 在输入应用程序名称中，输入 AWS 访问门户，然后在描述中输入描述性文本，本教程输入面向 Google Workspace 的AWS 访问门户教程，然后选择继续。

   d. 在 Google 身份提供商详细信息页面，选择继续。

   e. 在服务提供商详细信息页面，输入 ACS URL 和实体 ID 值。返回您的 IAM Identity Center 控制台，查找以下值：

      - 在 IAM Identity Center 控制台的服务提供商元数据下，复制 IAM Identity Center 断言使用者服务 (ACS) URL。

        返回 Google 管理控制台 - 服务提供商详细信息页面，然后将 URL 粘贴到 ACS URL 字段。

- 在 IAM Identity Center 控制台的服务提供商元数据下，复制 IAM Identity Center 发布者 URL。

  返回 Google 管理控制台 - 服务提供商详细信息页面，然后将 URL 粘贴到实体 ID 字段。

f. 在 Google 管理控制台 - 服务提供商详细信息页面，按如下所示，填写名称 ID 下的字段：

- 对于名称 ID 格式，请选择电子邮件
- 对于名称 ID，请选择基本信息 > 主电子邮件

  选择继续。

g. 在属性映射页面的属性下，选择添加映射，然后在 Google Directory 属性下配置这些字段：

- 选择基本信息，主电子邮件字段，然后在应用程序属性中输入 `https://aws.amazon.com/SAML/Attributes/RoleSessionName`
- 选择 Amazon，角色字段，然后在应用程序属性中输入 `https://aws.amazon.com/SAML/Attributes/Role`

> **Note**
>
> Amazon，角色是您在步骤 1 中创建的自定义属性。如果它不存在，请参阅 步骤 1：为创建自定义用户属性 AWS。

h. 选择完成。

6. 返回 IAM Identity Center 控制台，其中打开的是配置外部身份提供商页面。在身份提供商元数据下的 IdP SAML 元数据下，选择选择文件，然后上传您在步骤 2 中下载的 GoogleIDPMetadata.xml 文件。

   选择下一步。

7. 在确认更改页面，检查信息，然后在提供的空白处输入 ACCEPT。

   选择更改身份源。

现在，您已准备好在 Google Workspace 中启用 Amazon Web Services 应用程序，从而将用户预置到 IAM Identity Center。

第 5 步：启用中的应用程序 Google Workspace

1. 在 Google 管理控制台的左侧导航面板中，展开应用程序，选择 Web 和移动应用程序。
2. 在应用程序列表中，选择 Amazon Web Services 图标，以打开应用程序详情页面。
3. 在用户访问权限面板，选择用户访问权限旁边的向下箭头，展开用户访问权限，以显示服务状态面板。
4. 在服务状态中选择为所有人开启，然后选择保存。
5. 选择 AWS 访问门户图标，打开应用程序详细信息页面。
6. 在用户访问权限面板，选择用户访问权限旁边的向下箭头，展开用户访问权限，以显示服务状态面板。
7. 在服务状态中选择为所有人开启，然后选择保存。

> **Note**
>
> 为了维持最低权限原则，我们建议您在完成本教程后，将这两个应用程序的服务状态更改为为所有人关闭。只有需要访问权限的用户才 AWS 应启用该服务。您可以使用 Google Workspace 组或组织单位，将用户访问权限授予特定的用户子集。

步骤 6：设置 IAM 身份中心自动配置

1. 使用具有管理权限的角色登录 IAM Identity Center 控制台。
2. 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 终端节点和访问令牌信息。
3. 在入站自动预置对话框中，复制以下选项的各个值：

   - SCIM 端点
   - 访问令牌

   在本教程中，您稍后将输入这些值，以在 Google Workspace 中配置预置。
4. 选择关闭。

   现在，您已在 IAM Identity Center 控制台中设置了预置，下一步您将使用 Google Workspace 自动预置 IAM Identity Center 连接器，以完成剩余任务。

步骤 7：在中配置 auto 配置 Google Workspace

1. 使用管理员帐户登录 Google 管理控制台，然后导航至应用程序>网络和移动应用程序。
2. 选择 Amazon Web Services 应用程序。
3. 在自动预置部分，选择配置自动预置。
4. 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 Google Workspace 中的访问令牌字段，然后选择继续。此外，在前面的过程中，您复制了 IAM Identity Center 中的 SCIM 终端节点值。将该值粘贴到端点 URL 字段中。确保删除 URL 末尾的尾部正斜杠并选择继续。
5. 验证所有必需的 IAM Identity Center 属性（即标有 * 的属性）是否已映射到 Google Cloud Directory 属性。如果没有，请选择向下箭头并映射到适当的属性。选择继续。
6. 在预置范围中，您可以选择 Google Workspace 目录的一个组，以提供对 Amazon Web Services 应用程序的访问权限。跳过此步骤并选择继续。
7. 在取消预置中，您可以选择如何响应移除用户访问权限的不同事件。对于每种情况，您都可以指定在多久之后开始取消预置：

   - 24 小时内
   - 一天后
   - 七天后
   - 21 天后

   对于每种情况，都有一个时间设置，用来确定何时暂停账户的访问权限，以及何时删除账户。

   > **Tip**
   >
   > 设置删除用户账户前的等待时间时，其长度应始终长于暂停用户账户前的等待时间。

8. 选择完成。您将返回到 Amazon Web Services 应用程序页面。
9. 在自动预置部分，打开切换开关，将其从非活动更改为活动。

   > **Note**
   >
   > 如果未为用户打开 IAM Identity Center，激活滑块将被禁用。选择用户访问权限并打开应用程序以启用滑块。

10. 在确认对话框中，选择打开。

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。用户页面列出了您的 Google Workspace 目录中通过 SCIM 创建的用户。如果尚未列出用户，可能是由于预置仍在进行中。尽管在大多数情况下，预置可以在几分钟内完成，但最多可能需要 24 小时。确保每隔几分钟刷新一次浏览器窗口。

    选择一名用户并查看其详细信息。信息将与 Google Workspace 目录中的信息匹配。

> **恭喜您！**
>
> 您已成功在Google Workspace和之间建立 SAML 连接， AWS 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。

步骤 8：向Google Workspace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 AWS 账户。
2. 在 AWS 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 AWS 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 AWS 账户 正在配置中。等待该过程完成。

您将返回到该 AWS 账户 页面。系统会显示一条通知消息，告知您 AWS 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，他们可以选择角色。*AdministratorAccess*

> **Note**
>
> Google Workspace 的 SCIM 的自动同步仅支持预置用户，无法自动预置组。您无法使用 AWS Management Console为 Google Workspace 用户创建组。预置用户后，您可以使用 CLI 或 API 操作创建组

步骤 9：确认Google Workspace用户对 AWS 资源的访问权限

1. 使用测试用户账户登录 Google。
2. 选择 Google apps 启动器（华夫饼）图标。
3. 滚动到应用程序列表底部，您的自定义 Google Workspace 应用程序就在这里。显示了两个应用程序：Amazon Web Services 和 AWS 访问门户。
4. 选择 AWS 访问门户应用程序。您已登录门户并可以看到该 AWS 账户 图标。展开该图标可查看用户可以访问的 AWS 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。

> **Note**
>
> 如果您选择 Amazon Web Services 应用程序，会收到 SAML 错误。该应用程序适用于已预置为 IAM 用户的 Google Workspace 用户，而本教程是将您的 Google Workspace 用户预置为 IAM Identity Center 中的用户。

5. 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。
6. 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，您指定了同时启用管理控制台和编程访问权限，因此存在这两个选项。选择管理控制台，打开 AWS Management Console。
7. 用户已登录到控制台。

（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 AWS 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。

后续步骤

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

- 使用创建群组身份存储 AWS CLI 操作或 CreateGroupAPI 为您的用户创建群组。

在为 AWS 账户 和应用程序分配访问权限时，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账户和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。

  权限集定义用户和组对某一 AWS 账户账户的访问级别。权限集存储在 IAM Identity Center 中，可以配置给一个或多个 AWS 账户。您可以为用户分配多个权限集。

> **Note**
>
> 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。请务必查看如何为 Google Workspace 管理 SAML 证书。

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。此预置使用跨域身份管理系统 (SCIM) v2.0 协议。您可以使用 IAM Identity Center SCIM 终端节点和访问令牌在 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。
- 支持 IAM Identity Center 的账户（免费）。有关更多信息，请参阅启用 IAM Identity Center。
- 从您的 JumpCloud 账户到 IAM Identity Center 的 SAML 连接，如 IAM Identity Center JumpCloud 文档中所述。
- 将 IAM Identity Center 连接器与您想要允许访问 AWS 账户的组关联。

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 JumpCloud 中的 AWS 单点登录连接器关联的组才会与 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。
- 如果 Identity Center 目录中存在具有相同用户名和电子邮件的现有用户，该用户将被覆盖并与 JumpCloud 中的 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 终端节点和访问令牌信息。
4. 在入站自动预置对话框中，复制以下选项的每个值。稍后在 IdP 中配置预置时，您需要粘贴这些内容。
   a. SCIM 端点
   b. 访问令牌
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 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 终端节点值。将该值粘贴到 JumpCloud IAM Identity Center 连接器的基本 URL 字段中。确保删除 URL 末尾的尾部正斜杠。
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 内的账户。

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

如果您选择配置 IAM Identity Center 的属性来管理对 AWS 资源的访问，则这是 JumpCloud 的可选过程。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 Identity Center。
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 AWS 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

AWS 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 Microsoft Entra ID（以前称为 Azure Active Directory 或 Azure AD）中的用户和组信息自动预置（同步）到 IAM Identity C enter。

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。有关详细信息，请参阅 Microsoft 网站上的快速入门：设置租户。
- 已启用 AWS IAM Identity Center 的账户。有关更多信息，请参阅 AWS IAM Identity Center 用户指南中的启用 IAM Identity Center。

步骤 1：准备 Microsoft 租户

在本步骤中，您将了解如何安装和配置 AWS IAM Identity Center 企业应用程序并为新创建的 Microsoft Entra ID 测试用户分配访问权限。

Step 1.1 >

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

在此过程中，您将在 AWS IAM Identity Center 中安装 Microsoft Entra ID 企业应用程序。稍后您将需要通过此应用程序配置与 AWS 的 SAML 连接。

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 **`AWS IAM Identity Center`**。
4. 从结果区域中选择 AWS 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：在为 Nikki 分配 AWS IAM Identity Center 的权限之前测试其体验

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栏中，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 AWS 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 AWS 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 AWS 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. 在添加分配页面，选择分配。现在，NikkiWolf 出现在分配给 AWS IAM Identity Center 应用程序的用户列表中。

步骤 2：准备 AWS 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 AWS 资源所需的权限。

Step 2.1 >

步骤 2.1：在 IAM Identity Center 中创建 RegionalAmin 权限集

此权限集将用于向 Nikki 授予必要的 AWS 账户权限，以便其从 AWS Management Console 的账户页面管理区域。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. 在多账户权限下，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。您应该会看到 RegionalAdmin 显示在权限集列表中。

Step 2.2 >

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

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 - 输入创建 Microsoft Entra ID 用户时使用的 **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：在 IAM Identity Center 中将 Nikki 分配至 RegionalAdmin 权限集

在这里，您可以找到 Nikki 所管理区域中的 AWS 账户，然后为其分配成功访问 AWS 门户所需的必要权限。

1. 打开 IAM Identity Center 控制台。
2. 在多账户权限下，选择 AWS 账户。
3. 在要授予 Nikki 管理区域权限的账户名称（例如##）旁边，选择复选框，然后选择分配用户和组。
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。

步骤 3：配置和测试 SAML 连接

在此步骤中，您将使用 Microsoft Entra ID 中的 AWS IAM Identity Center 企业应用程序以及 IAM Identity Center 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 控制台启动更改身份源向导，并检索元数据文件和 AWS 的特定登录 URL（在下一步配置与 Microsoft Entra ID 的连接时需要输入）。

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的服务提供商元数据下，选择下载元数据文件，以将其下载到您的系统中。
5. 在同一部分，找到 AWS 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. 将此页面保持为打开状态，然后进入下一步（**Step 3.2**），在 Microsoft Entra ID 中配置 AWS IAM Identity Center 企业应用程序。稍后，您将返回此页面，完成整个过程。

Step 3.2 >

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

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 AWS IAM Identity Center。
2. 在左侧，选择单点登录。
3. 在使用 SAML 设置单点登录页面，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，验证标识符和回复 URL 的值现在是否都指向 AWS 中以 `https://<REGION>.signin.aws.amazon.com/platform/saml/` 开头的端点。

5. 在登录 URL（可选）下，粘贴您在上一步（**Step 3.1**）复制的 AWS 访问门户登录 URL 值，选择保存，然后点击 X 关闭窗口。
6. 如果提示测试 AWS IAM Identity Center 的单点登录，选择不，我稍后再测试。您将在稍后的步骤中进行此项验证。
7. 在使用 SAML 设置单点登录页面的 SAML 证书部分，在联合身份验证元数据 XML 旁边，选择下载，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 AWS 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 AWS 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 AWS 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，选择会将 Nikki 重定向到 AWS 访问门户的 AWS 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栏中，选择我的应用程序。
4. 在我的应用程序页面，选择名为 AWS 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 Microsoft 的登录页面，选择您的 NikkiWolf 凭证。如果再次提示您进行身份验证，请再次选择您的 NikkiWolf 凭证。这应该会自动将您重定向到 AWS 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 AWS 访问门户登录 URL 的值与您在 **Step 3.1** 中复制的值相匹配。

6. 确认是否显示 AWS 账户图标

。

> **Tip**
>
> 如果页面为空，且未显示 AWS 账户图标，请确认是否已成功将 Nikki 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 AWS 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 AWS 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 AWS 访问门户中，选择 AWS 账户图标

，

以展开账户列表。选择该图标后，对于您在其中定义了权限集的任何账户，其账户名称、账户 ID 和与之关联的电子邮件地址都将显示出来。

2. 选择对其应用了权限集的账户名称，例如##（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. 在 RegionalAdmin 旁边，选择管理控制台，以担任您在 RegionalAdmin 权限集中定义的角色。这会将您重定向至 AWS Management Console 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 AWS 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 终端节点和 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，https://scim.*us-east-2*.amazonaws.com/*1111111111-2222-3333-4444-555555555555*/scim/v2/

   b. 访问令牌 - 选择显示令牌以复制该值。

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 测试用户已就位，并且在 IAM Identity Center 启用了 SCIM，您可以继续在 Microsoft Entra ID 中配置 SCIM 同步设置。

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 AWS 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 4.1** 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，您应该会看到显示了 RichRoe 用户。请注意，在创建者列，值将设置为 SCIM。
3. 选择 RichRoe，在配置文件下，验证是否从 Microsoft Entra ID 复制了以下属性。

   - 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 AWS 资源的访问权限级别。例如，您可以将 RichRoe 分配给之前用于授予 Nikki 管理区域权限的 **RegionalAdmin** 权限集（请参阅 **Step 2.3**），然后使用 **Step 3.5** 测试他的访问权限级别。

> **恭喜您！**
>
> 您已成功在 Microsoft 和 AWS 之间建立了 SAML 连接，并验证了自动预置可以正常运作，确保一切同步。现在，您可以运用所学到的方法，更顺利地设置生产环境。

在生产环境中将 SCIM 与 Microsoft Entra ID 结合使用的注意事项

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。

> **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。

访问控制属性

访问控制属性用于确定身份源中的哪些人可以访问 AWS 资源的权限策略。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。只能读取和配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 Entra ID 文档中的基于分配的范围界定。

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 配置到 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 Entra ID 文档中的预览限制。

排查 Microsoft Entra ID 的 SCIM 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"}
```

您还可以检查 AWS CloudTrail 来查找失败事件。这可以通过使用以下过滤器在 CloudTrail 的事件历史记录控制台中搜索来完成：

```
"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 传递的值之一包含的值比预期多。这里的解决方案是检查 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。

有关故障排除提示，请参阅 排查 IAM Identity Center 问题。

步骤 5：（可选）配置 ABAC

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。

Method 1

方法 1：在 Microsoft Entra ID 中配置用户属性，用于实现 IAM Identity Center 中的访问控制

在以下步骤中，您将确定 IAM Identity Center 应使用 Microsoft Entra ID 中的哪些属性管理对 AWS 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 AWS 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`*。将 *`AttributeName`* 替换为您在 IAM Identity Center 中期望的属性名称。例如，`AccessControl:`**`Department`**。

   c. 对于 Namespace (命名空间)，请输入 **`https://aws.amazon.com/SAML/Attributes`**。

   d. 对于 Source (源)，请选择 Attribute (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。

Method 2

方法 2：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 AWS 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 Okta 和 IAM Identity Center 配置 SAML 和 SCIM

您可以使用跨域身份管理系统 (SCIM) v2.0 协议将用户和组信息从 Okta 自动预置（同步）到 IAM Identity Center。要在 Okta 中配置此连接，您可以使用 IAM Identity Center 的 SCIM 终端节点和 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 和您的 Okta 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。

如果您尚未启用 IAM Identity Center，请参阅 启用 AWS IAM Identity Center。

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 AWS 资源的访问权限。

> **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。

开始前的准备工作

在Okta和 IAM Identity Center 之间配置 SCIM 配置之前，我们建议您先进行审查使用自动预置的注意事项。

在开始之前，确认以下事项：

- 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。任何具有多个值的用户都将无法同步。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。
- 如果您更新用户的地址，则必须指定街道地址、城市、州、邮政编码和国家/地区代码值。如果同步时未为 Okta 用户指定这些值中的任何一个，则不会预置该用户（或对用户的更改）。

> **Note**
>
> 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。

步骤 1：从您的 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 AWS 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`。

将 Okta admin dashboard 保持为打开状态，您将在后续步骤中继续使用该控制台。

步骤 2：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. 在选择身份来源 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 IAM Identity Center 元数据文件，并将其保存在您的系统中。在本教程中，您稍后将向 Okta 提供 IAM Identity Center SAML 元数据文件。

      将以下项目复制到文本文件，以便于访问：

      - IAM Identity Center 断言使用者服务 (ACS) URL
      - 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，在 IdP SAML 元数据下，选择 “选择文件”，然后选择您在上一步中创建的`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 ACCEPT。
7. 选择更改身份源。

   保持 AWS 控制台处于打开状态，下一步中您将继续使用该控制台。

8. 返回 Okta admin dashboard，选择 AWS IAM Identity Center 应用程序的登录选项卡，然后单击编辑。
9. 在高级登录设置下，输入以下内容：

   - 在 ACS URL 中，输入您复制的 IAM Identity Center 断言使用者服务 (ACS) URL 值
   - 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，选择下拉菜单中的一个选项。

     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，您可以在 IAM Identity Center 预置 Okta 的用户了。保持Okta admin dashboard打开状态，然后返回 IAM Identity Center 控制台进行下一步。

步骤 3：预置 Okta 的用户

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：

   - SCIM 端点
   - 访问令牌

   在本教程的后面部分，您将输入这些值来配置配置Okta。
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 应用程序页面上，选择配置选项卡，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配置。
7. 使用您在本教程之前步骤中从 IAM Identity Center 复制的 SCIM 预置值，配置 Okta：

   a. 在基本 URL 字段，输入 SCIM 端点值。确保删除 URL 末尾的尾部正斜杠。

   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 AWS IAM Identity Center 验证成功！消息。
9. 选择保存。您将导航到 “设置” 区域，并选择 “集成”。
10. 在 “设置” 下，选择 “至应用程序”，然后选中要启用的每项 “向应用程序预配” 功能对应的 “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：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，与 IAM Identity Center 同步组和用户。

1. 在 OktaIAM Identity Center 应用程序页面中，选择任务选项卡。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。选择包含您分配给 IAM Identity Center 应用程序的所有组的 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. 如果有用户不属于您推送到 IAM Identity Center 的组，请使用以下步骤单独添加他们：

   在分配页面，选择分配，然后选择分配给人员。

5. 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 AWS 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。

6. 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 SAML 连接， AWS 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。

步骤 5：授予 Okta 用户对账户的访问权限

1. 在 IAM Identity Center 导航窗格的多账户权限下，选择 AWS 账户。
2. 在 AWS 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 AWS 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 AWS 账户 正在配置中。等待该过程完成。

您将返回到该 AWS 账户 页面。系统会显示一条通知消息，告知您 AWS 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*

> **Note**
>
> Okta 的 SCIM 的自动同步仅支持预置用户，无法自动预置组。您无法使用 AWS Management Console为 Okta 用户创建组。预置用户后，您可以使用 CLI 或 API 操作创建组

步骤 6：确认Okta用户对 AWS 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 AWS IAM Identity Center 图标。
3. 您已登录门户并可以看到该 AWS 账户 图标。展开该图标可查看用户可以访问的 AWS 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，您指定了同时启用管理控制台和编程访问权限，因此存在这两个选项。选择管理控制台，打开 AWS Management Console。
6. 用户已登录到控制台。

（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 AWS 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。

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 AWS 账户，请参阅将用户访问权限分配给 AWS 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。

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。您可以在 OneLogin 中使用 IAM Identity Center 的 SCIM 终端节点和 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 账户。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 的账户（免费）。有关更多信息，请参阅启用 IAM Identity Center。
- 从您的 OneLogin 账户到 IAM Identity Center 的 SAML 连接。有关详细信息，请参阅 AWS 合作伙伴网络博客上的在 OneLogin 和 AWS 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 终端节点和访问令牌信息。
4. 在入站自动预置对话框中，复制以下选项的每个值。稍后在 IdP 中配置预置时，您需要粘贴这些内容。

a. SCIM 端点

b. 访问令牌

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。此过程假设您已配置 OneLogin 中的 AWS 单点登录应用程序以进行 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 AWS 合作伙伴网络博客上的在 OneLogin 和 AWS 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，然后从左侧导航栏中选择配置。
3. 在上一过程中，您复制了 IAM Identity Center 中的 SCIM 终端节点值。将该值粘贴到 OneLogin 中的 SCIM Base URL 字段中。确保删除 URL 末尾的尾部正斜杠。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. 在左侧导航栏中，选择预置。
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. 在左侧导航栏中，选择用户。
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 AWS 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，请导航到预置页面，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、删除用户和/或更新用户，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

如果您选择配置将在 IAM Identity Center 中使用的属性来管理对 AWS 资源的访问，那么这是 OneLogin 的可选过程。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，然后从左侧导航栏中选择参数。
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 AWS 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。

故障排除

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 中删除了一个组，但没有先从 OneLogin 中删除它，现在我遇到了用户/组同步问题

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。您可以使用 IAM Identity Center SCIM 终端节点和访问令牌在 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

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 的账户（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。

额外注意事项

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 终端节点和访问令牌信息。
4. 在入站自动预置对话框中，复制以下选项的每个值。稍后在 IdP 中配置预置时，您需要粘贴这些内容。

   a. SCIM 端点

   b. 访问令牌
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 终端节点值。将该值粘贴到 PingFederate 控制台中的 SCIM URL 字段中。确保删除 URL 末尾的尾部正斜杠。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 过滤条件。
    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 Id PingFed entity Center 中按速率配置用户属性以进行访问控制

如果您选择配置将在 IAM Identity Center 中使用的属性来管理对 AWS 资源的访问，那么这是 PingFederate 的可选过程。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 AWS 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。

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 终端节点和访问令牌在 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。

本指南基于截至 2020 年 10 月的 PingOne。新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 PingOne 预置 IAM Identity Center 的更多信息。本指南还包含一些有关通过 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

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 的账户（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。

额外注意事项

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。

- 自 2020 年 10 月起，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预置，请删除相关 SCIM 持有者令牌，和/或在 IAM Identity Center 中禁用 自动预置。
- 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 PingOne 中的 SAML_SUBJECT 映射选择一个在 PingOne 中的目录中唯一、非空且格式为电子邮件/UPN（例如，user@domain.com）的用户属性。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 终端节点和访问令牌信息。
4. 在入站自动预置对话框中，复制以下选项的每个值。稍后在 IdP 中配置预置时，您需要粘贴这些内容。
   a. SCIM 端点
   b. 访问令牌
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 终端节点值。将该值粘贴到 PingOne IAM Identity Center 应用程序中的 SCIM URL 字段中。确保删除 URL 末尾的尾部正斜杠。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 额外注意事项 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 内的账户和应用程序。

    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

如果您选择配置 IAM Identity Center 的属性来管理对 AWS 资源的访问，那么这是 PingOne 的可选过程。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 AWS 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。

IAM Identity Center 中的常见任务入门

如果您是 IAM Identity Center 的新用户，可通过以下基本工作流程开始使用该服务：

1. 如果您使用的是 IAM Identity Center 的组织实例，或者如果您使用的是 IAM Identity Center 的账户实例， AWS 账户 请登录管理账户的控制台，然后导航到 IAM Identity Center 控制台。
2. 从 IAM Identity Center 控制台选择用于存储用户身份和组身份的目录。默认情况下，IAM Identity Center 会为您提供一个可用于配置用户访问权限的目录。如果您希望使用其他身份源，可以连接您的活动目录或外部身份提供商。
3. 对于组织实例，请选择组织中的账户，然后从目录中选择用户或组以及要授予他们的权限，为用户分配对 AWS 账户的访问权限。
4. 请通过以下方式为用户提供对应用程序的访问权限：
   a. 从应用程序目录中选择一个预集成的应用程序，或添加自己的 SAML 2.0 应用程序，以设置客户托管的 SAML 2.0 应用程序。
   b. 配置应用程序的属性。
   c. 分配用户访问权限至该应用程序。我们建议您通过组成员资格分配用户访问权限，而不是添加单独的用户权限。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。
5. 如果您使用的是默认 IAM Identity Center 目录，请告诉您的用户如何登录 AWS 访问门户。IAM Identity Center 中的新用户必须先激活其用户证书，然后才能使用他们登录 AWS 访问门户。有关更多信息，请参阅《AWS 登录 用户指南》中的登录 AWS 访问门户

在完成 IAM Identity Center 的初始配置后，这部分的主题将有助于您熟悉接下来执行的常见任务。

如果您尚未启用 IAM Identity Center，请参阅 启用 AWS IAM Identity Center。

主题

- 创建权限集
- 为 IAM 身份中心用户分配 AWS 账户 访问权限
- 使用您的 IAM 身份中心证书登录 AWS 访问门户
- 为群组分配 AWS 账户 访问权限
- 设置对应用程序的单点登录访问权限
- 查看用户和群组分配

创建权限集

权限集存储在 IAM Identity Center 中，定义用户和组对 AWS 账户的访问级别。您最先创建的权限集应该是管理权限集。如果您完成了任意一套 入门教程，则表示您已经创建了管理权限集。按《IAM 用户指南》中工作职能的AWS 托管策略主题所述，使用此过程创建权限集。

1. 请执行以下任一操作，登录 AWS Management Console。
   - AWS （root 用户）新手-选择 R oot 用户并输入您的 AWS 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 AWS （IAM 证书）— 使用具有管理权限的 IAM 凭证登录。
2. 打开 IAM Identity Center 控制台。
3. 在 IAM Identity Center 导航窗格的多账户权限下，选择权限集。
4. 选择创建权限集。
   a. 在选择权限集类型页面的权限集类型部分，选择预定义的权限集。
   b. 在预定义权限集的策略部分，选择以下选项之一：
      - AdministratorAccess
      - Billing
      - DatabaseAdministrator
      - DataScientist
      - NetworkAdministrator
      - PowerUserAccess
      - ReadOnlyAccess
      - SecurityAudit
      - SupportUser
      - SystemAdministrator
      - ViewOnlyAccess
5. 在指定权限集详细信息页面上，保留默认设置并选择下一步。默认设置将您的会话限制为一小时。
6. 在查看并创建页面上，确认以下信息：
   1. 对于 “步骤 1：选择权限集类型”，显示您选择的权限集类型。
   2. 对于 “步骤 2：定义权限集详细信息”，显示您选择的权限集的名称。

3. 选择 创建。

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，您可以运行 IAM Access Analyzer，以使用 AWS 托管策略监控主体。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 AWS 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。与使用权限的管理权限集不同，该AdministratorAccessPowerUserAccess 权限集不允许管理 IAM 用户和群组。当你登录 AWS 访问门户访问你的 AWS 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 AWS 托管策略。每项策略都授予对 AWS 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AWS 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 AWS 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) AWS 账户 并使用 AWS 管理控制台或 AWS 命令行界面 (AWS 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 AWS 账户之前 AWS 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 设置会话持续时间。
- 您还可以配置 AWS 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 AWS 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 配置 AWS 访问门户和 IAM Identity Center 集成应用程序的会话持续时间。

- 登录 AWS 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 AWS 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，请选择与可用于在账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，请参阅为群组分配 AWS 账户 访问权限。

为 IAM 身份中心用户分配 AWS 账户 访问权限

要为 IAM Identity Center 用户设置 AWS 账户 访问权限，您必须将该用户分配到 AWS 账户 和权限集。

1. 请执行以下任一操作，登录 AWS Management Console。

   - AWS （root 用户）新手-选择 R oot 用户并输入您的 AWS 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 AWS （IAM 证书）— 使用具有管理权限的 IAM 凭证登录。

2. 打开 IAM Identity Center 控制台。
3. 在导航窗格的多账户权限下，选择 AWS 账户。
4. 在 AWS 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 AWS 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。
5. 选择分配用户或组。
6. 对于“步骤 1：选择用户和组”，在“将用户和组分配给“***AWS ## ##***”页面上，执行以下操作：

   1. 在用户选项卡上，选择要向其授予管理权限的用户。

      要筛选结果，请开始在搜索框中键入所需用户的姓名。

   2. 确认选择正确的用户后，选择下一步。

7. 对于“步骤 2：选择权限集”，在“将权限集分配给“***AWS ## ##***”页面的“权限集”下，选择一个权限集以定义用户和组对此的访问级别 AWS 账户。
8. 选择下一步。
9. 对于步骤 3：审阅并提交，在查看作业并将其提交到“***AWS ## ##***”页面上，执行以下操作：

1. 查看选定的用户和权限集。
2. 确认已为权限集分配了正确的用户后，选择 “提交”。

> **Important**
>
> 用户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。

10. 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 AWS Managed Microsoft AD 目录或自我管理目录作为身份源，但没有将 RADIUS M AWS Directory Service FA 与一起使用。

> **Note**
>
> 如果您正在使用外部身份提供商，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账户访问权限时，IAM Identity Center 会创建相应的 IAM 角色。此角色由 IAM Identity Center 控制 AWS 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。

使用您的 IAM 身份中心证书登录 AWS 访问门户

AWS 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 AWS 账户 和应用程序的单点登录访问权限。

完成以下步骤以确认 IAM Identity Center 用户可以登录 AWS 访问门户并访问 AWS 账户。

1. 请执行以下任一操作，登录 AWS Management Console。

    - AWS （root 用户）新手-选择 R oot 用户并输入您的 AWS 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 AWS （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 AWS 访问门户 URL。
5. 使用以下方式之一登录：

   - 如果您使用 Active Directory 或外部身份提供商 (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。

门户体验会有所不同，具体取决于 AWS 区域 您 AWS 账户 所在的门户、标准 AWS 访问门户和传统 AWS 访问门户。

登录 AWS 访问门户后，如果您看到 AWS 账户 图

标，  请
按照传统访问门户选项卡中的步骤进行操作，否则请按照标准 AWS AWS 访问门户选项卡中的步骤进行操作。

Standard AWS access portal

1. 在 “帐户” 选项卡中，找到您的 AWS 账户 并将其展开。
2. 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 AWS 访问门户中。选择要用于会话的 IAM 角色名称。
3. 如果您被重定向到 AWS 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 AWS 账户。

