aws

用户指南

AWS 设置

AWS 设置: 用户指南

Table of Contents

概述

本指南提供按照最新的安全最佳实践创建新 AWS 账户 和在 AWS IAM Identity Center 中设置第一个管理用户的说明。

AWS 账户 是存取 AWS 服务 的必要条件，它有两个基本功能：

- 容器 — AWS 账户 是您作为 AWS 客户可以创建的所有 AWS 资源的容器。如果创建一个 Amazon Simple Storage Service（Amazon S3）存储桶或一个 Amazon Relational Database Service（Amazon RDS）数据库来存储数据，或者创建一个 Amazon Elastic Compute Cloud*（Amazon EC2）实例来处理数据，即是在您的账户中创建资源。每个资源均由一个 Amazon 资源名称（ARN）进行唯一标识，该 ARN 包含或拥有该资源的账户 ID。
- 安全边界 - AWS 账户 是 AWS 资源的基本安全边界。您在账户中创建的资源仅可供拥有该账户凭证的用户使用。

  您可以在账户中创建的关键资源包括身份（例如 IAM 用户和角色）和联合身份，例如来自企业用户目录、Web 身份提供商、IAM Identity Center 目录的用户，或任何其他使用通过身份源提供的凭证来访问 AWS 服务 的用户。这些身份具有用户可以用来登录 AWS 或进行身份验证的凭证。身份还有权限策略，这些策略指定登录者有权使用账户中的资源执行哪些操作。

术语

亚马逊 Web Services (AWS) 使用常用术语来描述登录过程。我们建议您阅读并理解这些术语。

管理员

也称为 AWS 账户 管理员或IAM管理员。管理员，通常是信息技术 (IT) 人员，是负责监督 AWS 账户。管理员拥有更高的权限级别 AWS 账户 而不是其组织的其他成员。管理员为以下各项建立和实施设置 AWS 账户。 他们还会创建IAM或IAM身份中心用户。管理员向这些用户提供他们的访问凭证和登录信息，URL供他们登录 AWS.

帐户

一个标准 AWS 账户 包含你的 AWS 资源以及可以访问这些资源的身份。账户与账户所有者的电子邮件地址和密码关联。

凭证

也称作访问凭证或安全凭证。凭证是用户向其提供的信息 AWS 登录并获得访问权限 AWS 资源的费用。凭证可以包括电子邮件地址、用户名、用户定义的密码、账户 ID 或别名、验证码和单次使用多因素身份验证 (MFA) 代码。在身份验证和授权中，系统使用凭证来识别谁在执行调用并决定是否允许请求的访问。In AWS，这些证书通常是访问密钥 ID 和私有访问密钥。

有关证书的更多信息，请参阅了解并获取您的 AWS 证书。

> **Note**
>
> 用户必须提交的凭证类型取决于其用户类型。

公司凭证

用户在访问公司网络和资源时提供的凭证。您的公司管理员可以设置您的 AWS 账户 可使用与访问公司网络和资源相同的凭据进行访问。这些凭证由管理员或帮助中心员工提供给您。

配置文件

当你注册时 AWS 生成器 ID，您可以创建个人资料。您的个人资料包括您提供的联系信息，以及管理多因素身份验证 (MFA) 设备和活动会话的能力。您还可以在配置文件中详细了解隐私条款以及我们如何处理您的数据。有关您的个人资料及其与个人资料的关系的更多信息 AWS 账户，请参阅 AWS 生成器 ID 和其他 AWS 证书。

用户

用户是指账户下的个人或应用程序，可向以下用户发出API呼叫 AWS 产品。每个用户在里面都有唯一的名字 AWS 账户 以及一组不与他人共享的安全证书。这些证书与安全证书是分开的 AWS 账户每个用户均与 且仅与一个账户关联。 AWS 账户.

