Amazon WorkDocs

管理指南

Amazon WorkDocs: 管理指南

Table of Contents

什么是 Amazon WorkDocs？

Amazon WorkDocs 是一项安全的完全托管的企业存储和共享服务，具有强大的管理控制和反馈功能，可提高用户生产率。文件安全地存储在云中。您的用户的文件仅对用户和用户指定的参与者和查看者可见。贵公司的其他成员无法访问其他用户的文件，除非他们被专门授予访问权限。

用户可以与其公司的其他成员共享您的文件用来协作或审查。Amazon WorkDocs 客户端应用程序可以用于查看许多不同类型的文件，具体取决于文件的 Internet 媒体类型。Amazon WorkDocs 支持所有常用文档和图像格式，并支持不断添加的其他媒体类型。

有关更多信息，请参阅 。Amazon WorkDocs.

Amazon WorkDocs

管理员使用Amazon WorkDocs 控制台以创建和停用 Amazon WorkDocs 站点。使用管理员控制面板，他们可以管理用户、存储和安全设置。有关更多信息，请参阅 管理站点设置 (p. 28) 和 邀请和管理 Amazon WorkDocs 用户 (p. 33)。

非管理员用户使用客户端应用程序访问其文件。他们从不使用 Amazon WorkDocs 控制台或管理控制面板。Amazon WorkDocs 提供多个不同的客户端应用程序和实用工具：

- 一个用于文档管理和审核的 Web 应用程序。
- 用于查看文档的移动设备本机应用程序。
- Amazon WorkDocs 驱动器，可将您的 macOS 或 Windows 桌面上的文件夹与您的 Amazon WorkDocs 文件同步。

有关用户如何下载 Amazon WorkDocs 客户端、编辑其文件以及支持的文件类型的更多信息，请参阅以下内容：

- Amazon WorkDocs 入门
- 编辑文件
- 受支持的文件类型

Pricing

Amazon WorkDocs 没有预付费用或长期合约。您只需为活动用户账户以及您使用的存储量付费。 有关更多信息，请参阅 。定价.

如何开始

要开始使用 Amazon WorkDocs，请尝试以下教程之一：

- 开始使用快速启动 (p. 17)
- 简单 AD 入门 标准设置 (p. 19)
- 开始使用现有目录 (p. 21)
- AD Connector 入门 (p. 22)

- 开始使用 AWS Managed Microsoft AD (p. 24)

如果您的 WorkSpaces 管理员账户具有为 Amazon WorkDocs 启用的目录，您可以登录到 Amazon WorkDocs 站点，并从管理控制面板. 有关更多信息，请参阅第 3 步：完成管理员控制面板设置 (p. 21)。

有关使用 WorkSpaces 开始使用 Amazon WorkDocs 的更多信息，请参阅开始使用 WorkSpaces 快速设置中的Amazon WorkSpaces 管理指南. 有关在 WorkSpaces 或 Amazon EC2 实例中使用 Amazon WorkDocs 客户端的信息，请参阅以下内容：Amazon S3 的终端节点中的Amazon VPC User Guide.

Amazon WorkDocs 的先决条件

要设置新的 Amazon WorkDocs 站点或管理现有站点，您必须完成以下任务。

任务

- 注册AWS (p. 3)
- 创建 IAM 用户和组（推荐）(p. 3)

注册AWS

您可以通过 AWS 账户访问所有服务，但您只需为所使用的资源付费。

如果您还没有 AWS 账户，请完成以下步骤创建一个。

注册 AWS 账户

1. 打开 https://portal.aws.amazon.com/billing/signup。
2. 按照屏幕上的说明进行操作。

   在注册时，您将接到一通电话，要求您使用电话键盘输入一个验证码。

您的AWS根帐户凭据将您标识到AWS并授予您无限制地使用您的AWS资源，例如您的 Amazon WorkDocs 站点。

创建 IAM 用户和组（推荐）

要允许其他用户设置新的 Amazon WorkDocs 站点或管理现有站点，而无需共享您的安全凭证，请使用AWS Identity and Access Management(IAM). 我们建议所有人以 IAM 用户的身份工作，即使是账户所有者。您应该为自己创建一个 IAM 用户，向该 IAM 用户提供管理权限，然后将其用于您的所有工作。

有关更多信息，请参阅适用于 Amazon WorkDocs 的身份和访问管理 (p. 4)。

Amazon WorkDocs 中的安全性

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

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

- 云的安全性 – AWS负责保护在AWS云中运行AWS服务的基础设施。AWS还向您提供可安全使用的服务。作为 AWS 合规性计划的一部分，第三方审核人员将定期测试和验证安全性的有效性。要了解适用于 Amazon WorkDocs 的合规性计划，请参阅AWS合规性计划范围内的服务.
- 云中的安全性 - 您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，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。

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

主题

适用于 Amazon WorkDocs 的身份和访问管理

AWS Identity and Access Management (IAM) 是一种 AWS 服务，可以帮助管理员安全地控制对 AWS 资源的访问。IAM 管理员可以控制哪些人身份验证器(已登录) 和Autity (具有权限) 来使用 Amazon WorkDocs 资源。IAM 是一个可以免费使用的AWS服务。

主题

Audience

如何使用AWS Identity and Access Management(IAM) 因您可以在 Amazon WorkDocs 中执行的操作而异。

服务用户— 如果您使用 Amazon WorkDocs 服务来完成作业，则您的管理员会为您提供所需的凭证和权限。随着您使用更多 Amazon WorkDocs 功能来完成工作，您可能需要额外权限。了解如何管理访问权限可帮助您向管理员请求适合的权限。如果您无法访问 Amazon WorkDocs 中的功能，请参阅Amazon WorkDocs 身份和访问疑难解答 (p. 12).

服务管理员— 如果您在公司负责管理 Amazon WorkDocs 资源，则您可能具有 Amazon WorkDocs 的完全访问权限。您有责任确定您的员工应访问哪些 Amazon WorkDocs 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要了解有关您的公司如何将 IAM 与 Amazon WorkDocs 搭配使用的更多信息，请参阅Amazon WorkDocs 如何与 IAM 协同工作 (p. 7).

IAM 管理员— 如果您是 IAM 管理员，您可能希望了解有关您可以如何编写策略以管理 Amazon WorkDocs 的访问权限的详细信息。要查看您可在 IAM 中使用的 Amazon WorkDocs 基于身份的策略示例示例示例，请参阅Amazon WorkDocs 基于身份的策略示例 (p. 9).

使用身份进行身份验证

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

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

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

无论使用何种身份验证方法，您可能还需要提供其他安全信息。例如，AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《IAM 用户指南》中的在 AWS 中使用多重身份验证 (MFA)。

AWS 账户根用户

当您首次创建AWS 账户时，最初使用的是一个对账户中所有AWS服务和资源有完全访问权限的单点登录身份。此身份称为AWS 账户根用户，使用您创建账户时所用的电子邮件地址和密码登录，即可获得该身份。强烈建议您不使用根用户执行日常任务，即使是管理任务。相反，请遵循仅使用根用户创建您的第一个 IAM 用户的最佳实践。然后请妥善保存根用户凭证，仅用它们执行少数账户和服务管理任务。

IAM 用户和组

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

IAM 组 是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅 IAM 用户指南中的何时创建 IAM 用户（而不是角色）。

IAM 角色

IAM 角色是AWS 账户中具有特定权限的身份。它类似于 IAM 用户，但与特定人员不关联。您可以通过切换角色，在 AWS Management Console 中暂时代入 IAM 角色。您可以调用 AWS CLI 或 AWS API 操作或使用自定义 URL 以代入角色。有关使用角色的方法的更多信息，请参阅 IAM 用户指南 中的使用 IAM 角色。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 临时 IAM 用户权限 – IAM 用户可以代入 IAM 角色，以暂时获得不同的权限以执行特定的任务。
- 联合身份用户访问 – 您可以不创建 IAM 用户，而是使用来自 AWS Directory Service、您的企业用户目录或 Web 身份提供商的现有身份。这些用户被称为联合用户。在通过身份提供商请求访问权限时，AWS将为联合身份用户分配角色。有关联合身份用户的更多信息，请参阅 IAM 用户指南 中的联合身份用户和角色。
- 跨账户访问 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信委托人）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅 IAM 用户指南 中的 IAM 角色与基于资源的策略有何不同。
- 跨服务访问 – 某些 AWS 服务使用其他 AWS 服务中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Amazon S3 中存储对象。服务可能会使用发出调用的委托人的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 委托人权限 – 当您使用 IAM 用户或角色在 AWS 中执行操作时，您将被视为委托人。策略向委托人授予权限。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中触发另一个操作。在这种情况下，您必须具有执行这两个操作的权限。要查看某个操作是否需要策略中的其他相关操作，请参阅服务授权参考。
  - 服务角色 – 服务角色是服务代表您在您的账户中执行操作而担任的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅 IAM 用户指南中的创建向AWS服务委派权限的角色。
  - 服务相关角色 – 服务相关角色是与 AWS 服务关联的一种服务角色。服务可以代入代表您执行操作的角色。服务相关角色显示在您的 IAM 账户中，并归该服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 Amazon EC2 上运行的应用程序 – 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时凭证。这优先于在 EC2 实例中存储访问密钥。要将AWS角色分配给 EC2 实例并使其对该实例的所有应用程序可用，您可以创建一个附加到实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅 IAM 用户指南 中的使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。

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

使用策略管理访问

您将创建策略并将其附加到 IAM 身份或AWS资源，以便控制AWS中的访问。策略是AWS中的对象；在与标识或资源相关联时，策略定义它们的权限。您可以通过 root 用户或 IAM 用户身份登录，也可以代入 IAM 角色。随后，当您提出请求时，AWS会评估相关的基于身份或基于资源的策略。策略中的权限确定是允许还是拒绝请求。大多数策略在 AWS 中存储为 JSON 文档。有关 JSON 策略文档的结构和内容的更多信息，请参阅JSON 策略概述中的IAM 用户指南.

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。也就是说，哪个委托人 可以对什么资源 执行操作，以及在什么 条件 下执行。

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

IAM 策略定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。具有该策略的用户可以从 AWS Management Console、AWS CLI 或 AWS API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅创建 IAM 策略中的IAM 用户指南.

基于身份的策略可以进一步归类为内联策略或托管策略。内联策略直接嵌入单个用户、组或角色中。托管策略是可以附加到中的多个用户、组和角色的独立策略。AWS 账户. 托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管策略或内联策略之间选择，请参阅在托管策略与内联策略之间进行选择中的IAM 用户指南.

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略 和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定委托人可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定委托人。委托人可以包括账户、用户、角色、联合身份用户或 AWS 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用来自 IAM 的 AWS 托管策略。

访问控制列表

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

Amazon S3、AWS WAF 和 Amazon VPC 是支持 ACL 的服务示例。要了解有关 ACL 的详细信息，请参阅访问控制列表 (ACL) 概述中的Amazon Simple Storage Service 开发人员指南.

其他策略类型

AWS 支持额外的、不太常用的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界 – 权限边界是一个高级功能，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体的基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅 IAM 用户指南 中的 IAM 实体的权限边界。
- 服务控制策略 (SCP)— SCP 是指定组织或组织单位 (OU) 的最大权限的 JSON 策略AWS Organizations.AWS Organizations是用于分组和集中管理多个服务AWS 账户您的企业拥有。如果在组织内启用了所有功能，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中实体的权限，包括每个AWS 账户根用户。有关 Organization 和 SCP 的更多信息，请参阅《AWS Organizations 用户指南》中的 SCP 的工作原理。
- 会话策略 – 会话策略是当您以编程方式为角色或联合身份用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 。会话策略中的IAM 用户指南.