> **Note**
>
> 如果您没有看到任何列出的 AWS 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 将用户访问权限分配给 AWS 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， AWS Management Console 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 AWS 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账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。

Legacy AWS access portal

1. 选择账户名称，以显示可用的权限集。

   登录时，分配给用户的权限集的名称在 AWS 访问门户中显示为可用角色。如果您为该用户分配了AdministratorAccess和账单权限集，则这些角色将显示在 AWS 访问门户中。
2. 在要用于会话的权限集的名称右侧，选择管理控制台链接。
3. 如果您被重定向到 AWS 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 AWS 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， AWS Management Console 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 AWS 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账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。

为群组分配 AWS 账户 访问权限

在 IAM Identity Center 中创建了管理用户并创建了可用于执行权限最低的任务的其他权限集之后，您可以 AWS 账户 向用户组提供访问权限。

我们建议您将访问权限直接分配给组而不是单个用户。例如，如果您基于组织单位创建组和权限集，将用户移至不同的组织单位时，您只需将该用户移至不同的组，他们将自动获得新组织单位所需的权限，并失去先前组织单位的权限。

将用户组访问权限分配给 AWS 账户

1. 打开 IAM Identity Center 控制台。

> **Note**
>
> 如果您的身份源是，请确 AWS Managed Microsoft AD 保 IAM Identity Center 控制台使用的是您的 AWS Managed Microsoft AD 目录所在的区域，然后再继续下一步操作。

2. 在导航窗格的多账户权限下，选择 AWS 账户。
3. 在 AWS 账户 页面上，将显示您的组织的树视图列表。选中要为其分配单点登录访问权限的一个或多个 AWS 账户 旁边的复选框。

> **Note**
>
> AWS 账户 每个权限集最多可以选择 10 个。

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“***AWS-account-name***”页面，选择组选项卡，然后选择一个或多个组。

   要筛选结果，请开始在搜索框中键入所需组的名称。

   要显示您选择的组，请选择选定的用户和组旁边的横向三角形。

   确认选择了正确的组后，选择下一步。
6. 对于步骤 2：选择权限集，在将权限集分配给“***AWS-account-name***”页面，选择一个或多个权限集

> **Note**
>
> 如果在开始此过程之前，您没有创建所需的权限集，请选择创建权限集，然后按照 创建权限集 中的步骤进行操作。创建要应用的权限集后，在 IAM Identity Center 控制台中，返回到 AWS 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。

   确认选择了正确的权限集后，选择下一步。
7. 对于步骤 3：查看并提交，在查看任务并将其提交到“***AWS-account-name***”页面上，执行以下操作：

1. 查看选定的组和权限集。
2. 确认选择了正确的组和权限集之后，选择提交。

> **Important**
>
> 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 AWS Organizations 管理账户进行操作的权限。由于它是高权限账户，因此其他安全限制要求您先拥有 IAM FullAccess 策略或同等权限，然后才能进行设置。您 AWS 组织中的任何成员账户都不需要这些额外的安全限制。

或者，您可以使用 AWS 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 AWS 访问门户或使用 AWS Command Line Interface (AWS CLI) 命令。

设置对应用程序的单点登录访问权限

IAM Identity Center 支持两种应用程序类型： AWS 托管应用程序和客户托管应用程序。

AWS 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。您可以从支持 SAML 2.0 的常用应用程序目录中进行选择，也可以设置自己的 SAML 2.0 应用程序或 OAuth 2.0 应用程序。

设置对应用程序的单点登录访问权限的配置步骤因应用程序类型而异。

设置 AWS 托管应用程序

AWS 诸如 Amazon Managed Grafana 和 Amazon Monitron 之类的托管应用程序与 IAM 身份中心集成，可以将其用于身份验证和目录服务。要将 AWS 托管应用程序设置为与 IAM Identity Center 配合使用，您必须直接从控制台为适用的服务配置应用程序，或者必须使用应用程序 API。

设置应用程序目录中的应用程序

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。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。

要设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 在 IAM Identity Center 控制台中配置应用程序属性。
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

请使用此过程在 IAM Identity Center 和您自己的 SAML 2.0 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，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 在 IAM Identity Center 控制台中配置应用程序属性。
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。

设置应用程序后，您的用户可以根据您分配的权限从其 AWS 访问门户中访问您的应用程序。

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访问 AWS 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，该应用程序可以在请求中传递用户的身份，以访问 AWS 服务中的数据。有关更多信息，请参阅 对客户托管的应用程序使用可信身份传播。

有关支持的应用程序类型的更多信息，请参阅管理对应用程序的访问。

查看用户和群组分配

您可以从 “用户和群组” 页面查看谁有权访问 IAM Identity Center 中的内容。使用此过程可以查看用户对 AWS 帐户、权限集、应用程序和组的访问级别。

1. 打开 IAM Identity Center 控制台。
2. 根据您是要编辑一组用户还是要编辑一个单独分配的用户，选择 “用户” 或 “组”。
3. 从列表中选择一个用户或群组。
4. 选择是要查看帐户分配、应用程序分配还是小组分配：

   - AWS 帐户和权限集分配
     1. 选择 Accounts 选项卡。
     2. 从列表中选择一个帐户以查看用户和组的权限集分配。
     3. 选择要查看的权限集以查看策略和分配的详细信息。
   - 应用程序分配
     1. 选择 “应用程序” 选项卡，查看哪些应用程序已分配给用户或组。
     2. 从列表中选择一个应用程序以查看任务详细信息。
   - 小组作业
     1. 在 “用户” 页面中，选择 “群组” 选项卡。
     2. 选择一个群组以查看用户的小组分配。

管理 IAM Identity Center 的组织实例和账户实例

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。

AWS 账户 可以启用 IAM 身份中心的类型

要启用 IAM Identit AWS Management Console 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 AWS 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 AWS 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 AWS 账户 — 用于创建 IAM Identity Center 的组织实例或账户实例。独立版 AWS 账户 不是由管理的 AWS Organizations。只有一个 IAM Identity Center 实例可以 AWS 账户 与独立实例相关联，您可以将该实例用于该独立实例中的应用程序分配 AWS 账户。

能力	AWS 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 AWS 账户
管理用户	 是	 是	 是
AWS 访问门户，可通过单点登录访问您的 AWS 托管应用程序	 是	 是	 是
多账户权限	 是	 否	 否

能力	AWS 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 AWS 账户
AWS 访问门户，通过单点登录即可访问您的 AWS 账户	 是	 否	 否
客户托管的应用程序	 是	 否	 否
委派管理员可以管理实例	 是	 否	 否

主题

IAM Identity Center 的组织实例

当你同时启用 IAM 身份中心时 AWS Organizations，你就是在创建 IAM 身份中心的组织实例。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。 AWS 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。

何时使用组织实例

组织实例是启用 IAM Identity Center 的主要方法，在大多数情况下，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 AWS 账户 中多个用户的权限以及为客户托管的应用程序分配访问权限。
- 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。
- 控制账户实例的创建 — 只要您尚未在可选区域（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AWS 区域 可以由组织中的成员账户创建账户实例。

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 AWS 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 AWS 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 AWS 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 AWS 区域。每个账户只能使用一个实例 AWS 账户。您可以通过以下任一途径创建账户实例：

- 中的成员帐户 AWS Organizations。
- 不由管理 AWS 账户 的独立服务器 AWS Organizations。

成员账户的可用性限制

如果满足以下条件，您就可以在组织的成员账户中部署账户实例：

- 2023 年 11 月 15 日之前，您的组织中没有部署 IAM Identity Center 实例。
- 在 2023 年 11 月 15 日之前，您已将 IAM Identity Cent AWS 区域 er 实例部署到您的组织，并且您的管理员已选择使用账户实例功能。
- 您的管理员没有创建服务控制策略阻止账户实例的创建。
- 无论在哪个 AWS 区域，您已在该相同的账户中拥有 IAM Identity Center 实例。
- 无论部署日期如何，您都没有将 IAM Identity Center 实例部署到可选区域（AWS 区域 默认情况下处于禁用状态）的组织。也就是说，只要在可选加入的 AWS 区域 部署了任何 IAM Identity Center 组织实例，您就无法创建账户实例。
- 您正在无法使用 IAM 身份中心 AWS 区域 的地方工作。有关区域的更多信息，请参阅 AWS IAM Identity Center 地区可用性。

主题

何时使用账户实例

在大多数情况下，建议使用组织实例。仅当符合以下任何一种情况时，才应使用账户实例：

- 您想对支持的 AWS 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 AWS 托管应用程序。
- 您有一个 IAM Identity Center 的组织实例，但您想将 AWS 受支持的托管应用程序部署到一组与组织实例中的用户不同的隔离用户。

> **Important**
>
> 如果您计划使用 IAM Identity Center 支持多个账户中的应用程序，请创建一个组织实例，不要使用账户实例。

账户实例注意事项

账户实例专为特殊用例而设计，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，因此不支持访问权限 AWS 账户。
- 您无法将账户实例转换为组织实例。
- 您无法将账户实例合并到组织实例中。
- 只有特定的 AWS 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时 AWS 账户 所在的位置。
- 如果您将 IAM Identity Center 实例部署到可选区域（默认情况下处于禁用状态）的组织，则在创建组织实例后AWS 区域 ，账户实例的创建将被阻止。现有账户实例将继续运行。

支持的 AWS 托管应用程序

以下是一些支持账户实例的 AWS 应用程序。使用您的 AWS 托管应用程序验证创建账户实例的可用性。

- Amazon Athena
- Amazon CodeCatalyst
- Amazon EMR
- AWS Lake Formation
- Amazon Redshift

在中启用账户实例 AWS Management Console

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 AWS Management Console启用账户实例功能，选择成员账户是否可以创建账户实例。

> **Note**
>
> 无论部署日期如何，只要您尚未将 IAM Identity Center 实例部署到可选区域（默认情况下处于禁用状态）的组织AWS 区域 ，成员账户就可以创建账户实例。通过选择加入方式部署的 IAM Identity Center 的任何组织实例都 AWS 区域 将阻止创建账户实例。有关区域的更多信息，请参阅 AWS IAM Identity Center 地区可用性。

要允许组织中的成员账户创建账户实例

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。

> **Important**
>
> 为成员账户启用 IAM Identity Center 的账户实例是一次性操作。这意味着此操作无法撤销。启用后，您可以通过创建服务控制策略 (SCP) 来限制账户实例的创建。有关说明，请参阅使用服务控制策略控制账户实例的创建。

通过服务控制策略控制账户实例的创建

用户可以创建绑定到 IAM Identity Center 的单个 AWS 账户账户实例的 IAM Identity Center 实例。您可以通过服务控制策略 (SCP) 控制账户实例的创建。

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。您将转到 AWS Organizations 控制台，以创建 SCP，或将其作为声明附加到现有的 SCP。

   服务控制策略是的一项功能 AWS Organizations。有关附加 SCP 的说明，请参阅 AWS Organizations 用户指南中的附加和分离服务控制策略。

您可以将账户实例的创建限制为组织 AWS 账户 内的特定账户，而不是阻止账户实例的创建：

Example ：控制实例创建的 SCP

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

```
    ]
}
```

创建 IAM Identity Center 账户实例

组织实例是启用 IAM Identity Center 的主要方法和推荐方法。请确保您的用例支持创建账户实例，并且您了解注意事项。

通过组织成员账户或独立 AWS 账户创建账户实例

1. 请执行以下任一操作，登录 AWS Management Console。
   - AWS （root 用户）新手 — 以账户所有者的身份登录，方法是选择 Root 用户并输入您的 AWS 账户 电子邮件地址。在下一页上，输入您的密码。
   - 已在使用 AWS （IAM 证书）— 使用具有管理权限的 IAM 凭证登录。
2. 打开 IAM Identity Center 控制台。
3. 在启用 IAM Identity Center下，选择启用。
4. 选择继续创建账户实例，然后选择继续。

   > **Note**
   >
   > 如果存在 IAM Identity Center 组织实例，请确保您的用例需要自己的 IAM Identity Center 账户实例。如果不需要，请选择取消并使用组织实例。

5. 可选。添加要与此账户实例关联的标签。

控制台中会显示通知，表明账户实例已创建成功，并包含实例 ID。您可以在设置摘要中命名实例。

> **Note**
>
> 账户实例默认启用多重身份验证 (MFA)。当用户的设备、浏览器或位置发生变化时，系统会提示其使用 MFA 登录。作为安全方面的最佳实践，我们强烈建议您使用 MFA 验证员工身份。了解 在 IAM Identity Center 中管理 MFA 设备。

确认身份来源、调整多因素身份验证设置和添加 AWS 托管应用程序等管理功能必须在 IAM Identity Center 控制台中完成。

身份验证

用户使用其用户名登录 AWS 访问门户。用户执行此操作时，IAM Identity Center 会根据与用户电子邮件地址关联的目录将请求重定向到 IAM Identity Center 身份验证服务。经过身份验证后，用户可以单点登录访问门户中显示的任何 AWS 账户和第三方 software-as-a-service (SaaS) 应用程序，而无需其他登录提示。这意味着用户不再需要跟踪他们每天使用的各种已分配 AWS 应用程序的多个账户凭证。

身份验证会话

IAM 身份中心维护的身份验证会话有两种类型：一种代表用户登录 IAM 身份中心，另一种代表用户对 AWS 托管应用程序（例如 Amazon SageMaker Studio 或 Amazon Managed Grafana）的访问权限。用户每次登录 IAM Identity Center 时，都会创建一个登录会话，持续时间为 IAM Identity Center 中配置的持续时间，最长可达 90 天。有关更多信息，请参阅管理 AWS 访问门户和 IAM Identity Center 集成应用程序的会话时长。用户每次访问应用程序时，都会使用 IAM Identity Center 登录会话来获取该应用程序的 IAM Identity Center 应用程序会话。IAM Identity Center 应用程序会话的生命周期为 1 小时，也就是说，只要获得这些会话的 IAM Identity Center 登录会话仍然有效，IAM Identity Center 应用程序会话就会每小时自动刷新一次。当用户使用 IAM 身份中心访问 AWS Management Console 或 CLI 时，将使用 IAM 身份中心登录会话来获取 IAM 会话，如相应的 IAM 身份中心权限集所述（更具体地说，IAM 身份中心在目标账户中担任 IAM 角色，由 IAM 身份中心管理）。

当您在 IAM Identity Center 中禁用或删除用户时，将立即阻止该用户登录以创建新的 IAM Identity Center 登录会话。IAM Identity Center 登录会话会被缓存一小时，这意味着，当您在用户的 IAM Identity Center 登录会话处于活动状态时禁用或删除该用户时，他们现有的 IAM Identity Center 登录会话将持续长达一个小时，具体取决于上次刷新登录会话的时间。在此期间，用户可以启动新的 IAM Identity Center 应用程序和 IAM 角色会话。

IAM Identity Center 登录会话到期后，用户无法再启动新的 IAM Identity Center 应用程序或 IAM 角色会话。但是，IAM Identity Center 应用程序会话也可以缓存长达一个小时，这样，在 IAM Identity Center 登录会话到期后，用户可以将应用程序的访问权限保留长达一个小时。任何现有的 IAM 角色会话都将根据在 IAM Identity Center 权限集中配置的持续时间继续进行（管理员可配置，最长 12 小时）。

下表总结了这些行为：

用户体验/系统行为	用户被禁用/删除后的时间
用户无法再登录 IAM Identity Center；用户无法获得新的 IAM Identity Center 登录会话	无（立即生效）
用户无法再通过 IAM Identity Center 启动新的应用程序或 IAM 角色会话	最长 1 小时
用户无法再访问任何应用程序（所有应用程序会话都已终止）	最长 2 小时（IAM Identity Center 登录会话到期时间最长 1 小时，加上 IAM Identity Center 应用程序会话到期时间最长 1 小时）
用户无法再 AWS 账户 通过 IAM 身份中心访问任何内容	最长 13 小时（根据权限集的 IAM Identity Center 会话持续时间设置，IAM Identity Center 登录会话到期时间最长 1 小时，管理员配置的 IAM 角色会话到期时间最长 12 小时）

有关会话的更多信息，请参阅设置会话持续时间。

管理员工身份

AWS Identity and Access Management(IAM) 可帮助您安全地管理身份以及对 AWS 服务和资源的访问。作为一项 IAM 服务，在 AWS IAM Identity Center 中，您可以使用 AWS 一次性创建或连接您的员工身份，并集中管理对多个 AWS 账户 和应用程序的访问。

对于 IAM Identity Center 客户，集中管理对多个 AWS 账户 或应用程序的访问的方式没有变化。对于 IAM Identity Center 的新客户，您可以灵活地将 IAM Identity Center 配置为与 IAM 一起运行或取代单一 AWS 账户 访问管理。

主题

应用场景

以下用例展示了如何使用 IAM Identity Center 来满足不同的业务需求。

主题

启用对您的 AWS 应用程序的单点登录访问（应用程序管理员角色）

如果您是管理 AWS 托管应用程序（如 Amazon SageMaker 或 AWS IoT SiteWise）的应用程序管理员，且您必须为用户提供单点登录访问权限，则此用例提供了指导。

在开始之前，请考虑以下因素：

- 您想在 AWS Organizations 的单独组织中创建测试或生产环境吗？
- 您的组织中是否已启用 IAM Identity Center？ 您是否有权在 AWS Organizations 的管理账户中启用 IAM Identity Center？

查看以下指导，根据业务需求确定后续步骤。

在独立 AWS 账户 中配置我的 AWS 应用程序

如果您必须提供对 AWS 应用程序的单点登录访问权限，且知道您的 IT 部门尚未使用 IAM Identity Center，则可能需要创建独立的 AWS 账户 才能开始使用。默认情况下，当您创建自己的 AWS 账户 时，您将拥有创建和管理自己的 AWS 组织所需的权限。要启用 IAM Identity Center，您必须有 AWS 账户根用户 权限。

IAM Identity Center 和 AWS Organizations 可以在某些 AWS 应用程序（例如 Amazon Managed Grafana）的设置过程中自动启用。如果您的 AWS 应用程序不提供启用这些服务的选项，则必须先设置 AWS Organizations 和 IAM Identity Center，然后才能为应用程序提供单点登录访问权限。

我的组织中未配置 IAM Identity Center

作为应用程序管理员，您可能无法启用 IAM Identity Center，具体取决于您的权限。IAM Identity Center 需要 AWS Organizations 管理账户中的特定权限。在这种情况下，请联系相应的管理员，以在组织管理账户中启用 IAM Identity Center。

如果您有足够的权限启用 IAM Identity Center，请先执行此操作，然后继续设置应用程序。有关更多信息，请参阅 IAM Identity Center 中的常见任务入门。

我的组织中目前已配置 IAM Identity Center

在这种情况下，您可以继续部署 AWS 应用程序，而无需采取任何进一步的操作。

> **Note**
>
> 如果您的组织于 2019 年 11 月 25 日之前在管理账户中启用了 IAM Identity Center，您还必须在管理账户中以及（可选）成员账户中启用 AWS 托管的应用程序。如果您仅在管理账户中启用它们，则稍后可以在成员账户中启用它们。要启用这些应用程序，请前往 IAM Identity Center 控制台的设置页面，在 AWS 托管的应用程序部分选择启用访问权限。有关更多信息，请参阅 配置 IAM Identity Center 以共享身份信息 。

启用对您的 Amazon EC2 Windows 实例的单点登录访问

如果您是管理 Identity Center 目录（IAM Identity Center 的默认身份来源）或受支持的外部身份提供者（IdP）中用户的应用程序管理员，则可以启用对 Amazon EC2 Windows 实例的单点登录访问，并且

您必须从 AWS Fleet Manager 控制台向 IAM Identity Center 提供对 Amazon EC2 Windows 桌面的访问权限。

使用此配置，您可以使用现有的公司凭证安全地访问您的 Amazon EC2 Windows 实例。您无需共享管理员凭证、多次访问凭证或配置远程访问客户端软件。您可以跨多个 AWS 账户 集中授予和撤销对 Amazon EC2 Windows 实例的大规模访问权限。例如，如果您从您的 IAM Identity Center 集成身份来源中删除员工，他们将自动失去对所有 AWS 资源（包括 Amazon EC2 Windows 实例）的访问权限。

有关更多信息，请参阅如何使用 IAM Identity Center 启用对 Amazon EC2 Windows 实例的安全无缝单点登录。

有关如何配置 IAM Identity Center 以启用此功能的演示，请参阅使用 IAM Identity Center 启用对 Amazon EC2 Windows 的单点登录。

用户、组和预调配

处理 IAM Identity Center 中的用户和组时，请记住以下注意事项。

用户名和电子邮件地址的唯一性

IAM Identity Center 的用户必须具有唯一可识别性。IAM Identity Center 采用的用户名是您的用户的主要标识符。尽管大多数人将用户名设置为用户的电子邮件地址，但 IAM Identity Center 和 SAML 2.0 标准并不要求这样做。但是，许多基于 SAML 2.0 的应用程序将电子邮件地址作为用户的唯一标识符。这些应用程序从 SAML 2.0 身份提供商在身份验证期间发送的断言中获得此信息。此类应用程序依赖每个用户电子邮件地址的唯一性。因此，IAM Identity Center 允许您为用户登录指定除电子邮件地址以外的其他内容。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 不支持将组添加到组（嵌套组）。分配对 AWS 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账户和应用程序的访问权限。

用户和组预调配

预调配是使用户和组信息可供 IAM Identity Center 以及 AWS 托管的应用程序或客户托管的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，也可以使用您在 Active Directory 或外

部身份提供商中拥有的用户和组。在您使用 IAM Identity Center 为用户和组分配 AWS 账户 中的访问权限之前，IAM Identity Center 必须先了解这些用户和组。同样，AWS 托管的应用程序和客户托管的应用程序可以与 IAM Identity Center 了解的用户和组一起使用。

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。

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。完成身份源配置后，您可以查找用户或组，然后向其授予单点登录访问 AWS 账户 和/或应用程序的权限。

在 AWS 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：

- 身份中心目录 – 当您首次启用 IAM Identity Center 时，会自动将 Identity Center 目录配置为您的默认身份源。在此位置中，您创建用户和组，并向其分配对您的 AWS 账户 账户和应用程序的访问级别。
- 活动目录 – 如果您想继续使用 AWS Directory Service 或 Active Directory (AD) 中的自管理目录管理您的 AWS Managed Microsoft AD 目录中的用户，请选择此选项。
- 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。

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

主题

更改身份来源的注意事项

尽管您可以随时更改身份来源，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 AWS 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 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。

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。
- API 无出界同步——如果您使用 Active Directory 作为身份源，我们建议您谨慎使用创建、更新和删除 API。IAM Identity Center 不支持出界同步，因此您的身份源不会根据您使用这些 API 对用户或组所做的更改自动更新。
- 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 AWS 访问门户的网址。

有关 IAM Identity Center 如何配置用户和组的信息，请参阅 连接到 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 NameID），您的用户分配、小组分配和小组成员资格就会继续生效。这些断言必须与 IAM Identity Center 中的用户名和群组相匹配。
- 没有出站同步 — IAM Identity Center 不支持出站同步，因此您的外部 IdP 不会根据您在 IAM Identity Center 中所做的用户和群组更改而自动更新。
- SCIM 配置 — 如果您使用的是 SCIM 配置，则只有在您的身份提供商将这些更改发送到 IAM Identity Center 之后，对身份提供商中的用户和群组所做的更改才会反映在 IAM 身份中心中。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 身份中心。请参阅 从外部 IdP 更改为 IAM Identity Center 。

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

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。

有关 IAM Identity Center 如何配置用户和组的信息，请参阅 在 IAM Identity Center 管理身份。

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 nameID），用户分配、组分配和组成员身份将继续有效。

  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——如果您使用 SCIM 预置到 IAM Identity Center，我们建议您查看本指南中特定于 IdP 的信息以及 IdP 提供的文档，以确保启用 SCIM 时新提供程序能够正确匹配用户和组。

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

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。

有关 IAM Identity Center 如何配置用户和组的信息，请参阅 连接到 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 更改身份来源的注意事项 中的信息。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。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 AWS 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。

   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：
   - 选择启动指导式设置。有关如何完成指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。

管理所有身份源类型的登录和属性的使用

IAM Identity Center 提供以下一组功能，使管理员能够控制 AWS 访问门户的使用，为 AWS 访问门户和应用程序中的用户设置会话持续时间，以及使用属性进行访问控制。这些功能使用 Identity Center 目录或外部身份提供者作为您的身份源。

> **Note**
>
> 如果您使用 Active Directory 作为 IAM Identity Center 的身份源，则不支持会话管理。

主题

- 管理 AWS 访问门户和 IAM Identity Center 集成应用程序的会话时长
- 配置 AWS 访问门户和 IAM Identity Center 集成应用程序的会话持续时间
- 删除 AWS 访问门户和 AWS 集成应用程序的会话
- 支持的用户和组属性

管理 AWS 访问门户和 IAM Identity Center 集成应用程序的会话时长

IAM 身份中心管理员可以为与 IAM 身份中心集成的应用程序和配置会话持续时间 AWS 访问门户。会话持续时间配置决定要求用户重新进行身份验证的频率。IAM Identity Center 管理员可以结束有效的 AWS 访问门户会话，这样也可以结束集成应用程序的会话。

有关更多信息，请参阅 配置 AWS 访问门户和 IAM Identity Center 集成应用程序的会话持续时间。有关如何管理和最终用户会话的更多信息，请参阅删除 AWS 访问门户和 AWS 集成应用程序的会话。

> **Note**
>
> 修改 AWS 访问门户会话持续时间和结束 AWS 访问门户会话不会影响您在权限集中定义的 AWS 管理控制台会话持续时间。

配置 AWS 访问门户和 IAM Identity Center 集成应用程序的会话持续时间

对 AWS 访问门户 和 IAM Identity Center 集成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。默认会话持续时间为 8 小时。IAM 身份中心管理员可以指定不同的持续时间，从最少 15 分钟到最长 90 天不等。有关身份验证会话持续时间和用户行为的更多信息，请参阅身份验证。

以下主题提供有关配置 AWS 访问门户和 IAM Identity Center 集成应用程序的会话持续时间的信息。

主题

先决条件和注意事项

以下是为 AWS 访问门户和 IAM Identity Center 集成应用程序配置会话持续时间的先决条件和注意事项。

外部身份提供者

IAM Identity Center 使用 SAML 断言中的`SessionNotOnOrAfter`属性来帮助确定会话的有效期。

- 如果`SessionNotOnOrAfter`未在 SAML 断言中通过，则 AWS 访问门户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 AWS 访问门户中重新进行身份验证。
- 如果在 SAML 断言中传递，`SessionNotOnOrAfter`则会话持续时间值将设置为 AWS 访问门户会话持续时间和您的 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 AWS 资源。
- 如果您的 IdP 的会话持续时间长于 IAM Identity Center 中设置的会话，则根据他们与您的 IdP 的登录会话仍然有效，您的用户无需重新输入证书即可开始新的 IAM 身份中心会话。

> **Note**
>
> 如果您使用 Active Directory 作为 IAM Identity Center 的身份源，则不支持会话管理。

AWS CLI 和 SDK 会话

如果您使用 AWS 软件开发套件 (SDK) 或其他 AWS 开发工具以编程方式访问 AWS 服务，则必须满足以下先决条件才能为 AWS 访问门户和 IAM Identity Center 集成应用程序设置会话持续时间。 AWS Command Line Interface

- 您必须在 IAM 身份中心控制台中配置 AWS 访问门户会话持续时间。
- 您必须在共享 AWS 配置文件中为单点登录设置定义配置文件。此配置文件用于连接到 AWS 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 AWS 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AWS SDK 和工具参考指南中的 SSO 令牌提供程序配置。
- 用户必须运行支持会话管理的版本 AWS CLI 或 SDK。

支持会话管理的 AWS CLI 最低版本

以下是支持会话管理的最低版本。 AWS CLI

- AWS CLI V2 2.9 或更高版本
- AWS CLI V1 1.27.10 或更高版本

有关如何安装或更新最新 AWS CLI 版本的信息，请参阅安装或更新最新版本的 AWS CLI。

如果您的用户正在运行 AWS CLI，则如果您在 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 AWS CLI 会话的最长运行时间为 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 AWS CLI 命令参考。

支持 IAM Identity Center 会话管理的 SDK 最低版本

以下是支持 IAM Identity Center 会话管理的 SDK 最低版本。

SDK	最低版本
Python	1.26.10
PHP	3.245.0
Ruby	aws-sdk-core 3.167.0
Java V2	AWS 适用于 Java 的 SDK v2 (2.18.13)
Go V2	整个 SDK：release-2022-11-11 和特定的 Go 模块：凭证/v1.13.0，配置/v1.18.0
JS V2	2.1253.0
JS V3	v3.210.0
C++	1.9.372
.NET	v3.7.400.0

如何配置会话持续时间

使用以下步骤配置 AWS 访问门户和 IAM Identity Center 集成应用程序的会话持续时间。

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. 在身份验证项下的会话设置旁边，选择配置。这时会出现一个配置会话设置对话框。
5. 在配置会话设置对话框中，选择下拉箭头为您的用户选择最长会话持续时间（以分钟、小时和天为单位）。选择会话时长，然后选择保存。然后您会返回到设置页面。

删除 AWS 访问门户和 AWS 集成应用程序的会话

使用以下步骤查看和删除 IAM 身份中心用户的活动会话。

删除 AWS 访问门户和 IAM Identity Center 集成应用程序的活动会话

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，选择活动会话选项卡。活动会话旁边括号中的数字表示该用户当前处于活动状态的会话数。
5. 选中要删除的会话旁边的复选框，然后选择删除会话。这时会出现一个对话框，确认您正在删除该用户的活动会话。阅读对话框中的信息，如果要继续，请选择删除会话。
6. 您将返回到用户页面。出现绿色闪光条，表示所选会话已成功删除。

有关已撤消的身份验证会话行为的更多信息，请参阅身份验证会话。

支持的用户和组属性

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 支持最常用的属性，无论这些属性是在用户创建期间手动输入的，还是使用同步引擎（如跨域身份管理系统 (SCIM) 规范中定义的）自动预调配的。有关此规范更多信息，请参阅 https://tools.ietf.org/html/rfc7642。有关手动和自动预调配的更多信息，请参阅当用户来自外部 IdP 时进行预置。

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。

用户对象

IAM Identity Center 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

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。

在 IAM Identity Center 管理身份

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 AWS 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 AWS 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。

更改您的身份来源

如果您更喜欢在中管理用户 AWS 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 AWS Directory Service。有关更多信息，请参阅 在 IAM Identity Center 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

- 添加用户
- 添加组
- 将用户添加到组
- 删除 IAM Identity Center 中的组

- 删除 IAM Identity Center 中的用户
- 在 IAM Identity Center 中禁用用户访问
- 编辑用户属性
- 重置最终用户的 IAM Identity Center 用户密码
- 为通过 API 创建的用户发送电子邮件 OTP
- 在 IAM Identity Center 中管理身份时的密码要求

添加用户

您在 Identity Center 目录中创建的用户和组仅在 IAM Identity Center 中可用。通过以下过程，使用 IAM Identity Center 控制台将用户添加到您的 Identity Center 目录。或者，您可以调用 AWS API 操作CreateUser来添加用户。

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 AWS 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，主题行是 “邀请加入” AWS IAM Identity Center（ AWS 单点登录的继任者）。该电子邮件邀请用户代表贵公司访问 IAM Identity Center AWS 访问门户。