根用户凭证

root 用户凭证与用于登录的凭据相同 AWS Management Console 作为 root 用户。有关根用户的更多信息，请参阅根用户。

验证代码

在登录过程中，验证码使用多重身份验证 () 来验证您的身份。MFA验证码的交付方式各不相同。它们可以通过短信或电子邮件发送。有关更多信息，请咨询您的管理员。

AWS 用户和凭证

当你与之互动时 AWS，你指定你的 AWS 安全证书，用于验证您的身份以及您是否有权访问所请求的资源。 AWS 使用安全证书对请求进行身份验证和授权。

例如，如果要从 Amazon Simple Storage Service (Amazon S3) 存储桶下载受保护的文件，则您的凭证必须允许该访问。如果您的凭证显示您无权下载该文件， AWS 拒绝您的请求。但是，下载公开共享的 Amazon S3 存储桶中的文件不需要安全凭证。

根用户

也称为账户所有者或账户根用户。作为 root 用户，您可以完全访问所有内容 AWS 您的服务和资源 AWS 账户。 当你第一次创建 AWS 账户，你从一个可以完全访问所有人的单一登录身份开始 AWS 账户中的服务和资源。这个身份是 AWS 帐户 root 用户。你可以登录 AWS Management Console以 root 用户身份使用您创建帐户时使用的电子邮件地址和密码。有关如何登录的分步说明，请参阅登录 AWS Management Console 作为 root 用户。

> **Important**
>
> 当你创建 AWS 账户，您从一个登录身份开始，该身份可以完全访问所有人 AWS 服务 以及账户中的资源。这个身份叫做 AWS 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关需要您以 root 用户身份登录的任务的完整列表，请参阅《用户指南》中的 “需要根用户凭据的IAM任务”。

有关包括根用户在内的IAM身份的更多信息，请参阅IAM身份（用户、用户组和角色）。

IAM身份中心用户

IAM身份中心用户通过登录 AWS 访问门户。这些区域有： AWS 访问门户或特定登录URL由您的管理员或帮助台员工提供。如果您为自己创建了IAM身份中心用户 AWS 账户，已向IAM身份中心用户的电子邮件地址发送了加入 Identity Center 的邀请 AWS 账户。 具体的登录信息包含URL在电子邮件邀请中。IAMIdentity Center 用户无法通过登录 AWS Management Console。 有关如何登录的分步说明，请参阅登录 AWS 访问门户。

> **Note**
>
> 我们建议您将特定的登录信息添加URL为书签 AWS 访问门户，以便以后可以快速访问它。

有关IAM身份中心的更多信息，请参阅什么是IAM身份中心？

联合身份

联合身份是指可以使用知名的外部身份提供商 (IdP) 登录的用户，例如 Login with Amazon、Facebook、Google 或任何其他兼容 OpenID Connect () OIDC 的 IdP。使用 Web 联合身份验证，您可以接收身份验证令牌，然后在中使用该令牌交换临时安全证书 AWS 这映射到一个有权使用你中的资源的IAM角色 AWS 账户。 您不使用登录 AWS Management Console 或者 AWS 访问门户。相反，使用的外部身份决定了您的登录方式。

有关更多信息，请参阅以联合身份登录。

IAM用户

IAM用户是您在其中创建的实体 AWS。 此用户是您内部的身份 AWS 账户 已被授予特定的自定义权限。您的IAM用户凭证由用于登录的用户名和密码组成 AWS Management Console。 有关如何登录的分步说明，请参阅登录 AWS Management Console 作为IAM用户。

有关包括IAM用户在内的IAM身份的更多信息，请参阅IAM身份（用户、用户组和角色）。

AWS 生成器 ID 用户

作为 AWS Builder ID 用户，您专门登录到 AWS 您要访问的服务或工具。网络 ACL 和安全组都允许 (因此可到达您的实例) 的发起 ping 的 AWS Builder ID 用户可以补充任何 AWS 账户 您已经拥有或想要创建。网络 ACL 和安全组都允许 (因此可到达您的实例) 的发起 ping 的 AWS Builder ID 代表你作为一个人，你可以用它来访问 AWS 服务和工具没有 AWS 账户。 您还有一个个人资料，可以在其中查看和更新您的信息。有关更多信息，请参阅使用登录 AWS 生成器 ID 。