> **Note**
>
> Amazon WorkDocs 不支持针对松弛 Organizations 的服务控制策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解AWS如何确定在涉及多种策略类型时是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

Amazon WorkDocs 如何与 IAM 协同工作

在使用 IAM 管理对 Amazon WorkDocs 的访问权限之前，您需要了解哪些 IAM 功能可用于 Amazon WorkDocs。要获取 Amazon WorkDocs 和其他AWS服务与 IAM 协同工作，请参阅AWS使用 IAM 的服务中的IAM 用户指南.

主题

Amazon WorkDocs 基于身份的策略

使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作。Amazon WorkDocs 支持特定操作。要了解您在 JSON 策略中使用的元素，请参阅IAM JSON 策略元素参考中的IAM 用户指南.

Actions

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。也就是说，哪个委托人 可以对什么资源 执行操作，以及在什么 条件 下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行相关操作的权限。

Amazon WorkDocs 中的策略操作在操作前面使用以下前缀：：`workdocs:`. 例如，要授予某人运行 Amazon WorkDocs 的权限`DescribeUsers`API 操作时，您可以包含`workdocs:DescribeUsers`行动在他们的政策。策略语句必须包含 `Action` 或 `NotAction` 元素。Amazon WorkDocs 定义了一组自己的操作，以描述您可以使用该服务执行的任务。

要在单个语句中指定多项操作，请使用逗号将它们隔开，如下所示：

```
"Action": [
      "workdocs:DescribeUsers",
      "workdocs:CreateUser"
```

您也可以使用通配符 (*) 指定多个操作。例如，要指定以单词 `Describe` 开头的所有操作，包括以下操作：

```
"Action": "workdocs:Describe*"
```

> **Note**
>
> 要确保向后兼容性，请将`zocalo`action. 例如：
>
> ```
> "Action": [
> "zocalo:*",
> "workdocs:*"
> ],
> ```

要查看 Amazon WorkDocs 操作的列表，请参阅Amazon WorkDocs 定义的操作中的IAM 用户指南.

Resources

Amazon WorkDocs 不支持在策略中指定资源 ARN。

条件键

Amazon WorkDocs 不提供任何特定于服务的条件键，但支持使用某些全局状况键。要查看所有AWS全局条件键，请参阅 IAM 用户指南中的 AWS全局条件上下文键。

Examples

要查看 Amazon WorkDocs 基于身份的策略的示例，请参阅Amazon WorkDocs 基于身份的策略示例 (p. 9).

Amazon WorkDocs 基于资源的策略

Amazon WorkDocs 不支持基于资源的策略。

基于 Amazon WorkDocs 标签的授权

Amazon WorkDocs 不支持标记资源或基于标签控制访问。

Amazon WorkDocs IAM 角色

IAM 角色 是AWS账户中具有特定权限的实体。

将临时凭证用于 Amazon WorkDocs

您可以使用临时凭证进行联合身份登录，担任 IAM 角色或担任跨账户角色。您可以通过调用 AWS STS API 操作（如 AssumeRole 或 GetFederationToken）获得临时安全凭证。

Amazon WorkDocs 支持使用临时凭证。

服务相关角色

服务相关角色允许 AWS 服务访问其他服务中的资源以代表您完成操作。服务相关角色显示在您的 IAM 账户中，并归该服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

Amazon WorkDocs 不支持服务相关角色。

服务角色

此功能允许服务代表您担任服务角色。此角色允许服务访问其他服务中的资源以代表您完成操作。服务角色显示在您的 IAM 账户中，并归该账户所有。这意味着，IAM 管理员可以更改该角色的权限。但是，这样做可能会中断服务的功能。

Amazon WorkDocs 不支持服务角色。

Amazon WorkDocs 基于身份的策略示例

默认情况下，IAM 用户和角色没有创建或修改 Amazon WorkDocs 资源的权限。它们还无法使用 AWS Management Console、AWS CLI 或 AWS API 执行任务。IAM 管理员必须创建 IAM 策略，以便为用户和角色授予权限以对所需的指定资源执行特定的 API 操作。然后，管理员必须将这些策略附加到需要这些权限的 IAM 用户或组。

> Note
>
> 要确保向后兼容性，请将`zocalo`操作。例如：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
```

```
            "Effect": "Deny",
            "Action": [
            "zocalo:*",
            "workdocs:*"
            ],
            "Resource": "*"
        }
    ]
}
```

要了解如何使用这些示例 JSON 策略文档创建 IAM 基于身份的策略，请参阅 IAM 用户指南 中的在 JSON 选项卡上创建策略。

主题

策略最佳实践

基于身份的策略非常强大。它们确定某个人是否可以创建、访问或删除您账户中的 Amazon WorkDocs 资源。这些操作可能会使AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下准则和建议：

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

使用 Amazon WorkDocs 控制台

要访问 Amazon WorkDocs 控制台，您必须具有一组最低的权限。这些权限必须允许您列出和查看您的 Amazon WorkDocs 资源的详细信息。AWSaccount. 如果创建比必需的最低权限更为严格的基于身份的策略，对于 IAM 用户或角色实体，控制台将无法按预期正常运行。

要确保这些实体可使用 Amazon WorkDocs 控制台，也可向其附加以下内容AWS托管策略添加到实体。有关附加策略的详细信息，请参阅向用户添加权限中的IAM 用户指南.

- AmazonWorkDocsFullAccess
- AWS 目录服务访问
- AmazonEC2FullAccess

这些策略授予 IAM 用户对 Amazon WorkDocs 资源、AWS Directory Service 操作以及 Amazon WorkDocs 正常工作所需的 Amazon EC2 操作的完全访问权限。

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

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管策略。此策略包括在控制台上完成此操作或者以编程方式使用 AWS CLI 或 AWS API 所需的权限。

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

允许用户对 Amazon WorkDocs 资源进行只读访问

以下AWS托管AmazonWorkDocsReadOnlyAccess策略向 IAM 用户授予对 Amazon WorkDocs 资源的只读访问权限。该策略向用户授予所有 Amazon WorkDocs 的访问权限`Describe`运算符。需要对两个 Amazon EC2 操作的访问权限才能获取您的 VPC 和子网的列表。需要对 AWS Directory Service `DescribeDirectories` 操作的访问权限才能获取有关您的 AWS Directory Service 目录的信息。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "workdocs:Describe*",
                "ds:DescribeDirectories",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

更多 Amazon WorkDocs 基于身份的策略示例

IAM 管理员可以创建其他策略，以允许 IAM 角色或用户访问 Amazon WorkDocs API。有关更多信息，请参阅 。管理应用程序的身份验证和访问控制中的Amazon WorkDocs 开发人员指南.

Amazon WorkDocs 身份和访问疑难解答

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

主题

我无权在 Amazon WorkDocs 中执行操作

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

我无权执行 iam:PassRole

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

有些 AWS 服务允许您将现有角色传递到该服务，而不是创建新服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为的 IAM 用户时，会发生以下示例错误：`marymajor`尝试使用控制台在 Amazon WorkDocs 中执行操作。但是，服务必须具有服务角色所授予的权限才可执行操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole
```

在这种情况下，Mary 请求她的管理员来更新其策略，以允许她执行 `iam:PassRole` 操作。

我想要查看我的访问密钥

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

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

> **Important**
>
> 请不要向第三方提供访问密钥，即便是为了帮助找到您的规范用户 ID 也不行。如果您这样做，可能会向某人提供对您的账户的永久访问权限。

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

我是管理员并希望允许其他人访问 Amazon WorkDocs

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

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

我想要允许我的AWS帐户以访问我的 Amazon WorkDocs 资源

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

要了解更多信息，请参阅以下内容：

- 要了解 Amazon WorkDocs 是否支持这些功能，请参阅Amazon WorkDocs 如何与 IAM 协同工作 (p. 7).
- 要了解如何为您拥有的AWS 账户中的资源提供访问权限，请参阅IAM 用户指南中的为您拥有的另一个 AWS 账户中的 IAM 用户提供访问权限。
- 要了解如何为第三方AWS 账户提供您的资源的访问权限，请参阅 IAM 用户指南中的为第三方拥有的AWS 账户提供访问权限。
- 要了解如何通过联合身份验证提供访问权限，请参阅 IAM 用户指南 中的为经过外部身份验证的用户（联合身份验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅 IAM 用户指南 中的 IAM 角色与基于资源的策略有何不同。

Amazon WorkDocs 中的日志记录和监控

Amazon WorkDocs 站点管理员可以查看和导出整个站点的活动源。他们还可以使用AWS CloudTrail以捕获 Amazon WorkDocs 控制台中的事件。

主题

站点范围活动源

管理员可以查看和导出整个站点的活动源。要使用此功能，您必须先安装 Amazon WorkDocs 伴侣。要安装 Amazon WorkDocs 伴侣，请参阅适用于 Amazon WorkDocs 的应用程序和集成.

查看和导出站点范围活动源

1. 在 Web 应用程序中，选择活动.
2. 选择筛选条件，然后移动站点范围活动滑块以打开过滤器。
3. 选择 Activity Type (活动类型) 筛选条件，根据需要选择 Date Modified (修改日期) 设置，然后选择 Apply (应用)。

4. 显示筛选后的活动源结果时，按文件、文件夹或用户名搜索以缩小结果的范围。您还可以根据需要添加或删除筛选条件。
5. 选择 Export (导出) 可将活动源导出为桌面上的 `.csv` 和 `.json` 文件。系统将文件导出到以下位置之一中：

   - Windows–WorkDocsDownloads文件夹中的下载folder
   - macOS – `/users/username/WorkDocsDownloads/folder`

   导出的文件会反映您应用的任何筛选器。

   Note

   非管理员用户只能查看和导出自己内容的活动源。有关更多信息，请参阅 。查看活动源中的Amazon WorkDocs 用户指南.

使用记录 Amazon WorkDocs API 调用AWS CloudTrail

Amazon WorkDocs 与AWS CloudTrail，提供用户、角色或AWS服 Amazon WorkDocs。CloudTrail 将对 Amazon WorkDocs 的所有 API 调用作为事件捕获，包括来自 Amazon WorkDocs 控制台的调用和对 Amazon WorkDocs API 的代码调用。如果创建跟踪，则可以使 CloudTrail 事件持续传送到 Amazon S3 存储桶（包括 Amazon WorkDocs 的事件）。如果您不配置跟踪，则仍可在 CloudTrail 控制台中的 Event history (事件历史记录) 中查看最新事件。使用 CloudTrail 收集的信息，您可以确定向 Amazon WorkDocs 发出了什么请求、发出请求的 IP 地址、何人发出的请求、请求的发出时间以及其他详细信息。

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

CloudTrail 中的 Amazon WorkDocs 信息

在您创建 AWS 账户时，将在该账户上启用 CloudTrail。当 Amazon WorkDocs 中发生活动时，该活动将记录在 CloudTrail 事件中，并与其他AWS中的服务事件事件历史记录. 可以在 AWS 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用 CloudTrail 事件历史记录查看事件。

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

- 创建跟踪概述
- CloudTrail 支持的服务和集成
- 为 CloudTrail 配置 Amazon SNS 通知
- 从多个区域接收 CloudTrail 日志文件和从多个账户中接收 CloudTrail 日志文件

CloudTrail 记录所有 Amazon WorkDocs 操作，并记录在Amazon WorkDocs API 参考. 例如，对`CreateFolder`、`DeactivateUser`和`UpdateDocument`部分将在 CloudTrail 日志文件中生成条目。