        > **Note**
        >
        > 在某些区域，IAM Identity Center 使用 Amazon Simple Email Service 从另一个 AWS 区域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 跨区域调用。
        > 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 AWS 访问门户 URL 和密码详细信息，您可以通过电子邮件地址手动将其发送给用户。

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 自动预置。

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。

添加组

通过以下过程，使用 IAM Identity Center 控制台将组添加到您的 Identity Center 目录。或者，您可以调用 AWS API 操作CreateGroup来添加群组。

添加组

1. 打开 IAM Identity Center 控制台。
2. 选择组。
3. 选择创建组。
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. 选择创建组。

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，请参阅将用户访问权限分配给 AWS 账户。

将用户添加到组

使用以下过程，将用户添加为之前使用 IAM Identity Center 控制台在 Identity Center 目录中创建的组的成员。或者，您可以调用 AWS API 操作CreateGroupMembership将用户添加为群组的成员。

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。

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 AWS 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。通过以下过程，可以使用 IAM Identity Center 控制台删除 Identity Center 目录中的组。

在 IAM Identity Center 中删除组

> **Important**
>
> 本页的说明适用于 AWS IAM Identity Center。它们不适用于 AWS 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 AWS Identity and Access Management 用户指南中的删除 IAM 用户组。

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 Delete group (删除组)。如果您选择删除多个组，请选择删除 # 个组。

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 AWS 账户 和应用程序的访问权限也会被删除。用户被删除后将无法撤消。通过以下过程，使用 IAM Identity Center 控制台删除 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 AWS 访问门户，也无法创建新的登录会话。有关更多信息，请参阅 身份验证会话。

在 IAM Identity Center 中删除用户

> **Important**
>
> 本页的说明适用于 AWS IAM Identity Center。它们不适用于 AWS 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 AWS Identity and Access Management 用户指南中的删除 IAM 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。

在 IAM Identity Center 中禁用用户访问

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。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 AWS 访问门户，也无法创建新的登录会话。有关更多信息，请参阅 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 AWS IAM Identity Center。它们不适用于 AWS 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 AWS 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. 在常规信息部分中，选择禁用用户访问。
5. 在禁用用户访问对话框中，选择禁用用户访问。

编辑用户属性

通过以下过程，可以使用 IAM Identity Center 控制台编辑 Identity Center 目录中的用户属性。或者，您可以调用 AWS API 操作UpdateUser来更新用户属性。

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. 在用户个人资料页面上的个人资料详细信息旁边，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。

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 或外部提供商，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 IAM Identity Center 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 AWS IAM Identity Center。它们不适用于 AWS 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 AWS 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 AWS 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。

为通过 API 创建的用户发送电子邮件 OTP

当您使用 CreateUserAPI 操作创建用户时，他们没有密码。您可以通过选择在使用 API 创建用户时向用户发送电子邮件一次性密码 (OTP) 来更改此设置。用户首次尝试登录时会收到电子邮件 OTP。收到电子邮件 OTP 后，用户登录时必须设置新密码。如果您不启用此设置，则必须生成 OTP 并与您使用 CreateUser API 创建的用户共享。

向使用 CreateUser API 创建的用户发送电子邮件 OTP

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. 随即显示对话框。选中发送电子邮件 OTP 旁边的框。然后，选择保存。状态从禁用更新为启用。

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。如果您已将 IAM Identity Center 以外的身份源配置为身份验证，例如Active Directory外部身份提供商，则您的用户的密码策略将在这些系统中而不是在 IAM Identity Center 中定义和执行。如果您的身份来源是 AWS Managed Microsoft AD，请参阅管理密码策略 AWS 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。

连接到 Microsoft AD 目录

使用 AWS IAM Identity Center，您可以使用连接 Active Directory (AD) 中的自管理目录或中的 AWS Managed Microsoft AD 目录。 AWS 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 AWS 账户应用程序或两者的访问权限。

AWS Directory Service 帮助您设置和运行 AWS 云端托管的独立 AWS Managed Microsoft AD 目录。您还可以使用 AWS Directory Service 将您的 AWS 资源与现有的自管理 AD 连接起来。 AWS 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 AWS Directory Service 对源 AD 实例执行直通身份验证。当您使用 AWS Managed Microsoft AD 作为身份源时，IAM Identity Center 可以处理来自 AWS 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。

> **注意事项**
>
> - 作为先决条件，请确保您的 AD Connector 或 AWS Managed Microsoft AD 中的目录 AWS Directory Service 位于您的 AWS Organizations 管理账户中。有关更多信息，请参阅在 IAM 身份中心确认您的身份来源。
> - IAM Identity Center 不支持基于 SAMBA 4 的 Simple AD 作为连接目录。

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 AWS Managed Microsoft AD，则必须在设置 AWS Managed Microsoft AD 目录的同一 AWS 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， AWS 访问门户使用的访问网址与您的目录相同。
- 使用驻留在管理账户中的 Active Directory：

  您必须在中设置现有 AD Con AWS Managed Microsoft AD nector 或目录 AWS Directory Service，并且该目录必须位于您的 AWS Organizations 管理账户中。一次只能连接一个 AD Connector AWS 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 AWS Managed Microsoft AD。有关更多信息，请参阅：

  - 将目录连接 AWS Managed Microsoft AD 到 IAM 身份中心
  - 将 Active Directory 中的自托管式目录连接到 IAM Identity Center
- 使用驻留在委托管理员账户中的 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 AWS Managed Microsoft AD AWS 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。

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 AWS Managed Microsoft AD 目录或自管理目录与 IAM 身份中心连接。如果您计划连接 Active Directory 中的 AWS Managed Microsoft AD 目录或自管理目录，请确保您的 Active Directory 配置满足中的在 IAM 身份中心确认您的身份来源先决条件。

> **Note**
>
> 强烈建议您启用多重验证，这是最佳安全实践。如果您计划连接 Active Directory 中的 AWS Managed Microsoft AD 目录或自管理目录，但未将 RADIUS MFA AWS Directory Service与一起使用，请在 IAM 身份中心启用 MFA。

AWS Managed Microsoft AD

1. 请查看 连接到 Microsoft AD 目录 中的指南。
2. 按照 将目录连接 AWS 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 中的自托管式目录

1. 请查看 连接到 Microsoft AD 目录 中的指南。
2. 按照 将 Active Directory 中的自托管式目录连接到 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 连接到外部身份提供商 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. 在已添加用户和群组下，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账户的管理访问权限。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。 AWS 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 AWS Managed Microsoft AD 到 IAM 身份中心
- 将 Active Directory 中的自托管式目录连接到 IAM Identity Center
- AWS Managed Microsoft AD 目录的属性映射
- 从 Active Directory 配置用户和组

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

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

连接 AWS 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 AWS 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 Active Directory，然后选择下一步。
5. 在连接活动目录下，从列表中的 AWS 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 中的自托管式目录连接到 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 AWS 账户 权限访问访问 AWS 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 AWS 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 AWS 服务和业务应用程序。单向信任不适用于 IAM Identity Center。

  AWS 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。 AWS Directory Service 相反方向的信任会授予读取用户和群组元数据的 AWS 权限。

  有关设置双向信任的详细信息，请参阅 AWS Directory Service 管理指南中的何时创建信任关系。
- 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托管式 AD，而无需在云中缓存任何信息。有关详细信息，请参阅 AWS Directory Service 管理指南中的连接到目录。

> **Note**
>
> 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 AWS 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 AWS Directory Service 。

> **Note**
>
> IAM Identity Center 不适用于基于 SAMBA4 的 Simple AD 目录。

AWS Managed Microsoft AD 目录的属性映射

属性映射用于将 IAM Identity Center 中存在的属性类型与 AWS Managed Microsoft AD 目录中的类似属性进行映射。IAM Identity Center 从您的 Microsoft AD 目录检索用户属性并将其映射到 IAM Identity Center 用户属性。这些 IAM Identity Center 用户属性映射还用于为您的应用程序生成 SAML 2.0 断言。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。

IAM Identity Center 在应用程序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，系统从您的 Microsoft AD 中检索这些用户属性。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。

IAM Identity Center 还在目录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，请参阅将 IAM 身份中心中的属性映射到 AWS Managed Microsoft AD 目录中的属性。

支持的目录属性属性

下表列出了所有支持的 AWS Managed Microsoft AD 目录属性，这些属性可以映射到 IAM Identity Center 中的用户属性。

Microsoft AD 目录支持的属性
`${dir:email}`
`${dir:displayname}`
`${dir:distinguishedName}`
`${dir:firstname}`
`${dir:guid}`
`${dir:initials}`

Microsoft AD 目录支持的属性
`${dir:lastname}`
`${dir:proxyAddresses}`
`${dir:proxyAddresses:smtp}`
`${dir:proxyAddresses:SMTP}`
`${dir:windowsUpn}`

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。例如，您可以选择 IAM Identity Center 列中的用户属性下的 `subject` 属性。然后将其映射到 `${dir:displayname}` 或 `${dir:lastname}${dir:firstname }` 或任何单个受支持的属性或受支持属性的任意组合。有关 IAM Identity Center 中用户属性的默认映射的列表，请参阅 默认映射。

> **Warning**
>
> 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，“用户名” 是 IAM 身份中心的必填属性。如果您将 “用户名” 映射到值为空的 AD 目录属性，IAM Identity Center 会将该`windowsUpn`值视为 “用户名” 的默认值。如果您想从当前映射中更改 “用户名” 的属性映射，请在进行更改之前确认依赖于 “用户名” 的 IAM Identity Center 流程将继续按预期运行。

如果您使用ListUsers或 ListGroupsAPI 操作或list-users和 list-groups AWS CLI 命令为用户和群组分配访问 AWS 账户 和访问应用程序的权限，则必须将的值指定`AttributeValue`为 FQDN。该值必须采用以下格式：user@example.com。在以下示例中，`AttributeValue` 设置为 `janedoe@example.com`。

```
aws identitystore list-users --identity-store-id d-12345a678b --filters
 AttributePath=UserName,AttributeValue=janedoe@example.com
```

支持的 IAM Identity Center 属性

下表列出了所有支持的 IAM Identity Center 属性，这些属性可以映射到您的 AWS Managed Microsoft AD 目录中的用户属性。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 支持的属性
`${user:AD_GUID}`
`${user:email}`
`${user:familyName}`
`${user:givenName}`
`${user:middleName}`
`${user:name}`
`${user:preferredUsername}`
`${user:subject}`

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商 (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}`

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

默认映射

下表列出了 IAM Identity Center 中用户属性与 AWS Managed Microsoft AD 目录中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。

> **Note**
>
> 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，则将使用下表中的默认映射。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。

IAM Identity Center 中的用户属性	映射到 Microsoft AD 目录中的这个属性
AD_GUID	${dir:guid}
email *	${dir:windowsUpn}
familyName	${dir:lastname}
givenName	${dir:firstname}
middleName	${dir:initials}
name	${dir:displayname}
preferredUsername	${dir:displayname}
subject	${dir:windowsUpn}

* IAM Identity Center 中的电子邮件属性在目录中必须是唯一的。否则，JIT 登录过程可能会失败。

您可以根据自己的需求，更改默认映射或向 SAML 2.0 断言添加更多属性。例如，假设您的应用程序需要在 User.Email SAML 2.0 属性中提供用户电子邮件地址。此外，假设电子邮件地址存储在 Microsoft AD 目录的 windowsUpn 属性中。要实现此映射，您必须在 IAM Identity Center 控制台中的以下两个位置进行更改：

1. 在 Directory (目录) 页面的 Attribute mappings (属性映射) 部分下方，您需要将用户属性 **email** 映射到 **${dir:windowsUpn}** 属性 (位于 Maps to this attribute in your directory (映射到目录中的这个属性) 列)
2. 在应用程序页面上，从表中选择应用程序。选择属性映射选项卡。然后将 User.Email 属性映射到 **${user:email}** 属性（在映射到 IAM Identity Center 列中的此字符串值或用户属性中）。

请注意，您必须以 ${dir:**AttributeName**} 的形式提供每个目录属性。例如，Microsoft AD 目录中的 firstname 属性将变为 ${dir:firstname}。重要的是，每个目录属性都会获得一个实际值。${dir: 之后缺失值的属性将导致用户登录问题。

将 IAM 身份中心中的属性映射到 AWS Managed Microsoft AD 目录中的属性

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 **${dir:windowsUpn}**。
5. 选择 保存更改。

从 Active Directory 配置用户和组

IAM Identity Center 提供以下两种从 Active Directory 预置用户和组的方法。

- IAM Identity Center 可配置的 Active Directory (AD) 同步（推荐）——使用此同步方法，您可以执行以下操作：
  - 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 AWS 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 AWS 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。

- IAM Identity Center AD 同步——通过此同步方法，您可以使用 IAM Identity Center 将 Active Directory 中的用户和组分配给 AWS 账户和应用程序。所有分配的身份都会自动同步到 IAM Identity Center。

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。

以下主题提供的信息使您能够配置和管理可配置的 AD 同步。

主题

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 AWS 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。 AWS 账户

  - AD 同步——当您使用 IAM Identity Center 控制台或相关分配 API 操作为新用户和组进行分配时，IAM Identity Center 会直接在域控制器中搜索指定的用户或组，完成分配，然后定期同步用户或将元数据分组到 IAM Identity Center。
  - 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 AWS 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

  属于其他群组成员的群组称为嵌套群组（或子群组）。当您向 Active Directory 中包含嵌套群组的群组分配任务时，分配的应用方式取决于您使用的是广告同步还是可配置的 AD 同步。

  - AD 同步 — 当您向 Active Directory 中包含嵌套群组的群组分配任务时，只有该群组的直接成员才能访问该帐户。例如，如果您将访问权限分配给组 A，而组 B 是组 A 的成员，则只有组 A 的直接成员可以访问该帐户。B 组的任何成员都不会继承访问权限。
  - 可配置的 AD 同步 — 使用可配置的 AD 同步将任务分配给 Active Directory 中包含嵌套群组的群组，可能会扩大有权访问 AWS 账户 或访问应用程序的用户范围。在这种情况下，分配适用于所有用户，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账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。

  - AD 同步——首先发生分配过程。您可以为用户和群组分配访问 AWS 账户 和访问应用程序的权限。为用户和组分配访问权限后，它们会自动配置（同步到 IAM Identity Center）。如果您有自动化工作流程，这意味着当您将新用户添加到 Active Directory 时，您的自动化工作流程可以使用身份存储 `ListUser` API 操作查询 Active Directory 中的用户，然后使用 IAM Identity Center 分配用户访问权限 分配 API 操作。由于用户有分配，因此该用户会自动配置到 IAM Identity Center。
  - 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。

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。

创建

将 Active Directory 中的自管 AWS Managed Microsoft AD 目录或由管理的目录连接 AWS 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。

属于其他群组（称为嵌套群组或子群组）成员的群组也会被写入身份存储。当您向 Active Directory 中包含嵌套群组的群组分配任务时，分配的应用方式取决于您使用的是广告同步还是可配置的 AD 同步。有关更多信息，请参阅Making assignments to nested groups in Active Directory。

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。默认情况下，IAM Identity Center 会在同步周期内每小时同步来自您的活动目录的数据。根据您的 Active Directory 的大小，数据可能需要 30 分钟到 2 小时才能同步到 IAM 身份中心。

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 身份中心中。

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。

配置和管理您的同步范围

您可以通过以下任一方式配置同步范围：

- 指导式设置：如果您是首次将用户和组从 Active Directory 同步到 IAM Identity Center，请按照 引导式设置 中的步骤配置同步范围。完成引导式设置后，您可以随时按照本部分中的其他过程修改同步范围。
- 如果您已经有同步到 IAM Identity Center 的用户和组，或者您不想按照引导式设置进行操作，请选择管理同步。跳过引导式设置过程，根据需要按照本部分中的其他步骤配置和管理同步范围。

过程

- 引导式设置
- 将用户和组添加到您的同步范围
- 从同步范围中删除用户和组
- 暂停和恢复同步
- 配置用于同步的属性映射
- 自动执行同步配置以实现可配置的 AD 同步

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 AWS Managed Microsoft AD 目录所在的控制台。 AWS 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

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。

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。
9. 在组页面上，您指定的组可能需要一些时间才会显示在列表中。选择刷新图标以更新组列表。

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。

移除群组

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。

配置用于同步的属性映射

有关属性的更多信息，请参阅 AWS Managed Microsoft AD 目录的属性映射。

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。

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，您可以将群组命名为 IAM IdentityCenterAllUsersAndGroups。
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。

IAM Identity Center AD 同步

通过 IAM Identity Center AD 同步，您可以使用 IAM 身份中心为 Active Directory 中的用户 AWS 账户和群组分配 AWS 托管应用程序或客户托管应用程序的访问权限。所有分配的身份都会自动同步到 IAM Identity Center。

IAM Identity Center 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。

创建

当您使用 AWS 控制台或分配 API 调用将用户 AWS 账户 或组分配给或应用程序时，有关用户、群组和成员资格的信息会定期同步到 IAM Identity Center 身份存储中。添加到 IAM Identity Center 分配的用户或群组通常会在两小时内出现在 AWS 身份存储中。根据同步的数据量，此过程可能需要更长的时间。只有直接分配了访问权限的用户和组，或者是被分配了访问权限的组的成员的用户和组才会被同步。

作为其他组成员的组（称为嵌套组）也会写入身份存储。当您向 Active Directory 中包含嵌套群组的群组分配任务时，分配的应用方式取决于您使用的是广告同步还是可配置的 AD 同步。

- AD 同步 — 当您向 Active Directory 中包含嵌套群组的群组分配任务时，只有该群组的直接成员才能访问该帐户。例如，如果您将访问权限分配给组 A，而组 B 是组 A 的成员，则只有组 A 的直接成员可以访问该帐户。B 组的任何成员都不会继承访问权限。
- 可配置的 AD 同步 — 使用可配置的 AD 同步将任务分配给 Active Directory 中包含嵌套群组的群组，可能会扩大有权访问 AWS 账户 或访问应用程序的用户范围。在这种情况下，分配适用于所有用户，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。

如果用户在其用户对象首次同步之前访问了 IAM Identity Center，则该用户的身份存储对象将使用 just-in-time (JIT) 配置按需创建。通过 JIT 预置创建的用户除非直接分配或基于组的 IAM Identity Center 权限，否则他们不会同步。JIT 配置的用户的组成员身份在同步之后才可用。

有关如何向用户分配访问权限的说明 AWS 账户，请参阅单点登录访问权限 AWS 账户。

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。在 Active Directory 中更改的 AWS 身份数据通常会在四小时内出现在身份存储中。根据同步的数据量，此过程可能需要更长的时间。

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 控制台的管理访问控制属性部分中列出的属性子集会在 IAM Identity Center 中更新。此外，用户属性会随着每个用户身份验证事件而更新。

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。

连接到外部身份提供商

如果您使用的是 Active Directory 或中的自管理目录 AWS Managed Microsoft AD，请参阅连接到 Microsoft AD 目录。对于其他外部身份提供商 (IdPs)，您可以使用 AWS 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。这使您的用户能够使用其公司凭据登录 AWS 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 AWS 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 AWS 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 AWS Command Line Interface (AWS CLI)，即可从自动生成和轮换短期凭证中受益。

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 AWS 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 自动预置，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。AWS Management Console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。

如何连接到外部身份提供商

以下是针对支持的 step-by-step 教程 IdPs：

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

对于不同的支持的外部设备，有不同的先决条件、注意事项和配置程序 IdPs。下方概述了所有外部身份提供商使用的过程。

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. 在选择身份来源 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。

   b. 在身份提供程序元数据下，选择选择文件，然后找到从外部身份提供程序下载的元数据文件。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 ACCEPT。
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。

主题

- 对外部身份提供商使用 SAML 和 SCIM 联合身份验证
- SCIM 配置文件和 SAML 2.0 实施

对外部身份提供商使用 SAML 和 SCIM 联合身份验证

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 RFC 2822 (https://tools.ietf.org/html/rfc2822) addr-spec 兼容（“`name@domain.com`”）字符串 (https://tools.ietf.org/html/ rfc2822#section-3.4.1)。
  - 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。

- SCIM
  - IAM Identity Center SCIM 的实施基于 SCIM RFC 7642 (https://tools.ietf.org/html/rfc7642)、7643 (https://tools.ietf.org/html/rfc7643) 和 7644 (https://tools.ietf.org/html/rfc7644)，以及 2020 年 3 月的 B FastFed asic SCIM Profile 1.0 草案 () 中规定的互操作性要求。 https://openid.net/specs/fastfed-scim-1_0-02.html#rfc.section.4 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：

- AWS CloudTrail 通过筛选事件名称来记录日志 ExternalIdP DirectoryLogin

- IdP 特定日志和/或调试日志
- 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。入门教程如果您的 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 “AWS”、“AWS 联合” 或类似的通用 “AWS” 名称的项目可能使用其他联合方法和/或终端节点，并且可能无法按预期在 IAM Identity Center 上运行。

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 AWS 账户 和配置应用程序。

IAM Identity Center 为您的 IAM 身份中心存储 AWS 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 AWS Management Console 和第三方应用程序Microsoft 365，例如Concur、和。Salesforce

然而，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 自动预置。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

自动预置

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 终端节点和您在 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

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。有关其他配置注意事项，请参阅入门教程适用于您的 IdP 的。

- 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 AWS 授权、分配或权限。
- 尚未分配到应用程序或 AWS 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。
- 用户取消配置行为由身份提供商管理，可能因实施情况而异。有关取消用户配置的详细信息，请咨询您的身份提供商。

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，AWS 会在 IAM Identity Center 控制台和控制 AWS 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。 AWS 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。

如何启用自动预置

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，请参阅入门教程适用于您的 IdP 的。

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 终端节点和访问令牌信息。
4. 在入站自动预置对话框中，复制以下选项的每个值。稍后在 IdP 中配置预置时，您需要粘贴这些内容。
   a. SCIM 端点
   b. 访问令牌
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，请参阅入门教程适用于您的 IdP 的。

如何禁用自动预置

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 如何删除访问令牌。

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。

如何生成新的访问令牌

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 如何启用自动预置。

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。

如何删除访问令牌

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。

如何轮换访问令牌

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 如何生成新的访问令牌 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 如何删除访问令牌 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。

手动预置

有些 IdPs 不支持跨域身份管理系统 (SCIM)，或者SCIM实现不兼容。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。

管理 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 Delete（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

在管理 SAML 2.0 证书页面上，您可能会注意到彩色状态指示器图标。这些图标显示在列表中每个证书旁边的过期时间列中。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。

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。

使用 AWS 访问门户

AWS 访问门户为你（最终用户）提供了对所有 AWS 账户 和最常用的云应用程序的单点登录访问权限，例如 Office 365、Concur、Salesforce 等。您只需选择门户中的 AWS 账户 或应用程序图标即可快速启动多个应用程序。 AWS 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 AWS 账户 或应用程序的权限。这也意味着您可以从访问门户 AWS 访问所有这些账户或应用程序，而无需其他登录提示。

在以下情况下，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 AWS 账户 或应用程序。
- 您对给定账户或应用程序的访问权限不是您所期望的。

主题

接受加入 IAM Identity Center 的邀请

如果这是您首次登录 AWS 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 AWS 访问门户。

   a. 如果您收到一封主题为加入 AWS IAM Identity Center（ AWS 单点登录的继任者）的电子邮件，请将其打开并选择接受邀请。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，AWS 访问门户会自动为您登录。如果没有发生这种情况，您可以按照下一部分中提供的说明手动登录 AWS 访问门户。

登录 AWS 访问门户

此时，管理员应该已经向您提供了 AWS 访问门户的特定登录 URL。获得此 URL 后，您就可以继续登录门户。有关更多信息，请参阅登录 AWS 访问门户。

> **Note**
>
> 登录后，AWS 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。

受信任装置

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。

AWS 访问门户的登录提示

以下是一些可帮助您管理 AWS 访问门户体验的提示。

- 有时，您可能需要注销并重新登录 AWS 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 AWS 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 AWS 访问门户。关闭应用程序只是从应用程序注销。您从 AWS 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 AWS 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 AWS 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 AWS 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AWS 登录指南中的退出 AWS 访问门户。

要退出 AWS 访问门户

- 在 AWS 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 AWS 访问门户。

重置您的 IAM Identity Center 用户密码

AWS 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 AWS 账户和云应用程序的单点登录访问权限。 AWS 访问门户不同于 AWS Management Console，后者是一组用于管理 AWS 资源的服务控制台。

使用此过程重置 AWS 访问门户的 IAM Identity Center 用户密码。在AWS 登录 用户指南中了解有关用户类型的更多信息。

注意事项

AWS 访问门户的重置密码功能仅适用于使用 Identity Center 目录或AWS Managed Microsoft AD作为其身份源的身份中心实例的用户。如果您的用户已连接到外部身份提供商，则必须通过外部身份提供商重置用户密码。

- 如果您的身份源是 IAM 身份中心目录，请参阅在 IAM Identity Center 中管理身份时的密码要求。
- 如果您的身份来源是 AWS Managed Microsoft AD，请参阅中 AWS Managed Microsoft AD重置密码时的密码要求。

重置 AWS 访问门户的密码

1. 打开 Web 浏览器，进入 AWS 访问门户的登录页面。

   如果您没有 AWS 访问门户 URL，请查看您的电子邮件。您应该已经收到加入 AWS IAM Identity Center 的电子邮件邀请，其中包括 AWS 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 AWS 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 AWS 访问门户的更多信息，请参阅《AWS 登录 用户指南》中的登录 AWS 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 AWS 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 AWS CLI 或 AWS 软件开发工具包的 IAM Identity Center 用户证书

您可以使用 AWS Command Line Interface 或带有 IAM Identity Center 用户证书的 AWS 软件开发套件 (SDK)，以编程方式访问 AWS 服务。本主题介绍如何在 IAM Identity Center 中获取用户的临时凭证。

AWS 访问门户为 IAM Identity Center 用户提供了对其应用程序 AWS 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 AWS 访问门户后，您可以获得临时证书。然后，您可以使用 AWS CLI 或 AWS 软件开发工具包中的证书（也称为 IAM Identity Center 用户证书）来访问中的资源。 AWS 账户

如果您使用以编程方式访问 AWS 服务，则可以使用本主题中的过程来启动对服务的访问。 AWS CLI AWS CLI有关信息 AWS CLI，请参阅《AWS Command Line Interface 用户指南》。

如果您使用 AWS 软件开发工具包以编程方式访问 AWS 服务，则按照本主题中的步骤还可以直接为软件开发工具包建立身份验证。 AWS 有关 AWS SDK 的信息，请参阅 AWS SDK 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 AWS 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， AWS 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 AWS 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 IAM Identity Center 中的常见任务入门。
- 用户访问权限 AWS 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 AWS 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 将用户访问权限分配给 AWS 账户。
- AWS CLI 已安装-要使用临时证书，必须安装 AWS CLI。有关说明，请参阅 AWS CLI 用户指南中的安装或更新最新版本的 AWS 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 AWS 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 联合用户或服务账户。
  - 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 AWS Identity and Access Management 用户指南中的使用临时安全凭证 AWS CLI。
- 您可以为权限集设置会话持续时间 — 登录 AWS 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 设置会话持续时间。

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 AWS 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 AWS 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 AWS CLI 从浏览器窗口对其进行授权。只要您的 AWS 访问门户会话处于活动状态， AWS 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 AWS 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 AWS 访问门户。如果您创建了 IAM Identity Center 用户，则会 AWS 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AWS 登录 AWS 访问门户。
2. 在 “帐户” 选项卡中或通过选择 AWS 账户 图标，找到要 AWS 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 AWS 账户，则可能尚未为该帐户分配权限集。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 将用户访问权限分配给 AWS 账户。

3. 在账户名称下方，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 AWS 访问门户中显示为PowerUserAccess。
4. 根据角色名称旁边的选项，选择访问密钥或选择命令行或编程访问权限。
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。 AWS CLI

6. 在 AWS 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 AWS CLI需要这些值。要完成此配置，请按照 AWS 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 AWS CLI 需要继续使用， AWS 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 AWS 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 AWS 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 AWS 访问门户。如果您创建了 IAM Identity Center 用户，则会 AWS 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AWS 登录 AWS 访问门户。
2. 在“账户”选项卡中或通过选择 AWS 账户 图标，找到要 AWS 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）。根据您在 IAM 角色名称旁边的选项，选择访问密钥或选择命令行或编程访问权限。

   > **Note**
   >
   > 如果您没有看到列出的任何 AWS 账户，则可能尚未为该帐户分配权限集。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 将用户访问权限分配给 AWS 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。 AWS CLI
4. 选择以下任一选项：

   - 选项 1：设置 AWS 环境变量

     选择此选项可覆盖所有凭据设置，包括`credentials`文件和`config`文件中的任何设置。有关更多信息，请参阅 AWS CLI 用户指南中的环境变量配置 AWS CLI。

要使用此选项，请将命令复制到剪贴板，将命令粘贴到 AWS 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 AWS 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 AWS `credentials`文件中以设置新的命名配置文件。有关更多信息，请参阅 AWS 开发工具包和工具参考指南中的共享配置和凭证文件。要使用此凭证，请在 AWS 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 AWS 服务客户端中使用个人值

  选择此选项可从 AWS 服务客户端访问 AWS 资源。有关更多信息，请参阅构建工具 AWS。

  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。

为 IAM 角色添加书签

为了更快地从访问门户 AWS 访问常用的 IAM 角色，您可以为与特定角色关联的给定角色创建书签。AWS 账户

为特定角色的 IAM 角色添加书签 AWS 账户

1. 登录 AWS 访问门户后，在 “账户” 选项卡中或通过选择 AWS 账户 图标，找到 AWS 账户 要添加书签的并将其展开以选择 IAM 角色名称（例如管理员访问权限）。
2. 根据您的选项，右键单击 IAM 角色名称（例如管理员）或管理控制台，复制链接地址，然后使用该 URL 创建书签。

为设备注册 MFA

在 AWS 访问门户中使用以下步骤注册您的新设备以进行多因素身份验证 (MFA)。

> **Note**
>
> 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，以便在 MFA 上使用

1. 登录您的 AWS 访问门户。有关更多信息，请参阅 登录 AWS 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 Show QR code（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 Assign MFA (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。 AWS

- 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**
>
> 体验将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。

自定义 AWS 访问门户 URL

默认情况下，您可以使用遵循以下格式的 URL AWS 访问访问门户：`d-xxxxxxxxxx.awsapps.com/start`。您可以按如下方式自定义 URL：`your_subdomain.awsapps.com/start`。

> **Important**
>
> 如果您更改了 AWS 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 AWS 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 AWS 访问门户 URL 链接下方的自定义按钮。

> **Note**
>
> 如果未显示自定义按钮，则表示 AWS 访问门户过去已被修改。此 URL 只能修改一次。

4. 输入您想要的子域名，然后选择保存。

现在，您可以使用自定义 `awsapps.com/start` URL 通过 AWS 访问门户登录 AWS 控制台。

Identity Center 用户的多重身份验证

多重身份验证（MFA）提供了一种简单而安全的方式，可以在用户名和密码的默认身份验证机制基础上再额外增加一层保护。

管理员启用 MFA 后，用户必须使用以下两个因素才能登录 AWS 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。

除非顺利完成有效的 MFA 挑战，否则这多重因素可以防止未经授权访问您的 AWS 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。