先决条件和注意事项

在开始设置流程之前，请查看账户要求，考虑是否需要多个 AWS 账户，并了解在 IAM Identity Center 中设置账户以获得管理访问权限的要求。

AWS 账户 要求

要注册 AWS 账户，您需要提供以下信息：

- 账户名称 - 账户名称出现在多个位置，例如在发票上以及控制台中（如“账单和成本管理”控制面板和 AWS Organizations 控制台）。

  我们建议您使用账户命名标准，以便轻松识别账户名称并将其与您可能拥有的其他账户区分开来。如果是公司账户，请考虑使用组织-目的-环境之类的命名标准（例如，AnyCompany-audit-prod）。如果是个人账户，可以考虑使用名字-姓氏-目的之类的命名标准（例如，paulo-santos-testaccount）。
- 电子邮件地址 – 此电子邮件地址用作账户根用户的登录名，也是账户恢复（例如忘记密码）所必需的信息。您必须能够接收发送到此电子邮件地址的消息。在执行某些任务之前，必须验证您有权访问该电子邮件账户。

  > **Important**
  >
  > 如果此账户适用于企业，我们建议您使用公司通讯组列表（例如 `it.admins@example.com`）。避免使用个人的公司电子邮件地址（例如 `paulo.santos@example.com`）。这有助于确保如果员工更换岗位或离开公司，公司可以访问 AWS 账户。该电子邮件地址可用于重置账户的根用户凭证。请务必保护此通讯组列表或地址的访问权限。
- 电话号码 - 需要确认账户所有权时，可以使用此号码。您必须能够通过此电话号码接听电话。

  > **Important**
  >
  > 如果此账户用于企业，我们建议使用公司电话号码，而不是个人电话号码。这有助于确保如果员工更换岗位或离开公司，公司可以访问 AWS 账户。
- 多重身份验证设备 - 为了保护您的 AWS 资源，请在根用户账户上启用多重身份验证（MFA）。除了常规登录凭证外，激活 MFA 时还需要进行二次身份验证，从而提供额外的安全层。有关 MFA 的更多信息，请参阅 IAM 用户指南中的什么是 MFA？。

- AWS Support 计划 – 在账户创建过程中，系统会要求您选择一个可用的计划。有关可用计划的描述，请参阅比较 AWS Support 计划。

IAM Identity Center 考虑事项

以下主题提供有关针对特定环境设置 IAM Identity Center 的指导。在继续 第 2 部分：创建 IAM Identity Center 中的管理用户 之前，请先了解适用于您环境的指导。

主题

- Active Directory 或外部 IdP
- AWS Organizations
- IAM 角色
- 下一代防火墙和安全 Web 网关

Active Directory 或外部 IdP

如果您已经在管理 Active Directory 或外部 IdP 中的用户和群组，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。

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 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。
- 使用驻留在您管理账户中的 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。一次只能连接一个 AD Connector 或一个 AWS Managed Microsoft AD。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：

  - AWS IAM Identity Center 用户指南中的将 AWS Managed Microsoft AD 中的目录连接到 IAM Identity Center。
  - AWS IAM Identity Center 用户指南中的将 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 身份源，则可以使用现有 AD Connector 或 AWS Managed Microsoft AD 目录，在驻留于委托管理员账户内的 AWS 目录中设置此目录。

  如果您决定将 IAM Identity Center 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。

AWS Organizations

您的 AWS 账户 必须由 AWS Organizations 管理。如果您还没有设置组织，则不必执行此操作。启用 IAM Identity Center 后，您将选择是否让 AWS 自动创建组织。

如果您已经设置 AWS Organizations，请确保所有功能都已启用。有关更多信息，请参阅 AWS Organizations 用户指南中的启用组织中的所有功能。

要启用 IAM Identity Center，您必须使用 AWS Organizations 管理账户的凭证登录 AWS Management Console。使用来自 AWS Organizations 成员账户的凭证登录时，您无法启用 IAM Identity Center。有关更多信息，请参阅 AWS Organizations 用户指南中的创建并管理 AWS 组织。

IAM 角色

如果您已经在 AWS 账户 中配置 IAM 角色，我们建议您检查自己的账户是否已接近 IAM 角色的限额。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。