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

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

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

了解 Amazon WorkDocs 日志文件条目

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

Amazon WorkDocs 生成了两类不同的 CloudTrail 条目，一类来自控制层面，另一类来自数据层面。两者之间的重要区别在于，控制层面条目的用户身份是 IAM 用户。数据层面条目的用户身份是 Amazon WorkDocs 目录用户。

将在日志条目中遮掩敏感信息，例如密码、身份验证标记、文件评论和文件内容。

以下示例显示了 Amazon WorkDocs 的两条 CloudTrail 日志条目：第一条记录对应的是控制层面操作，第二条记录对应的是数据层面操作。


```
{
  Records : [
    {
      "eventVersion" : "1.01",
      "userIdentity" :
      {
        "type" : "IAMUser",
        "principalId" : "user_id",
        "arn" : "user_arn",
        "accountId" : "account_id",
        "accessKeyId" : "access_key_id",
        "userName" : "user_name"
      },
      "eventTime" : "event_time",
      "eventSource" : "workdocs.amazonaws.com",
      "eventName" : "RemoveUserFromGroup",
      "awsRegion" : "region",
      "sourceIPAddress" : "ip_address",
      "userAgent" : "user_agent",
      "requestParameters" :
      {
        "directoryId" : "directory_id",
        "userSid" : "user_sid",
        "group" : "group"
      },
      "responseElements" : null,
      "requestID" : "request_id",
      "eventID" : "event_id"
    },
    {
      "eventVersion" : "1.01",
      "userIdentity" :
      {
        "type" : "Unknown",
        "principalId" : "user_id",
        "accountId" : "account_id",
        "userName" : "user_name"
      },
      "eventTime" : "event_time",
      "eventSource" : "workdocs.amazonaws.com",
      "eventName" : "LogoutUser",
      "awsRegion" : "region",
      "sourceIPAddress" : "ip_address",
      "userAgent" : "user_agent",
      "requestParameters" :
      {
        "AuthenticationToken" : "**-redacted-**"
```

```
      },
      "responseElements" : null,
      "requestID" : "request_id",
      "eventID" : "event_id"
    }
  ]
}
```

Amazon WorkDocs 的合规性验证

作为多个中的一部分，第三方审计员将评估 Amazon WorkDocs 的安全性和合规性。AWS合规性计划. 这些合规性计划包括 SOC、PCI DSS、FedRAMP、HIPAA、ISO 9001、ISO 27001、ISO 27017 和 ISO 27018。

有关列表AWS服务的详细信息，请参阅合规性计划范围内的 AWS 服务. 有关一般信息，请参阅AWS合规性计划。

您可以使用 AWS Artifact 下载第三方审计报告。有关更多信息，请参阅 。在 AWS Artifact 件中下载报告.

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

- 安全性与合规性快速入门指南— 这些部署指南讨论了架构注意事项，并提供了在AWS.
- 《设计符合 HIPAA 安全性和合规性要求的架构》白皮书 — 此白皮书介绍了公司如何使用AWS创建符合 HIPAA 标准的应用程序。
- AWS合规性资源 – 此业务手册和指南集合可能适用于您的行业和位置。
- AWS Config – 此 AWS 服务评估您的资源配置对内部实践、行业指南和法规的遵循情况。
- AWS Security Hub — 此AWS服务提供了AWS中安全状态的全面视图，可帮助您检查是否符合安全行业标准和最佳实践。

Amazon WorkDocs 中的恢复能力

AWS 全球基础设施围绕 AWS 区域和可用区构建。AWS区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。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。

Amazon WorkDocs 中的基础设施安全性

作为一项托管式服务，Amazon WorkDocs 由AWS全局网络安全过程，请参阅Amazon Web Services：安全过程概述白皮书。

您使用AWS发布的 API 调用通过网络访问 Amazon WorkDocs。客户端必须支持传输层安全性 (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。

Amazon WorkDocs 入门

Amazon WorkDocs 使用目录来存储和管理您的用户及其文档的组织信息。反过来，您可以在置备站点时将目录附加到站点。当您执行此操作时，名为 “自动激活” 的 Amazon WorkDocs 功能会将目录中的用户作为托管用户添加到站点，这意味着他们不需要单独的凭据即可登录到您的站点，他们可以共享和协作处理文件，并具有 1 TB 的存储空间。

您不再需要手动添加和激活用户，尽管您仍然可以。您还可以随时更改用户角色和权限。有关执行此操作的更多信息，请参阅邀请和管理 Amazon WorkDocs 用户 (p. 33)，请参阅本指南下文中的。

如果您需要创建目录，您可以：

- 使用 Quick Start 或标准设置创建 Simple AD 目录。
- 创建 AD Connector 目录以连接到您的本地目录。
- 使 Amazon WorkDocs 能够与现有AWS目录。
- 让 Amazon WorkDocs 为您创建一个目录。

您也可以在 AD 目录和 AWS Managed Microsoft AD 目录之间创建信任关系。

> Note
>
> 如果您参加了合规性计划 (例如，PCI、FedRAMP 或 DoD)，则必须设置AWS Managed Microsoft AD满足合规性要求的目录。

目录

开始使用快速启动

以下部分中的步骤介绍了如何设置新的 Amazon WorkDocs 站点以及如何使用快速启动. 您只能使用快速启动选项，如果您以前从未启动过 Amazon WorkDocs 站点，则可以使用。

> Note
>
> 如果需要对目录配置进行更多的控制，例如，指定您自己的目录域名或将现有的 Virtual Private Cloud (VPC) 与目录一起使用，请使用 Standard Setup (标准设置) 选项。有关更多信息，请参阅 简单 AD 入门 标准设置 (p. 19)。

任务

开始前的准备工作

- 您必须具有AWS帐户创建或管理 Amazon WorkDocs 站点。用户不需要AWS帐户连接并使用 Amazon WorkDocs。有关更多信息，请参阅Amazon WorkDocs 的先决条件 (p. 3)。
- 当您启动新的 Amazon WorkDocs 站点时，必须为管理员指定配置文件信息，包括名字和姓氏以及电子邮件地址。
- 如果您参加了合规性计划 (例如，PCI、FedRAMP 或 DoD)，则您必须设置 Microsoft AD 目录以满足合规性要求。请改为遵循开始使用 AWS Managed Microsoft AD (p. 24)上的说明操作。

第 1 步：启动 Amazon WorkDocs 网站

使用快速启动，您可以在几分钟内启动您的第一个 Amazon WorkDocs 站点。

启动 Amazon WorkDocs 站点

1. 从打开 Amazon WorkDocs 控制台https://console.aws.amazon.com/zocalo/.

   如果您从未在选定区域中创建目录或连接到目录，则会看到 Amazon WorkDocs 起始页。在特定区域中创建目录之后，起始页将不再可用，您将会看到 Manage Your WorkDocs Sites (管理您的 WorkDocs 站点) 页。
2. 选择Get Started Now从 Amazon WorkDocs 起始页面或选择创建新的 WorkDocs 站点来自 的管理您的 WorkDocs 站点页.
3. 在 Get Started with WorkDocs (开始使用 WorkDocs) 页面上，选择 Quick Start (快速启动) 旁边的 Launch (启动)。

第 2 步：创建访问点并设置管理员

按照以下步骤创建访问点并设置管理员。

创建访问点并设置管理员

1. 从 WorkDocs Quick Start (WorkDocs 快速启动) 页面上，为 Access Point (访问点) 输入以下值：

   区域

   验证区域。

   Site URL

   输入 Amazon WorkDocs 站点的 URL。
2. 为 Set WorkDocs Administrator (设置 WorkDocs 管理员) 输入以下值：

   电子邮件

   目录管理员的电子邮件地址，也用作用户名。注册电子邮件发送到此处。

   名

   目录管理员的名字。

   姓

   目录管理员的姓氏。

3. 选择 Complete Setup (完成设置)。

   连接目录并构建 Amazon WorkDocs 站点需要几分钟时间。当目录连接时，状态值将更改为`Active`.

快速启动将帮您完成以下任务：

- 创建 Virtual Private Cloud (VPC)。
- 在 VPC 中设置用于存储用户和 Amazon WorkDocs 站点信息的 Simple AD 目录。
- 创建目录管理员账户。系统将向管理员发送电子邮件，其中包含用于完成注册的说明。使用此账户来管理目录。
- 创建指定用户账户并将其添加到目录。
- 如果启用自动激活功能，快速启动将激活目录中的所有用户。

> Note
>
> 快速入门不会通知用户有关新站点的信息。您需要将 URL 传达给他们，并让他们知道他们不需要单独登录即可使用该网站。

第 3 步：完成管理员控制面板设置

在您收到管理员注册电子邮件后，使用您选择的客户端连接到 Amazon WorkDocs 站点，并从管理控制面板中完成设置。

完成管理员控制面板设置

1. 在管理员注册电子邮件中，使用链接登录到 Amazon WorkDocs。
2. UNER管理员中，选择打开管理控制面板.
3. 更改首选电子邮件头语言、存储、安全和恢复站的设置。有关更多信息，请参阅管理站点设置 (p. 28)。
4. 在 Manage Users (管理用户) 下，选择 Invite Users (邀请用户)。您还可以编辑用户设置。

有关更多信息，请参阅邀请和管理 Amazon WorkDocs 用户 (p. 33)。

简单 AD 入门 标准设置

本节中的步骤介绍如何设置 Amazon WorkDocs 站点，方法是使用标准设置在云中创建 Simple AD 目录。

任务

开始前的准备工作

- 您必须满足Simple AD 先决条件中的AWS Directory Service管理指南.
- 如果您参加了合规性计划 (例如，PCI、FedRAMP 或 DoD)，则必须设置AWS Managed Microsoft AD满足合规性要求的目录。有关更多信息，请参阅开始使用 AWS Managed Microsoft AD (p. 24)。

- 当您启动新的 Amazon WorkDocs 站点时，必须为管理员指定配置文件信息，包括名字和姓氏以及电子邮件地址。

第 1 步：启动 Amazon WorkDocs 网站

按照以下步骤使用启动您的 Amazon WorkDocs 站点标准设置.

启动 Amazon WorkDocs 站点

1. 从打开 Amazon WorkDocs 控制台https://console.aws.amazon.com/zocalo/.

   如果您从未在选定区域中创建目录或连接到目录，则会看到 Amazon WorkDocs 起始页。在特定区域中创建目录之后，起始页将不再可用，您将会看到 Manage Your WorkDocs Sites (管理您的 WorkDocs 站点) 页。
2. 选择Get Started Now从 Amazon WorkDocs 起始页面或选择创建新的 WorkDocs 站点来自 的管理您的 WorkDocs 站点页.
3. 在 Get Started with WorkDocs (开始使用 WorkDocs) 页面上，选择 Standard Setup (标准设置) 旁边的 Launch (启动)。

第 2 步：创建目录并设置管理员

按照以下步骤创建 Simple AD 目录并设置管理员。

创建 Simple AD 目录

1. 在 Set up a Directory (设置目录) 页面上，选择 Create Simple AD (创建 Simple AD)。
2. 对于 Access Point (访问点)，输入以下值，然后选择 Continue (继续)。

   区域

   验证区域。

   Site URL

   输入 Amazon WorkDocs 站点的 URL。
3. 为 Directory Details (目录详细信息) 输入以下值：

   Directory DNS

   目录的完全限定名称，例如 `corp.example.com`。

   NetBIOS name

   目录的 NetBIOS 名称，例如 `CORP`。
4. 为 Set WorkDocs Administrator (设置 WorkDocs 管理员) 输入以下值：

   电子邮件

   目录管理员的电子邮件地址，也用作用户名。注册电子邮件发送到此处。

   名

   目录管理员的名字。

   姓

   目录管理员的姓氏。

5. 适用于VPC 详细信息中，选择代表我设置新 VPC让 Amazon WorkDocs 为您创建并配置 VPC。要使用现有 VPC，请选择 Select an existing VPC to use with WorkDocs (选择要与 WorkDocs 结合使用的现有 VPC)，然后输入以下值。

   VPC

   在其中创建目录的 VPC。

   Subnets (子网)

   在其中创建目录的 VPC 中的子网。两个子网必须位于不同的可用区。如果选择无首选项，WorkDocs 会随机选择两个不同的子网。
6. 查看目录信息并进行必要的更改。如果信息正确，请选择 Create Directory。

   连接目录并构建 Amazon WorkDocs 站点需要几分钟时间。当目录连接时，状态值将更改为`Active`.