> **Important**
>
> 强烈建议您启用 MFA，这是最佳安全实践。

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，以便为您的账户额外添加一层保护。

IAM Identity Center MFA 支持以下设备类型。所有 MFA 类型均支持基于浏览器的控制台访问以及搭配使用 AWS CLI v2 和 IAM Identity Center。

- 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
- 通过 AWS Managed Microsoft AD 连接您自己的 RADIUS MFA 实施

一个用户最多可以将八台 MFA 设备注册到一个账户，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。您还可以将 MFA 启用设置配置为在用户每次登录时都需要 MFA，或者启用不需要在每次登录时都使用 MFA 的信任设备。有关如何为您的用户配置 MFA 类型的更多信息，请参阅选择 MFA 类型和配置 MFA 设备实施。

FIDO2 身份验证器

FIDO2 标准包含 CTAP2 和 WebAuthn，基于公有密钥加密。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 AWS。

AWS 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。您可将安装在移动设备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) 是一种行业标准客户端/服务器协议，提供身份验证、授权和账户管理，因此用户能够连接到网络服务。AWS Directory Service 包括一个 RADIUS 客户端，此客户端将连接到您在其上已实现 MFA 解决方案的 RADIUS 服务器。有关更多信息，请参阅为 AWS 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。如果您想使用 AWS 原生双重因素身份验证来访问门户，IAM Identity Center 中的 MFA 可以作为 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 AWS 访问门户。如果您之前使用 RADIUS MFA，则在 IAM Identity Center 启用 MFA 实际上会覆盖登录 AWS 访问门户的用户的 RADIUS MFA。但是，当用户登录所有其他可与 AWS Directory Service 配合使用的应用程序（例如 Amazon WorkDocs）时，RADIUS MFA 会继续向用户发出挑战。

如果您的 MFA 在 IAM Identity Center 控制台上被禁用，并且您已通过 AWS Directory Service 配置 RADIUS MFA，则 RADIUS MFA 将控制 AWS 访问门户的登录。这意味着，如果禁用 MFA，IAM Identity Center 将回退到 RADIUS MFA 配置。

配置 MFA

以下主题提供了在 IAM Identity Center 中配置 MFA 设备的说明。

主题

- 在 IAM Identity Center 中启用 MFA 之前的注意事项
- 在 IAM Identity Center 中启用 MFA
- 选择 MFA 类型
- 配置 MFA 设备实施

- 允许用户注册自己的 MFA 设备

在 IAM Identity Center 中启用 MFA 之前的注意事项

在启用 MFA 之前，请考虑以下情况：

- 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 AWS 访问门户才能访问他们的电子邮件，请勿选择要求他们提供电子邮件发送的一次性密码选项。例如，您的用户可以在 AWS 访问门户中使用 Microsoft 365 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 AWS 访问门户。有关更多信息，请参阅配置 MFA 设备实施。
- 如果您已经在使用通过 AWS Directory Service 配置的 RADIUS MFA，则无需在 IAM Identity Center 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。
- 当您的身份源配置有 IAM Identity Center 的身份存储、AWS Managed Microsoft AD 或 AD Connector 时，您可以在 IAM Identity Center 中使用 MFA 功能。目前，外部身份提供者不支持 IAM Identity Center 中的 MFA。

在 IAM Identity Center 中启用 MFA

您可以通过启用多重身份验证（MFA）来启用对 AWS 访问门户、IAM Identity Center 集成的应用程序以及 AWS CLI 的安全访问。

主题

- 提示用户完成 MFA
- 为 IAM Identity Center 目录禁用 MFA

提示用户完成 MFA

使用以下步骤在 IAM Identity Center 控制台中启用 MFA。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。

> **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 Identity Center 管理这些设置。

如需启用 MFA

1. 打开 IAM Identity Center 控制台。
2. 在左侧导航窗格中，选择 Settings (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：

   - 仅当他们的登录上下文发生变化时（上下文感知）

     在此模式（默认）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。

     此模式为经常在工作场所登录的用户提供了方便，因而他们无需在每次登录时都完成 MFA。只有当他们的登录上下文发生变化时，才会提示他们完成 MFA。

   - 他们每次登录时（始终开启）

     在此模式下，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。如果您的组织或合规政策要求您的用户每次登录 AWS 访问门户时都必须完成 MFA，则应使用此模式。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。

   - 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。

> **Note**
>
> 如果您已经在搭配使用 RADIUS MFA 和 AWS 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 MFA 类型
- 配置 MFA 设备实施
- 允许用户注册自己的 MFA 设备

为 IAM Identity Center 目录禁用 MFA

为 IAM Identity Center 目录禁用多重身份验证（MFA）后，用户只能使用其标准用户名和密码登录。虽然 Identity Center 目录用户禁用 MFA，但您无法在其用户详细信息中管理 MFA 设备，并且 Identity Center 目录用户无法通过 AWS 访问门户管理 MFA 设备。

如需为 IAM Identity Center 目录禁用 MFA

> **Important**
>
> 本部分中的说明适用于 AWS IAM Identity Center。它们不适用于 AWS 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 AWS Identity and Access Management 用户指南中的停用 MFA 设备。

1. 打开 IAM Identity Center 控制台。
2. 在左侧导航窗格中，选择 Settings (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 部分，选择从不（已禁用）单选按钮。

6. 选择 Save changes（保存更改）。

选择 MFA 类型

AWS 访问门户提示用户完成 MFA 时，使用以下步骤选择用户可以用来进行身份验证的设备类型。

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 Settings (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。
   - FIDO2 身份验证器，包括内置身份验证器和安全密钥
   - 虚拟身份验证器应用程序
6. 选择 Save changes（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 AWS 访问门户时是否必须拥有已注册的 MFA 设备。

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 Settings (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。这样，您就可

以使用 MFA 确保贵组织的 AWS 环境安全，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账户中移除即可，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 AWS 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

  使用此选项表明您的用户无需使用 MFA 设备即可登录 AWS 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 Save changes（保存更改）。

允许用户注册自己的 MFA 设备

使用以下步骤允许您的用户自行注册自己的 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 Settings (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 Save changes（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 为设备注册 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。

在 IAM Identity Center 中管理 MFA 设备

以下主题提供了关于在 IAM Identity Center 中管理 MFA 设备的说明。

主题

- 注册 MFA 设备
- 管理用户的 MFA 设备

注册 MFA 设备

使用以下步骤设置新的 MFA 设备以供特定用户在 IAM Identity Center 控制台中访问。您必须拥有对用户的 MFA 设备的物理访问权限才能对其进行注册。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 Users (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 Show QR code（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，然后使用设备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 Assign MFA (分配 MFA)。MFA 设备现在可以开始生成一次性密码，而且可以与 AWS 配合使用了。

- 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 AWS 访问门户中看到此友好名称。

管理用户的 MFA 设备

如果您需要重命名或删除用户的 MFA 设备，请按以下步骤操作。

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 Users (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 Users (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。

管理访问权限 AWS 账户

AWS IAM Identity Center 与集成 AWS Organizations，这使您 AWS 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，以控制他们对特定权限的访问权限 AWS 账户。

AWS 账户 类型

有两种类型 AWS 账户 的 AWS Organizations：

- 管理账户-用于创建组织的账户。 AWS 账户
- 成员账户- AWS 账户 属于组织的其余账户。

有关 AWS 账户 类型的更多信息，请参阅AWS Organizations 用户指南中的AWS Organizations 术语和概念。

您也可以选择将成员账户注册为 IAM Identity Center 的委派管理员。此账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。

对于每种任务和账户类型，下表指明了账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	成员账户	委托管理员账户	管理账户
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

IAM Identity Center 管理任务	成员账户	委托管理员账户	管理账户
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
更改或管理身份源	 否	 是	 是
创建、编辑或删除应用程序	 否	 是	 是
配置 MFA	 否	 是	 是
管理管理账户中未配置的权限集	 否	 是	 是
管理管理账户中已配置的权限集	 否	 否	 是

IAM Identity Center 管理任务	成员账户	委托管理员账户	管理账户
启用 IAM Identity Center	 否	 否	 是
删除 IAM Identity Center 配置	 否	 否	 是
在管理账户中启用或禁用用户访问权限	 否	 否	 是
将成员账户作为委派管理员注册或取消注册	 否	 否	 是

分配 AWS 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 AWS 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 AWS 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 AWS 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 管理对应用程序的访问。

最终用户体验

AWS 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 AWS 账户 和应用程序的单点登录访问权限。 AWS 访问门户不同于 AWS Management Console，后者是一组用于管理 AWS 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 AWS 访问门户中。用户登录 AWS 访问门户，选择一个 AWS 账户，然后选择角色。选择角色后，他们可以使用访问 AWS 服务 AWS Management Console 或检索临时凭证以编程方式访问 AWS 服务。

要打开 AWS Management Console 或检索临时凭证以 AWS 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 AWS 访问门户。
2. 他们使用其目录凭据登录 AWS 访问门户。
3. 身份验证后，在 AWS 访问门户页面上，他们选择 “帐户” 选项卡 AWS 账户 以显示他们有权访问的列表。
4. 然后，用户选择 AWS 账户 他们想要使用的。
5. 在的名称下方 AWS 账户，分配给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 AWS 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。用户可以选择自己的角色来访问 AWS Management Console。
6. 除角色外， AWS 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，请参阅使用 AWS 访问门户和获取 AWS CLI 或 AWS 软件开发工具包的 IAM Identity Center 用户证书。

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。您还可以在服务控制策略（SCP）中使用。

委派和强制访问权限

服务相关角色是一种直接链接到 AWS 服务的 IAM 角色。启用 IAM Identity Center 后，IAM Identity Center 可以在组织 AWS 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 AWS 账户 中的 AWS 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账户访问权限的用户，才能使用此角色。有关更多信息，请参阅 服务相关角色 和 使用 IAM Identity Center 的服务相关角色。

限制成员账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，有权访问成员账户的用户可以使用需要读取权限的 API 操作。成员账户有权访问 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AWS IAM Identity Center 目录的操作、资源和条件密钥以及 Ident AWS ity Store 的操作、资源和条件密钥。

为防止成员账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 阻止成员账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**
>
> 限制成员账户的访问权限可能会影响启用 IAM Identity Center 的应用程序的功能。

有关更多信息，请参阅《AWS Organizations 用户指南》中的服务控制策略（SCP）。

委派管理

委派管理为注册成员账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 AWS 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账户中配置、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 AWS 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账户的人员数量，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账户

有关 IAM 身份中心如何使用的更多信息 AWS Organizations，请参阅管理访问权限 AWS 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AWS 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。

- 向管理账户授予最小权限 – 我们知道管理账户是一个高权限账户，为了遵守最小权限原则，我们强烈建议您将管理账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账户的人数。
- 创建仅在管理账户中使用的权限集 – 这样可以更轻松地管理专为访问您的管理账户的用户定制的权限集，并有助于将它们与您委派的管理员账户管理的权限集区分开来。
- 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账户中找到该目录。如果您决定将 IAM Identity Center 身分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（如果存在）中（归该账户所有）；否则，它必须位于管理账户中。
- 仅在管理账户中创建用户分配 – 委派管理员无法更改管理账户中配置的权限集。但是，委派管理员可以添加、编辑和删除组和组分配。

先决条件

在将账户注册为委派管理员之前，必须先部署以下环境：

- AWS 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。

注册成员账户

要配置委派管理，必须先将组织中的成员账户注册为委派管理员。该成员账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账户可以执行的任务，请参阅 AWS 账户 类型。

IAM Identity Center 一次仅支持将一个成员账户注册为委派管理员。只有使用管理账户的凭证登录后，您才能注册成员账户。

通过将 AWS 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账户中的管理员用户。对此委派管理员账户拥有足够权限的所有用户都可以从该账户执行所有 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
> - 在管理账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。

注册成员账户

1. AWS Management Console 使用您的管理账户的凭据登录 AWS 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，选择注册账户。
5. 在 “注册委托管理员” 页面上，选择 AWS 账户 要注册的，然后选择 “注册账户”。

取消注册成员账户

只有使用管理账户的凭证登录后，您才能取消注册成员账户。

使用以下步骤取消 AWS 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**
>
> 当您取消注册账户时，您实际上移除了所有管理员用户从该账户管理 IAM Identity Center 的能力。因此，他们无法再通过该账户管理 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 AWS 访问门户 AWS 账户 中访问其应用程序。

取消注册成员账户

1. AWS Management Console 使用您的管理账户的凭据登录 AWS 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，选择取消注册账户。
5. 在取消注册账户对话框中，查看安全隐患，然后输入成员账户的名称以确认您已理解。
6. 选择取消注册账户。

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 AWS Organizations 已配置为 IAM Identity Center 的委托管理员。

查看已注册的成员账户

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账户名。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。

临时提升访问权限

对您的所有访问权限都 AWS 账户 涉及一定级别的权限。敏感操作，例如更改高价值资源（例如生产环境）的配置，由于范围和潜在影响，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。

AWS IAM Identity Center 为在不同的业务和技术环境中临时提升访问权限管理提供了以下选项：

- 供应商管理和支持的解决方案 — AWS 已验证了精选合作伙伴产品的 IAM Identity Center 集成，并根据一组常见的客户要求评估了他们的能力。选择最符合您的情景的解决方案，并按照提供者的指导通过 IAM Identity Center 启用该功能。
- 自我管理和自我支持 — 如果您 AWS 只对临时提升访问权限感兴趣，并且可以自己部署、定制和维护该功能，则此选项提供了一个起点。有关更多信息，请参阅临时提升的访问权限管理 (TEAM)。

经过验证 AWS 的安全合作伙伴可获得临时提升访问权限

AWS 安全合作伙伴使用不同的方法来满足一组常见的临时提升访问权限要求。我们建议您仔细审查每种合作伙伴解决方案，以便选择最适合您的需求和偏好的解决方案，包括您的业务、云环境的架构和预算。

> **Note**
>
> 为了进行灾难恢复，我们建议您在中断发生 AWS Management Console之前设置对的紧急访问权限。

AWS Identity 已经验证了 AWS 安全合作伙伴 just-in-time 提供的以下产品的功能和与 IAM Identity Center 的集成：

- CyberArk Secure Cloud Access— 作为其中的一部分CyberArk Identity Security Platform，该产品可按需提供对多云环境的访问权限 AWS 和多云环境。批准是通过与 ITSM 或 ChatOps 工具集成来实现的。可以记录所有会话以进行审计和合规。

- Tenable (previously Ermetic)— 该Tenable平台包括为多云环境中的 AWS 管理操作提供 just-in-time 特权访问权限。来自所有云环境的会话日志（包括 AWS CloudTrail 访问日志）均可在单一界面中进行分析和审计。该功能与 Slack 和 Microsoft Teams 等企业和开发者工具集成。
- Okta访问请求 — Okta 身份管理的一部分，允许您使用Okta作为 IAM 身份中心外部身份提供商 (IdP) 和您的 IAM 身份中心权限集来配置 just-in-time 访问请求工作流程。

此列表将进行更新，以 AWS 验证其他合作伙伴解决方案的功能以及这些解决方案与 IAM Identity Center 的集成。

> **Note**
>
> 如果您使用的是基于资源的策略，请先参阅 Amazon Elastic Kubernetes Service (Amazon EKS AWS Key Management Service) 或 (引用资源策略中的权限集、Amazon EKS 和 AWS KMS)AWS KMS，请在选择解决方案之前参阅。 just-in-time

评估了临时提升的访问权限以供 AWS 合作伙伴验证

AWS Identity 已验证CyberArk Secure Cloud AccessTenable、和访问请求提供的临时提升Okta访问权限可以满足以下常见的客户需求：

- 用户可以请求在用户指定的时间段内访问权限集，指定 AWS 帐户、权限集、时间段和原因。
- 用户可以收到其请求的批准状态。
- 用户无法调用具有给定范围的会话，除非存在具有相同范围的已批准请求，并且他们在批准的时间段内调用了该会话。
- 有一种方法可以指定谁可以批准请求。
- 批准者无法批准自己的请求。
- 批准者有一份待处理、已批准和已拒绝的请求的列表，可以将其导出给审计员。
- 批准者可以批准和拒绝待处理的请求。
- 批准者可以添加注释来解释他们的决定。
- 批准者可以撤销已批准的申请，从而防止将来使用提升的访问权限。

> **Note**
>
> 如果用户在撤销已批准的请求时使用提升的访问权限登录，则在撤销批准后，他们的会话将在长达一小时内保持活动状态。有关身份验证会话的更多信息，请参阅身份验证。

- 用户操作和批准可供审核。

单点登录访问权限 AWS 账户

您可以 AWS Organizations 根据常见的工作职能，将已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，您可以在开发账户中授予数据库管理员广泛的 Amazon RDS 权限，但限制其在生产账户中的权限。IAM Identity Center 自动在您的 AWS 账户 账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 AWS Organizations 管理账户进行操作的权限。由于它是高权限账户，因此其他安全限制要求您先拥有 IAM FullAccess 策略或同等权限，然后才能进行设置。您 AWS 组织中的任何成员账户都不需要这些额外的安全限制。

将用户访问权限分配给 AWS 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。

要检查现有用户和群组的访问权限，请参阅查看用户和群组分配。

> **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 AWS 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 AWS Managed Microsoft AD 目录所在的区域，然后再继续执行下一步骤。

2. 在导航窗格中的多账户权限下，选择 AWS 账户。
3. 在 AWS 账户 页面上，将显示您的组织的树视图列表。选中您要为其分配单点登录访问权限的一个或多个 AWS 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 AWS 账户 个。要向同一组用户和组分配 10 个 AWS 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“***AWS-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“***AWS-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 AWS 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：查看并提交，在查看任务并将其提交到“*AWS-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。

> **Important**
>
> 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 AWS Organizations 管理账户进行操作的权限。由于它是高权限账户，因此其他安全限制要求您先拥有 IAM FullAccess 策略或同等权限，然后才能进行设置。您 AWS 组织中的任何成员账户都不需要这些额外的安全限制。

移除用户和组访问权限

使用此过程可以删除所连接目录中一个或多个用户和组 AWS 账户 对的的单点登录访问权限。

删除用户和群组对的访问权限 AWS 账户

1. 打开 IAM Identity Center 控制台。
2. 在导航窗格的多账户权限下，选择 AWS 账户。
3. 在 AWS 账户 页面上，将显示您的组织的树视图列表。选择 AWS 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 AWS 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。

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 控制台为主账户分配单点登录访问管理账户的权限。默认情况下，只有附加 AWS 账户根用户 了AWSSSOMasterAccountAdministrator和IAMFullAccess AWS 托管策略的用户才能向管理账户分配单点登录访问权限。AWSSSOMasterAccountAdministrator和IAMFullAccess策略管理对 AWS Organizations 组织内管理账户的单点登录访问权限。

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. 以管理账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 AWS Management Console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。

    3. 在您要在权限集中包含哪些策略？下，选中附加 AWS 托管式策略复选框。
    4. 在 IAM 策略列表中，选择AWSSSOMasterAccountAdministrator和IAMFullAccess AWS 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 AWS IAM Identity Center 资源添加标签。
    7. 检查您的选择，然后选择创建。
3. 按照 将用户访问权限分配给 AWS 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. 向分配的用户传达以下信息：当他们登录 AWS 访问门户并选择 “帐户” 选项卡时，他们必须选择相应的角色名称才能使用您刚才委派的权限进行身份验证。

权限集

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 AWS 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 AWS 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 AWS 账户 AWS 目标列表的访问权限。

IAM Identity Center 使用权限集向一个或多个 AWS 账户 用户或群组分配访问权限。当您分配权限集时，IAM Identity Center 会在每个账户中创建 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 AWS 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 AWS 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AWS 管理型策略添加到您的权限集中。您也可以指定 AWS 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。

主题

预定义的权限

您可以使用 AWS 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 AWS 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 AWS 托管策略列表中进行选择，使您可以访问整个托管策略 AWS 账户。您可以添加以下策略之一：

- AdministratorAccess
- PowerUserAccess
- ReadOnlyAccess
- ViewOnlyAccess

工作职能策略

从 AWS 托管策略列表中进行选择，这些策略允许访问您中 AWS 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 AWS Identity and Access Management 用户指南中的适用于工作职能的AWS 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。

自定义权限

当您创建具有自定义权限的权限集时，您可以将您在 AWS 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以及设置任何其他策略可以授予您的权限集用户的最大可能权限的权限边界相结合。 AWS

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
- AWS 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 AWS 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 AWS 账户 位置创建一个 IAM 策略。当您将权限集分配给账户时，IAM Identity Center 会创建策略。然后，该策略将附加到您的用户担任 AWS 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 AWS 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 AWS 账户 自己创建策略。

AWS 托管策略

您可以将AWS 托管策略附加到您的权限集。 AWS 托管策略是用于 AWS 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。 AWS 托管策略解决了您的常见的最低权限用例 AWS 账户。您可以将 AWS 托管策略分配为 IAM Identity Center 创建的角色的权限或权限边界。

AWS 维护工作职能的AWS 托管策略，这些策略可为您的 AWS 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 AWS 账户 还包含大量针对特定策略 AWS 服务 和组合的 AWS 托管 IAM 策略 AWS 服务。创建具有自定义权限的权限集时，可以从许多其他 AWS 托管策略中进行选择，将其分配给您的权限集。

AWS 每个都填 AWS 账户 充 AWS 托管策略。要部署包含 AWS 托管策略的权限集，您无需先在中创建策略 AWS 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 AWS 账户 自己创建策略。

有关 AWS 托管策略的更多信息，请参阅 IAM 用户指南中的AWS 托管策略。

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账户中创建和维护的 IAM 策略。相比之下，您的账户中AWS 托管策略是否有 IAM 策略可以 AWS 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 AWS 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 AWS 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 AWS 账户中创建的 IAM 角色。最佳做法是在每个您分配权限集的账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。

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 AWS 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 AWS 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 AWS 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 AWS 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 AWS 账户账户的访问级别。权限集存储在 IAM Identity Center 中，可以配置给一个或多个 AWS 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 权限集。

创建权限集时，请记住以下注意事项：

- 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 AWS 托管策略。每项策略都授予对 AWS 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AWS 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

  当用户联合到他们的管理控制台或命令行界面 (CLI) AWS 账户 并使用 AWS 管理控制台或 AWS 命令行界面 (AWS 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 设置会话持续时间。

- 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 AWS 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 配置 AWS 访问门户和 IAM Identity Center 集成应用程序的会话持续时间。

- 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 AWS 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，请选择与可用于在账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 AWS 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 AWS 托管式策略的预定义权限集，或者创建使用多达 10 个 AWS 托管式策略或客户托管式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。

创建权限集

1. 打开 IAM Identity Center 控制台。
2. 在多账户权限下，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. 选择下一步。
     2. 在预定义策略下，选择列表中的 IAM 工作职能策略或通用权限策略之一，然后选择下一步。有关更多信息，请参阅 AWS Identity and Access Management 用户指南 中的 工作职能的 AWS 托管式策略 和 AWS 托管式策略。
     3. 在查看并创建屏幕上，查看您所做的选择，然后选择创建。

   - 自定义权限集

     1. 选择下一步。
     2. 在指定策略页面上，选择要应用于新权限集的 IAM policy 类型。默认情况下，您可以将多达 10 个 AWS 托管式策略和客户托管式策略的任意组合添加到您的权限集中。此限额由 IAM 设置。要提高该权限，请在每个要分配权限集 AWS 账户 的地方的 Service Quotas 控制台中请求增加附加到 IAM 角色的 IAM 配额托管策略。

        - 扩展AWS 托管策略以添加来自 IAM 的 AWS 构建和维护策略。有关更多信息，请参阅 AWS 托管策略。

          a. 在权限集中搜索并选择要应用于用户的 AWS 托管式策略。

          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。

        - 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账户中，使用您输入的名称创建策略。最佳做法是为每个账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。

        - 展开自定义内联策略以添加自定义 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账户中创建的 IAM 资源中。有关更多信息，请参阅 内联策略。

          a. 选择设计，使用交互式编辑器选择要包含在内联策略中的权限。选择要粘贴到预格式化策略 JSON 中的代码。

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。

- 展开权限边界，将 AWS 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 AWS 托管式策略来设置来自 IAM 的策略，该策略将 AWS 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。

6. 在 指定堆栈详细信息 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 AWS 访问门户中。用户登录 AWS 访问门户，选择一个 AWS 账户，然后选择角色。
   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 AWS 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 设置会话持续时间。
   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账户中的用户。有关更多信息，请参阅 设置中继状态。

      > **Note**
      >
      > 中继状态 URL 必须在 AWS Management Console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 AWS IAM Identity Center 资源添加标签。

   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 AWS 账户）。要在中配置权限集 AWS 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 单点登录访问权限 AWS 账户。

委派权限集管理

IAM Identity Center 允许您通过创建引用 IAM Identity Center 的 Amazon 资源名称（ARN）的 IAM 策略来委派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账户中为具有特定标签的权限集管理分配。

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 Identity Center 资源 ARN 区分大小写。

以下内容显示了引用 IAM Identity Center 权限集和账户资源类型的正确案例。

资源类型	ARN	上下文键
PermissionSet	`arn:${Partition}:sso:::permissionSet/${InstanceId}/${PermissionSetId}`	`aws:ResourceTag/${TagKey}`
账户	`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 AWS 账户中创建策略。相反，您必须在要分配权限集的每个账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 AWS 账户 中的时，IAM Identity Center 会创建一个 AWS Identity and Access Management (IAM) 角色并将您的 IAM 策略附加到该角色。

> **Note**
>
> 在使用 IAM policy 分配权限集之前，您必须准备好您的成员账户。您的成员账户中的 IAM policy 名称必须与您的管理账户中的策略名称区分大小写。如果您的成员账户中不存在权限集，IAM Identity Center 将无法分配权限集。
> 策略授予的权限不必在账户之间完全匹配。

将 IAM policy 分配给权限集

1. 在您要分配权限集的每个 AWS 账户 位置中创建一个 IAM 策略。
2. 向 IAM policy 分配权限。您可以在不同的账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 AWS 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《AWS CloudFormation 用户指南》 AWS CloudFormation StackSets中的 “使用”。
3. 在您的管理账户中创建权限集，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、 AWS 托管式策略或其他 IAM policy。
5. 创建并分配您的权限集。

配置权限集属性

在 IAM Identity Center 中，您可以通过配置以下权限集属性来自定义用户体验。

主题

- 设置会话持续时间
- 设置中继状态

设置会话持续时间

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 AWS 账户账户的时间长度。当指定的持续时间过后，用户 AWS 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 会在每个分配的账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 AWS 账户 控制台或使用 AWS Command Line Interface (AWS 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。

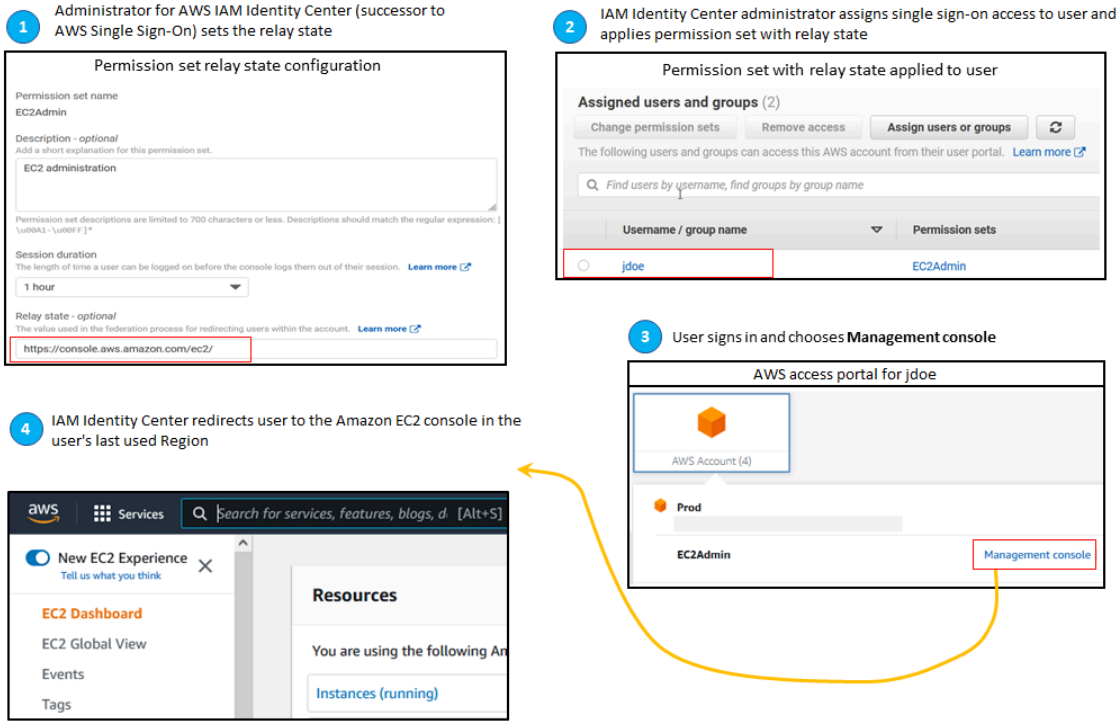
创建权限集后，您可以对其进行更新以应用新的会话持续时间。使用以下过程修改该权限集的会话持续时间长度。

设置会话持续时间

1. 打开 IAM Identity Center 控制台。
2. 在多账户权限下，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 AWS 账户，则帐户名称将显示在下面，AWS 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 AWS 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 AWS 账户 该权限集的用户。
7. 选择 保存更改。
8. AWS 账户 页面顶部会显示一条通知。
   - 如果在一个或多个 AWS 账户中配置了权限集，则通知会确认 AWS 账户 已成功重新配置，并且更新的权限集已应用于账户。
   - 如果未在中配置权限集 AWS 账户，则通知将确认权限集的设置已更新。

设置中继状态

默认情况下，当用户登录 AWS 访问门户，选择账户，然后选择根据分配的权限集 AWS 创建的角色时，IAM Identity Center 会将用户的浏览器重定向到。 AWS Management Console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 AWS 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 AWS 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`**。

使用以下过程为权限集配置中继状态 URL。

配置中继状态

1. 打开 IAM Identity Center 控制台。
2. 在多账户权限下，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 AWS 服务的控制台 URL。例如：

   `https://console.aws.amazon.com/ec2/`

   > **Note**
   >
   > 中继状态 URL 必须在 AWS Management Console中。

6. 如果以任何方式配置了权限集 AWS 账户，则帐户名称将显示在下面，AWS 账户 以便自动重新置备。权限集的中继状态 URL 更新后，将重新配置所有使用 AWS 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 AWS 账户 该权限集的用户。
7. 选择 保存更改。
8. 在 AWS 组织页面的顶部会显示一条通知。

   - 如果在一个或多个 AWS 账户中配置了权限集，则通知会确认 AWS 账户 已成功重新配置，并且更新的权限集已应用于账户。
   - 如果未在中配置权限集 AWS 账户，则通知将确认权限集的设置已更新。

> **Note**
>
> 您可以使用 AWS API、 AWS SDK 或 AWS Command Line Interface(AWS 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
> - AWS CLI 命令参考的 sso-admin 部分中的 `create-permission-set` 或 `update-permission-set` 命令。

引用资源策略中的权限集、Amazon EKS 和 AWS KMS

当您为 AWS 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：

名称	ARN
`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`*

例如，如果您创建了向数据库管理员授予 AWS 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：

名称	ARN
`AWSReservedSSO_DatabaseAdministrator_1234567890abcdef`	`arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_1234567890abcdef`

如果您删除 AWS 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。

名称	ARN
`AWSReservedSSO_DatabaseAdministrator_` **`abcdef0123456789`**	`arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_Dat`