下一代防火墙和安全 Web 网关

如果您使用 NGFW 或 SWG 等网络内容筛选解决方案来筛选对特定 AWS 域或 URL 端点的访问权限，则必须将以下域或 URL 端点添加到您的 Web 内容筛选解决方案允许列表中。

特定的 DNS 域

- *.awsapps.com (http://awsapps.com/)
- *.signin.aws

特定的 URL 端点

- https://*[yourdirectory]*.awsapps.com/start
- https://*[yourdirectory]*.awsapps.com/login
- https://*[yourregion]*.signin.aws/platform/login

使用多个AWS 账户

AWS 账户 充当基本 AWS 中的安全边界。它们充当资源容器，提供有用的隔离级别。隔离资源和用户的能力是建立安全、治理良好的环境的关键要求。

将资源分成不同的 AWS 账户 有助于您在云环境中支持以下原则：

- 安全控制 – 不同的应用程序可能具有不同的安全配置文件，这些配置文件需要不同的控制策略和机制。例如，可以更轻松地与审计员交谈，并能够指向单个 AWS 账户，其中托管遵从支付卡行业（PCI）安全标准的所有工作负载元素。
- 隔离 — AWS 账户 是安全保护的单位。应在不影响其他账户的情况下，遏制 AWS 账户 中的潜在风险和安全威胁。由于采用不同的团队或不同的安全配置文件，可能会带来不同的安全需求。
- 许多团队 – 不同的团队有不同的职责和资源需求。可以通过将团队移至单独的 AWS 账户 来防止他们互相干扰。
- 数据隔离 – 除了隔离团队之外，将数据存储隔离到一个账户中也很重要。这有助于限制可以访问和管理该数据存储的人数。这有助于遏制高度私有数据的披露，因此有助于遵守欧盟的《通用数据保护条例》（GDPR）。
- 业务流程 – 不同的业务单位或产品可能有完全不同的目的和流程。借助多个 AWS 账户，您可以支持业务单位的特定需求。
- 账单 – 账户是在账单级别分开项目的唯一真正方式。多个账户有助于在账单级别上分开业务单位、职能团队或个人用户的项目。您仍然可以将所有账单合并为单个付款人（使用 AWS Organizations 和整合账单），同时按 AWS 账户 分开行项目。
- 配额分配 — 分别为每个 AWS 账户 强制执行 AWS 服务配额。将工作负载分成不同的 AWS 账户 可以防止它们相互占用配额。

本指南中描述的所有建议和程序均符合 AWS Well-Architected Framework。该框架旨在帮助您设计灵活、有弹性且可扩展的云基础设施。即使您从小规模起步，我们也建议您按照框架中的指导推进。这样做可以帮助您安全地扩展环境，而不会随着企业成长而影响您的持续运营。

在开始添加多个账户之前，您需要制定管理这些账户的计划。为此，我们建议您使用 AWS Organizations（一项免费 AWS 服务）来管理组织中的所有 AWS 账户。

AWS 还提供 AWS Control Tower，该工具为 Organizations 增加多层 AWS 托管自动化，并自动将其与其他 AWS 服务（例如 AWS CloudTrail、AWS Config、Amazon CloudWatch、AWS Service Catalog 等）集成。这些服务可能会产生额外费用。有关更多信息，请参阅 AWS Control Tower 定价。

第 1 部分：设置新的 AWS 账户

这些说明将帮助您创建 AWS 账户 并保护根用户凭证。请先完成所有步骤，然后再继续 第 2 部分：创建 IAM Identity Center 中的管理用户。

主题

步骤 1：注册 AWS 账户

1. 打开 https://portal.aws.amazon.com/billing/signup。
2. 选择创建 AWS 账户。

   > **Note**
   >
   > 如果您最近登录 AWS，请选择登录控制台。如果创建新 AWS 账户 选项不可见，请先选择登录其他账户，然后选择创建新 AWS 账户。