第 3 步：完成管理员控制面板设置

在您收到管理员注册电子邮件后，使用您选择的客户端连接到 Amazon WorkDocs 站点，并从管理控制面板中完成设置。

完成管理员控制面板设置

1. 在管理员注册电子邮件中，使用链接登录到 Amazon WorkDocs。
2. UNER管理员中，选择打开管理控制面板.
3. 更改首选电子邮件头语言、存储、安全和恢复站的设置。有关更多信息，请参阅管理站点设置 (p. 28)。
4. 在 Manage Users (管理用户) 下，选择 Invite Users (邀请用户)。您还可以编辑用户设置。

有关更多信息，请参阅邀请和管理 Amazon WorkDocs 用户 (p. 33)。

开始使用现有目录

本节中的步骤介绍如何通过启用现有的AWS Directory Service目录。

任务

开始前的准备工作

- 您必须在当前区域中有一个现有 AWS Directory Service 目录。这可以是 Simple AD 目录或 AD Connector 目录。
- 如果您参加了合规性计划 (例如，PCI、FedRAMP 或 DoD)，则必须设置AWS Managed Microsoft AD满足合规性要求的目录。有关更多信息，请参阅开始使用 AWS Managed Microsoft AD (p. 24)。
- 当您启动新的 Amazon WorkDocs 站点时，必须为管理员指定配置文件信息。此信息包括名字和姓氏以及电子邮件地址。请勿使用任何形式的管理员、管理员、管理员，或者管理员作为您的账户用户名。Amazon WorkDocs 保留该用户角色。

第 1 步：启动 Amazon WorkDocs 网站

按照以下步骤启动您的 Amazon WorkDocs 站点，使用现有的AWS Directory Service目录。

启动 Amazon WorkDocs 站点

1. 从打开 Amazon WorkDocs 控制台https://console.aws.amazon.com/zocalo/.
2. 在 Manage Your WorkDocs Sites 页面上，选择 Create a New WorkDocs Site。

第 2 步：启用目录并设置管理员

按照以下步骤启用您的现有目录并设置管理员。

启用现有目录

1. 在存储库的选择目录页面上，选择AWS Directory Service目录中的可用目录列表，然后选择启用目录.
2. 在存储库的设置 WorkDocs 管理员页面上，输入AWS Directory Service目录，然后选择选择管理员.

   连接目录并构建 Amazon WorkDocs 站点需要几分钟时间。当目录连接时，状态值将更改为`Active`.

默认情况下，目录中的所有用户都将作为活动 Amazon WorkDocs 用户添加到您的账户中。他们可以随时登录并开始使用 Amazon WorkDocs。有关用户角色的更多信息，请参阅用户角色概述 (p. 33)。

第 3 步：完成管理员控制面板设置

在您收到管理员注册电子邮件后，使用您选择的浏览器连接到 Amazon WorkDocs 站点，然后从管理控制面板中完成设置。

完成管理员控制面板设置

1. 在管理员注册电子邮件中，使用链接登录到 Amazon WorkDocs。
2. UNER管理员中，选择打开管理控制面板.
3. 更改首选电子邮件 heade4r 语言、存储、安全和恢复站的设置。有关更多信息，请参阅管理站点设置 (p. 28)。
4. （可选）在 Manage Users (管理用户) 下，选择 Invite Users (邀请用户)。您还可以编辑用户设置。

有关更多信息，请参阅邀请和管理 Amazon WorkDocs 用户 (p. 33)。

AD Connector 入门

本节中的步骤介绍如何设置 Amazon WorkDocs 站点，使用AWS Directory ServiceAD Connector 目录连接到您的本地目录。

任务

开始前的准备工作

- 您必须满足AD Connector 先决条件中的AWS Directory Service管理指南.
- 当您启动新的 Amazon WorkDocs 站点时，必须为管理员指定配置文件信息。此信息包括名字和姓氏以及电子邮件地址。
  - 请勿使用任何形式的管理员、管理员、管理员，或者管理员作为您的账户用户名。Amazon WorkDocs 保留该用户角色。

第 1 步：启动 Amazon WorkDocs 网站

按照以下步骤启动您的 Amazon WorkDocs 站点并连接到您的本地目录。

启动 Amazon WorkDocs 站点

1. 从打开 Amazon WorkDocs 控制台https://console.aws.amazon.com/zocalo/.

   如果您从未在选定区域中创建目录或连接到目录，则会看到 Amazon WorkDocs 起始页。在特定区域中创建目录之后，起始页将不再可用，您将会看到 Manage Your WorkDocs Sites (管理您的 WorkDocs 站点) 页。
2. 选择Get Started Now从 Amazon WorkDocs 起始页面或选择创建新的 WorkDocs 站点来自 的管理您的 WorkDocs 站点页.
3. 在 Get Started with WorkDocs (开始使用 WorkDocs) 页面上，选择 Standard Setup (标准设置) 旁边的 Launch (启动)。

第 2 步：Connect 目录

按照以下步骤使用连接到您的本地目录AWS Directory ServiceAD Connector 目录。

连接您的目录

1. 在存储库的设置目录页面，在AD Connector选择创建 AD Connector.
2. 对于 Directory Details (目录详细信息)，输入以下值，然后选择 Continue (继续)。

   Directory DNS

   本地目录的完全限定名称，例如 corp.example.com。Amazon WorkDocs 只能访问此目录中的用户帐户。用户账户不能包含在父目录中，例如 example.com。

   NetBIOS Name

   本地目录的 NetBIOS 名称，例如 CORP。

   Account Username

   本地目录中用户的用户名称。

   Account Password

   内部用户账户的密码。

   确认密码

   重新输入内部用户账户的密码。这对于在连接目录前防止出现键入错误是必要的。

   DNS Address

   您的本地目录中的 DNS 服务器或域控制器的 IP 地址。此服务器必须可从下面指定的各个子网访问。

3. 对于 Access Point (访问点)，输入以下值：

   区域

   验证区域。

   Site URL

   输入 Amazon WorkDocs 站点的 URL。
4. 对于 VPC Configuration (VPC 配置)，输入以下值：

   VPC

   目录连接到的 VPC。

   Subnets (子网)

   VPC 中的子网，用于连接到您的内部目录。两个子网必须位于不同的可用区。
5. 请确认目录信息正确，然后选择 Connect Directory (连接目录)。

   连接目录并构建 Amazon WorkDocs 站点需要几分钟时间。当目录连接时，状态值将更改为`Active`.

默认情况下，目录中的所有用户都将作为活动 Amazon WorkDocs 用户添加到您的账户中。他们可以随时登录并开始使用 Amazon WorkDocs。有关用户角色的更多信息，请参阅用户角色概述 (p. 33)。

第 3 步：完成管理员控制面板设置

在您收到管理员注册电子邮件后，使用您选择的客户端连接到 Amazon WorkDocs 站点，并从管理控制面板中完成设置。

完成管理员控制面板设置

1. 在管理员注册电子邮件中，使用链接登录到 Amazon WorkDocs。
2. UNER管理员中，选择打开管理控制面板.
3. 更改首选电子邮件头语言、存储、安全和恢复站的设置。有关更多信息，请参阅管理站点设置 (p. 28)。
4. （可选）在 Manage Users (管理用户) 下，选择 Invite Users (邀请用户)。您还可以编辑用户设置。

有关更多信息，请参阅邀请和管理 Amazon WorkDocs 用户 (p. 33)。

开始使用 AWS Managed Microsoft AD

您必须在 Amazon Directory Service 目录和AWS Managed Microsoft AD. Amazon WorkDocs 不支持来自受信任域的用户。要添加来自受信任域的用户，您必须邀请他们。有关更多信息，请参阅 。何时创建信任关系中的AWS 管理服务管理指南.

本节中的步骤介绍如何通过连接到您的本地来设置 Amazon WorkDocs 站点。AWS Managed Microsoft AD 目录。

Note

如果您参加了合规性计划 (例如，PCI、FedRAMP 或 DoD)，则必须设置AWS Managed Microsoft AD满足合规性要求的目录。

任务

开始前的准备工作

- 您必须创建一个 AWS Managed Microsoft AD。有关更多信息，请参阅如何创建 Microsoft AD 目录。
- 您必须在 AD 目录和 AWS Managed Microsoft AD 之间创建信任关系。有关更多信息，请参阅何时创建信任关系。
- 当您启动新的 Amazon WorkDocs 站点时，必须为管理员指定配置文件信息。此信息包括名字和姓氏以及电子邮件地址。请勿使用管理员作为您的账户用户名。管理员是 Amazon WorkDocs 中的保留用户角色。

第 1 步：启动 Amazon WorkDocs 网站

按照以下步骤启动您的 Amazon WorkDocs 站点。

启动 Amazon WorkDocs 站点

1. 从打开 Amazon WorkDocs 控制台https://console.aws.amazon.com/zocalo/.

   如果您从未在选定区域中创建目录或连接到目录，则会看到 Amazon WorkDocs 起始页。在特定区域中创建目录之后，起始页将不再可用，您将会看到 Manage Your WorkDocs Sites (管理您的 WorkDocs 站点) 页。
2. 选择Get Started Now从 Amazon WorkDocs 起始页面或选择创建新的 WorkDocs 站点来自 的管理您的 WorkDocs 站点页.
3. 在 Get Started with WorkDocs (开始使用 WorkDocs) 页面上，选择 Standard Setup (标准设置) 旁边的 Launch (启动)。

第 2 步：启用AWS Managed Microsoft AD并设置管理员

按照以下步骤启用您的 AWS Managed Microsoft AD 并设置管理员。

启用您的 AWS Managed Microsoft AD

1. 从可用目录列表中，选择AWS Managed Microsoft AD以用于您的 Amazon WorkDocs 站点。

   Note

   确保您在所在区域中创建站点。AWS Managed Microsoft AD.
2. 选择 Enable directory。
3. 在存储库的设置 WorkDocs 管理员页面上，从AWS Managed Microsoft AD目录设置为 Amazon WorkDocs 管理员，然后选择选择管理员.

   连接目录并构建 Amazon WorkDocs 站点需要几分钟时间。当目录连接时，状态值将更改为`Active`.

默认情况下，系统将目录中的所有用户都将作为活动 Amazon WorkDocs 用户添加到您的账户中。他们可以随时登录并开始使用 Amazon WorkDocs。有关用户角色的更多信息，请参阅用户角色概述 (p. 33)。

第 3 步：完成管理员控制面板设置

在您收到管理员注册电子邮件后，使用您选择的客户端连接到 Amazon WorkDocs 站点，并从管理控制面板中完成设置。

完成管理员控制面板设置

1. 在管理员注册电子邮件中，使用链接登录到 Amazon WorkDocs。
2. UNER管理员中，选择打开管理控制面板.
3. 更改首选语言、存储、安全和恢复站的设置。有关更多信息，请参阅管理站点设置 (p. 28)。
4. （可选）在 Manage Users (管理用户) 下，选择 Invite Users (邀请用户)。您还可以编辑用户设置。

有关更多信息，请参阅邀请和管理 Amazon WorkDocs 用户 (p. 33)。

启用单点登录

AWS Directory Service允许用户从已加入注册到的同一目录的计算机访问 Amazon WorkDocs，而无需单独输入凭证。Amazon WorkDocs 管理员可以使用AWS Directory Service控制台。有关更多信息，请参阅 。单点登录中的AWS Directory Service管理指南.