名称	ARN
	abaseAdministrator_ **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：

- 在 Amazon Elastic Kubernetes Service (Amazon EKS) 的 `aws-auth ConfigMap` 文件中
- 在 AWS Key Management Service (AWS KMS) 密钥的基于资源的策略中。该策略也被称为关键策略。

尽管您可以更新大多数 AWS 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， AWS 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。对于 AWS KMS，它必须存在于您的密钥策略中。如果您在这两种情况下都没有备份 IAM 角色，则必须联系 AWS Support。

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 AWS 服务基于资源的策略的 AWS 账户中 AWS KMS保留此分配。

  例如，如果您创建`EKSAccess`权限集并从 AWS 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。
- 适用于 Amazon EKS 和 AWS KMS：包括在 IAM 中创建的角色。

  如果您在 Amazon EKS 集群的 `aws-auth ConfigMap` 中或在 AWS KMS 密钥的密钥策略中引用权限集的角色 ARN，我们建议您还至少包含一个在 IAM 中创建的角色。该角色必须允许您访问 Amazon EKS 集群或管理 AWS 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。 AWS 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 AWS 账户委托人。在此策略中， AWS 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，策略也将允许权限集承担在 IAM 中创建的角色。

```
{
  "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 AWS 资源的紧急访问权限。 AWS KMS keys

删除权限集

在从 IAM Identity Center 删除权限集之前，您必须将其从使用该权限集的所有 AWS 账户 中移除。要检查现有用户和群组的访问权限，请参阅查看用户和群组分配。

从中移除权限集 AWS 账户

1. 打开 IAM Identity Center 控制台。
2. 在多账户权限下，选择 AWS 账户。
3. 在 AWS 账户 页面上，将显示您的组织的树视图列表。选择要 AWS 账户 从中移除权限集的名称。
4. 在的概述页面上 AWS 账户，选择权限集选项卡。
5. 选中要移除的权限集旁边的复选框，然后选择移除。
6. 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。

使用以下步骤删除一个或多个权限集，这样组织 AWS 账户 中的任何人就无法再使用这些权限集。

> **Note**
>
> 已分配此权限集的所有用户和群组，无论使用 AWS 账户 的是什么，都将无法再登录。要检查现有用户和群组的访问权限，请参阅查看用户和群组分配。

从中删除权限集 AWS 账户

1. 打开 IAM Identity Center 控制台。
2. 在多账户权限下，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。

基于属性的访问控制

基于属性的访问控制（ABAC）是一种授权策略，该策略基于属性来定义权限。您可以使用 IAM Identity Center AWS 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 AWS 资源的访问权限。在中 AWS，这些属性称为标签。在中使用用户属性作为标签 AWS 可以帮助您简化在中创建细粒度权限的过程， AWS 并确保您的员工只能访问带有匹配标签的 AWS 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 AWS 账户，IAM Identity Center 会在 AWS 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 AWS 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 AWS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 AWS 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 AWS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， AWS CloudTrail 从而轻松确定会话的身份 AWS。

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 API 启用和配置 ABAC 的信息，请参阅 IAM 身份中心 API 参考指南CreateInstanceAccessControlAttributeConfiguration中的。

主题

- 清单： AWS 使用 IAM 身份中心配置 ABAC

- 访问控制属性

清单： AWS 使用 IAM 身份中心配置 ABAC

此清单包括准备您的 AWS 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	任务	参考
1	查看如何为所有 AWS 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 AWS 资源添加标签。	• 为资源添加标签 AWS
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。 AWS	• 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 AWS 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。请参阅教程中有关您的特定 IdP 的`Optional`章节。	• 入门教程
	• 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。	• 自动预置 • 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	任务	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。	• 使用 AWS Managed Microsoft AD 作为身份源时选择属性 • 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 AWS 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 AWS 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 AWS 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 AWS 资源时，他们只能根据匹配的标签获得访问权限。	• 将用户访问权限分配给 AWS 账户

完成这些步骤后，联合 AWS 账户 使用单点登录的用户将根据匹配的属性访问其 AWS 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 AWS 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账户。然后，该属性用于根据策略确定访问。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 AWS 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 AWS 账户 页面以创建或编辑权限集以使用 ABAC 的属性。

使用 AWS Managed Microsoft AD 作为身份源时选择属性

当您将 IAM Identity Center 配置 AWS 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 AWS 资源的访问权限。有关 IAM Identity Center 中用户属性与 AWS Managed Microsoft AD 目录中用户属性的默认映射列表，请参阅默认映射。

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。

- 您可以将 IdP 配置为通过 SAML 断言发送属性。在这种情况下，IAM Identity Center 会传递来自 IdP 的属性名称和值以进行策略评估。

  > **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 AWS 账户时，这些属性将始终被传递。在相同属性通过 SAML 和 SCIM 传入 IAM Identity Center 的情景中，SAML 属性值在访问控制决策中具有优先级。

- 您可以从 IAM Identity Center 控制台的访问控制属性页面配置要使用的属性。您在此处选择的属性值将替换通过断言来自 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。SCIM 属性列表中可能不存在访问控制所需的其他属性。在这种情况下，请考虑与 IdP 中的 IT 管理员合作，使用所需的

`https://aws.amazon.com/SAML/Attributes/AccessControl:` 前缀通过 SAML 断言将此类属性发送到 IAM Identity Center。有关如何在 IdP 中配置用于访问控制的用户属性以通过 SAML 断言发送的信息，请参阅适用于入门教程您的 IdP 的。

- 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。

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

要在所有情况下使用 ABAC，您必须首先使用 IAM Identity Center 控制台或 IAM Identity Center API 启用 ABAC。如果您选择使用 IAM Identity Center 选择属性，则可以使用 IAM Identity Center 控制台或 IAM Identity Center API 中的访问控制属性页面。如果您使用外部身份提供者（IdP）作为身份源并选择通过 SAML 断言发送属性，则可以将 IdP 配置为传递属性。如果 SAML 断言传递了这些属性中的任何一个，IAM Identity Center 将使用 IAM Identity Center Identity Store 中的值替换属性值。当用户对其其账户进行联合身份验证时，只会发送在 IAM Identity Center 中配置的属性以做出访问控制决策。

> **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 AWS 账户 。这些属性在 IAM Identity Center 中不可用于映射。

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。如果您没有在账户中创建任何权限集，则不需要这些额外的安全限制。

启用访问控制的属性

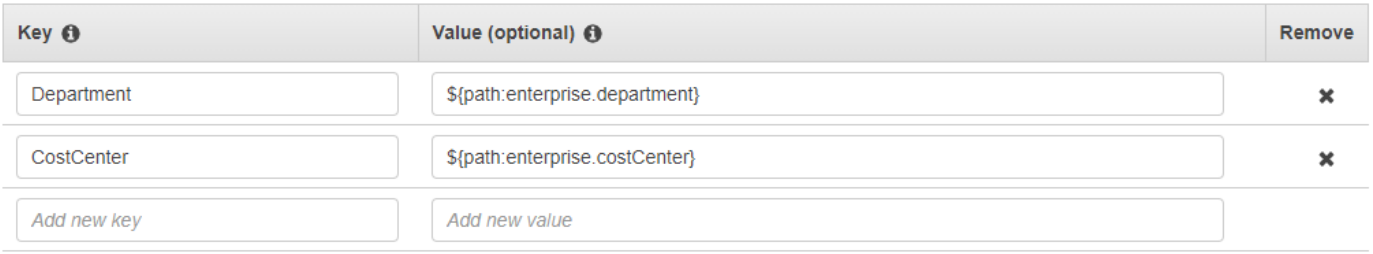
1. 打开 IAM Identity Center 控制台。
2. 选择 设置
3. 在设置页面上，找到访问控制属性 框，然后选择启用。继续执行下一个步骤以对其进行配置。

选择您的属性

按照以下过程为 ABAC 配置设置 ABAC 配置属性。

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密钥和值的详细信息。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 AWS Managed Microsoft AD 目录的属性映射 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 ABAC 规则并将其添加到您的权限集和/或基于资源的策略中。这是必需的，这样您才能向用户身份授予对 AWS 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，然后选择禁用。
4. 在禁用访问控制属性对话框中，查看信息，准备就绪后输入 DELETE，然后选择确认。

> **Important**
>
> 此步骤将删除所有已配置的属性。删除后，从身份源接收的任何属性以及您之前配置的任何自定义属性都不会被传递。

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 AWS 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，在以下信任策略中，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 AWS 账户时，您可以在会 AWS 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。

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

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”。

IAM 身份提供者

当您向添加单点登录访问权限时 AWS 账户，IAM Identity Center 会在每个 AWS 账户中创建一个 IAM 身份提供商。IAM 身份提供者可帮助您确保 AWS 账户 的安全，因为您不必在应用程序中分配或嵌入长期安全凭证（如访问密钥）。

修复 IAM 身份提供者

如果您意外删除或修改了身份提供者，则必须手动重新应用用户和组分配。重新应用您的用户和组分配会重新创建身份提供者。有关更多信息，请参阅：

- 管理访问权限 AWS 账户
- 管理对应用程序的访问

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 AWS Organizations中的组织内的特定 AWS 账户 账户拥有单点登录访问权限。该服务通过在其组织 AWS 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 AWS 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 AWS Organizations 和服务相关角色。

当您启用 IAM Identity Center 时，IAM Identity Center 在 AWS Organizations中的组织内的所有账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账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。有关更多信息，请参阅 管理访问权限 AWS 账户。

在每个角色中创建的服务相关角色 AWS 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。

管理对应用程序的访问

借 AWS IAM Identity Center助，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：AWS 托管应用程序和客户托管应用程序。 AWS 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。

您也可以向员工授予 AWS Management Console 对组织 AWS 账户 中特定人员的访问权限。有关更多信息，请参阅 管理访问权限 AWS 账户。

主题

AWS 托管应用程序

AWS 托管应用程序与 IAM Identity Center 集成，可以将其用于身份验证和目录服务。

AWS 托管应用程序与 IAM Identity Center 的集成使您可以更轻松地分配用户访问权限，而无需为每个应用程序设置单独的联合或用户和群组同步。您只需连接一次要用于身份验证的身份源，即可获得用户和群组分配的单一视图。启用可信身份传播的应用程序的管理员可以根据用户或用户的群组成员资格定义和审核对其应用程序资源的访问权限，而无需将其映射到 IAM 角色。

AWS 托管应用程序提供了一个管理用户界面，可用于管理对应用程序资源的访问。例如， QuickSight 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 AWS 托管应用程序还提供允许您将用户分配给应用程序的 AWS Management Console 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。

AWS 与 IAM 身份中心集成的托管应用程序包括：

AWS 与 IAM 身份中心集成的托管应用程序

AWS 托管应用程序	与 IAM 身份中心的组织实例集成	与 IAM 身份中心的账户实例集成	通过 IAM 身份中心启用可信身份传播
亚马逊 Athena SQL	 是	 是	 是
Amazon CodeCatalyst	 是	 是	 否
Amazon CodeWhisperer	 是	 否	 否
亚马逊 EMR 笔记本电脑	 是	 否	 否
亚马逊 EC2 上的亚马逊 EMR	 是	 是	 是
Amazon EMR Studio	 是	 是	 是

AWS 托管应用程序	与 IAM 身份中心的组织实例集成	与 IAM 身份中心的账户实例集成	通过 IAM 身份中心启用可信身份传播
Amazon Kendra	 是	 否	 否
Amazon Managed Grafana	 是	 否	 否
Amazon Monitron	 是	 否	 否
Amazon Nimble Studio	 是	 否	 否
Amazon Pinpoint	 是	 否	 否
Amazon QuickSight	 是	 是	 是
Amazon Redshift	 是	 是	 是
亚马逊 S3 访问授权	 是	 是	 是

AWS 托管应用程序	与 IAM 身份中心的组织实例集成	与 IAM 身份中心的账户实例集成	通过 IAM 身份中心启用可信身份传播
亚马逊 SageMaker Studio	 是	 否	 否
Amazon WorkSpaces Web	 是	 否	 否
AWS CLI	 是	 否	 否
AWS IoT Events	 是	 否	 否
AWS IoT Fleet Hub	 是	 否	 否
AWS IoT SiteWise	 是	 否	 否
AWS Lake Formation	 是	 是	 是
AWS Supply Chain	 是	 否	 否

AWS 托管应用程序	与 IAM 身份中心的组织实例集成	与 IAM 身份中心的账户实例集成	通过 IAM 身份中心启用可信身份传播
AWS Systems Manager	 是	 否	 否
AWS Verified Access	 是	 否	 否

主题

- 控制访问权限
- 协调管理任务
- 配置 IAM Identity Center 以共享身份信息
- 在中共享身份信息的注意事项 AWS 账户
- 限制 AWS 托管应用程序的使用
- 查看 AWS 托管的应用程序的详细信息
- 禁用 AWS 托管应用程序

控制访问权限

通过两种方式控制对 AWS 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，AWS 托管应用程序需要分配。
- 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。

协调管理任务

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，则当用户登录 AWS 访问门户时，只有直接或通过小组分配分配到应用程序的用户才能查看应用程序磁贴。或者，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，应用程序管理对资源的访问权限，访问 AWS 访问门户的所有用户都可以看到应用程序图块。

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 AWS 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。

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 AWS Command Line Interface (AWS 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 在 IAM Identity Center 管理身份。
- 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 连接到 Microsoft AD 目录。
  - 外部身份提供商 - 有关更多信息，请参阅 连接到外部身份提供商。

  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 AWS 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 AWS Cloud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 AWS 账户中的许多应用程序。

在中共享身份信息的注意事项 AWS 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这些信息的访问。您可以选择仅在 AWS 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 AWS Organizations。或者，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 AWS Organizations中哪些账户的信息。例如，如果您仅在 AWS 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，如果您在所有账户中启用访问权限，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。

限制 AWS 托管应用程序的使用

首次启用 IAM Identity Center 时， AWS 允许在中的所有账户中自动使用 AWS 托管应用程序 AWS Organizations。要限制应用程序访问，必须采用 SCP。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。

查看 AWS 托管的应用程序的详细信息

使用应用程序的控制台或 API 将 AWS 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 控制台查看有关该应用程序的详细信息。

在 IAM 身份中心控制台中查看有关 AWS 托管应用程序的信息

1. 打开 IAM Identity Center 控制台。
2. 选择应用程序。
3. 选择 AWS 托管的应用程序选项卡。
4. 在应用程序列表中，选择要查看其详细信息的应用程序名称。
5. 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 跨应用程序的可信身份传播。

禁用 AWS 托管应用程序

要防止用户对 AWS 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。

> **Warning**
>
> 禁用应用程序会删除该应用程序的所有用户权限，断开该应用程序与 IAM Identity Center 的连接，并使该应用程序无法访问。如果您是 IAM Identity Center 管理员，我们建议您在执行此任务之前与应用程序管理员进行协调。

禁用 AWS 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 AWS 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. 在暂停应用程序对话框中，选择暂停。
6. 在 AWS 托管的应用程序列表中，应用程序的状态会显示为非活动。

客户托管的应用程序

借助 IAM Identity Center，您可以创建或连接员工用户，并集中管理他们对所有用户 AWS 账户 和应用程序的访问权限。IAM Identity Center 将充当中央身份服务，为用户提供不同的身份验证方式。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。

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。IAM Identity Center 提供支持 SAML 2.0 的常用应用程序目录，其中包括 Salesforce 和 Microsoft 365 等。此目录可通过 IAM Identity Center 控制台找到。您也可以设置自己的 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访问 AWS 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，该应用程序可以在请求中传递用户的身份，以访问 AWS 服务中的数据。有关更多信息，请参阅 对客户托管的应用程序使用可信身份传播。

主题

- SAML 2.0 和 OAuth 2.0
- 设置客户托管的 SAML 2.0 应用程序

SAML 2.0 和 OAuth 2.0

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
- OAuth 2.0

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 使用此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 AWS 访问权限。

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。OAuth 2.0 授予的基本流程涉及用户、称为客户端的应用程序、授权服务器和资源服务器。

IAM Identity Center 通过 OpenID Connect (OIDC) 网络服务支持基于 OAuth 2.0 的身份联合验证。OIDC 服务允许诸如之类的应用程序注册公共 OAuth 2.0 客户端。 AWS CLI有关更多信息，请参阅 AWS IAM Identity Center OIDC API 参考。这些注册的客户端可以在用户通过身份验证和授权后，利用受支持的 OAuth 2.0 授予获取访问令牌，并且如果适用，还可以获取刷新令牌。然后，应用程序可以使用此访问令牌代表用户访问受 OAuth 2.0 保护的资源，例如 IAM Identity Center 集成的 API 端点。有些 OAuth 2.0 授予还提供刷新令牌，刷新令牌的使用寿命更长，可用于在现有访问令牌过期后生成新的访问令牌。

受支持的授予

OAuth 2.0 框架规范提供了不同的授予类型，以支持各种客户端，并提供了创建自定义授予类型的规范。授予类型是指应用程序获取访问令牌的方式。IAM Identity Center 目前支持以下授予类型。

设备授权授予

IAM Identity Center 目前支持 OAuth 2.0 设备授权授予 (RFC 8628) 的部分内容。OIDC 服务允许应用程序注册为 OAuth 客户端，并使用设备授权授予流程生成访问令牌，以访问受 IAM Identity Center 保护的 API。要使用此授予，应用程序必须先向 IAM Identity Center OIDC 服务注册公共客户端。应用程序注册后，OIDC 服务会为应用程序提供客户端 ID 和客户端密钥，您可以使用这些客户端 ID 和客户端密钥通过设备授权授予生成令牌。

如果应用程序将来需要访问受保护的资源，它会向 OIDC 服务发送请求以启动设备授权。此请求会返回验证 URL 和设备代码。通过 IAM Identity Center 身份验证的用户需要使用此设备代码，并明确授予

应用程序对所请求资源的访问权限。用户授予访问权限后，应用程序可以将设备代码交换为访问令牌和刷新令牌。

访问范围

范围定义了 OAuth 客户端向用户或授权服务器请求的代表用户执行某些操作或访问特定资源的特定权限或访问权限。范围是资源服务器对与操作和资源相关的权限进行分组的一种方式，它们指定了客户端可以请求的粗粒度操作。

OIDC 服务客户端使用 OAuth 2.0 (RFC 6749) 第 3.3 节中定义的 `scope` 值来指定要为访问令牌请求哪些访问权限。与访问令牌关联的范围决定了哪些资源在用于访问受保护的资源（例如 IAM Identity Center 集成的服务 API）时可用。

在请求访问令牌时，您最多可以指定 25 个范围。

注册公共客户端时，IAM Identity Center OIDC 服务支持的访问范围

范围	描述	支持的区域	支持的服务
`sso:account:access`	访问 IAM Identity Center 管理型账户和权限集。	IAM Identity Center 支持的所有区域	IAM Identity Center
`codewhisperer:completions`	Amazon CodeWhisperer 将通过分析您的代码来检测安全漏洞。	仅限美国东部（弗吉尼亚州北部）(us-east-1)	AWS 构建者 ID
`codewhisperer:analysis`	Amazon CodeWhisperer 将根据您的 IDE 中的现有代码和自然语言注释以代码形式生成建议。	仅限美国东部（弗吉尼亚州北部）	AWS 构建者 ID
`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。	仅限美国东部（弗吉尼亚州北部）	AWS 构建者 ID

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访问 AWS 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，该应用程序可以在请求中传递用户的身份，以访问 AWS 服务中的数据。有关更多信息，请参阅 对客户托管的应用程序使用可信身份传播。

主题

IAM Identity Center 应用程序目录

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。

主题

设置应用程序目录中的应用程序

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，获得服务提供商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 在 IAM Identity Center 控制台中配置应用程序属性。
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 在 IAM Identity Center 控制台中配置应用程序属性。
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。

跨应用程序的可信身份传播

可信身份传播为需要访问 AWS 服务中数据的查询工具和商业智能 (BI) 应用程序的用户提供了简化的单点登录体验。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。用户对 AWS 服务和其他事件的访问记录在服务特定的日志和 CloudTrail 事件中，以便审计员知道用户采取了哪些操作以及用户访问了哪些资源。

通过可信身份传播，用户可以登录应用程序，该应用程序可以在请求中传递用户的身份，以访问 AWS 服务中的数据。由于访问权限根据用户身份进行管理，因此用户无需使用数据库本地用户证书或担任 IAM 角色即可访问数据。

主题

可信身份传播概述

可信身份传播建立在 OAuth 2.0 授权框架之上，允许应用程序在不共享密码的情况下，安全访问和共享用户数据。OAuth 2.0 提供对应用程序资源的安全委派访问。之所以说访问权限是被委派的，是因为需要资源管理员批准，或者授权用户登录的应用程序访问其他应用程序。

为避免共享用户密码，可信身份传播会使用令牌。令牌为可信应用程序提供了一种标准方法，可以声明用户是谁以及两个应用程序之间允许哪些请求。 AWS 与可信身份传播集成的托管应用程序直接从 IAM Identity Center 获取令牌。IAM Identity Center 还为应用程序提供了一个选项，用于交换来自外部 OAuth 2.0 授权服务器的身份令牌和访问令牌。这使得应用程序可以在外部进行身份验证和获取令牌 AWS，将令牌兑换 IAM Identity Center 令牌，并使用新令牌向 AWS 服务发出请求。有关更多信息，请参阅 通过可信令牌发布者使用应用程序。

OAuth 2.0 流程在用户登录应用程序时启动。用户登录的应用程序会发起访问其他应用程序资源的请求。发起（请求）的应用程序可以通过向授权服务器请求令牌，代表用户访问接收端应用程序。授权服务器将返回令牌，而发起端应用程序会将该令牌连同访问请求一起，传递给接收端应用程序。

可信身份传播用例

作为 IAM Identity Center 管理员，可能会要求您帮助在以下支持此功能的启动应用程序和连接的 AWS 服务之间配置可信身份传播。以下各节提供了有关可以启动可信身份传播的应用程序所支持的特定用例的更多信息。

主题

- Amazon EMR
- Amazon QuickSight
- 亚马逊 Redshift 查询编辑器 v2
- 第三方商业智能应用程序
- 定制开发的应用程序

Amazon EMR

您可以使用 Amazon EMR 作为以下可信身份传播用例的启动应用程序。

描述	使用的其他 AWS 服务	了解更多信息
通过亚马逊 EMR Studio 在亚马逊 EC2 集群上使用 Spark 在亚马逊 EMR 上运行交互式分析。通过 Amazon S3 访问授权，根据员工身份和相关属性对 AWS Glue 目录通过 Amazon S3 位置 AWS Lake Formation 和 Amazon S3 位置应用访问控制。	亚马逊 EC2 上的亚马逊 EMR 通过亚马逊 S3 访问授权 AWS Lake Formation、亚马逊 S3 授权、亚马逊 S3	• 在《亚马逊 EMR 管理指南》中将 Amazon EMR 与 IAM 身份中心集成。 • 亚马逊简单存储服务用户指南中的 Amazon S3 访问权限和公司目录身份。 • 在《AWS Lake Formation 开发人员指南》中@@ 连接 AWS Lake Formation IAM 身份中心
通过 Amazon EMR Studio 在 Athena 上使用 Trino 进行即席分析。根据员工身份和相关属性对 AWS Glue 目录应用访问控制，AWS Lake Formation 并通过 Amazon S3 访问权限授予隔离查询结果位置。	Athena 通过 A AWS Lake Formation mazon S3 访问授权	• 在《亚马逊 EMR 管理指南》中将 Amazon EMR 与 IAM 身份中心集成。 • 使用 IAM 身份中心启用 Amazon Athena 用户指南中的 Athena 工作组。 • 亚马逊简单存储服务用户指南中的 Amazon S3 访问权限和公司目录身份。 • 在AWS Lake Formation 开发人员指南中@@ 连接 AWS Lake Formation IAM 身份中心。

描述	使用的其他 AWS 服务	了解更多信息
		• 在大数据博客中@@ 将你的员工身份带到亚马逊 EMR Studio 和 Athena。AWS

Amazon QuickSight

您可以将 Amazon QuickSight 用作以下可信身份传播用例的启动应用程序。

描述	使用的其他 AWS 服务	了解更多信息
亚马逊 QuickSight 用户可以查询亚马逊 Redshift 数据。亚马逊 Redshift 管理员在亚马逊 Redshift 中授予数据访问权限。	Amazon Redshift	• 在《亚马逊 Redshift 管理指南》中将 Redshift 与 IAM 身份中心连接，为用户提供单点登录体验。 • QuickSight在《亚马逊 Redshift 管理指南》中，通过亚马逊将亚马逊 R edshift 与 IA M 身份中心连接起来。
亚马逊 QuickSight 可以向亚马逊 Redshift Spectrum 查询亚马逊 S3 中的结构化数据，访问权限由 AWS Lake Formation 管理员授权。	亚马逊 Redshift，亚马逊 S3 结构化数据 *通过亚马逊 Redshift Spectrum 授权通过 AWS Lake Formation	• 在《亚马逊 Redshift 管理指南》中将 Redshift 与 IAM 身份中心连接，为用户提供单点登录体验。 • QuickSight在《亚马逊 Redshift 管理指南》中，通过亚马逊将亚马逊 R edshift 与 IA M 身份中心连接起来。 • 在AWS Lake Formation 开发人员指南中@@ 连接 AWS Lake Formation IAM 身份中心。 • 使用 Amazon Redshift 以及 AWS Lake FormationAWS 大数据博客中外部身份提供商中的用户简化访问管理。

描述	使用的其他 AWS 服务	了解更多信息
亚马逊 QuickSight 可以在 Amazon Redshift 数据共享中查询 Amazon S3 中的结构化数据，其访问权限由管理员授权。 AWS Lake Formation	亚马逊 Redshift 数据共享、亚马逊 S3 结构化数据 *通过授权 AWS Lake Formation	• QuickSight在《亚马逊 Redshift 管理指南》中，通过亚马逊将亚马逊 R edshift 与 IA M 身份中心连接起来。 • 在AWS Lake Formation 开发人员指南中@@ 连接 AWS Lake Formation IAM 身份中心。 • 使用 Amazon Redshift 以及 AWS Lake FormationAWS 大数据博客中外部身份提供商中的用户简化访问管理。

亚马逊 Redshift 查询编辑器 v2

您可以使用 Amazon Redshift 查询编辑器 v2 作为以下可信身份传播用例的启动应用程序。

描述	使用的其他 AWS 服务	了解更多信息
AWS Management Console 用户可以使用 Amazon Redshift 查询编辑器 v2 向亚马逊 Redshift 查询数据，访问权限由亚马逊 Redshift 管理员授权。	Amazon Redshift	• 在《亚马逊 Redshift 管理指南》中将 Redshift 与 IAM 身份中心连接，为用户提供单点登录体验。 • 在《亚马逊 Redshift 管理指南》中连接到亚马逊 Redshift 数据库。 • 使用 AWS IAM Identity Center 大数据博客中的无缝单点登录，Okta与 Amazon Redshift 查询编辑器 V2 集成。AWS
AWS Management Console 用户可以使用 Amazon Redshift 查询编辑器 v2 在亚马逊 Redshift Spectrum 中查询 Amazon S3 中	亚马逊 Redshift，亚马逊 S3 结构化数据	• 在《亚马逊 Redshift 管理指南》中将 Redshift 与 IAM 身份中心连接，为用户提供单点登录体验。

描述	使用的其他 AWS 服务	了解更多信息
的结构化数据，访问权限由管理员授权。 AWS Lake Formation	*通过亚马逊 Redshift Spectrum 授权通过 AWS Lake Formation	• 在《亚马逊 Redshift 管理指南》中连接到亚马逊 Redshift 数据库。 • 在AWS Lake Formation 开发人员指南中@@ 连接 AWS Lake Formation IAM 身份中心。
AWS Management Console 用户可以使用 Amazon Redshift 查询编辑器 v2 在亚马逊 Redshift 数据共享中查询 Amazon S3 中的结构化数据，访问权限由管理员授权。 AWS Lake Formation	亚马逊 Redshift 数据共享、亚马逊 S3 结构化数据 *通过授权 AWS Lake Formation	• 在《亚马逊 Redshift 管理指南》中连接到亚马逊 Redshift 数据库。 • 在AWS Lake Formation 开发人员指南中@@ 连接 AWS Lake Formation IAM 身份中心。

第三方商业智能应用程序

您可以使用第三方商业智能应用程序（例如 Tableau）作为特定可信身份传播用例的启动应用程序。修改后的第三方商业智能应用程序可以通过 OAuth 身份令牌或访问令牌向 Amazon Redshift 驱动程序传递用户身份，以查询亚马逊 Redshift 以获取数据，访问权限由亚马逊 Redshift 管理员授权。

定制开发的应用程序

您可以使用自己定制开发的应用程序作为以下可信身份传播用例的启动应用程序。

描述	使用的其他 AWS 服务	了解更多信息
创建通过 OIDC 授权服务器对用户进行身份验证的应用程序，然后使用 AWS IAM Identity Center 和 IAM 获取身份增强型 IAM 角色证书。此证书用于请求访问 Amazon S3 中的非结构化数据，访问权限由 Amazon S3 访问授权管理员授权。	AWS IAM Identity Center，Amazon S3 非结构化数据 *通过 Amazon S3 访问授权进行授权	• 亚马逊简单存储服务用户指南中的 Amazon S3 访问权限和公司目录身份。 • 如何在AWS 存储博客中使用 IAM 身份中心和 Amazon S3 访问授权（第 1 部分）和（第 2 部分）开发面向用户的数据应用程序。

设置可信身份传播

可信身份传播支持应用程序以不同的方式进行身份验证，以便它们可以将用户的身份传递给 AWS 服务。可信身份传播的设置因应用程序类型及其身份验证方式而异。

> **Note**
>
> 如果您有客户托管的应用程序请求访问托管应用程序，但不使用 AWS API 进行 AWS 连接，则必须设置可信令牌颁发者。

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。

- 已部署 IAM Identity Center 并预置了用户和组

  要使用可信身份传播，您必须启用 IAM Identity Center，并预置用户和组。有关信息，请参阅 IAM Identity Center 中的常见任务入门。

  推荐组织实例 — 我们建议您使用在 Organizati ons 的管理账户中启用的 IAM Identity Center AWS 组织实例。如果您计划使用可信身份传播来使用户能够访问同一组织 AWS 账户 内不同机构的 AWS 服务和相关资源，则可以将您的 IAM Identity Center 实例的管理委托给成员账户。

如果您计划使用 IAM Identity Center 的单一账户实例，则您希望用户通过可信身份传播访问的所有AWS服务和资源都必须位于同一个独立账户中 AWS 账户，或者位于您启用 IAM Identity Center 的组织中的同一个成员账户中。有关更多信息，请参阅 IAM Identity Center 的账户实例。

- 适用于 AWS 托管应用程序；连接到 IAM 身份中心

  要使用可信身份传播， AWS 托管应用程序必须与 IAM Identity Center 集成。

额外注意事项

使用可信身份传播时，请记住以下额外注意事项。

- 不要修改 AWS 托管应用程序的 “需要分配” 设置

  AWS 托管应用程序具有默认设置配置，用于确定是否需要为用户和组进行分配。我们建议您不要修改此项设置。即使您配置了允许用户访问特定资源的细粒度权限，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。
- 不需要多账户权限（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。

在 AWS 托管应用程序中使用可信身份传播

可信身份传播使 AWS 托管应用程序能够代表用户请求访问 AWS 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。

可信身份传播基于 OAuth 2.0 标准。要使用此功能， AWS 托管应用程序必须与 IAM 身份中心集成。 AWS 分析服务可能会提供基于驱动程序的接口，使兼容的应用程序能够使用可信身份传播。例如，JDBC、ODBC 和 Python 驱动程序允许兼容的查询工具使用可信身份传播，您无需完成其他设置步骤。

主题

- 为可信身份传播设置 AWS 托管应用程序
- AWS 托管应用程序的可信身份传播请求流
- 应用程序获取令牌后
- 身份增强型 IAM 角色会话

- 身份增强型 IAM 角色会话的类型
- AWS 托管应用程序的设置流程和请求流程

为可信身份传播设置 AWS 托管应用程序

AWS 支持可信身份传播的服务提供了管理用户界面和 API，可用于设置此功能。无需在 IAM Identity Center 配置这些服务。

以下是设置可信身份传播 AWS 服务的高级流程。具体步骤因应用程序提供的管理界面和 API 而异。

1. 使用应用程序控制台或 API 将应用程序连接到您的 IAM Identity Center 实例

   使用 AWS 托管应用程序或应用程序 API 的控制台将应用程序连接到您的 IAM Identity Center 实例。当您使用应用程序控制台时，管理用户界面会包含一个小部件，用于简化设置和连接过程。

2. 使用应用程序控制台或 API 设置用户对应用程序资源的访问权限

   完成此步骤以授权用户可以访问哪些资源或数据。访问权限取决于用户身份或组成员资格。授权模式因应用程序而异。

> **Important**
>
> 您必须完成此步骤，才能允许用户访问 AWS 服务的资源。否则，即使发出请求的应用程序对访问服务的请求得到授权，用户也无法访问资源。

AWS 托管应用程序的可信身份传播请求流

所有流向 AWS 托管应用程序的可信身份传播流程都必须从从 IAM Identity Center 获取令牌的应用程序开始。此令牌是必需的，因为它包含对 IAM Identity Center 已知用户和在 IAM Identity Center 注册的应用程序的引用。

以下各节介绍 AWS 托管应用程序如何从 IAM Identity Center 获取令牌以启动可信身份传播。

主题

- 基于 Web 的 IAM Identity Center 身份验证
- 基于控制台、由用户发起的身份验证请求

基于 Web 的 IAM Identity Center 身份验证

在此流程中， AWS 托管应用程序使用 IAM Identity Center 进行身份验证提供基于 Web 的单点登录体验。

当用户打开 AWS 托管应用程序时，会触发使用 IAM Identity Center 的单点登录流程。如果 IAM Identity Center 中没有该用户的活动会话，则会根据您指定的身份源，向用户展示登录页面，然后 IAM Identity Center 会为该用户创建一个会话。

IAM Identity Center 为 AWS 托管应用程序提供了一个令牌，其中包括用户的身份以及应用程序注册使用的受众 (Aud) 和相关范围列表。然后，应用程序可以使用该令牌向其他接收端 AWS 服务端发出请求。

基于控制台、由用户发起的身份验证请求

在此流程中， AWS 托管应用程序提供了用户启动的控制台体验。

在这种情况下， AWS 托管应用程序是在担任角色后从 AWS 管理控制台进入的。要使应用程序获取令牌，用户必须发起一个过程，触发应用程序对用户进行身份验证。这将使用 IAM Identity Center 发起身份验证，将用户重定向至您配置的身份源。

应用程序获取令牌后

发出请求的应用程序从 IAM Identity Center 获取令牌后，该应用程序会定期刷新令牌，令牌可在用户会话的生命周期内使用。在此期间，该应用程序可能会：

- 获取有关令牌的更多信息，以确定用户是谁，以及该应用程序可以在哪些范围内与其他接收端 AWS 托管应用程序一起使用。
- 在调用中将令牌传递给其他支持使用令牌的接收 AWS 托管应用程序。
- 获取身份增强型 IAM 角色会话，用于向使用 AWS 签名版本 4 的其他 AWS 托管应用程序发出请求。

  身份增强型 IAM 角色会话是一种 IAM 角色会话，包含了在 IAM Identity Center 创建的令牌中存储的用户传播身份。

身份增强型 IAM 角色会话

使应用程序 AWS Security Token Service 能够获得身份增强型 IAM 角色会话。 AWS 在角色会话中支持用户上下文的托管应用程序可以使用身份信息根据角色会话中的用户来授权访问权限。这种新的上下文使应用程序能够通过 AWS 签名版本 4 API 请求向支持可信身份传播的 AWS 托管应用程序发出请求。

当 AWS 托管应用程序使用身份增强型 IAM 角色会话访问资源时，会 CloudTrail 记录用户的身份（用户 ID）、启动会话和采取的操作。

当应用程序使用身份增强型 IAM 角色会话向接收端应用程序发出请求时，它会为会话添加上下文，以便接收端应用程序可以根据用户的身份、组成员资格或 IAM 角色对访问授权。如果接收端应用程序或请求的资源未配置为根据用户身份或组成员资格对访问授权，支持可信身份传播的接收端应用程序将返回错误。

要避免此问题，请执行以下操作之一：

- 验证接收端应用程序是否连接到 IAM Identity Center。
- 使用接收端应用程序的控制台或应用程序 API，将应用程序设置为根据用户身份或组成员资格对访问资源授权。这里的设置要求因应用程序而异。

有关更多信息，请参阅接收端 AWS 托管应用程序的文档。

身份增强型 IAM 角色会话的类型

应用程序通过向 AWS STS `AssumeRole` API 发出请求并在请求的`ProvidedContexts`参数中传递上下文断言来获得身份增强型 IAM 角色会话。`AssumeRole`上下文断言从 `idToken` 声明中获取，该声明在 `SSO OIDC` `CreateTokenWithIAM` 请求的响应中提供。

AWS 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`

- 仅将用户身份记录到的会话 CloudTrail。
- 基于传播的用户身份启用授权并将其记录到的会话。 CloudTrail

要从中获取仅提供在 CloudTrail 跟踪中注册 AWS STS 的审计信息的身份增强型 IAM 角色会话，请向请求提供`sts:audit_context`声明的值。`AssumeRole`要获得同时允许接收 AWS 服务授权 IAM Identity Center 用户执行操作的会话，请向`AssumeRole`请求提供`sts:identity_context`索赔的价值。您只能提供一个上下文。

通过 **`sts:audit_context`** 创建的身份增强型 IAM 角色会话

当使用使用创建的身份增强型 IAM 角色会话向 AWS 服务发出请求时`sts:audit_context`，用户的 IAM Identity Center `userId` 将登录到该`OnBehalfOf`元素 CloudTrail 中。