3. 输入您的账户信息，然后选择继续。

   请务必正确输入账户信息，尤其是电子邮件地址。如果您输入的电子邮件地址不正确，则无法访问您的账户。

4. 选择个人或专业。

   这些选项之间的区别仅在于我们要求您提供的信息。两种账户类型具有相同的特性和功能。

5. 根据 AWS 账户 要求 中提供的指导输入您的公司或个人信息。
6. 阅读并接受 AWS 客户协议。
7. 选择创建账户并继续。

   此时，您将收到一个电子邮件消息，确认您的 AWS 账户 已准备就绪。可以使用在注册时提供的电子邮件地址和密码登录新账户。但是，在完成账户激活操作之前，您无法使用任何 AWS 服务。

8. 在付款信息页面上，输入有关您付款方式的信息。如果您想使用与创建账户时不同的地址，请选择使用新地址，然后输入要用于计费的地址。

9. 选择验证并添加。

> **Note**
>
> 如果您的联系地址位于印度，则您账户的用户协议是与 AISPL 签订的，这是一家位于印度本地的 AWS 卖家。您必须在验证过程中提供 CVV。您可能还需要输入一次性密码，具体取决于您的银行。在验证过程中，AISPL 将对您提供的付款方式收取 2 INR。AISPL 在完成验证后退回 2 INR。

10. 要验证您的电话号码，请从列表中选择您的国家或区域代码，然后输入在接下来的几分钟内可以拨打的电话号码。输入 CAPTCHA 代码并提交。
11. AWS 自动验证系统会致电给您并提供 PIN。使用手机输入 PIN，然后选择继续。
12. 选择 AWS Support 计划。

    有关可用计划的描述，请参阅比较 AWS Support 计划。

    此时会显示确认页面，表明您的账户正在激活。激活通常仅需要几分钟，但有时最长需要 24 小时。在激活期间，您可以登录新的 AWS 账户。在激活完成之前，您可能会看到完成注册按钮。您可以忽略它。

    AWS 在账户激活完成时会发送一条确认电子邮件消息。检查您的电子邮件和垃圾邮件文件夹中是否有确认电子邮件消息。收到此消息后，您就可以完全访问所有 AWS 服务。

步骤 2：以根用户身份登录

当你第一次创建 AWS 账户，您从一个登录身份开始，该身份可以完全访问所有人 AWS 服务 以及账户中的资源。这个身份叫做 AWS 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问。

> **Important**
>
> 强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关需要您以 root 用户身份登录的任务的完整列表，请参阅《用户指南》中的 “需要根用户凭据的IAM任务”。

以根用户身份登录

1. 打开 AWS Management Console 在 https://console.aws.amazon.com/。

   > **Note**
   >
   > 如果您之前在此浏览器中以 root 用户身份登录，则您的浏览器可能会记住该浏览器的电子邮件地址 AWS 账户.
   > 如果您之前以IAM用户身份使用此浏览器登录，则您的浏览器可能会改为显示IAM用户登录页面。要返回主登录页面，请选择 Sign in using root user email（使用根用户电子邮件登录）。

2. 如果您之前没有使用此浏览器登录过，则会显示主登录页面。如果您是账户所有者，请选择根用户。输入你的 AWS 账户 与您的帐户关联的电子邮件地址，然后选择 “下一步”。
3. 系统可能会提示您完成安全检查。完成此检查以前进至下一步。如果您无法完成安全检查，请尝试收听音频或刷新安全检查以获得一组新字符。
4. 输入密码并选择登录。

第 3 步：MFA为您激活 AWS 账户 根用户

为了增强根用户凭证的安全性，我们建议您按照安全最佳实践为自己激活多因素身份验证 (MFA) AWS 账户。 由于 root 用户可以在您的账户中执行敏感操作，因此添加这一额外的身份验证层可以帮助您更好地保护您的账户。有多种类型MFA可供选择。

有关为 root 用户激活MFA的说明，请参阅中的为用户启用MFA设备 AWS（在 IAM 用户指南中）。

第 2 部分：创建 IAM Identity Center 中的管理用户

完成 第 1 部分：设置新的 AWS 账户 之后，以下步骤将帮助您为管理用户设置 AWS 账户 访问权限，该用户将用于执行日常任务。

> **Note**
>
> 本主题提供在 IAM Identity Center 中成功设置 AWS 账户 的管理员访问权限和创建管理用户所需的最少步骤。有关更多信息，请参阅 AWS IAM Identity Center 用户指南中的入门。