在 Amazon WorkDocs 管理员启用单点登录后，Amazon WorkDocs 站点用户还可能需要修改其 Web 浏览器设置来允许单点登录。有关更多信息，请参阅 。IE 和 Chrome 的单点登录和Firefox 的单点登录中的AWS Directory Service管理指南.

启用多重验证

以下步骤介绍如何为 AD Connector 目录启用多重验证。

> Note
>
> 多重验证对 Simple AD 目录不可用。

启用多重验证

1. 从打开 Amazon WorkDocs 控制台https://console.aws.amazon.com/zocalo/.
2. 在 Manage Your WorkDocs Sites 页中，选择所需站点，然后选择 Actions 和 Manage MFA。
3. 输入下列值并选择 Update MFA。

   Enable Multi-Factor Authentication

   选中此项可启用多重验证。

   RADIUS server IP address(es)

   您的 RADIUS 服务器终端节点的 IP 地址或者您的 RADIUS 服务器负载均衡器的 IP 地址。您可以通过用逗号分隔来输入多个 IP 地址。例如，192.0.0.00.0.0,192.0.0.0.0.0.0.0.12.

   端口

   RADIUS 服务器用来通信的端口。您的本地网络必须允许通过默认的 RADIUS 服务器端口 (1812) 从 AD Connector 服务器传入站流量。

   Shared secret code

   在创建 RADIUS 终端节点时指定的共享密码。

Confirm shared secret code (确认共享密码)

确认您的 RADIUS 终端节点的共享密码。

协议

选择在创建 RADIUS 终端节点时指定的协议。

Server timeout

等待 RADIUS 服务器响应的时间长度 (以秒为单位)。请输入 1 到 60 之间的值。

最大重试次数

将尝试与 RADIUS 服务器通信的次数。请输入 0 到 10 之间的值。

当 RADIUS Status 更改为 Enabled 时，多重验证将可用。当您设置多重身份验证时，您的用户无法登录 Amazon WorkDocs 站点。

将用户提升为管理员

使用 Amazon WorkDocs 控制台可以将用户提升为管理员。请记住，您只能提升激活的用户。有关激活用户的更多信息，请参阅编辑用户 (p. 35).

将用户提升为管理员

1. 从打开 Amazon WorkDocs 控制台https://console.aws.amazon.com/zocalo/.
2. 在 Manage Your WorkDocs Sites 页中，选择所需目录，然后选择 Actions 和 Set an Administrator。
3. 在设置 WorkDocs 管理员页上，输入要提升的用户名并选择设置管理员.

您还可以使用 Amazon WorkDocs 管理控制面板对管理员进行降级。有关更多信息，请参阅编辑用户 (p. 35)。

管理站点设置

管理员可以管理站点范围的设置，例如为电子邮件通知选择首选语言、设置存储限制以及指定恢复站保留策略。管理员还可以更改公共共享、邀请和新用户的站点安全设置。

首选语言设置

您可以指定电子邮件通知的语言。

更改语言设置

1. 在 My Account (我的账户) 下面，选择 Open admin control panel (打开管理员控制面板)。
2. 对于 Preferred Language Settings (首选语言设置)，选择您的首选语言。

Hancom 在线编辑和办公在线

启用或禁用Hancom 在线编辑和在线办公室设置从管理控制面板。有关更多信息，请参阅允许协作编辑 (p. 42)。

Storage

指定新用户接收的存储量。

更改存储设置

1. 在 My Account (我的账户) 下面，选择 Open admin control panel (打开管理员控制面板)。
2. 适用于存储中，选择变更。
3. 在存储限制对话框中，选择是为新用户提供无限制存储还是有限存储空间。
4. 选择 Save Changes。

更改存储设置仅影响设置更改后添加的用户。它不会更改分配给现有用户的存储量。要更改现有用户的存储限制，请参阅编辑用户 (p. 35)。

IP 允许列表

Amazon WorkDocs 站点管理员可以添加IP 允许列表设置以限制对一系列允许的 IP 地址的站点访问。最多可以添加 32 个IP 允许列表每个站点的设置。

> Note
>
> IP Allow List (IP 允许列表) 目前仅适用于 IPv4 地址。IP 地址拒绝列表当前不受支持。

将 IP 范围添加到 IP Allow List (IP 允许列表)

1. 在 My Account (我的账户) 下面，选择 Open admin control panel (打开管理员控制面板)。

2. 适用于IP 允许列表中，选择变更。
3. 适用于输入 CIDR 值中，输入要允许列出的 IP 地址范围的无类域间路由 (CIDR) 块，然后从Add。
   - 要允许从单个 IP 地址访问，请指定/32作为 CIDR 前缀。
4. 选择 Save Changes。
5. 连接到您的站点的用户通过IP 允许列表被允许访问。试图从未经授权的 IP 地址连接到您的站点的用户会收到未经授权的响应。

   Warning

   如果输入的 CIDR 值阻止您使用当前 IP 地址访问站点，则会显示一条警告消息。如果您选择继续使用当前的 CIDR 值，您将被阻止使用当前 IP 地址访问站点。只能通过联系 AWS Support 来撤消此操作。

安全性 — 公共共享设置

在管理控制面板(在下面) 下安全中，选择应允许谁创建可公开共享的链接？以指定允许哪些用户向组织外部的人员发送文件查看链接。从以下设置中进行选择：

没有公共共享

用户不能将查看链接发送给组织外部的任何人。

所有托管用户都可以公开共享

所有用户都可以将查看链接发送给组织外部的任何人。

只有高级用户可以公开共享

只有高级用户可以将查看链接发送给组织外部的人。

安全性 — 邀请设置

从以下设置中进行选择Wocs site (应允许哪些人加入您的 WorkDocs 网站？。

Users can invite new people from anywhere by sharing files or folders with them

用户可以通过与组织外部的任何地方邀请新成员。

Users can invite new people from a few specific domains by sharing files or folders with them

用户可以通过与指定域中的新成员共享文件或文件夹来邀请这些新成员。

安全性 — — 外部邀请

从 Who should be allowed to invite external users to your WorkDocs site? (应当允许谁邀请外部用户访问您的 WorkDocs 站点?) 的以下设置中进行选择。

Only administrators can invite new external users

只有管理员才能邀请外部用户使用 Amazon WorkDocs。

所有托管用户都可以邀请新外部用户

所有用户都可以邀请新外部用户使用 Amazon WorkDocs。

只有高级用户才能邀请新外部用户

只有高级用户才能邀请新外部用户使用 Amazon WorkDocs。

恢复站保留

用户删除的文件在用户的回收站中存储 30 天。之后，这些文件会暂时移动到恢复站 60 天，然后才会被永久删除。恢复站仅对管理员可见。通过更改站点范围的数据保留策略，站点管理员可以更改恢复站保留期，最长可达 365 天。系统会在保留期结束时永久删除文件。

更改恢复站保留期

1. 在 My Account (我的账户) 下面，选择 Open admin control panel (打开管理员控制面板)。
2. 旁边的恢复站保留中，选择变更。
3. 键入在恢复站中保留文件的天数，然后选择Save。

   Note

   默认保留期为 60 天。这可以更改为 0—365 天。

您可以在永久删除用户文件之前从恢复站恢复这些文件。

恢复用户的文件

1. 在 My Account (我的账户) 下面，选择 Open admin control panel (打开管理员控制面板)。
2. 在 Manage Users (管理用户) 下面，选择用户的文件夹图标。
3. Unly恢复站，选择要恢复的文件，然后选择恢复图标。
4. 对于 Restore file (还原文件)，选择要将文件还原到的位置，然后选择 Restore (还原)。

管理用户设置

您可以管理用户的设置，包括更改用户角色和邀请、启用或禁用用户。有关更多信息，请参阅邀请和管理 Amazon WorkDocs 用户 (p. 33)。

删除站点

使用亚 Amazon WorkDocs 控制台删除亚 Amazon WorkDocs 站点。

Warning

删除站点时，将丢失所有用户信息和文件。仅当您确定不再需要此信息时才删除站点。

删除站点

1. 从打开 Amazon WorkDocs 控制台https://console.aws.amazon.com/zocalo/。
2. 如果需要，请在导航栏中选择所需的 AWS 区域。有关更多信息，请参阅 。区域和终端节点中的Amazon Web Services 一般参考。
3. 在 Manage Your WorkDocs Sites (管理员控制面板) 页面上，选择要删除的站点。选择操作，然后选择删除 WorkDocs site。
4. 在删除选定的 WorkDocs 站点对话框中，选择是否同时删除用户目录。

- 选择我也想想删除用户目录以删除AWS Directory Service本地 Microsoft Active Directory 的 Simple AD 或 AD Connector。要删除目录，该目录不能包含已启用的任何其他 AWS 应用程序。有关更多信息，请参阅 。删除 Simple AD 目录或者删除 AD Connector 目录中的AWS Directory Service管理指南。

5. 确认您要删除的是正确的站点，在确认字段中键入 DELETE (删除)，然后选择 Delete WorkDocs Site (删除 WorkDocs 站点)。

   该站点将立即删除且不再可用。

   Note

   如果您未为 Amazon WorkDocs 提供自己的目录，则我们会为您创建目录。在删除 Amazon WorkDocs 网站时，除非您删除该目录或者将其用于其他 AWS 应用程序，否则我们将对为您创建的目录收取费用。有关定价信息，请参阅其他目录类型定价。

将亚马逊 WorkDocs 驱动器部署到多台计算机

如果您有加入域的计算机群，您可以使用组策略对象 (GPO) 或系统中心配置管理器 (SCCM) 来安装 Amazon WorkDocs Drive 客户端。您可以从下载客户端https://amazonworkdocs.com/en/clients。

请记住 Amazon WorkDocs Drive 需要在端口 443 上对所有 AWS IP 地址进行 HTTPS 访问。您还需要确认您的目标系统符合 Amazon WorkDocs 驱动器的安装要求。有关更多信息，请参阅 。安装 Amazon WorkDocs Drive中的Amazon WorkDocs 用户指南。

> **Note**
>
> 作为使用 GPO 或 SCCM 的最佳做法，请在用户登录后安装 Amazon WorkDocs 驱动器客户端。

Amazon WorkDocs Drive 的 MSI 安装程序支持以下可选安装参数：

- **`SITEID`**— 在注册期间预先填充 Amazon WorkDocs 站点信息。例如，`SITEID=`*`site-name`*.
- **`DefaultDriveLetter`**— 预填充要用于安装 Amazon WorkDocs Drive 的驱动器盘符。例如，`DefaultDriveLetter=`*`W`*。请记住，每个用户必须具有不同的驱动器号。此外，用户可以在首次启动 Amazon WorkDocs 硬盘后更改驱动器名称，但不能更改驱动器号。

以下示例部署 Amazon WorkDocs 驱动器，而不使用任何用户界面，也不会重新启动。请注意，它使用 MSI 文件的默认名称：

```
msiexec /i "AWSWorkDocsDriveClient.msi" SITEID=your_workdocs_site_ID
DefaultDriveLetter=your_drive_letter REBOOT=REALLYSUPPRESS /norestart /qn
```