```
"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"
    }
}
```

> **Note**
>
> 这些会话不能用于授权 Identity Center 用户。但它们仍然可以用来授权 IAM 角色。

要从中获取此类角色会话 AWS STS，请在请求参数中为`AssumeRole`请求提供该`sts:audit_contextProvidedContexts`字段的值。使用 `arn:aws:iam::aws:contextProvider/IdentityStore` 作为 `ProviderArn` 的值。

通过 **`sts:identity_context`** 创建的身份增强型 IAM 角色会话

当用户使用使用创建的身份增强型 IAM 角色会话向 AWS 服务发出请求时，用户的 IAM Identity Center `userId` 将以与`sts:identity_context`创建的会话相同的方式登录到 CloudTrail 该`onBehalfOf`元素。`sts:audit_context`

除了将 IAM Identity Center 用户登录`userId`到之外 CloudTrail，支持的 API 还使用此类会话根据传播的用户身份授权操作。有关支持的 API 的 IAM 操作列表，请参

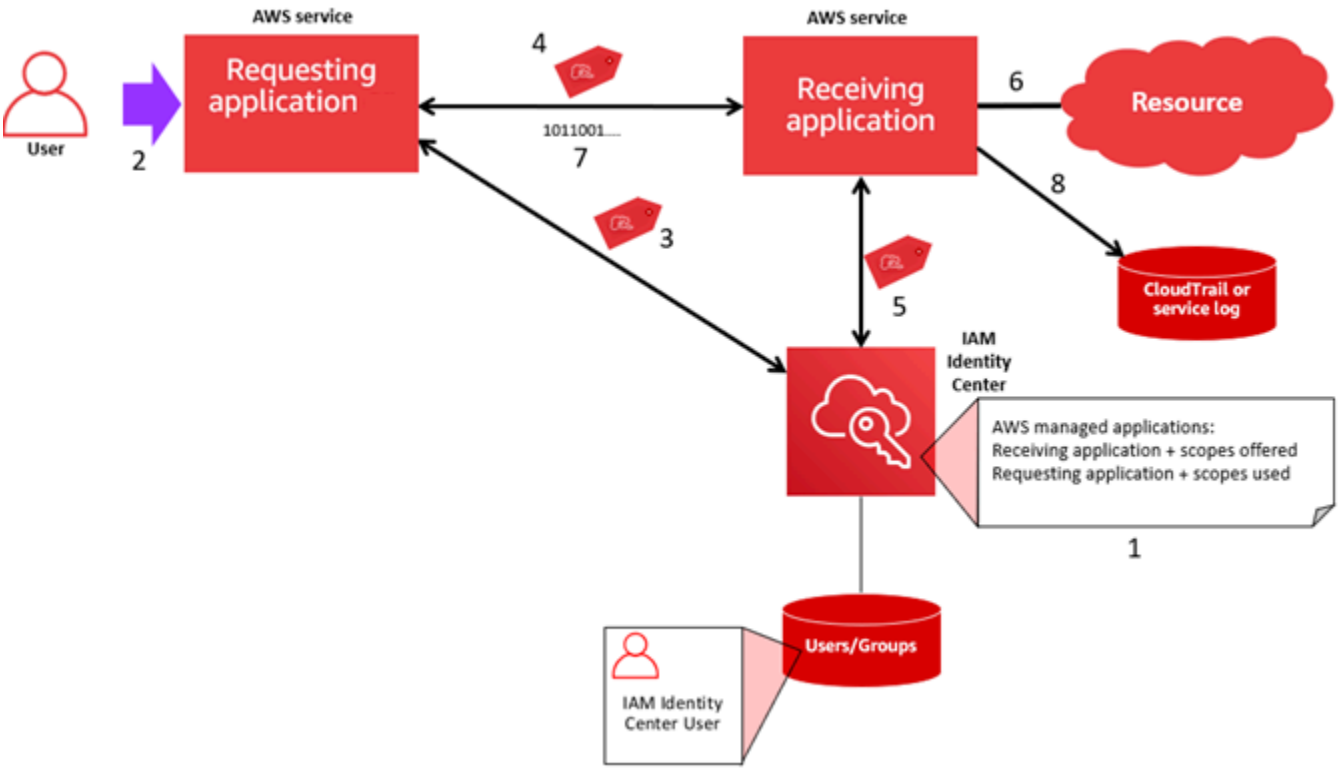
阅AWSIAMIdentityCenterAllowListForIdentityContext AWS 托管策略。当使用创建身份增强型 IAM 角色会话时，此 AWS 托管策略作为会话策略提供。sts:identity_context该策略禁止您将角色会话与不支持的 AWS 服务一起使用。

要从中获取此类角色会话 AWS STS，请在请求参数中为AssumeRole请求提供该sts:identity_contextProvidedContexts字段的值。使用 arn:aws:iam::aws:contextProvider/IdentityStore 作为 ProviderArn 的值。

AWS 托管应用程序的设置流程和请求流程

本节介绍使用可信身份传播并提供基于 Web 单点登录体验的 AWS 托管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. 使用 AWS 托管应用程序或应用程序 API 的控制台执行以下操作：
   a. 将应用程序连接到您的 IAM Identity Center 实例。
   b. 设置权限，授权用户可以访问哪些应用程序资源。
2. 当用户打开可以请求访问资源的 AWS 托管应用程序（请求应用程序）时，请求流就开始了。

3. 要获取访问接收 AWS 托管应用程序的令牌，请求 AWS 的托管应用程序会向 IAM Identity Center 发起登录请求。

   如果用户未登录，IAM Identity Center 会针对您指定的身份源，触发用户身份验证流程。这将为用户创建一个新的 AWS 访问门户会话，其持续时间与您在 IAM Identity Center 中配置的时间相同。然后，IAM Identity Center 会生成与会话关联的令牌，应用程序可以在用户 AWS 访问门户会话的剩余时间内运行。如果用户退出应用程序，或者您删除了他们的会话，会话将在两小时内自动结束。
4. AWS 托管应用程序向接收应用程序发起请求并提供其令牌。
5. 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。接收端应用程序还可能从 Identity Center 目录中请求获取用户属性或用户的组成员资格。
6. 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。
7. 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。
8. 用户的身份、代表其执行的操作以及其他事件记录在接收端应用程序的日志和 AWS CloudTrail 事件中。记录这些信息的具体方式因应用程序而异。

对客户托管的应用程序使用可信身份传播

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 AWS 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，用户可以登录客户管理的应用程序，并且该应用程序可以在请求访问 AWS 服务中的数据时传递用户的身份。

> **Important**
>
> 要访问 AWS 服务，客户托管的应用程序必须从 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 AWS 服务访问请求（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
- 指定可信的应用程序

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 AWS 访问门户中的 AWS 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。

     应用程序磁贴可见性 - 除非将应用程序可见性在 AWS 访问门户中设置为不可见，否则所有登录 AWS 访问门户的用户都能看到应用程序磁贴。

3. 在 AWS 访问门户下，输入可以让用户访问应用程序的 URL，并指定应用程序磁贴在 AWS 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 AWS IAM Identity Center 资源添加标签。
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。这些令牌授权那些发起请求（请求应用程序）以访问 AWS 托管应用程序（接收应用程序）的应用程序。

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. 要使用户在使用此应用程序时无需重新进行身份验证，请选择自动刷新活动应用程序会话的用户身份验证。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 AWS 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，也称为最低权限许可。

该策略需要使用 `sso-oauth:CreateTokenWithIAM` 操作。

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 AWS Identity and Access Management 用户指南中的使用基于资源的策略进行跨账户存取和 IAM ARN。
   - 要手动编辑策略（如果指定非AWS 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 AWS 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，必须为身份传播指定一个或多个 AWS 服务或可信应用程序。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 AWS 服务或可信应用程序。指定一项 AWS 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 AWS 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，选择可信应用程序。

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。 AWS通过可信令牌发布者，您可以授权这些应用程序代表其用户对 AWS 托管的应用程序提出访问请求。

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

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 AWS 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。这些令牌授权应用程序发起 AWS 服务访问请求（请求应用程序）（接收应用程序）。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。

AWS 接收请求的服务根据其用户和群组成员资格（如身份中心目录中所示）来管理对其资源的精细授权。 AWS 服务不能直接使用来自外部令牌发行者的令牌。

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 AWS 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（可信令牌颁发者）。尽管可信令牌发行者通常是您用作 IAM Identity Center 身份源的身份提供商，但不一定是这样。有关如何设置可信令牌发行者的信息，请参阅相关身份提供商的文档。

  > **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（颁发者网址）。
- 由可信代币发行者发行的代币

  来自可信代币发行者的代币必须满足以下要求：

  - 令牌必须使用 RS256 算法进行签名并采用 JSON 网络令牌 (JWT) 格式。
  - 令牌必须包含以下声明：
    - 发行者 (iss)-发行代币的实体。此值必须与可信令牌发行者的 OIDC 发现端点（发行者 URL）中配置的值相匹配。
    - 主题（sub）-经过身份验证的用户。

    - 受众 (aud)-代币的预期接收者。在将令牌交换为 IAM 身份中心的令牌后，将访问该 AWS 服务。有关更多信息，请参阅 Aud 声明。
    - 到期时间 (exp)-令牌过期的时间。
    -
  - 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。
- 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：
  - 使用跨域身份管理系统 (SCIM) 2.0 协议，将用户同步到 IAM Identity Center。
  - 直接在 IAM Identity Center 创建用户。

  > **Note**
  >
  > 如果您使用 Active Directory 域服务作为身份源，将无法支持可信令牌发布者。

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（颁发者网址）

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**
>
> 您必须将发现端点的 URL 粘贴到上面和不粘贴`.well-known/openid-configuration`。如果包含在 URL 中，`.well-known/openid-configuration`则可信令牌发行者配置将不起作用。由于 IAM Identity Center 不会验证此 URL，因此，如果 URL 的格式不正确，则可信令牌发行者的设置将失败，且不会发出通知。

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 AWS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（ AWS 服务）发起请求。

主题

- 协调管理角色和职责
- 设置可信令牌发布者的任务
- 如何向 IAM Identity Center 控制台添加可信令牌发布者
- 如何在 IAM Identity Center 控制台中查看或编辑可信令牌发布者设置
- 使用可信令牌发布者的应用程序的设置过程和请求流程

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 AWS 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 AWS 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 AWS 服务管理员。	外部 IdP（可信令牌发布者）管理员 AWS 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。 向 AWS 服务管理员提供受众名称（Aud 声明）。	IAM Identity Center 管理员 AWS 服务管理员
AWS 服务管理员	检查 AWS 服务控制台中是否有受信任的令牌发行者。当 IAM Identity Center 管理员将可信令牌发布者添加到 IAM Identity Center 控制台后，可信令牌发布者将在 AWS 服务控制台中出现。 将 AWS 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 AWS 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）。
   - 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 AWS 服务连接到 IAM 身份中心 — AWS 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 AWS 服务控制台中可见，可供 AWS 服务管理员选择。

3. 配置令牌交换的使用-在 AWS 服务控制台中， AWS 服务管理员将 AWS 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 AWS 服务对应的澳元索赔值。

   可信令牌发布者在其颁发的令牌中放置 Aud 声明值，以表明该令牌供 AWS 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 “颁发者 URL” 中，指定将为可信身份传播颁发令牌的外部 IdP 的 OIDC 发现 URL。您必须指定发现端点的 URL，直到和不是`.well-known/openid-configuration`。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而颁发的令牌中的颁发者 (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 AWS IAM Identity Center 资源添加标签。
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。

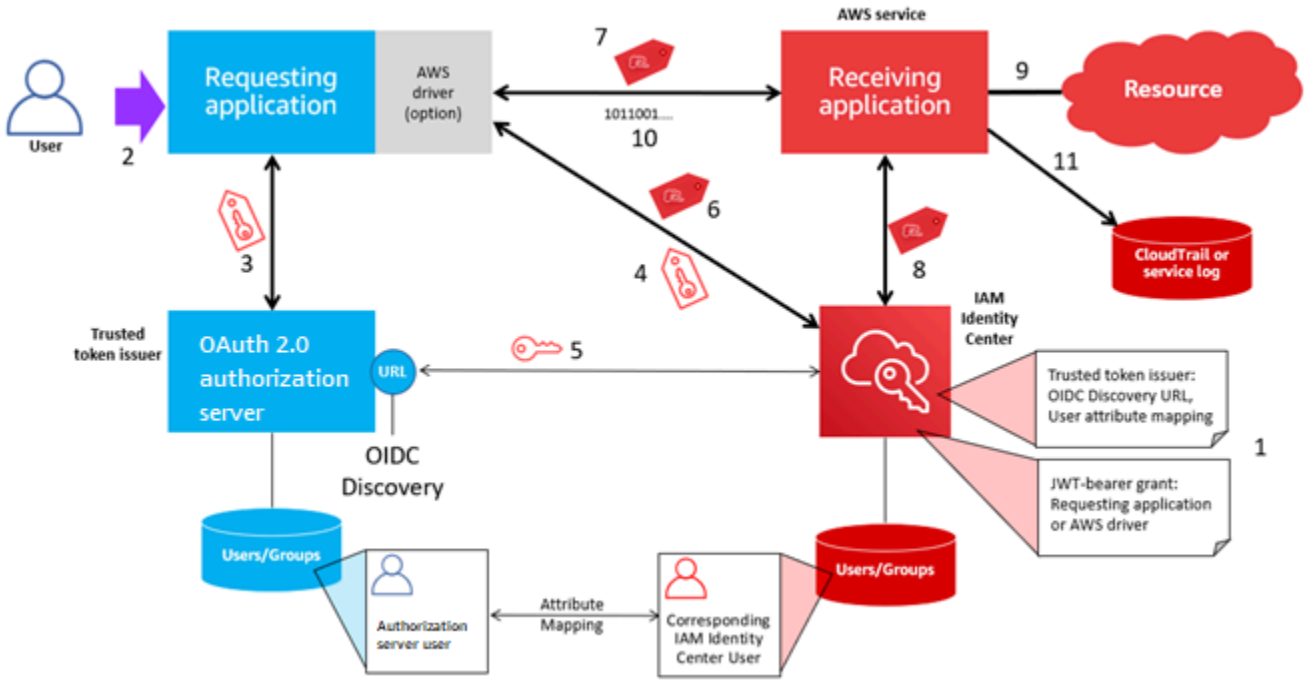
要在 IAM Identity Center 控制台中查看或编辑可信令牌发布者设置

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 AWS 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 AWS 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 AWS 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 AWS 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 AWS 驱动程序，则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 AWS 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 AWS 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 AWS 托管的应用程序配置为不需要对用户和组进行分配，则处理将继续。

     > **Note**
     >
     > AWS 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对接收的 AWS 托管应用程序使用有效的范围。
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 AWS 托管应用程序的受众 (Aud)，以及请求的应用程序在向接收 AWS 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接收应用程序日志和事件中记录的其他 CloudTrail事件。记录这些信息的具体方式因应用程序而异。

管理 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。

主题

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 Identity Center 在签署 SAML 断言/响应时使用的算法。您可以将此值设置为 SHA-1 或 SHA-256。 AWS 建议尽可能使用 SHA-256，除非您的服务提供商需要 SHA-1。有关密码算法工作原理的一般信息，请参阅公钥加密。

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

在应用程序属性的应用程序页面上，您可能会注意到彩色状态指示器图标。这些图标显示在列表中每个证书旁边的过期时间列中。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。

要检查证书的当前状态

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。

在 IAM Identity Center 控制台中配置应用程序属性

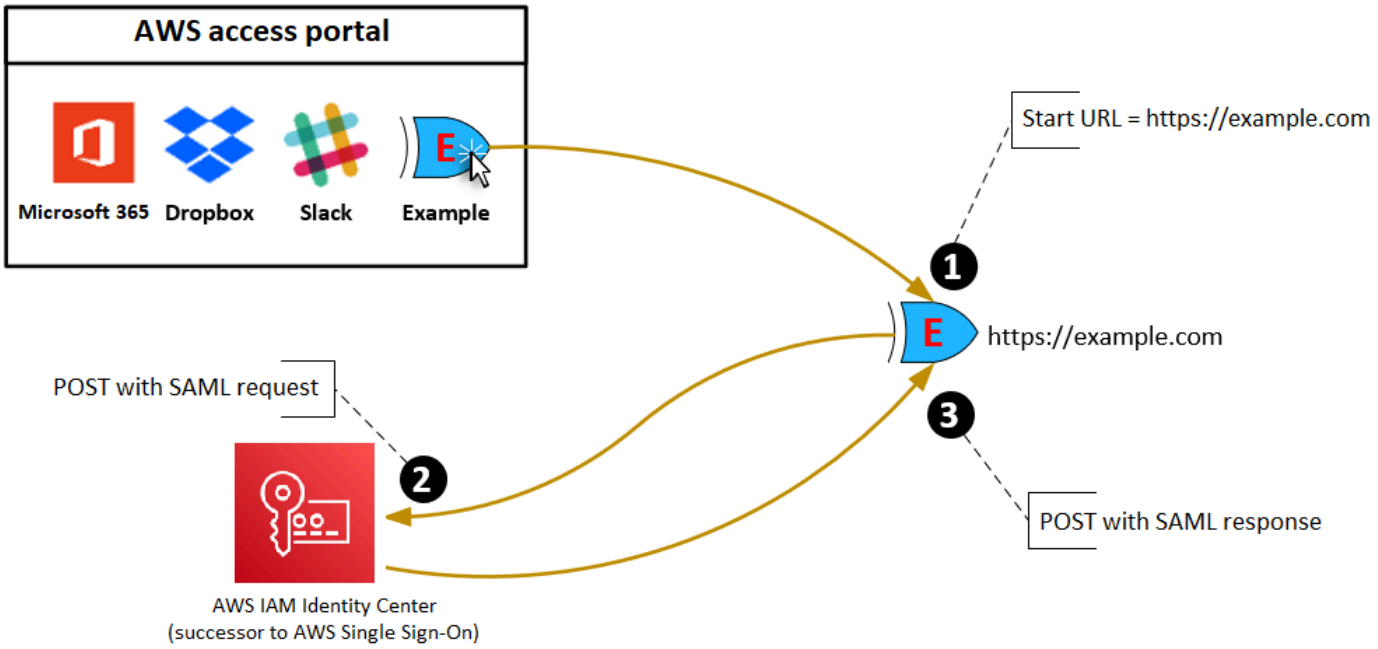
在 IAM Identity Center 中，您可以通过配置应用程序启动 URL、中继状态和会话持续时间来自定义用户体验。

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。

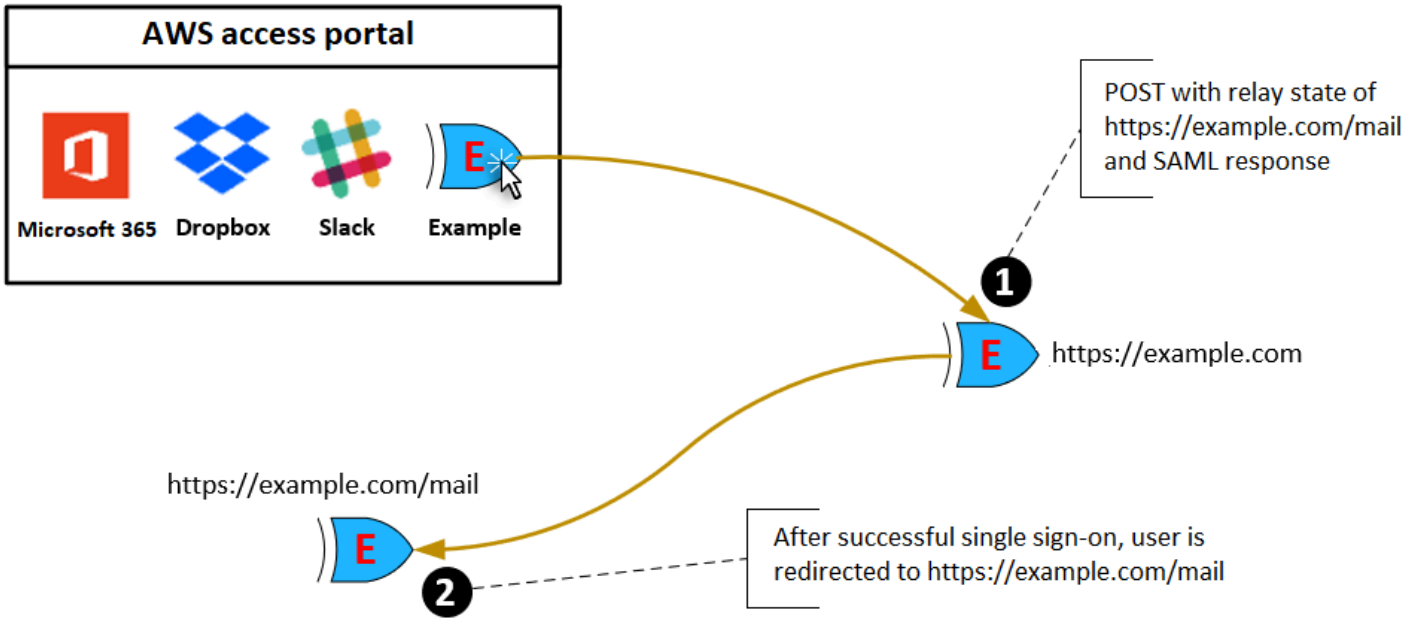
以下步骤和图表说明了当用户在 AWS 访问门户中选择应用程序时应用程序启动 URL 身份验证工作流程：

1. 用户的浏览器使用应用程序启动 URL 的值（在此示例中为 https://example.com）重定向身份验证请求。
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 AWS 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 AWS Managed Microsoft AD，请确保 IAM Identity Center 控制台使用您的 AWS Managed Microsoft AD 目录所在的 AWS 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，输入用户名或组名。您还可以搜索用户和组。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账户。
6. 选择 分配用户。

在 IAM Identity Center 控制台中删除用户访问权限

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。

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。

要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 AWS Managed Microsoft AD 目录的属性映射 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。

故障恢复能力设计和区域行为

IAM Identity Center 服务是完全托管的，并使用高度可用且耐用的 AWS 服务，例如 Amazon S3 和 Amazon EC2。为了确保发生可用区中断时的可用性，IAM Identity Center 跨多个可用区运行。有关 IAM Identity Center 可用性设计目标的信息，请参阅《可靠性支柱指南》中的附录 A：为特定 AWS 服务设计的可用性。

您在 AWS Organizations 管理账户中启用 IAM Identity Center。这是必需的，以便 IAM Identity Center 可以在您的所有 AWS 账户 中配置、取消配置和更新角色。当您启用 IAM Identity Center 时，它会部署到当前选择的 AWS 区域。如果您想要部署到特定的 AWS 区域，请在启用 IAM Identity Center 之前更改区域选择。

> **Note**
>
> IAM Identity Center 仅控制来自其主要区域对其权限集和应用程序的访问。我们建议您考虑 IAM Identity Center 在单个区域中运行时与访问控制相关的风险。

尽管 IAM Identity Center 确定来自您启用服务的区域的访问权限，但 AWS 账户 是全局的。这意味着用户登录 IAM Identity Center 后，通过 IAM Identity Center 访问 AWS 账户 时可以在任何区域中进行操作。但是 SageMaker，大多数AWS托管应用程序（例如 Amazon）必须安装在与 IAM 身份中心相同的区域，用户才能对这些应用程序进行身份验证和分配访问权限。有关将应用程序与 IAM Identity Center 结合使用时的区域限制的信息，请参阅应用程序的文档。

您还可以使用 IAM Identity Center 对可通过公共 URL 访问的基于 SAML 的应用程序进行身份验证和授权访问，无论应用程序构建于哪个平台或云上。

我们不建议使用 IAM Identity Center 的账户实例作为实现弹性的手段，因为这会创建另一个与组织实例无关联的孤立控制点。

设置对 AWS Management Console 的紧急访问。

IAM Identity Center 基于高度可用的 AWS 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AWS 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AWS Management Console。

内容

- 紧急访问配置汇总
- 如何设计关键操作角色
- 如何规划您的访问模型
- 如何设计紧急角色、帐户和组映射
- 如何创建紧急访问配置
- 应急准备工作
- 紧急故障转移流程
- 恢复正常运营
- 在 Okta 中一次性设置直接 IAM 联合身份验证应用程序

概述

AWS 让您能够：

- 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 AWS 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 Identity Center 作为 AWS 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凭证，通过直接联合身份验证来登录 AWS Management Console。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。

> **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。

紧急访问配置汇总

配置紧急访问需要完成以下任务：

1. 在 AWS Organizations 中的组织中创建一个紧急操作帐户。

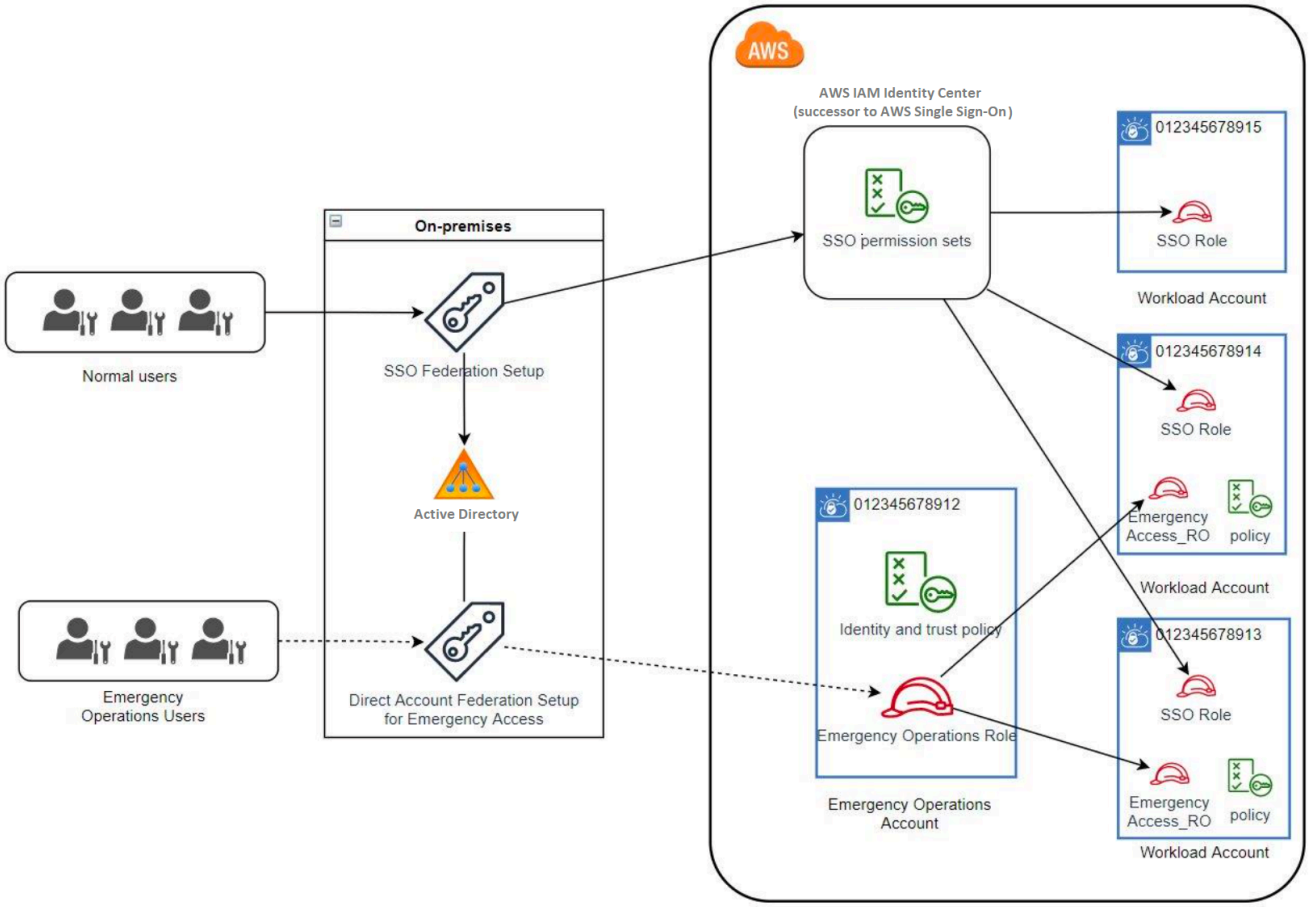
2. 使用基于 SAML 2.0 的联合身份验证将您的 IdP 连接到紧急操作帐户。
3. 在紧急操作帐户中，为第三方身份提供商联合身份验证创建角色。此外，在每个工作负载帐户中创建紧急操作角色，并具有所需的权限。
4. 为您在紧急操作账户中创建的 IAM 角色委派对工作负载账户的访问权限。要授权访问您的紧急操作帐户，请在您的 IdP 中创建一个没有成员的紧急操作组。
5. 通过在 IdP 中创建启用 SAML 2.0 联合身份验证访问 AWS Management Console 的规则，使 IdP 中的紧急操作组能够使用紧急操作角色。

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 AWS Management Console，并在紧急操作帐户中承担紧急操作角色。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

通过此设计，您可以配置一个通过 IAM 联合身份验证的 AWS 账户，以便用户可以承担关键操作角色。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。

下图提供了设计概述。



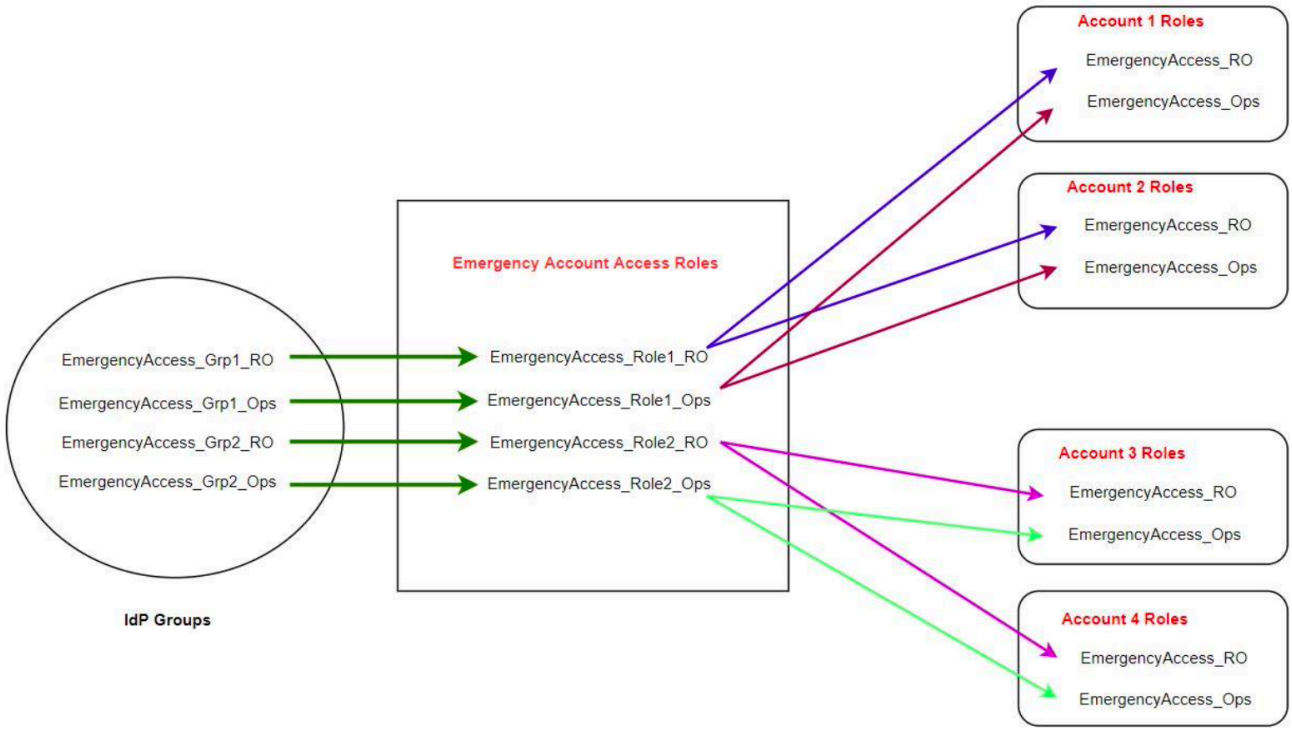
如何规划您的访问模型

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. 确定在 IAM Identity Center 中断期间紧急操作员访问至关重要的 AWS 账户。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账户中创建跨账户角色的工作。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。该图还显示了跨账户角色信任关系，这些关系使紧急访问账户角色能够访问工作负载账户中的相应角色。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 AWS 托管策略或客户托管策略。

账户	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

账户	要创建的角色	信任策略	权限策略
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
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。有关更多信息，请参阅 在 Okta 中一次性设置直接 IAM 联合身份验证应用程序。

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 实例不可用并且您确定必须提供对 AWS 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，他们可以在与紧急账户角色具有跨账户信任的相应工作负载账户中担任角色。

恢复正常运营

检查 AWS Health Dashboard 以确认 IAM Identity Center 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。

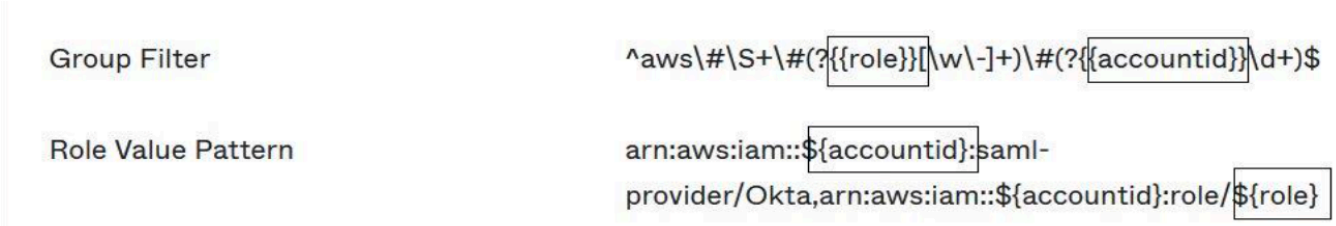
1. 当 IAM Identity Center 服务的状态图标指示该服务运行正常后，登录 IAM Identity Center。
2. 如果您可以成功登录 IAM Identity Center，请告知紧急访问用户 IAM Identity Center 可用。指示这些用户注销并使用 AWS 访问门户重新登录 IAM Identity Center。
3. 所有紧急访问用户注销后，在 IdP 中禁用 IdP 联合身份验证应用程序。我们建议您在下班后执行此任务。
4. 从 IdP 中的紧急访问组中删除所有用户。

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 AWS 帐户联合身份验证。然后选择添加集成。
4. 按照如何为 AWS 账户联合身份验证配置 SAML 2.0 中的步骤，设置与 AWS 的进行直接 IAM 联合身份验证。
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过滤条件。



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 AWS 账户 123456789012 中创建了 EmergencyAccess_Role1_RO 角色（如映射表中所述），并且您的组过滤设置如上图所示配置，则您的组名称应为 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 下图中的紧急账户。

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
         "Effect":"Allow",
         "Principal":{
            "Federated":"arn:aws:iam::123456789012:saml-provider/Okta"
         },
         "Action":[
            "sts:AssumeRoleWithSAML",
            "sts:SetSourceIdentity",
            "sts:TagSession"
         ],
         "Condition":{
            "StringEquals":{
```

```
                "SAML:aud":"https:~/~/signin.aws.amazon.com/saml"
            }
         }
      }
   ]
}
```