主题

步骤 1：启用 IAM Identity Center

> **Note**
>
> 如果您未激活根用户的多重身份验证（MFA），请在继续操作之前完成 第 3 步：MFA为您激活 AWS 账户 根用户。

要启用 IAM Identity Center

1. 选择 Root user（根用户）并输入您的 AWS 账户 电子邮件地址，以账户拥有者身份登录 AWS Management Console。在下一页上，输入您的密码。
2. 打开 IAM Identity Center 控制台。
3. 在启用 IAM Identity Center下，选择启用。
4. IAM Identity Center 需要 AWS Organizations。如果您未建立组织，则必须选择是否让 AWS 自动创建一个组织。选择创建 AWS 组织完成此过程。

AWS Organizations 会自动向与管理账户关联的地址发送验证电子邮件。在您接收到验证电子邮件之前可能会有一段延迟。在 24 小时内验证您的电子邮件地址。

> **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AWS IAM Identity Center 用户指南中的委托管理。

步骤 2：选择身份源

您在 IAM Identity Center 中的身份源定义了用户和组的管理位置。您可以选择以下一个选项作为身份源：

- IAM Identity Center 目录 – 当您首次启用 IAM Identity Center 后，IAM Identity Center 会自动配置 IAM Identity Center 目录作为您的默认身份源。在此位置中，您创建用户和组，并向其分配对您 AWS 账户和应用程序的访问级别。
- Active Directory – 如果您想继续管理 AWS Managed Microsoft AD 目录（使用 AWS Directory Service）或 Active Directory（AD）中的自托管式目录中的用户，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 Azure Active Directory）中的用户，请选择此选项。

启用 IAM Identity Center 后，您必须选择自己的身份源。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。选择身份源后，您将创建或指定用户，并为其分配 AWS 账户的管理权限。

> **Important**
>
> 如果您已经在管理 Active Directory 或外部身分提供者（IdP）中的用户和群组，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。

主题

连接 Active Directory 或其他 IdP 并指定用户

如果您已经在使用 Active Directory 或外部身份提供商（IdP），则以下主题可帮助您将目录连接到 IAM Identity Center。

您可以将 AWS Managed Microsoft AD 目录、Active Directory 中的自托管式目录或外部 IdP 与 IAM Identity Center 连接起来。如果您计划连接 Active Directory 中的 AWS Managed Microsoft AD 目录或自托管式目录，请确保您的 Active Directory 配置满足 Active Directory 或外部 IdP 中的先决条件。

> **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。如果您计划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 IdP 不支持使用 IAM Identity Center 中的 MFA。有关更多信息，请参阅AWS IAM Identity Center 用户指南中的启用 MFA。

AWS Managed Microsoft AD

1. 查看连接到 Microsoft Active Directory 中的指导。
2. 按照将 AWS Managed Microsoft AD 中的目录连接到 IAM Identity Center 的步骤执行操作。
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. 查看连接到 Microsoft Active Directory 中的指导。
2. 按照将 Active Directory 中的自托管式目录连接到 IAM Identity Center 中的步骤进行操作。
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. 查看连接到外部身份提供商中的指导。
2. 按照如何连接到外部身份提供商中的步骤进行操作。
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置（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。

下一步： 步骤 3：创建管理权限集

使用默认目录并在 IAM Identity Center 中创建用户

当您首次启用 IAM Identity Center 后，IAM Identity Center 会自动配置 IAM Identity Center 目录作为您的默认身份源。要在 IAM Identity Center 中创建用户，请完成以下步骤。

1. 选择根用户并输入您的 AWS 账户电子邮件地址，以账户拥有者身份登录 AWS Management Console。在下一页上，输入您的密码。
2. 打开 IAM Identity Center 控制台。
3. 按照添加用户中的步骤创建用户。