邀请和管理 Amazon WorkDocs 用户

默认情况下，当您在站点置备期间附加目录时，Amazon WorkDocs 中的自动激活功能会将该目录中的所有用户添加到新站点，作为托管用户。在 WorkDocs 中，托管用户无需使用单独凭据登录站点，他们可以共享和协作处理文件，并且自动拥有 1 TB 的存储空间。但是，当您只想在目录中添加一些用户时，您可以关闭自动激活，下面各节中的步骤将说明如何执行此操作。

此外，您还可以邀请、启用或禁用用户，以及更改用户角色和设置。您还可以将用户提升为管理员 有关升级用户的更多信息，请参阅将用户提升为管理员 (p. 27)。

您可以在 Amazon WorkDocs Web 客户端的管理控制面板中执行这些任务，以下部分中的步骤将说明如何执行这些任务。但是，如果您是 Amazon WorkDocs 的新手，请花几分钟时间了解各种用户角色，然后再深入了解管理任务。

目录

用户角色概述

Amazon WorkDocs 定义以下用户角色。您可以通过编辑用户配置文件来更改用户的角色。有关更多信息，请参阅 编辑用户 (p. 35)。

- 管理员：对整个站点具有管理权限的付费用户，包括用户管理和站点设置配置。有关如何将用户提升为管理员的更多信息，请参阅将用户提升为管理员 (p. 27)。
- 高级用户：具有管理员特殊权限集的付费用户。有关如何为高级用户设置权限的更多信息，请参阅安全性 — 公共共享设置 (p. 29)和安全性 — — 外部邀请 (p. 29)。
- 用户：付费用户，可以保存文件并与 Amazon WorkDocs 站点中的其他用户协作。
- 访客用户：只能查看文件的未付费用户。您可以将 Guest user 升级为 User、Power user 或 Administrator 角色。

  Note

  当您更改来宾用户的角色时，您将执行一次性操作，您无法撤消。

Amazon WorkDocs 还定义了这些额外的用户类型。

WS 用户

具有已分配工作空间 WorkSpaces 的用户。

- 可访问所有 Amazon WorkDocs 功能

- 默认存储空间为 50 GB (可付费升级到 1 TB)
- 无月度费用

升级的 WS 用户

具有分配的工作空间 WorkSpaces 和升级存储空间的用户。

- 可访问所有 Amazon WorkDocs 功能
- 默认存储空间为 1 TB (可按即付即用方式购买更多存储空间)
- 需支付月度费用

Amazon WorkDocs 用户

没有分配的工作空间 WorkSpaces WorkSpace 的活跃亚马逊 WorkDocs 用户。

- 可访问所有 Amazon WorkDocs 功能
- 默认存储空间为 1 TB (可按即付即用方式购买更多存储空间)
- 需支付月度费用

启动管理控制面板

您可以使用管理控制面板关闭和打开自动激活，更改用户角色和设置等。

打开管理控制面板

1. 在 Amazon WorkDocs 中，选择浏览器右上角的个人资料图标。
2. UNDER管理员中，选择打开管理控制面板。

   Note

   某些控制面板选项在云目录和连接目录之间有所不同。

禁用 Auto Activate

如果不想将目录中的所有用户添加到新站点，并且希望为邀请到新站点的用户设置不同的权限和角色，则可以关闭“自动激活”。关闭“自动激活”后，您还可以决定应邀请新用户加入站点的人员 — 当前用户、高级用户或管理员。以下步骤说明了如何执行这两个任务。

禁用 Auto Activate

1. 选择浏览器右上角的个人资料图标。
2. UNDER管理员中，选择打开管理控制面板。
3. 向下滚动到安全并选择变更。

   这些区域有：策略设置对话框。
4. UNDERAuto Activate，清除允许您目录中的所有用户在首次登录到 WorkDocs 站点时自动激活。

   选项在应允许谁激活 WorkDocs 站点中的目录用户。您可以允许当前用户邀请新用户，也可以将此功能授予高级用户或其他管理员。

5. 选择一个选项，然后选择保存更改。。

重复步骤 1-4 以重新启用自动激活。

启用自动激活的情况下控制用户邀请

当您启用自动激活（请记住，默认情况下启用）时，您可以让用户能够邀请其他用户。您可以将权限授予以下任一以下选项之一：

- 所有用户
- 高级用户
- 管理员。

您还可以完全禁用权限，这些步骤将说明如何使用。

设置邀请权限

1. 选择浏览器右上角的个人资料图标。
2. UNDER管理员中，选择打开管理控制面板。
3. 向下滚动到安全并选择变更。

   这些区域有：策略设置对话框。
4. UNDER应允许谁激活 WorkDocs 站点中的目录用户下面，选择Share with external users (与外部用户共享)复选框中，选择复选框下方的一个选项，然后选择保存更改。。

   — 或 —

   如果您不希望任何人邀请新用户，请清除该复选框，然后选择保存更改。。

邀请新用户

您可以邀请新用户加入目录。还可以允许现有用户邀请新用户。有关更多信息，请参阅 安全性 — 邀请设置 (p. 29)。

邀请新用户

1. 以管理员身份登录 Amazon WorkDocs。
2. UNDER管理员中，选择打开管理控制面板。
3. 在 Manage Users (管理用户) 下，选择 Invite Users (邀请用户)。
4. 在邀请用户对话框，对于你想邀请谁？，输入被邀请者的电子邮件地址，然后选择Send。对每个邀请重复此步骤。

Amazon WorkDocs 会向每个收件人发送邀请电子邮件。该邮件包含有关如何创建 Amazon WorkDocs 账户的链接和说明。邀请链接将在 30 天后到期。

编辑用户

您可以更改现有的用户信息和设置。

编辑用户

1. 以管理员身份登录 Amazon WorkDocs。
2. UNDER管理员中，选择打开管理控制面板。
3. 在 Manage Users (管理用户) 下面，选择用户姓名旁边的铅笔图标 ()。
4. 在 Edit User (编辑用户) 对话框中，您可以编辑以下选项：

   First Name (名) (仅限 Cloud Directory)

   用户的名字。

   Last Name (姓) (仅限 Cloud Directory)

   用户的姓氏。

   状态

   指定用户是否为处于活动状态或者非活动。有关更多信息，请参阅 禁用用户 (p. 36)。

   角色

   指定某个用户是用户还是管理员。您也可以升级或降级已分配有 WorkSpaces 的用户。有关更多信息，请参阅 用户角色概述 (p. 33)。

   存储

   指定现有用户的存储限制。
5. 选择 Save Changes。

禁用用户

您可以通过将用户的状态更改为非活动。

要将用户状态更改为Inactive

1. 以管理员身份登录 Amazon WorkDocs。
2. UNDER管理员中，选择打开管理控制面板。
3. 在 Manage Users (管理用户) 下面，选择用户姓名旁边的铅笔图标 ()。
4. 选择 Inactive (非活动)，然后选择 Save Changes (保存更改)

已取消激活的用户无法访问您的 Amazon WorkDocs 站点。

Note

将用户更改为非活动状态不会删除文件、文件夹或反馈。但是，您可以将非活动用户的文件和文件夹传输到活动的用户。有关更多信息，请参阅 移交文档所有权 (p. 37)。

删除待处理用户（仅限 Simple AD）

您只能删除Pending状态。要删除这些用户之一，请选择垃圾桶图标 ()。

您的 Amazon WorkDocs 站点必须始终至少有一个不是来宾用户的活动用户。如果您需要删除所有用户，请删除整个 Amazon WorkDocs 站点。

建议您不要删除已注册用户。相反，您应该将用户从处于活动状态到非活动状态，以防止他们访问您的 Amazon WorkDocs 站点。

移交文档所有权

您可以将非活动用户的文件和文件夹传输到活动的用户。有关如何取消激活用户的更多信息，请参阅禁用用户 (p. 36)。

> **Warning**
>
> 您不能撤消此操作。

移交文档所有权

1. 以管理员身份登录 Amazon WorkDocs。
2. UNDER管理员中，选择打开管理控制面板。
3. 在 Manage Users (管理用户) 下面，搜索非活动用户。
4. 选择非活动用户名称旁边的铅笔图标 ( )。
5. Select移交文档所有权并输入新所有者的电子邮件地址。
6. 选择 Save Changes。

下载用户列表

要从管理控制面板，您必须安装 Amazon WorkDocs 伴侣。要安装 Amazon WorkDocs 助手，请参阅适用于 Amazon WorkDocs 的应用程序和集成。

下载用户列表

1. 以管理员身份登录 Amazon WorkDocs。
2. UNDER管理员中，选择打开管理控制面板。
3. 在 Manage Users (管理用户) 下，选择 Download user (下载用户)。
4. 对于 Download user (下载用户)，选择以下选项之一，将用户列表以 `.json` 文件格式导出到桌面中：
   - 所有用户
   - 访客用户
   - WS 用户
   - User
   - 高级用户
   - 管理员
5. WorkDocs 将文件保存到以下位置之一中：
   - Windows–`Downloads/WorkDocsDownloads.` 文件夹
   - macOS – *`hard drive`*`/users/`*`username`*`/WorkDocsDownloads/folder`

     > **Note**
     >
     > 下载可能需要一些时间。此外，下载的文件不会降落在您的`/~users`folder。

有关这些用户角色的更多信息，请参阅用户角色概述 (p. 33)。

共享与协作

用户可以通过发送链接或邀请来共享内容。如果启用了外部共享，他们还可以与外部用户协作。

Amazon WorkDocs 使用权限来控制对文件夹和文件的访问。权限根据用户的角色应用。

目录

Sharing

在 Amazon WorkDocs 中，用户可以通过多种方式来共享内容。

共享链接

用户可以选择共享链接快速复制 Amazon WorkDocs 内容的超链接并与其组织内部和外部的同事和外部用户共享这些超链接。当用户共享链接时，他们可以将其配置为允许以下访问选项之一：

- Amazon WorkDocs 站点的所有成员都可以搜索、查看和评论文件。
- 任何具有此链接的人都可以查看该文件，即使不是 Amazon WorkDocs 站点成员也可以。此链接选项会将权限限制为“仅查看”。

具有查看权限的收件人只能查看文件。注释权限允许用户注释并执行更新或删除操作，例如上传新文件或删除现有文件。

默认情况下，所有托管用户都可以创建公共链接。要更改此设置，请更新安全设置，请执行以下操作：有关更多信息，请参阅管理站点设置 (p. 28)。

通过邀请共享

用户可以选择 Share by invite (通过邀请共享)，通过使用电子邮件地址邀请其他用户以与其共享文件或文件夹。用户还可以为每个受邀用户设置适当的权限级别。受邀用户会自动收到邀请电子邮件，通知已经与他们共享内容。单击电子邮件中的链接会打开共享文件。用户可与其他站点成员或外部用户共享文件和文件夹。

用户还可以创建团队文件夹，以通过邀请与您创建的目录组共享。

外部共享

外部共享允许 Amazon WorkDocs 站点的托管用户以便利的方式与外部用户共享文件和文件夹并进行协作，而不会产生额外费用。站点的用户可与外部用户共享文件和文件夹，而不要求接收者是 Amazon WorkDocs 站点的付费用户。如果启用了外部共享，用户可以键入要与其共享的外部用户的电子邮件地址，并设置相应的查看者共享权限。添加外部用户时，权限仅限于查看者，其他权限不可用。外部用户会收到一封电子邮件通知，其中包含指向共享文件或文件夹的链接。选择此链接会使外部用户进入站点，他们键入其凭证即可登录到 Amazon WorkDocs。他们可以在与我共享查看。

文件所有者可以随时修改共享权限或移除外部用户对文件或文件夹的访问权限。站点管理员必须启用站点的外部共享，以便托管用户能够与外部用户共享内容。适用于访客用户成为贡献者或共同所有者，则必须将他们升级到用户级别由站点管理员提供。有关更多信息，请参阅用户角色概述 (p. 33)。