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 下图中的紧急账户。

```
{
    "Version": "2012-10-17",
    "Statement":[
      {
         "Effect":"Allow",
         "Action":"sts:AssumeRole",
         "Resource":[
            "arn:aws:iam::<account 1>:role/EmergencyAccess_RO",
            "arn:aws:iam::<account 2>: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。

```
{
    "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。

安全性 AWS IAM Identity Center

云安全 AWS 是重中之重。作为 AWS 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 AWS 的责任。责任共担模式将其描述为云的 安全性和云中 的安全性：

- 云安全 — AWS 负责保护在 AWS 云中运行 AWS 服务的基础架构。 AWS 还为您提供可以安全使用的服务。作为 AWS 合规性计划的一部分，第三方审核人员将定期测试和验证安全性的有效性。要了解适用的合规计划 AWS IAM Identity Center，请参阅按合规计划划分的范围内的AWS 服务。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您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 AWS 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 AWS 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 AWS 资源（例如 AWS 托管应用程序）的权限。

AWS 访问门户的身份验证由您连接到 IAM Identity Center 的目录控制。但是， AWS 访问门户内部可供用户访问的权限由两个因素决定： AWS 账户

1. 谁被分配了 IAM 身份中心控制台 AWS 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 AWS 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 AWS 账户。有关更多信息，请参阅 创建、管理和删除权限集。

以下各节说明您作为管理员如何控制对 IAM Identity Center 控制台的访问权限或如何从 IAM Identity Center 控制台为 day-to-day 任务委派管理访问权限。

- 身份验证
- 访问控制

身份验证

了解如何 AWS 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。

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
- IAM Identity Center 基于身份的策略示例
- 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 AWS 资源都归人所有 AWS 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，账户管理员可以向 IAM 身份（即用户、组和角色）添加权限。某些服务（例如 AWS Lambda）还支持向资源添加权限。

> **Note**
>
> 账户管理员（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 AWS 账户 是创建资源的人。也就是说，资源所有者是 AWS 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 AWS 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， AWS 账户 则您就是该资源的所有者。
- 如果您在自己的 AWS 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 AWS 账户拥有这些资源。
- 如果您在 AWS 账户中创建具有创建 IAM 身份中心资源的权限的 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 AWS 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 AWS 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

- 基于身份的策略（IAM 策略）
- 基于资源的策略

基于身份的策略（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 AWS 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（授予跨账户权限）– 您可以向 IAM 角色附加基于身份的权限策略，以授予跨账户的权限。

  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 (*) 表示可对该账户拥有的所有 IAM Identity Center 资源执行操作。

```
{
   "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 IAM Identity Center 基于身份的策略示例。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）。

基于资源的策略

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、账户、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 AWS 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 AWS 条件键。有关 AWS 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。

IAM Identity Center 基于身份的策略示例

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、组和/或角色。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
- 示例 2：允许用户 AWS 账户 在 IAM 身份中心管理权限
- 示例 3：允许用户管理 IAM Identity Center 中的应用程序
- 示例 4：允许用户管理 Identity Center 目录中的用户和组

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` AWS 托管策略。

```
{
    "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: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 AWS 账户 在 IAM 身份中心管理权限

以下权限策略授予允许用户为您的 AWS 账户创建、管理和部署权限集的权限。

```
{
    "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": "AccessToSSOProvisiondRoles" 部分下列出的"Sid": "IAMListPermissions"其他权限仅用于使用户能够在 AWS 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 AWS 账户 其分配用户和组。如果用户必须在 IAM Identity Center 中管理 AWS 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 AWS 账户 在 IAM 身份中心管理权限。

截至 2020 年 10 月，其中许多操作只能通过 AWS 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。

```
{
    "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。

```
{
    "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 policy 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。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:DescribeAccountAssignmentCreationStatus",
                "sso:DescribeAccountAssignmentDeletionStatus",
                "sso:DescribePermissionSet",
                "sso:DescribePermissionSetProvisioningStatus",
                "sso:DescribePermissionsPolicies",
                "sso:DescribeRegisteredRegions",
                "sso:GetApplicationInstance",
                "sso:GetApplicationTemplate",
                "sso:GetInlinePolicyForPermissionSet",
                "sso:GetManagedApplicationInstance",
                "sso:GetMfaDeviceManagementForDirectory",
                "sso:GetPermissionSet",
                "sso:GetPermissionsPolicy",
                "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": "*"
        }
    ]
}
```

AWS IAM 身份中心的托管策略

要创建 IAM 客户托管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 AWS 托管策略。这些策略涵盖常见使用案例，可在您的 AWS 账户中使用。有关 AWS 托管策略的更多信息，请参阅《IAM 用户指南》中的AWS 托管策略。

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

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

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。

AWS 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 AWS 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。当您将AWSSSOMasterAccountAdministrator策略附加到身份时，即授予管理 AWS IAM Identity Center 权限。拥有此政策的委托人可以在 AWS 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 AWS 组织成员账户中实例化这些分配，并在 AWS 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。

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 管理访问权限 AWS 账户。
- AWSSSOMemberAccountAdministrator— 允许 IAM Identity Center 在多账户 AWS 环境中执行账户管理员操作。有关更多信息，请参阅 AWS 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。

```
{
   "Version":"2012-10-17",
   "Statement":[
     {
         "Sid": "AWSSSOCreateSLR",
         "Effect": "Allow",
         "Action": "iam:CreateServiceLinkedRole",
         "Resource": "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
         "Condition": {
            "StringLike": {
```

```
                "iam:AWSServiceName": "sso.amazonaws.com"
            }
         }
     },
     {
         "Sid":"AWSSSOMasterAccountAdministrator",
         "Effect":"Allow",
         "Action":"iam:PassRole",
         "Resource":"arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
         "Condition":{
             "StringLike":{
               "iam:PassedToService":"sso.amazonaws.com"
             }
         }
      },
      {
         "Sid":"AWSSSOMemberAccountAdministrator",
         "Effect":"Allow",
         "Action":[
            "ds:DescribeTrusts",
            "ds:UnauthorizeApplication",
            "ds:DescribeDirectories",
            "ds:AuthorizeApplication",
            "iam:ListPolicies",
            "organizations:EnableAWSServiceAccess",
            "organizations:ListRoots",
            "organizations:ListAccounts",
            "organizations:ListOrganizationalUnitsForParent",
            "organizations:ListAccountsForParent",
            "organizations:DescribeOrganization",
            "organizations:ListChildren",
            "organizations:DescribeAccount",
            "organizations:ListParents",
            "organizations:ListDelegatedAdministrators",
            "sso:*",
            "sso-directory:*",
            "identitystore:*",
            "identitystore-auth:*",
            "ds:CreateAlias",
            "access-analyzer:ValidatePolicy"
         ],
         "Resource":"*"
      },
```

```
      {
         "Sid": "AWSSSOManageDelegatedAdministrator",
         "Effect": "Allow",
         "Action": [
            "organizations:RegisterDelegatedAdministrator",
            "organizations:DeregisterDelegatedAdministrator"
         ],
         "Resource": "*",
         "Condition": {
            "StringEquals": {
               "organizations:ServicePrincipal": "sso.amazonaws.com"
        }
            }
        }

   ]
}
```

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 AWS 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。所需的操作是 `iam:CreateServiceLinkedRole` 和 `iam:PassRole`，如以下代码片段所示。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "AWSSSOCreateSLR",
         "Effect": "Allow",
         "Action": "iam:CreateServiceLinkedRole",
         "Resource": "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
         "Condition": {
            "StringLike": {
               "iam:AWSServiceName": "sso.amazonaws.com"
            }
         }
      },
      {
         "Sid":"AWSSSOMasterAccountAdministrator",
         "Effect":"Allow",
         "Action":"iam:PassRole",
```

```
         "Resource":"arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
         "Condition":{
             "StringLike":{
               "iam:PassedToService":"sso.amazonaws.com"
             }
         }
      },
   ]
}
```

AWS 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。当您将AWSSSOMemberAccountAdministrator策略附加到身份时，即授予管理 AWS IAM Identity Center 权限。拥有此政策的委托人可以在 AWS 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 AWS 组织成员账户中实例化这些分配，并在 AWS 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。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSSSOMemberAccountAdministrator",
      "Effect": "Allow",
      "Action": [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
        "organizations:EnableAWSServiceAccess",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
```

```
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedAdministrators",
        "sso:*",
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "ds:CreateAlias",
        "access-analyzer:ValidatePolicy"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSSSOManageDelegatedAdministrator",
      "Effect": "Allow",
      "Action": [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource": "*",
        "Condition": {
           "StringEquals": {
              "organizations:ServicePrincipal": "sso.amazonaws.com"
        }
            }
        }
  ]
}
```

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 AWS 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 AWS 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 AWS 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（账户）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 AWS 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 AWS Organizations，请参阅与其他 AWS 服务 AWS Organizations 一起使用。

AWS 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。下面的代码段显示了此策略声明的内容。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSSSODirectoryAdministrator",
            "Effect": "Allow",
            "Action": [
                "sso-directory:*",
                "identitystore:*",
                "identitystore-auth:*",
                "sso:ListDirectoryAssociations"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 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。下面的代码段显示了此策略声明的内容。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSSSOReadOnly",
            "Effect": "Allow",
            "Action": [
                "ds:DescribeDirectories",
                "ds:DescribeTrusts",
                "iam:ListPolicies",
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:ListAccountsForParent",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListDelegatedAdministrators",
                "sso:Describe*",
                "sso:Get*",
                "sso:List*",
                "sso:Search*",
                "sso-directory:DescribeDirectory",
                "access-analyzer:ValidatePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 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。下面的代码段显示了此策略声明的内容。

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

```
    "Statement": [
        {
            "Sid": "AWSSSODirectoryReadOnly",
            "Effect": "Allow",
            "Action": [
                "sso-directory:Search*",
                "sso-directory:Describe*",
                "sso-directory:List*",
                "sso-directory:Get*",
                "identitystore:Describe*",
                "identitystore:List*",
                "identitystore-auth:ListSessions",
                "identitystore-auth:BatchGetSession"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 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

此策略包括访问 Active Directory 时的以下权限。

- ds:AuthorizeApplication——允许身份同步在同步配置文件创建过程中授予对应用程序的访问权限。
- ds:UnauthorizeApplication——允许身份同步在同步配置文件删除过程中删除对应用程序的访问权限。

下面的代码段显示了此策略声明的内容。

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

```
            "Action": [
                "ds:AuthorizeApplication",
                "ds:UnauthorizeApplication"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "identity-sync:DeleteSyncProfile",
                "identity-sync:CreateSyncProfile",
                "identity-sync:GetSyncProfile",
                "identity-sync:StartSync",
                "identity-sync:StopSync",
                "identity-sync:CreateSyncFilter",
                "identity-sync:DeleteSyncFilter",
                "identity-sync:ListSyncFilters",
                "identity-sync:CreateSyncTarget",
                "identity-sync:DeleteSyncTarget",
                "identity-sync:GetSyncTarget",
                "identity-sync:UpdateSyncTarget"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 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。下面的代码段显示了此策略声明的内容。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "identity-sync:GetSyncProfile",
                "identity-sync:ListSyncFilters",
```

```
                "identity-sync:GetSyncTarget",
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 托管策略： AWSSSOServiceRolePolicy

您不可以将 AWSSSOServiceRolePolicy 策略附加得到 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 AWS 账户 用户。 AWS Organizations启用 IAM 后，将在组织 AWS 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账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。在每个角色中创建的服务相关角色 AWS 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。

AWS 托管策略：AWSIAMIdentityCenterAllowListForIdentityContext

在 IAM Identity Center 身份上下文中担任角色时， AWS Security Token Service (AWS 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。下面的代码段显示了此策略声明的内容。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TrustedIdentityPropagation",
            "Effect": "Deny",
            "NotAction": [
                "athena:BatchGetNamedQuery",
                "athena:BatchGetPreparedStatement",
                "athena:BatchGetQueryExecution",
                "athena:CreateNamedQuery",
                "athena:CreatePreparedStatement",
                "athena:DeleteNamedQuery",
                "athena:DeletePreparedStatement",
                "athena:GetNamedQuery",
```

```
                "athena:GetPreparedStatement",
                "athena:GetQueryExecution",
                "athena:GetQueryResults",
                "athena:GetQueryResultsStream",
                "athena:GetQueryRuntimeStatistics",
                "athena:GetWorkGroup",
                "athena:ListNamedQueries",
                "athena:ListPreparedStatements",
                "athena:ListQueryExecutions",
                "athena:StartQueryExecution",
                "athena:StopQueryExecution",
                "athena:UpdateNamedQuery",
                "athena:UpdatePreparedStatement",
                "athena:GetDatabase",
                "athena:GetDataCatalog",
                "athena:GetTableMetadata",
                "athena:ListDatabases",
                "athena:ListDataCatalogs",
                "athena:ListTableMetadata",
                "athena:ListWorkGroups",
                "elasticmapreduce:GetClusterSessionCredentials",
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:GetTable",
                "glue:GetTables",
                "glue:GetTableVersions",
                "glue:GetPartition",
                "glue:GetPartitions",
                "glue:BatchGetPartition",
                "glue:GetColumnStatisticsForPartition",
                "glue:GetColumnStatisticsForTable",
                "glue:SearchTables",
                "glue:CreateDatabase",
                "glue:UpdateDatabase",
                "glue:DeleteDatabase",
                "glue:CreateTable",
                "glue:DeleteTable",
                "glue:BatchDeleteTable",
                "glue:UpdateTable",
                "glue:BatchCreatePartition",
                "glue:CreatePartition",
                "glue:DeletePartition",
                "glue:BatchDeletePartition",
                "glue:UpdatePartition",
```

```
                "glue:BatchUpdatePartition",
                "glue:DeleteColumnStatisticsForPartition",
                "glue:DeleteColumnStatisticsForTable",
                "glue:UpdateColumnStatisticsForPartition",
                "glue:UpdateColumnStatisticsForTable",
                "lakeformation:GetDataAccess",
                "s3:GetAccessGrantsInstanceForPrefix",
                "s3:GetDataAccess"
            ],
            "Resource": "*"
        }
    ]
}
```

IAM 身份中心对 AWS 托管策略的更新

下表描述了自该服务开始跟踪这些更改以来对 IAM Identity Center AWS 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
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 AWS 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 AWS 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	此策略现在包含在 ListDelegatedAdministrators 中调用 AWS Organizations的新权限。	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 AWS 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 Identity Store 服务操作。 有关 IAM Identity Center Identity Store 服务中可用操作的信息，请参阅 IAM Identity Center Identity Store API 参考。	2022 年 3 月 29 日
AWSSSOMemberAccountAdministrator	此策略现在允许所有 IAM Identity Center Identity Store 服务操作。	2022 年 3 月 29 日
AWSSSODirectoryAdministrator	此策略现在允许所有 IAM Identity Center Identity Store 服务操作。	2022 年 3 月 29 日
AWSSSODirectoryReadOnly	此策略现在授予对 IAM Identity Center Identity Store 服务读取操作的访问权限。需要此访问权限才能从 IAM Identity Center Identity Store 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

更改	描述	日期
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
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 身份中心已开始跟踪 AWS 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

AWS IAM Identity Center 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种独特类型的 IAM 角色，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 AWS 服务所需的所有权限。有关更多信息，请参阅 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它 IAM 实体。

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

IAM Identity Center 的服务相关角色权限

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 AWS 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`

AWSServiceRoleForSSO 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 “_” 的角色完成以下操作：AWSReservedSSO

- `iam:AttachRolePolicy`

- iam:CreateRole
- iam:DeleteRole
- iam:DeleteRolePermissionsBoundary
- iam:DeleteRolePolicy
- iam:DetachRolePolicy
- iam:GetRole
- iam:ListRolePolicies
- iam:PutRolePolicy
- iam:PutRolePermissionsBoundary
- iam:ListAttachedRolePolicies

AWSServiceRoleForSSO 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

AWSServiceRoleForSSO 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

AWSServiceRoleForSSO 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

AWSServiceRoleForSSO 服务相关角色权限策略允许 IAM Identity Center 在 “arn: aws:: iam:: *: role/ / sso.amazonaws.com/” 上完成以下操作：aws-service-roleAWSServiceRoleForSSO

- `iam:GetServiceLinkedRoleDeletionStatus`
- `iam:DeleteServiceLinkedRole`

角色权限策略允许 IAM Identity Center 对资源完成以下操作。

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

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

为 IAM Identity Center 创建服务相关角色

您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 AWS 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账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。

注意事项

- 如果您登录了 AWS Organizations 管理账户，则该账户将使用您当前登录的角色，而不是服务相关角色。这可以防止权限升级。

- 当 IAM Identity Center 在 AWS 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 账户中的新角色。

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账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。创建服务相关角色后，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》中的编辑服务相关角色。

删除 IAM Identity Center 的服务相关角色

您无需手动删除该 AWSServiceRoleForSSO 角色。从 AWS 组织中移除后，IAM I AWS 账户 dentity Center 会自动清理资源并从中删除服务相关角色。 AWS 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. 移除用户和组访问权限 适用于有权访问 AWS 账户的所有用户和组。
2. 与 AWS 账户关联的 删除权限集。

使用 IAM 手动删除服务相关角色

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，请参见《IAM 用户指南》中的删除服务相关角色。

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

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

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
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

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
DeleteApplicationProfileForAwsAccount	DeleteProfile	DeleteAccountAssignment
DeletePermissionsPolicy	DeletePermissionsPolicy	DeleteInlinePolicyFromPermissionSet
DeletePermissionSet	DeletePermissionSet	DeletePermissionSet
DescribePermissionsPolicies	DescribePermissionsPolicies	ListManagedPoliciesInPermissionSet
DetachManagedPolicy	DeletePermissionsPolicy	DetachManagedPolicyFromPermissionSet
DisassociateProfile	DisassociateProfile	DeleteAccountAssignment
GetApplicationInstanceForAWSAccount	GetApplicationInstance	ListAccountAssignments
GetAWSAccountProfileStatus	GetProfile	ListPermissionSetsProvisionedToAccount
GetPermissionSet	GetPermissionSet	DescribePermissionSet
GetPermissionsPolicy	GetPermissionsPolicy	GetInlinePolicyForPermissionSet
ListAccountsWithProvisionedPermissionSet	ListApplicationInstances | GetApplicationInstance	ListAccountsForProvisionedPermissionSet
ListAWSAccountProfiles	ListProfiles | GetProfile	ListPermissionSetsProvisionedToAccount
ListPermissionSets	ListPermissionSets	ListPermissionSets
ListProfileAssociations	ListProfileAssociations	ListAccountAssignments

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
ProvisionApplicationInstanceForAWSAccount	GetApplicationInstance | CreateApplicationInstance	CreateAccountAssignment
ProvisionApplicationProfileForAWSAccountInstance	GetProfile | CreateProfile | UpdateProfile	CreateAccountAssignment
ProvisionSAMLProvider	GetTrust | CreateTrust | UpdateTrust	CreateAccountAssignment
PutPermissionsPolicy	PutPermissionsPolicy	PutInlinePolicyToPermissionSet
UpdatePermissionSet	UpdatePermissionSet	UpdatePermissionSet

AWS 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 AWS，会将请求信息 AWS 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、针对的请求以及请求本身的元数据。服务特定的条件密钥是为与单个 AWS 服务一起使用而定义的。

IAM Identity Center 包含一个 AWS STS 上下文提供商，允许 AWS 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。这些密钥包含在 IAM 角色中。密钥值是在应用程序向传递令牌时设置的 AWS STS。应用程序通过以下任一方式获取传递给 AWS STS 它的令牌：

- 在 IAM 身份中心进行身份验证期间。
- 在与可信令牌发行者交换令牌以进行可信身份传播之后。在这种情况下，应用程序从可信令牌发行者那里获取令牌，然后将该令牌兑换成来自 IAM Identity Center 的令牌。

这些密钥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，如果存在密钥值，则可以在您创建的 IAM 策略中使用这些密钥来允许或拒绝权限。

例如，您可能希望根据的值为资源提供有条件的访问权限`UserId`。此值表示哪个 IAM 身份中心用户正在使用该角色。该示例与使用类似`SourceId`。但是`SourceId`，与之不同的是，的值`UserId` 表示身

份存储中经过验证的特定用户。该值存在于应用程序获取然后传递给 AWS STS的令牌中。它不是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

此上下文密钥是 IAM 身份中心用户的密钥，他是 IAM Identity Center 发布的上下文断言的主题。`UserId`上下文断言传递给。 AWS STS您可以使用此密钥将代表其发出请求的 IAM Identity Center 用户的标识符与您在策略中指定的用户标识符进行比较。`UserId`

- 可用性 — 在设置由 IAM Identity Center 发出的上下文断言之后，当使用 AWS CLI 或 AWS STS `AssumeRole` API 操作中的任何 AWS 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 — 单值

identitystore：IdentityStoreArn

此上下文密钥是附加到发布上下文断言的 IAM Identity Center 实例的身份存储的 ARN。它也是身份存储，您可以在其中查找属性`identitystore:UserID`。您可以在策略中使用此密钥来确定是否`identitystore:UserID`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 AWS CLI 或 AWS STS `AssumeRole` API 操作中的任何 AWS 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、Strin g
- 值类型 — 单值

身份中心：ApplicationArn

此上下文密钥是 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密钥来确定是否`identitycenter:ApplicationArn`来自预期的应用程序。使用此密钥可以帮助防止 IAM 角色被意外应用程序访问。

- 可用性-此密钥包含在 AWS STS `AssumeRole` API 操作的请求上下文中。请求上下文包括 IAM Identity Center 发布的上下文断言。
- 数据类型 — Arn、Strin g
- 值类型 — 单值

身份中心：CredentialId

此上下文密钥是身份增强型角色凭证的随机 ID，仅用于记录。由于此密钥值不可预测，因此我们建议您不要将其用于策略中的上下文断言。

- 可用性-此密钥包含在 AWS STS `AssumeRole` API 操作的请求上下文中。请求上下文包括 IAM Identity Center 发布的上下文断言。
- 数据类型 – 字符串
- 值类型 — 单值

身份中心：InstanceArn

此上下文密钥是发布上下文断言的 IAM Identity Center 实例的 ARN。`identitystore:UserID`您可以使用此密钥来确定`identitystore:UserID`和上下文断言是否来自预期的 IAM Identity Center 实例 ARN。

- 可用性-此密钥包含在 AWS STS `AssumeRole` API 操作的请求上下文中。请求上下文包括 IAM Identity Center 发布的上下文断言。
- 数据类型 — Arn、Strin g
- 值类型 — 单值

IAM Identity Center 中的日志记录和监控

您应对组织进行监控，确保对所做的更改进行记录，这是最佳实践。这可以帮助您确保可以调查任何意外更改并回退不需要的更改。 AWS IAM Identity Center 目前支持两项 AWS 服务，可帮助您监控您的组织及其内部发生的活动。

主题

使用记录 IAM 身份中心 API 调用 AWS CloudTrail

AWS IAM Identity Center 与一项服务集成 AWS CloudTrail，该服务提供用户、角色或 AWS 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、谁提出了请求、何时发出请求以及其他详细信息。

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

主题

IAM 身份中心信息位于 CloudTrail

CloudTrail 在您创建账户 AWS 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 AWS 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 AWS 账户。有关更多信息，请参阅使用事件历史查看 CloudTrail 事件。

要持续记录您的事件 AWS 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 AWS 区域。跟踪记录 AWS 分区中所有区域的事件，并将日志文件传送到您指定的 Amazon S3 存储

桶。此外，您可以配置其他 AWS 服务，以进一步分析 CloudTrail 日志中收集的事件数据并对其采取行动。有关更多信息，请参阅下列内容：

- 创建跟踪记录概述
- 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 AWS 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 AWS 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。

支持以下 IAM 身份中心 CloudTrail 操作：

控制台 API 操作	公有 API 操作
AssociateDirectory	AttachManagedPolicyToPermissionSet
AssociateProfile	CreateAccountAssignment
BatchDeleteSession	CreateInstanceAccessControlAttributeConfiguration
BatchGetSession	CreatePermissionSet
CreateApplicationInstance	DeleteAccountAssignment
CreateApplicationInstanceCertificate	DeleteInlinePolicyFromPermissionSet
CreatePermissionSet	DeleteInstanceAccessControlAttributeConfiguration
CreateProfile	DeletePermissionSet
DeleteApplicationInstance	DescribeAccountAssignmentCreationStatus

控制台 API 操作	公有 API 操作
DeleteApplicationInstanceCertificate	DescribeAccountAssignmentDeletionStatus
DeletePermissionsPolicy	DescribeInstanceAccessControlAttributeConfiguration
DeletePermissionSet	DescribePermissionSet
DeleteProfile	DescribePermissionSetProvisioningStatus
DescribePermissionsPolicies	DetachManagedPolicyFromPermissionSet
DisassociateDirectory	GetInlinePolicyForPermissionSet
DisassociateProfile	ListAccountAssignmentCreationStatus
GetApplicationInstance	ListAccountAssignmentDeletionStatus
GetApplicationTemplate	ListAccountAssignments
GetMfaDeviceManagementForDirectory	ListAccountsForProvisionedPermissionSet
GetPermissionSet	ListInstances
GetSSOStatus	ListManagedPoliciesInPermissionSet
ImportApplicationInstanceServiceProviderMetadata	ListPermissionSetProvisioningStatus
ListApplicationInstances	ListPermissionSets

控制台 API 操作	公有 API 操作
ListApplicationInstanceCertificates	ListPermissionSetsProvisionedToAccount
ListApplicationTemplates	ListTagsForResource
ListDirectoryAssociations	ProvisionPermissionSet
ListPermissionSets	PutInlinePolicyToPermissionSet
ListProfileAssociations	TagResource
ListProfiles	UntagResource
ListSessions	UpdateInstanceAccessControlAttributeConfiguration
PutMfaDeviceManagementForDirectory	UpdatePermissionSet
PutPermissionsPolicy	
StartSSO	
UpdateApplicationInstanceActiveCertificate	
UpdateApplicationInstanceDisplayData	
UpdateApplicationInstanceServiceProviderConfiguration	
UpdateApplicationInstanceStatus	
UpdateApplicationInstanceResponseConfiguration	

控制台 API 操作	公有 API 操作
UpdateApplicationInstanceResponseSchemaConfiguration	
UpdateApplicationInstanceSecurityConfiguration	
UpdateDirectoryAssociation	
UpdateProfile	

有关 IAM Identity Center 的公共 API 操作的更多信息，请参阅 IAM Identity Center API 参考指南。

支持以下 IAM 身份中心身份存储 CloudTrail 操作：

- AddMemberToGroup
- CompleteVirtualMfaDeviceRegistration
- CompleteWebAuthnDeviceRegistration
- CreateAlias
- CreateExternalIdPConfigurationForDirectory
- CreateGroup
- CreateUser
- DeleteExternalIdPConfigurationForDirectory
- DeleteGroup
- DeleteMfaDeviceForUser
- DeleteUser
- DescribeDirectory
- DescribeGroups
- DescribeUsers
- DisableExternalIdPConfigurationForDirectory
- DisableUser
- EnableExternalIdPConfigurationForDirectory
- EnableUser

- GetAWSSPConfigurationForDirectory
- ListExternalIdPConfigurationsForDirectory
- ListGroupsForUser
- ListMembersInGroup
- ListMfaDevicesForUser
- PutMfaDeviceManagementForDirectory
- RemoveMemberFromGroup
- SearchGroups
- SearchUsers
- StartVirtualMfaDeviceRegistration
- StartWebAuthnDeviceRegistration
- UpdateExternalIdPConfigurationForDirectory
- UpdateGroup
- UpdateMfaDeviceForUser
- UpdatePassword
- UpdateUser
- VerifyEmail

支持以下 IAM 身份中心 OIDC CloudTrail 操作：

- CreateToken
- RegisterClient
- StartDeviceAuthorization

支持以下 IAM 身份中心门户网站 CloudTrail 操作：

- Authenticate
- Federate
- ListApplications
- ListProfilesForApplication
- ListAccounts
- ListAccountRoles

- GetRoleCredentials
- Logout

每个事件或日记账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 AWS Identity and Access Management (IAM) 用户凭证发出。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务发出。

有关更多信息，请参阅CloudTrail 用户身份元素。

了解 IAM Identity Center 日志文件条目

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

以下示例显示了在 IAM Identity Center 控制台中发生的管理员 CloudTrail 日志条目 (samadams@example.com)：