   指定用户详细信息时，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），也可以生成一次性密码。如果您发送电子邮件，请务必指定可以访问的电子邮件地址。
4. 添加用户之后，返回到此过程。如果您保留发送包含密码设置说明的电子邮件的默认选项，请执行以下操作：

   a. 您将收到一封主题为邀请您加入 AWS 单点登录的电子邮件。打开此电子邮件并选择接受邀请。

   b. 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。

   > **Note**
   >
   > 请务必保存您的密码。您以后将需要此密码步骤 5：使用您的管理凭证登录 AWS 访问门户。

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。

下一步： 步骤 3：创建管理权限集

步骤 3：创建管理权限集

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。执行以下步骤来创建授予管理权限的权限集。

1. 选择 Root user（根用户）并输入您的 AWS 账户 电子邮件地址，以账户拥有者身份登录 AWS Management Console。在下一页上，输入您的密码。

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 Create permission set (创建权限集合)。
5. 对于步骤 1：选择权限集类型，在选择权限集类型页面上，保留默认设置并选择下一步。默认设置允许使用 AdministratorAccess 预定义权限集授予对 AWS 服务和资源的完全访问权限。

   > **Note**
   >
   > 预定义的 AdministratorAccess 权限集使用 AdministratorAccess AWS 托管策略。

6. 对于步骤 2：指定权限集详细信息，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。
7. 对于步骤 3：查看并创建，在查看并创建页面上，执行以下操作：

   1. 查看权限集类型并确认其为 AdministratorAccess。
   2. 查看 AWS 托管策略并确认其为 AdministratorAccess。
   3. 选择 Create（创建）。

步骤 4：为管理员用户设置 AWS 账户 访问权限

要为 IAM Identity Center 中的管理用户设置 AWS 账户 访问权限，您必须为该用户分配给 AdministratorAccess 权限集。

1. 选择根用户并输入您的 AWS 账户电子邮件地址，以账户拥有者身份登录 AWS Management Console。在下一页上，输入您的密码。
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，将显示您组织的树状视图列表。选中要向其分配管理访问权限的 AWS 账户旁边的复选框。如果您的组织中有多个账户，请选中该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：选择用户和群组，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-account-name***" 页面的权限集下，选择 AdministratorAccess 权限集。
8. 选择 Next（下一步）。
9. 对于步骤 3：查看并提交，在查看分配并将其提交至 "***AWS-account-name***" 页面上，执行以下操作：

   1. 查看选定的用户和权限集。
   2. 确认已将正确的用户分配给 AdministratorAccess 权限集后，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，请按照启用 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。
    - 您正在使用 Active Directory 中的 AWS Managed Microsoft AD 目录或自托管式目录作为身份源，但没有将 RADIUS MFA 与 AWS Directory Service 搭配使用。

    > **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 IdP 不支持使用 IAM Identity Center 中的 MFA。

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。该角色由 IAM Identity Center 控制，在相关 AWS 账户 中创建，并将在权限集中指定的策略附加到该角色。

步骤 5：使用您的管理凭证登录 AWS 访问门户

完成以下步骤，确认您可以使用管理用户的凭证登录 AWS 访问门户，并且可以访问 AWS 账户。

1. 选择 Root user（根用户）并输入您的 AWS 账户 电子邮件地址，以账户拥有者身份登录 AWS Management Console。在下一页上，输入您的密码。
2. 打开 AWS IAM Identity Center 控制台，网址为 https://console.aws.amazon.com/singlesignon/。

3. 在导航窗格中，选择 Dashboard (控制面板)。
4. 在控制面板页面的设置摘要下，复制 AWS 访问门户 URL。
5. 打开单独的浏览器，粘贴您复制的 AWS 访问门户 URL，然后按 Enter。
6. 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，请使用您分配给 IAM Identity Center 中 AdministratorAccess 权限集的 Active Directory 或 IdP 用户的凭证登录。
   - 如果您使用默认的 IAM 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。
7. 登录后，门户中会出现一个 AWS 账户 图标。
8. 选择 AWS 账户 图标后，将显示与该账户关联的账户名、账户 ID 和电子邮件地址。
9. 选择账户名称以显示 AdministratorAccess 权限集，然后选择 AdministratorAccess 右侧的管理控制台链接。