默认情况下，外部共享处于启用状态，所有用户都可以邀请外部用户。要更改此设置，请更新安全设置，请执行以下操作：有关更多信息，请参阅管理站点设置 (p. 28)。

Permissions

Amazon WorkDocs 使用权限控制对文件夹和文件的访问。权限根据用户角色应用。

目录

Roles

文件夹权限和文件权限均根据用户角色来授予。Amazon WorkDocs 定义以下角色：

- 文件夹拥有者 — 文件夹或文件的拥有者。
- 文件夹共有者 — 拥有者指定为文件夹或文件共有者的用户或组。
- 文件夹贡献者 — 对文件夹具有无限制访问权限的人。
- 文件夹查看器 — 对文件夹具有有限访问权限（只读权限）的用户。

以下角色适用于文件：

- 所有者 — 文件的所有者。
- 共有者 — 拥有者指定为文件共有者的用户或组。
- 贡献者 — 允许对档案提供反馈的人。
- 查看器 — 对文件具有有限访问权限（只读权限）的用户。
- 匿名查看者 — 组织外部的非注册用户，可以使用外部查看链接查看共享的文件。除非另行指定，否则匿名查看者与查看者的权限相同。

共享文件夹权限

Amazon WorkDocs 为共享文件夹提供以下权限。作为提醒，应用于文件夹的权限也应用于该文件夹中的文件。

- 查看 — 查看共享文件夹的内容。
- 查看子文件夹 — 查看子文件夹。
- 查看共享文件夹的其他用户。
- 下载文件夹 — 下载文件夹。
- 添加子文件夹 — 添加子文件夹。
- Share (共享与其他用户共享顶级文件夹。
- 撤销共享 — 撤销顶级文件夹的共享。
- 删除子文件夹 — 删除子文件夹。

- 删除顶级文件夹 — 删除顶级共享文件夹。

共享文件夹的权限

许可	文件夹所有者	文件夹共有者	文件夹参与者	文件夹查看者
查看	X	X	X	X
查看子文件夹	X	X	X	X
查看共享	X	X	X	X
下载	X	X	X	X
添加子文件夹	X	X	X	
共享	X	X		
撤销共享	X	X		
删除子文件夹	X	X		
删除顶级文件夹	X	X		

文件权限

Amazon WorkDocs 为不在共享文件夹中的文件提供以下权限：

- 查看 — 查看文件。
- 删除 — 删除文件。
- 注释 — 向文件添加反馈。
- 查看共享文件的其他用户。
- 查看注释 — 查看其他用户的反馈。
- 查看活动 — 查看文件的活动历史记录。
- 查看版本 — 查看文件的早期版本。
- 下载 — 下载文件。这是默认权限。您可以使用文件属性来允许或拒绝下载共享文件的功能。
- 禁止下载 — 禁止下载文件。
- 上传 — 上传文件的新版本。
- 共享 — 与其他用户共享文件。
- 撤销共享 — 撤销文件的共享。

不在共享文件夹中的文件的权限

许可	所有者/共有者	贡献者	查看者	匿名查看者
查看	X	X	X	X
查看共享	X	X	X	X
下载	X	X	X	
注释	X	X		
查看注释	X	X		

许可	所有者/共有者	贡献者	查看者	匿名查看者
查看活动	X	X		
查看版本	X	X		
上传	X	X		
Delete	X			
禁止下载	X			
共享	X			
撤销共享	X			

共享文件权限

Amazon WorkDocs 为共享文件夹中的文件提供以下权限：

- 查看 — 查看共享文件夹中的文件。
- 查看共享文件的其他用户。
- 下载 — 下载文件。
- 注释 — 向文件添加反馈。
- 查看注释 — 查看其他用户的反馈。
- 查看活动 — 查看文件的活动历史记录。
- 查看版本 — 查看文件的早期版本。
- 上传 — 上传文件的新版本。
- 删除 — 删除共享文件夹中的文件。
- 禁止下载 — 禁止下载文件。这是文件夹中的文件的默认权限。
- 共享 — 与其他用户共享文件。
- 撤销共享 — 撤销文件的共享。
- 私有评论 — 拥有者/共有者可以查看文档的所有私有评论，即使这些评论并非针对其评论的回复。

共享文件夹中的文件的权限

许可	文件夹所有者/共有者	文件所有者*	文件夹参与者	文件夹查看者	匿名查看者
查看	X	X	X	X	X
查看共享	X	X	X	X	X
下载	X	X	X	X	
注释	X	X	X		
查看注释	X	X	X		
查看活动	X	X	X		
查看版本	X	X	X		
上传	X	X	X		

许可	文件夹所有者/共有者	文件所有者*	文件夹参与者	文件夹查看者	匿名查看者
Delete	X	X			
重命名	X	X			
禁止下载	X	X			
共享	X	X			
撤销共享	X	X			
查看所有私有评论**	X	X			

* 文件所有者，在这种情况下是将文件原始版本上传到共享文件夹中的人员。此角色的权限仅适用于所拥有的文件，不包括共享文件夹中的所有文件。

** 文件所有者/共有者可以查看所有私有评论。贡献者只有回复评论之后才能看到私有评论。

允许协作编辑

您可以启用协作编辑选项，在在线编辑设置部分管理控制面板.

目录

启用 Hancom ThinkFree

您可以为您的亚马逊 WorkDocs 站点启用 Hancom Thare 免费，这样用户可从亚马逊 WorkDocs Web 应用程序创建并协作编辑 Microsoft Office 文件。有关更多信息，请参阅 。使用 Hancom ThinkFree 进行编辑.

Hancom Thare 免费供亚马逊 WorkDocs 用户免费使用。无需其他许可或软件安装。

启用 Hancom ThinkFree

启用 Hancom ThinkFree 编辑从管理控制面板.

1. 在 My account (我的账户) 下面，选择 Open admin control panel (打开管理员控制面板)。
2. 适用于Hancom 在线编辑中，选择变更.
3. 选择 Enable Hancom Online Editing Feature (启用 Hancom 在线编辑功能)，查看使用条款，然后选择 Save (保存)。

禁用 Hancom ThinkFree

禁用 Hancom ThinkFree 编辑从管理控制面板.

1. 在 My account (我的账户) 下面，选择 Open admin control panel (打开管理员控制面板)。
2. 适用于Hancom 在线编辑中，选择变更.
3. 清除 Clear启用 Hancom 在线编辑功能复选框，然后选择Save.

允许使用 Office Online 打开

您可以为 Amazon WorkDocs 站点启用 “使用 Office Online 打开” 功能，这样用户可从亚马逊 WorkDocs Web 应用程序协作编辑 Microsoft Office 文件。

使用办公室在线打开是不需要额外费用的 Amazon WorkDocs 用户也有微软 Office 365WORK或者學校帐户，并具有在 Office 联机中编辑的许可证。有关更多信息，请参阅使用 Office Online 打开。

启用 “使用 Office Online 打开” 功能

启用 “使用 Office Online 打开” 功能管理控制面板.

1. 在 My account (我的账户) 下面，选择 Open admin control panel (打开管理员控制面板)。
2. 适用于Office Online中，选择变更.
3. Select启用 Office Online，然后选择Save.

禁用 “使用 Office Online 打开” 功能

禁用 “使用 Office Online 打开” 功能。管理控制面板.

1. 在 My account (我的账户) 下面，选择 Open admin control panel (打开管理员控制面板)。
2. 适用于Office Online中，选择变更.
3. 清除 Clear启用 Office Online复选框，然后选择Save.

将文件迁移到 Amazon WorkDocs

Amazon WorkDocs 管理员可以使用 Amazon WorkDocs 迁移服务将多个文件和文件夹大规模迁移到其 Amazon WorkDocs 站点。Amazon WorkDocs 迁移服务与 Amazon Simple Storage Service (Amazon S3) 配合使用。这使您可以将部门文件共享和主驱动器或用户文件共享迁移到 Amazon WorkDocs。

此过程中的 Amazon WorkDocs 提供AWS Identity and Access Management(IAM) 策略。使用此策略可以创建一个新的 IAM 角色，以授予对 Amazon WorkDocs 迁移服务的访问权限，以执行以下操作：

- 读取并列出您指定的 Amazon S3 存储桶。
- 读取和写入您指定的 Amazon WorkDocs 站点。

完成以下任务以将文件和文件夹迁移到 Amazon WorkDocs。在您开始之前，确认您具有以下权限：

- Amazon WorkDocs 站点的管理员权限
- 创建 IAM 角色的权限

如果您的 Amazon WorkDocs 站点设置为与 WorkSpaces 队列位于同一目录中，则必须遵循以下要求：

- 请勿使用管理员查看您的 Amazon WorkDocs 账户用户名。管理员是 Amazon WorkDocs 中的保留用户角色。
- 您的 Amazon WorkDocs 管理员用户类型必须为升级的 WS 用户. 有关更多信息，请参阅 用户角色概述 (p. 33) 和 编辑用户 (p. 35)。

> **Note**
>
> 迁移到 Amazon WorkDocs 时，将保留目录结构、文件名和文件内容。不保留文件所有权和权限。

任务

第 1 步：准备迁移

准备迁移

1. 在您的 Amazon WorkDocs 网站上，在我的文档，创建要将文件和文件夹迁移到的文件夹。
2. 确认要迁移的每个文件都小于 5 TB。每个文件名不得超过 255 个字符。Amazon WorkDocs Docs Docs Drice 仅显示完整目录路径不超过 260 个字符的文件。

> **Warning**
>
> 尝试迁移名称中包含以下字符的文件或文件夹可能会导致出现错误并致使迁移过程终止。如果发生这种情况，请选择 Download report (下载报告) 以下载列出错误的日志、无法迁移的文件以及任何成功迁移的文件。

- 尾随空格-例如：文件名末尾的额外空格。
- 开始或结束时的期间— 例如:`.file`、`.file.ppt`、`.`、`..`，或者`file.`
- 开头或结尾的波浪号— 例如:`file.doc~`、`~file.doc`，或者`~$file.doc`
- 以结尾的文件名**`.tmp`**— 例如:`file.tmp`
- 文件名与这些区分大小写的词语完全匹配–`Microsoft User Data`、`Outlook files`、`Thumbs.db`，或者`Thumbnails`
- 包含任何这些字符的文件名–`*`(星号),`/`（正斜杠）、`\`（反斜杠）、`:`(冒号),<(小于),>（大于）、`?`(问号),`|`(竖线),`"`（双引号）或`\202E`（字符代码 202E）。

第 2 步：将文件上载到 Amazon S3

将文件上传到 Amazon S3

1. 在您的AWS帐户中要将文件和文件夹上传到其中。Amazon S3 存储桶必须位于同一AWS账户和AWS区域作为您的 Amazon WorkDocs 站点。有关更多信息，请参阅 。开始使用 Amazon Simple Storage Service中的Amazon Simple Storage Service 用户指南.
2. 将文件上传到上一步中创建的 Amazon S3 存储桶。我们建议使用AWS DataSync将您的文件和文件夹上传到 Amazon S3 存储桶中。DataSync 提供更多跟踪、报告和同步功能。有关更多信息，请参阅 。操作方法AWS DataSync工作原理和将基于身份的策略（IAM 策略）用于 DataSync中的AWS DataSync用户指南.

第 3 步：计划迁移

完成步骤 1 和 2 后，使用 Amazon WorkDocs 迁移服务计划迁移。迁移服务最长可能需要一周时间来处理您的迁移请求，并向您发送一封电子邮件，说明您可以开始迁移。如果您在收到电子邮件之前开始迁移，管理控制台将显示一条消息，提示您等待。

在计划迁移时，您的 Amazon WorkDocs 用户账户存储设置会自动更改为无限.