```
{
   "Records":[
      {
         "eventVersion":"1.05",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDAJAIENLMexample",
            "arn":"arn:aws:iam::08966example:user/samadams",
            "accountId":"08966example",
            "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":"08966example"
      }
   ]
}
```

以下示例显示了 AWS 访问门户中发生的最终用户 (bobsmith@example.com) 操作的 CloudTrail 日志条目：

```
{
   "Records":[
      {
         "eventVersion":"1.05",
         "userIdentity":{
            "type":"Unknown",
            "principalId":"example.com//
S-1-5-21-1122334455-3652759393-4233131409-1126",
            "accountId":"08966example",
            "userName":"bobsmith@example.com"
         },
         "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":"08966example"
```

```
      }
   ]
}
```

以下示例显示了在 IAM Identity Center OIDC 中发生的最终用户 (bobsmith@example.com) 操作的 CloudTrail 日志条目：

```
{
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "Unknown",
        "principalId": "example.com//S-1-5-21-1122334455-3652759393-4233131409-1126",
        "accountId": "08966example",
        "userName": "bobsmith@example.com"
      },
      "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": "08966example",
          "type": "IdentityStoreId",
          "ARN": "d-1234example"
        }
```

```
      ],
      "eventType": "AwsApiCall",
      "recipientAccountId": "08966example"
}
```

了解 IAM Identity Center 登录事件

AWS CloudTrail 记录所有 AWS IAM Identity Center 身份源的成功和失败登录事件。原生 SSO 和 Active Directory（AD Connector 和 AWS Managed Microsoft AD）来源的身份将包括每次提示用户解决特定凭据质疑或因素时捕获的其他登录事件，以及该特定凭证验证请求的状态。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 AWS 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 AWS 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。	所有身份来源

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。

事件名称	事件目的	登录事件适用性	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）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/...”

IAM Identity Center 登录场景的示例事件

以下示例显示了不同登录场景的预期 CloudTrail 事件顺序。

主题

- 仅使用密码进行身份验证即可成功登录
- 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 TOTP 身份验证器应用程序进行身份验证时成功登录

- 使用密码进行身份验证并需要强制 MFA 注册时成功登录
- 仅使用密码进行身份验证时登录失败

仅使用密码进行身份验证即可成功登录

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":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "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",
      "CredentialType":"PASSWORD"
   },
   "requestID":"5be44ffb-6946-4f47-acaf-1adebd4afead",
   "eventID":"27ea7725-c1fd-4355-bdba-d0e628e0e604",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
```

```
}
```

成功 CredentialVerification（密码）

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "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":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "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":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":""
   },
   "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"
   },
   "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 TOTP 身份验证器应用程序进行身份验证时成功登录

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":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "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"
   },
   "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":"Unknown",
```

```
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "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":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
```

```
   "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":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "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":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "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

以下事件序列捕获了成功使用密码登录的示例，但用户需要在完成登录之前成功注册 MFA 设备。

CredentialChallenge（密码）


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "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"
   },
   "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":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "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":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "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"
   }
}
```

仅使用密码进行身份验证时登录失败

以下事件序列捕获了仅密码登录失败的示例。

CredentialChallenge（密码）

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "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"
   },
   "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",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "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"
    }
}
```

亚马逊 CloudWatch 活动

当组织中发生管理员指定的操作时，IAM Identity Center 可以与 CloudWatch 事件配合使用来引发事件。例如，大多数管理员希望每次在组织中创建新账户时，或成员账户的管理员尝试离开组织时收到提醒，因为这些都是敏感操作。您可以配置 CloudWatch 事件规则来查找这些操作，然后将生成的事件发送到管理员定义的目标。目标可以是 Amazon SNS 主题，向订阅者发送电子邮件或短信。您也可以创建一个 AWS Lambda 函数来记录操作的详细信息以供日后查看。

要了解有关 CloudWatch 事件的更多信息，包括如何配置和启用 CloudWatch 活动，请参阅 Amazon Events 用户指南。

记录 AD 同步和可配置的 AD 同步错误

您可以在 Active Directory (AD) 同步和可配置的 AD 同步配置上启用日志功能，以接收包含同步过程中可能发生的错误信息的日志。利用这些日志，您可以监控 AD 同步和可配置的 AD 同步是否存在问题，并在适用时采取措施。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 AWS 服务启用日志记录。

> **Note**
>
> 您需要为登录付费。有关更多信息，请参阅 Amazon CloudWatch 定价页面上的销售日志。

启用 AD 同步和可配置的 AD 同步错误日志

1. 登录 IA M 身份中心控制台。
2. 选择设置。
3. 在 “设置” 页面上，选择 “身份来源” 选项卡，选择 “操作”，然后选择 “管理日志”。

4. 选择添加日志传送和以下目标类型之一。
   a. 选择 “收到 Amazon CloudWatch 日志”。然后选择或输入目标日志组。
   b. 选择 “前往亚马逊 S3”。然后选择或输入目标存储桶。
   c. 选择 To Firehose。然后选择或输入目标传送流。
5. 选择提交。

禁用 AD 同步和可配置的 AD 同步错误日志

1. 登录 IA M 身份中心控制台。
2. 选择设置。
3. 在 “设置” 页面上，选择 “身份来源” 选项卡，选择 “操作”，然后选择 “管理日志”。
4. 对于要删除的目的地，选择 “删除”。
5. 选择提交。

AD 同步和可配置的 AD 同步错误日志字段

有关可能的错误日志字段，请参阅以下列表。

`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的错误代码。

`error_message`

一条包含有关所发生错误的详细信息的消息。

`sync_source`

同步源是实体同步的地方。对于 IAM 身份中心，这是由管理的活动目录 (AD) AWS Directory Service。同步源包含受影响目录的域和 ARN。

`sync_target`

同步目标是保存实体的目的地。对于 IAM 身份中心来说，这是一个身份存储。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。对于 IAM 身份中心，这是实体的 SID。

`source_entity_type`

导致错误的实体类型。该值可以是 USER 或 GROUP。

`eventTimestamp`

错误发生的时间戳。

AD 同步和可配置的 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

作为多个合规计划的一部分，第三方审计师会评估 AWS 服务 诸 AWS IAM Identity Center 如此类的安全 AWS 性和合规性。

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

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

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

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

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

- AWS 合规资源AWS — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- AWS 客户合规指南 — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践， AWS 服务 并将指南映射到跨多个框架（包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO)）的安全控制。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。

- AWS Security Hub— 这 AWS 服务 提供了您内部安全状态的全面视图 AWS。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 Security Hub 控件参考。
- AWS Audit Manager— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

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。

AWS 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。

AWS 为想要详细了解如何使用 AWS 服务 它来处理和存储健康信息的客户提供了一份以 HIPAA 为重点的白皮书。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 AWS 产品和服务存储、处理或传输持卡人数据的客户可以使用 IAM Identity Center 中的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 AWS 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： • AWS SOC 1 报告——使用 Ar ti AWS fact 下载 • AWS SOC 2：安全、可用性和机密性报告——使用 Ar ti AWS fact 下载 • AWS SOC 3：安全性、可用性和机密性报告 IAM 身份中心属于 AWS 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 的故障恢复能力

AWS 全球基础设施是围绕 AWS 区域和可用区构建的。 AWS 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故障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设施相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域和可用区的更多信息，请参阅AWS 全球基础设施。

要了解有关 AWS IAM Identity Center 弹性的更多信息，请参阅故障恢复能力设计和区域行为。

IAM Identity Center 的基础设施安全

作为一项托管服务 AWS IAM Identity Center ，受安全、身份和合规性最佳实践中描述的 AWS 全球网络安全程序的保护。

您可以使用 AWS 已发布的 API 调用通过网络访问 IAM 身份中心。客户端必须支持传输层安全性协议 (TLS) 1.0 或更高版本。建议使用 TLS 1.2 或更高版本。客户端还必须支持具有完全向前保密（PFS）的密码套件，例如 Ephemeral Diffie-Hellman（DHE）或 Elliptic Curve Ephemeral Diffie-Hellman（ECDHE）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service（AWS STS）生成临时安全凭证来对请求进行签名。

为 AWS IAM Identity Center 资源添加标签

标签 是自定义的属性标签，您将其添加到 AWS 资源以便更轻松地确定、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。

标签有助于您标识和组织 AWS 资源。许多 AWS 服务支持标记，因此，您可以将同一标签分配给来不同服务的资源，以指示这些资源是相关的。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 AWS 一般参考 指南中的标记 AWS 资源和标记最佳实践。

除了通过标签标识、组织和跟踪 AWS 资源之外，您还可以在 IAM 策略中使用标签，帮助控制哪些人可以查看并与您的资源交互。要了解有关使用标签控制访问的更多信息，请参阅 IAM 用户指南中的使用标签控制对 AWS 资源的访问。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。

目前，您只能将标签应用于权限集。您无法将标签应用到 IAM Identity Center 在 AWS 账户 中创建的相应角色。您可以使用 IAM Identity Center 控制台 AWS CLI 或 IAM Identity Center API 添加、编辑或删除权限集的标签。

以下部分提供有关 IAM Identity Center 标签的更多信息。

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 AWS 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。

AWS CLI 示例

AWS CLI 提供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
```

删除标签

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

您可以在 IAM Identity Center API 中使用以下操作来管理权限集的标签。

IAM Identity Center 实例标签的 API 操作

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 AWS CLI 与 IAM Identity Center 集成

AWS 命令行界面 (CLI) 版本 2 与 IAM Identity Center 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 的相同 Active Directory 或 IAM Identity Center 凭证直接登录 AWS CLI，并访问其分配的账户和角色。例如，管理员将 IAM Identity Center 配置为使用 Active Directory 进行身份验证后，开发人员可以直接使用其 Active Directory 凭证登录 AWS CLI。

AWS CLI 与 IAM Identity Center 集成具有以下优势：

- 通过使用 AWS 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 AWS CLI 与 IAM Identity Center 集成

要使用 AWS CLI 与 IAM Identity Center 集成，您需要下载、安装和配置 AWS Command Line Interface 版本 2。有关如何下载 AWS CLI 并将其与 IAM Identity Center 集成的详细步骤，请参阅 AWS Command Line Interface 用户指南中的配置 AWS CLI 以使用 IAM Identity Center。

AWS IAM Identity Center 地区可用性

IAM 身份中心有几种常用版本 AWS 区域。这种可用性使您可以更轻松地配置用户对多个应用程序 AWS 账户 和业务应用程序的访问权限。当您的用户登录 AWS 访问门户时，他们可以选择他们有权访问的，然后访问 AWS Management Console。 AWS 账户 有关 IAM 身份中心支持的完整列表 AWS 区域 ，请参阅 I AM 身份中心终端节点和配额。

IAM Identity Center 区域数据

首次启用 IAM Identity Center 时，您在 IAM Identity Center 中配置的所有数据都存储在您配置它的区域中。这些数据包括目录配置、权限集、应用程序实例和对 AWS 账户 应用程序的用户分配。如果您使用的是 IAM Identity Center 身份存储，则您在 IAM Identity Center 中创建的所有用户和群组也存储在同一区域中。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。

AWS Organizations AWS 区域 一次只能支持一个。要在其他区域启用 IAM Identity Center，必须先删除当前的 IAM Identity Center 配置。切换到其他区域也会更改 AWS 访问门户的 URL，您必须重新配置所有权限集和分配。

跨区域调用

当最终用户尝试使用一次性密码（OTP）作为第二个身份验证因素登录时，IAM Identity Center 使用 Amazon Simple Email Service (Amazon SES) 向他们发送电子邮件。还会针对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）发送这些电子邮件。Amazon SES 在 IAM 身份中心支持的子集中提供。 AWS 区域

当 Amazon SES 在 AWS 区域本地可用时，IAM Identity Center 会调用 Amazon SES 本地端点。当 Amazon SES 在本地不可用时，IAM Identity Center 会调用不同 AWS 区域中的 Amazon SES 端点，如下表所示。

Amazon SES 区域代码列在下表中。

IAM Identity Center 区域代码	IAM Identity Center 区域名称	Amazon SES 区域代码	Amazon SES 区域名称
us-gov-east-1	AWS GovCloud （美国东部）	us-gov-west-1	AWS GovCloud （美国西部）

IAM Identity Center 区域代码	IAM Identity Center 区域名称	Amazon SES 区域代码	Amazon SES 区域名称
ap-east-1	亚太地区（香港）	ap-northeast-2	亚太地区（首尔）
ap-southeast-4	亚太地区（墨尔本）	ap-southeast-2	亚太地区（悉尼）
ap-south-2	亚太地区（海得拉巴）	ap-south-1	亚太地区（孟买）
eu-central-2	欧洲（苏黎世）	eu-central-1	欧洲地区（法兰克福）
eu-south-2	欧洲（西班牙）	eu-west-3	欧洲地区（巴黎）
me-central-1	中东（阿联酋）	eu-central-1	欧洲地区（法兰克福）

在这些跨区域调用中，IAM Identity Center 可能会发送以下用户属性：

- 电子邮件地址
- 名
- 姓
- 账号进入 AWS Organizations
- AWS 访问门户网址
- 用户名
- 目录 ID
- 用户 ID

在可选区域（默认情况下禁用的区域）中管理 IAM 身份中心

默认情况下，所有 AWS 服务中的操作 AWS 区域 都启用了大多数功能。将自动激活这些区域以通过 IAM Identity Center 使用。以下 AWS 区域 是可选区域，您必须将其启用：

- 非洲（开普敦）
- 亚太地区（香港）

- 亚太地区（雅加达）
- 亚太地区（墨尔本）
- 亚太地区（海得拉巴）
- 欧洲地区（米兰）
- 欧洲（苏黎世）
- 欧洲（西班牙）
- 以色列（特拉维夫）
- 中东（巴林）
- 中东（阿联酋）

当您在选择加入中为管理账户启用 IAM Identity Center 时 AWS 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。

- 账户 ID
- 账户名称
- 账户电子邮件
- IAM Identity Center 在成员账户中创建的 IAM 角色的 Amazon 资源名称（ARN）

如果您禁用已安装 IAM Identity Center 的区域，IAM Identity Center 也会被禁用。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 AWS 账户 和应用程序。 AWS 将您的 IAM 身份中心配置中的数据保留至少 10 天。如果您在这段时间内重新启用 IAM Identity Center，则您的 IAM Identity Center 配置数据仍将在该地区可用。

要在选择加入模式下重新启用 IAM 身份中心 AWS 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 AWS 区域。 AWS 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。 AWS 区域

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

删除您的 IAM Identity Center 配置

删除 IAM Identity Center 配置后，该配置中的所有数据都将被删除且无法恢复。下表描述了根据当前在 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	已连接的目录 （AWS Managed Microsoft AD 或 AD Connector）	IAM Identity Center Identity Store
您为其配置的所有权限集 AWS 账户	✓	✓
您在 IAM Identity Center 中配置的所有应用程序	✓	✓
您为其配置的所有用户分配 AWS 账户 和应用程序	✓	✓
目录或存储中的所有用户和群组	不适用	✓

当您需要删除当前的 IAM Identity Center 配置时，请按以下步骤操作。

删除 IAM Identity Center 配置

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”。

AWS IAM Identity Center 配额

下表描述了 IAM Identity Center 内的配额。配额增加请求必须来自管理账户或委托管理员账户。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 AWS CLI 和 API。有关 CLI 的更多信息，请参阅 将 AWS CLI 与 IAM Identity Center 集成。有关 API 的更多信息，请参阅欢迎使用 IAM Identity Center API 参考。

应用程序配额

资源	默认限额	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	5 万个字符	否
上传到 IAM 身份中心的 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

AWS 账户 配额

资源	默认限额	能否增加
IAM Identity Center 中允许的权限集合数	2000	是
每组允许的已配置权限集数量 AWS 账户	250	是

资源	默认限额	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 AWS 托管策略和客户托管策略数量	20 [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 AWS 账户	1	否

[1]AWS 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 AWS 账户 的地方申请增加附加到 IAM 角色的 IAM 配额托管策略。

> **Note**
>
> 权限集 AWS 账户 作为 IAM 角色进行配置，或者在中使用现有 IAM 角色 AWS 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	默认限额	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	默认限额	能否增加
IAM Identity Center 中支持的用户数	100000	是
IAM Identity Center 中支持的组数	100000	否
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	默认限额
IAM Identity Center API	IAM Identity Center API 的集体节流限制最大为每秒 20 个事务 (TPS)。的CreateAccountAssignment未完成异步调用的最大速率为 10 个。这些配额不能更改。

其他配额

资源	默认限额	能否增加
可以配置的 AWS 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

* 最多支持 3000 个 AWS 账户 或应用程序（总计）。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。

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 控制台或受支持的 AWS 托管应用程序的设置体验创建账户实例，请验证是否存在以下使用情况：

- 在您试图创建账户实例的 AWS 账户 中，检查其他 AWS 区域。对于每个 AWS 账户，IAM Identity Center 实例数量都被限制为一个。要启用该应用程序，请切换到具有 IAM Identity Center 实例的 AWS 区域，或者切换到没有 IAM Identity Center 实例的账户。
- 如果您的组织在 2023 年 9 月 14 日之前启用了 IAM Identity Center，您的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。

尝试查看预配置为与 IAM Identity Center 配合使用的云应用程序列表时，收到错误消息

如果您的策略允许 `sso:ListApplications`，但不允许其他 IAM Identity Center API，将发生以下错误。请更新策略，以解决此错误。

`ListApplications` 权限会授权多个 API：

- `ListApplications` API。
- 在 IAM Identity Center 控制台中使用的内部 API，例如 `ListApplicationProviders` API。

为了帮助解决重复问题，内部 API 现在也使用 `ListApplicationProviders` 操作进行授权。要允许公共的 `ListApplications` API，但拒绝内部 API，您的策略必须包含拒绝 `ListApplicationProviders` 操作的声明：

```
    "Statement": [
```

```
    {
         "Effect": "Deny",
         "Action": "ListApplicationProviders",
         "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": "ListApplications",
        "Resource": "<instanceArn>" // (or "*" for all instances)
    }
]
```

要允许内部 API，但拒绝 `ListApplications`，策略需要只允许 `ListApplicationProviders`。如果未明确允许，将拒绝 `ListApplications` API。

```
      "Statement": [
    {
         "Effect": "Allow",
         "Action": "ListApplicationProviders",
         "Resource": "*"
    }
]
```

您的政策更新后，请联系 AWS Support，移除此主动措施。

与 IAM Identity Center 创建的 SAML 断言内容有关的问题

从 AWS 访问门户访问 AWS 账户 和 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。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. 登录到 AWS 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

如果在您的 IdP 中配置为预调配到 IAM Identity Center 中的一部分用户的 SCIM 同步成功，但其他用户的 SCIM 同步失败，则您可能会看到类似于身份提供者 `'Request is unparsable, syntactically incorrect, or violates schema'` 的错误。您还可以在 AWS CloudTrail 中看到详细的预调配失败消息。

此问题通常表明您的 IdP 中的用户的配置方式是 IAM Identity Center 所不支持的。有关 IAM Identity Center SCIM 实施的完整详细信息，包括用户对象的必需、可选和禁止参数和操作的规范，请参阅 IAM Identity Center SCIM 实施开发人员指南。有关 SCIM 要求的信息，SCIM 开发人员指南应被视为权威性指南。但是，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、姓氏和/或显示名称。
   - 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。
   - 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 AWS 中的任何操作都不需要该属性，请从 IdP 中用户对象的 SCIM 预调配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。

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 AWS 访问门户。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) 或其 UPN 登录名 (`UserName@Corp.Example.com`) 登录用户门户。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，用户必须使用其下级登录名 (DOMAIN\UserName) 登录。有关更多信息，请参阅 Identity Center 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 服务在账户中创建的角色，它们来自向账户分配权限集。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 AWS'
```

这些角色只能从 IAM Identity Center 管理员控制台中进行修改，该控制台位于 AWS Organizations 的管理账户中。修改完成后，您可以将更改推送到分配的 AWS 账户。

目录用户无法重置密码

当目录用户使用忘记密码？选项在登录 AWS 访问门户期间重置密码时，他们的新密码必须遵守默认密码策略，如 在 IAM Identity Center 中管理身份时的密码要求 中所述。

如果用户输入了符合策略的密码后收到错误消息 `We couldn't update your password`，请检查 AWS CloudTrail 是否记录了故障。这可以通过使用以下过滤器在 CloudTrail 的事件历史记录控制台中搜索来完成：

```
"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 AWS 支持中心。

我的用户在权限集中被引用，但无法访问分配的账户或应用程序

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 AWS 账户 访问权限，您可以从最初向旧用户或组分配访问权限的 AWS 账户中移除访问权限，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。

您还可以在 CloudTrail 日志中搜索引用相关用户或组名称的 SCIM 同步事件，以查看是否 AWS 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 账户中启用了 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 AWS CloudTrail 并筛选事件名称 ExternalIdPDirectoryLogin，从而进一步解决外部身份提供者登录失败的问题。

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

Google Chrome、Mozilla Firefox、Microsoft Edge 和 Apple Safari 网络浏览器以及 Windows 10 和 Android 平台目前支持 WebAuthn。WebAuthn 支持的某些组件可能有所不同，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)，了解有关浏览器/平台支持的更多信息。有关 IAM Identity Center 中的 WebAuthn 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 协议将其账户完全预调配到 IAM Identity Center 之前，如果用户尝试使用外部身份提供者提供的账户（例如 Okta 或 Microsoft Entra ID）登录 IAM Identity Center，就会发生此错误。将用户账户预调配到 IAM Identity Center 后，应解决此问题。确认该账户已预调配到 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已正确同步到可靠的时间源，或手动设置设备上的时间以匹配可靠来源，例如 NIST (https://www.time.gov/) 或其他本地/区域等效时间。

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`。必须配置您的电子邮件系统，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：您无法删除/修改/移除/分配对管理账户中预调配的权限集的访问权限

此消息表示该 委派管理 功能已启用，并且只有在 AWS 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 注册成员账户。

文档历史记录

下表介绍 AWS IAM Identity Center 文档的重要补充部分。我们还经常更新文档来处理发送给我们的反馈意见。

- 最近主要文档更新时间：2022 年 9 月 23 日

变更	说明	日期
更新了 AWS 托管策略	更新了 `AWSIAMIdentityCenterAllowListForIdentityContext` AWS 托管策略的权限。	2023 年 11 月 26 日
新的 AWS 托管策略主题	添加了 `AWSIAMIdentityCenterAllowListForIdentityContext` AWS 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
更新了身份中心 API 参考中的用户和群组	此更新包括身份中心 API 参考指南中对新的 “创建、更新和删除 API”的参考。	2022 年 8 月 31 日
AWS 单点登录 (AWS SSO) 已重命名为 AWS IAM Identity Center	AWS 引入了 AWS IAM Identity Center。IAM Identity Center 扩展了 AWS Identity and Access Management (IAM) 的功能，可帮助您集中管理账户以及员工用户对应用程序的访问权限。IAM Identity Center	2022 年 7 月 26 日

	的功能包括应用程序分配、多账户权限和 AWS 访问门户。	
支持权限集中的权限边界和客户管理型策略	添加了使用带权限集的 AWS 托管策略和客户托管 AWS Identity and Access Management (IAM) 策略的内容。	2022 年 7 月 14 日
支持手动启用的 AWS 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
更新了 AWS 托管策略	更新了 `AWSSSOServiceRolePolicy` AWS 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
更新了 AWS 托管策略	更新了 `AWSSSOMasterAccountAdministrator` 、`AWSSSOMemberAccountAdministrator` 和 `AWSSSOReadOnly` AWS 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 AWS 托管策略主题	添加了 `AWSSSOMasterAccountAdministrator` AWS 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
支持 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
支持 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来源，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
对 AWS 账户的会话持续时间的支持	增加了有关如何为 AWS 账户设置会话持续时间的内容。	2018 年 10 月 30 日

使用身份中心目录的新选项	增加了如何选择身份中心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
支持多账户访问管理账户	增加了有关如何向托管账户中的用户委派多账户访问权限的内容。	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	增加了有关如何获取临时凭证来运行 AWS 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

AWS 术语表

有关最新的 AWS 术语，请参阅《AWS 词汇表参考》中的 AWS 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。