   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。由于您已将该用户分配给 `AdministratorAccess` 权限集，因此该角色将在 AWS 访问门户中显示为：`AdministratorAccess/`*`username`*
10. 如果您被重定向到 AWS 管理控制台，则表示您成功完成对 AWS 账户 的管理访问权限的设置。继续执行步骤 10。
11. 切换到您用来登录 AWS Management Console 和设置 IAM Identity Center 的浏览器，然后从 AWS 账户 根用户注销。

> **Important**
>
> 强烈建议您在登录 AWS 访问门户时遵守以下使用管理用户凭证的最佳实践，不要将根用户凭证用于日常任务。

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。

排查 AWS 账户 创建问题

使用此处的信息有助于排查与创建 AWS 账户 相关的问题。

问题

我没有接到 AWS 验证新账户的电话

创建 AWS 账户 时，必须提供一个可以接收 SMS 文本消息或语音呼叫的电话号码。您可以指定使用哪种方法来验证此电话号码。

如果您没有收到短信或来电，请验证以下内容：

- 在注册过程中，您输入了正确的电话号码并选择正确的国家/地区代码。
- 如果您使用的是手机，请确保手机信号未被屏蔽，可以接收 SMS 文本消息或来电。
- 您为付款方式输入的信息正确无误。

如果您没有收到完成身份验证流程的 SMS 文本消息或电话，AWS Support 可以帮助您手动激活 AWS 账户。使用以下步骤：

1. 请确保可通过您为 AWS 账户 提供的电话号码与您取得联系。
2. 打开 AWS Support 控制台，然后选择创建案例。
   a. 选择账户和账单支持。
   b. 在类型中，选择账户。
   c. 在类别中，选择激活。
   d. 在案例描述部分，提供可以联系您的日期和时间。
   e. 在联系人选项部分，选择聊天以获取联系方式。
   f. 选择提交。

> **Note**
>
> 即使您的 AWS 账户 未激活，您也可以使用 AWS Support 创建案例。

当我尝试通过电话验证自己的 AWS 账户 时，我收到关于“最大失败尝试次数”的错误

AWS Support 可以帮助您手动激活账户。按照以下步骤进行操作：

1. 使用您在创建账户时指定的电子邮件地址和密码登录您的 AWS 账户。
2. 打开 AWS Support 控制台，然后选择创建案例。
3. 选择账户和账单支持。
4. 在类型中，选择账户。
5. 在类别中，选择激活。
6. 在案例描述部分，提供可以联系您的日期和时间。
7. 在联系人选项部分，选择聊天以获取联系方式。
8. 选择提交。

AWS Support 将与您联系并尝试手动激活您的 AWS 账户。

已经过去 24 小时，但我的账户还没有激活

账户激活有时可能会延迟。如果该过程耗时超过 24 小时，请检查以下内容：

- 完成账户激活过程。

  如果您在添加所有必要信息之前关闭注册过程窗口，请打开注册页面。选择登录现有 AWS 账户，然后使用您为账户选择的电子邮件地址和密码登录。
- 查看与您的付款方式关联的信息。

  在 AWS Billing and Cost Management 控制台中，检查付款方式是否有错误。
- 联系您的金融机构。

有时，金融机构会拒绝来自 AWS 的授权请求。联系与您的付款方式关联的机构，并要求他们批准来自 AWS 的授权请求。 一旦您的金融机构批准授权请求，AWS 就会立即将其取消，因此您无需为授权请求付费。授权请求可能仍会以少量费用（通常为 1 USD）的形式出现在金融机构的对账单上。

- 请检查您的电子邮件和垃圾邮件文件夹，以获取请求的更多信息。
- 尝试使用其他浏览器。
- 联系 AWS Support。

联系 AWS Support 寻求帮助。提及您已经尝试过的所有问题排查步骤。

> **Note**
>
> 请勿在与 AWS 的任何通信中提供敏感信息，例如信用卡号。

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。