> Note
>
> 迁移超出 Amazon WorkDocs Storage (Amazon WorkDocs 存储限制) 的文件可能会产生额外费用。有关更多信息，请参阅 。Amazon WorkDocs 定价.

亚 Amazon WorkDocs 迁移服务提供了AWS Identity and Access Management(IAM) 策略供您用于迁移。使用此策略，您可以创建一个新的 IAM 角色，以授予 Amazon WorkDocs 迁移服务对您指定的 Amazon S3 存储桶和 Amazon WorkDocs 站点的访问权限。您还订阅 Amazon SNS 电子邮件通知，以便在计划迁移请求时以及开始和结束时接收更新信息。

计划迁移

1. 在 Amazon WorkDocs 控制台中，选择应用程序、迁移.
   - 如果这是您第一次访问 Amazon WorkDocs 迁移服务，系统会提示您订阅 Amazon SNS 电子邮件通知。订阅，在您收到的电子邮件中确认，然后选择 Continue (继续)。
2. 选择 Create Migration (创建迁移)。
3. 对于 Source Type (源类型)，选择 Amazon S3。
4. 选择 Next (下一步)。
5. 适用于数据源和验证，在示例策略，复制提供的 IAM 策略。
6. 使用您在上一步中复制的 IAM 策略，创建新的 IAM 策略和角色，如下所示：
   a. 打开 IAM 控制台：https://console.aws.amazon.com/iam/。

b. 选择 Policies (策略)，然后选择 Create policy (创建策略)。
c. 选择JSON并粘贴您之前复制到剪贴板的 IAM 策略。
d. 选择 Review policy (查看策略)。输入策略名称和描述。
e. 选择创建策略。
f. 依次选择 Roles (角色)、Create role (创建角色)。
g. Select另一个 AWS 账户. 对于 Account ID (账户 ID)，输入以下内容之一：

   - 对于美国东部（弗吉尼亚北部）区域，输入`899282061130`
   - 对于美国西部（俄勒冈）区域，输入`814301586344`
   - 对于亚太地区（新加坡）区域，输入`900469912330`
   - 对于亚太地区（悉尼）区域，输入`031131923584`
   - 对于亚太地区（东京）区域，输入`178752524102`
   - 对于欧洲（爱尔兰）区域，输入`191921258524`

h. 选择您创建的新策略，然后选择后续：审核。如果没有看到新策略，请选择刷新图标。
i. 输入角色名称和描述。选择 Create role（创建角色）。
j. 在 Roles (角色) 页面上的 Role name (角色名称) 下方，选择您创建的角色名称。
k. 在 Summary (摘要) 页面上，将 Maximum CLI/API session duration (最大 CLI/API 会话持续时间) 更改为 12 小时。
l. 将 Role ARN (角色 ARN) 复制到剪贴板中以便在下一步中使用。

7. 返回到Amazon WorkDocs Migration Service. 适用于数据源和验证，在角色 ARN，请粘贴您在上一步中复制的 IAM 角色中的角色 ARN。
8. 适用于存储桶中，选择要从中迁移文件的 Amazon S3 存储桶。
9. 选择 Next (下一步)。
10. 适用于选择目标 WorkDocs 文件夹下，选择要将文件迁移到的 Amazon WorkDocs 中的目标文件夹。
11. 选择 Next (下一步)。
12. 在 Review (审核) 下，对于 Title (标题)，输入迁移的名称。
13. 选择迁移的日期和时间。
14. 选择 Send (发送)。

第 4 步：跟踪迁移

您可以从 Amazon WorkDocs 迁移服务登录页面中跟踪您的迁移。要从 Amazon WorkDocs 站点访问登陆页面，请选择应用程序、迁移. 选择您的迁移以查看其详细信息并跟踪其进度。如果需要取消，也可以选择 Cancel Migration (取消迁移)，或选择 Update (更新) 以更新迁移的时间表。迁移完成后，您可以选择 Download report (下载报告) 以下载已成功迁移的文件、任何失败或错误的日志。

以下迁移状态用于表示迁移的状态：

已安排

迁移已安排但尚未开始。您最晚可以在计划开始时间之前五分钟取消迁移或更新迁移开始时间。

正在迁移

迁移正在进行中。

成功

迁移已完成。

部分成功

迁移已部分成功。有关更多详细信息，请查看迁移摘要并下载提供的报告。

已失败

迁移失败。有关更多详细信息，请查看迁移摘要并下载提供的报告。

Canceled

迁移已取消。

第 5 步：清理资源

迁移完成后，删除从 IAM 控制台创建的迁移策略和角色。

删除 IAM 策略和角色

1. 打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 选择策略。
3. 搜索并选择您创建的策略。
4. 对于 Policy actions (策略操作)，选择 Delete (删除)。
5. 选择 Delete。
6. 选择 Roles (角色)。
7. 搜索并选择您创建的角色。
8. 选择 Delete role (删除角色)、Delete (删除)。

在计划迁移开始时，您的 Amazon WorkDocs 用户账户存储设置会自动更改为无限. 迁移后，您可以通过从管理员控制面板编辑用户账户来更改 Storage (存储) 设置。有关更多信息，请参阅编辑用户 (p. 35)。

Amazon WorkDocs 问题排查

以下信息可帮助您排除与 Amazon WorkDocs 相关的问题。

问题

无 Amazon WorkDocs 定的AWS区域

如果要设置新的 Amazon WorkDocs 站点，请在设置过程中选择 AWS 区域。有关详细信息，请参阅 Amazon WorkDocs 入门 (p. 17) 下的特定使用案例的教程。

想在现有的 Amazon VPC 中设置我的 Amazon WorkDocs 站点

设置新的 Amazon WorkDocs 站点时，使用现有的 Virtual Private Cloud (VPC) 创建目录。Amazon WorkDocs 使用此目录来对用户进行身份验证。

用户需要重置密码

用户可以通过在登录屏幕上选择 Forgot password? (忘记密码？) 重置密码。

用户意外共享了一个敏感文档

要撤销对文档的访问权限，请选择文档旁边的 Share by invite (通过邀请共享)，然后删除不应再具有访问权限的用户。如果文档是使用链接共享的，请选择 Share a link (共享链接) 并禁用该链接。

用户离开了组织，没有移交文档所有权

在管理员控制面板中将文档所有权转移给其他用户。有关更多信息，请参阅移交文档所有权 (p. 37)。

需要将 Amazon WorkDocs Drive 或 Amazon WorkDocs Companion 部署到多个用户

通过使用组策略部署到企业中的多个用户。有关更多信息，请参阅适用于 Amazon WorkDocs 的身份和访问管理 (p. 4)。有关将 Amazon WorkDocs 硬盘部署到多个用户的具体信息，请参阅将亚马逊 WorkDocs 驱动器部署到多台计算机 (p. 32)。

在线编辑不起作用

验证您是否安装了 Amazon WorkDocs Companion。要安装 Amazon WorkDocs Companion，请参阅适用于 Amazon WorkDocs 的应用程序和集成。

管理适用于 Amazon Business 的 Amazon WorkDocs

如果您是亚马逊企业采购商城 WorkDocs 的管理员，您可以通过登录https://workdocs.aws/使用您的亚马逊企业资格认证。

邀请新用户加入亚马逊企业采购商城的亚马逊 WorkDocs

1. 在 https://workdocs.aws/ 上使用 Amazon Business 凭证进行登录。
2. 在适用于 Amazon WorkDocs 的 Amazon Business 的主页上，打开左侧的导航窗格。
3. 选择管理员设置。
4. 选择添加人员。
5. 适用于收件人中，输入要邀请的用户的电子邮件地址或用户名。
6. （可选）自定义邀请消息。
7. 选择完成。

在亚马逊 WorkDocs 上搜索亚马逊企业采购商城的用户

1. 在 https://workdocs.aws/ 上使用 Amazon Business 凭证进行登录。
2. 在适用于 Amazon WorkDocs 的 Amazon Business 的主页上，打开左侧的导航窗格。
3. 选择管理员设置。
4. 适用于搜索用户，输入用户的名字，然后按**Enter**。

为亚马逊企业采购商城选择 Amazon WorkDocs 上的用户角色

1. 在 https://workdocs.aws/ 上使用 Amazon Business 凭证进行登录。
2. 在适用于 Amazon WorkDocs 的 Amazon Business 的主页上，打开左侧的导航窗格。
3. 选择管理员设置。
4. UTER人员，在用户旁边，选择角色向用户分配。

删除亚马逊企业采购商城 WorkDocs 上的用户

1. 在 https://workdocs.aws/ 上使用 Amazon Business 凭证进行登录。
2. 在适用于 Amazon WorkDocs 的 Amazon Business 的主页上，打开左侧的导航窗格。
3. 选择管理员设置。
4. UTER人员中，选择省略号（...）旁边的用户。
5. 选择 Delete。
6. 如果出现提示，请输入要将用户文件传输到的新用户，然后选择Delete。

文档历史记录

下表介绍了对Amazon WorkDocs 管理指南，从 2018 年 2 月起开始。如需有关此文档更新的通知，您可以订阅 RSS 源。

更新-历史记录-更改	更新-历史记录-描述	更新-历史记录-日期
Amazon WorkDocs Backup (p. 51)	已从《Amazon WorkDocs 管理指南》中删除了 Amazon WorkDocs Backup 文档，因为该组件不再受支持。	2019 年 6 月 24 日
管理 Amazon WorkDocs (p. 51)	亚马逊企业采购商城工作 Docs 支持管理员进行用户管理。有关更多信息，请参阅 。管理 Amazon WorkDocs，请参阅 Amazon WorkDocs 管理指南。	2020 年 3 月 26 日
将文件迁移到 Amazon WorkDocs (p. 51)	Amazon WorkDocs 管理员可以使用 Amazon WorkDocs 迁移服务将多个文件和文件夹大规模迁移到其 Amazon WorkDocs 站点。有关更多信息，请参阅 。将文件迁移到 Amazon WorkDocs，请参阅 Amazon WorkDocs 管理指南。	2019 年 8 月 8 日
IP 允许列表设置 (p. 51)	IP 允许列表设置可用于按 IP 地址范围筛选对 Amazon WorkDocs 站点的访问。有关更多信息，请参阅 。IP 允许列表设置，请参阅 Amazon WorkDocs 管理指南。	2018 年 10 月 22 日
Hancom ThinkFree (p. 51)	开始提供 Hancom ThinkFree。用户可从 Amazon WorkDocs Web 应用程序创建并协作编辑 Microsoft Office 文件。有关更多信息，请参阅 。启用 Hancom ThinkFree，请参阅 Amazon WorkDocs 管理指南。	2018 年 6 月 21 日
使用 Office Online 打开 (p. 51)	开始提供“使用 Office Online 打开”功能。用户可从 Amazon WorkDocs Web 应用程序协作编辑 Microsoft Office 文件。有关更多信息，请参阅 。使用 Office Online 启用，请参阅 Amazon WorkDocs 管理指南。	2018 年 6 月 6 日
问题排查 (p. 51)	增加了故障排除主题。有关更多信息，请参阅 。Amazon WorkDocs 故障排查，请参阅 Amazon WorkDocs 管理指南。	2018 年 5 月 23 日

更改恢复站保留期 (p. 51)	可以修改恢复站保留期。有关更多信息，请参阅 。恢复站保留设置，请参阅 Amazon WorkDocs 管理指南。	2018 年 2 月 27 日

AWS词汇表

有关最新AWS术语，请参阅AWS一般参考中的AWS术语表。

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。