# Amazon WorkDocs

## 管理指南

Version 1.0

# Amazon WorkDocs: 管理指南

# Table of Contents

# 什么是 Amazon WorkDocs？

Abstract

使用 Zocalo 在云中共享和同步文件。

Amazon WorkDocs 是一项完全托管型且安全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。您的文件安全可靠地存储在云中。Amazon WorkDocs 还包括一个同步应用程序，能够持续让您计算机上选定的文件夹与您的云文件夹同步。您的文件仅对您和您指定的参与者和查看者可见。贵公司的其他成员无法访问任何您的文件，除非您特别授予他们访问权限。

您可以与贵公司的其他成员共享您的文件用来协作或审查。Amazon WorkDocs 协作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。

Topics



## 相关服务

Amazon WorkDocs 与 Amazon WorkSpaces 密切相关。实际上，您甚至可将 Amazon WorkDocs 连接到您的 Amazon WorkSpaces 用户目录。有关更多信息，请参阅 启用现有 AWS Directory Service 目录 (p. 6)。

## 访问

管理员使用 Amazon WorkDocs 控制台来创建和停用 Amazon WorkDocs 站点，并且使用Amazon WorkDocs 管理控制面板 (p. 13)来管理权限和用户。

最终用户使用客户端应用程序访问其文件。非管理员用户从不需要使用 Amazon WorkDocs 控制台或管理控制面板。Amazon WorkDocs 提供了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。此外还提供了可供在 iPad 和 Android 平板电脑上查看文档的本机应用程序。这些应用程序称为协作客户端。

- 一个文档同步应用程序，可用于将您的 Mac 或 Windows 桌面上的文件夹与您的 Amazon WorkDocs 文件同步。
- 适用于多个常用 Web 浏览器的 Web 剪辑程序浏览器扩展，可用于将网页图像保存到 Amazon WorkDocs 文件。

# 定价

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。有关定价的更多特定信息，请转至定价。

# 设置 Amazon WorkDocs

Abstract

设置 Amazon WorkDocs。

要设置新的 Amazon WorkDocs 站点或管理现有站点，您必须满足以下先决条件：

Topics



## AWS 账户

您的 AWS 账户可让您访问所有服务，但您只需为所使用的资源付费。

如果您没有 AWS 账户，请通过以下步骤创建一个账户。

### 注册 AWS

1. 打开 http://aws.amazon.com/，然后单击 Sign Up (注册)。
2. 按照屏幕上的说明进行操作。

您的根账户凭证使 AWS 中的服务可以识别您，并授予您对 AWS 资源（例如您的 Amazon WorkDocs 站点）的无限制使用权限。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。

## IAM 用户和群组

AWS 管理控制台 需要您提供用户名称和密码，这样服务才能确定您是否有权访问其资源。我们建议您避免使用根账户凭证访问 AWS，因为无法使用任何方法来撤销或限制根账户凭证。应该改为使用 AWS

Identity and Access Management (IAM) 创建 IAM 用户，然后将 IAM 用户添加到具有管理权限的 IAM 组。这会向 IAM 用户授予管理权限。您可以使用 IAM 用户的凭证访问 AWS 管理控制台。

如果您已注册 AWS 但尚未为自己创建一个 IAM 用户，则可以使用 IAM 控制台自行创建。有关创建 IAM 用户的更多信息，请参阅 *使用 IAM* 指南中的创建单独的 IAM 用户。

# 适用于 Amazon WorkDocs 的 IAM 策略

默认情况下，IAM 用户无权管理 Amazon WorkDocs 资源；您必须创建一个向 IAM 用户明确授予这些权限的 IAM 策略，并将该策略附加到需要这些权限的特定 IAM 用户或组。有关 IAM 策略的更多信息，请参阅 *使用 IAM* 指南中的权限与策略。

以下策略声明向 IAM 用户授予对 Amazon WorkDocs 资源的完全访问权限。该策略向用户授予对所有 Amazon WorkDocs 和 AWS Directory Service 操作以及 Amazon WorkDocs 需要能够代表您执行的多个 Amazon EC2 操作的访问权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
          "zocalo:*",
          "ds:*",
          "ec2:CreateVpc",
          "ec2:CreateSubnet",
          "ec2:CreateNetworkInterface",
          "ec2:CreateTags",
          "ec2:CreateSecurityGroup",
          "ec2:DescribeVpcs",
          "ec2:DescribeSubnets",
          "ec2:DescribeNetworkInterfaces",
          "ec2:DescribeAvailabilityZones",
          "ec2:AuthorizeSecurityGroupEgress",
          "ec2:AuthorizeSecurityGroupIngress",
          "ec2:DeleteSecurityGroup",
          "ec2:DeleteNetworkInterface",
          "ec2:RevokeSecurityGroupEgress",
          "ec2:RevokeSecurityGroupIngress"
          ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

以下策略声明向 IAM 用户授予对 Amazon WorkDocs 资源的只读访问权限。该策略向用户授予对所有 Amazon WorkDocs `Describe` 操作的访问权限。Amazon WorkDocs 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": [
    {
      "Action": [
```

```
            "zocalo:Describe*",
            "ds:DescribeDirectories",
            "ec2:DescribeVpcs",
            "ec2:DescribeSubnets"
            ],
        "Effect": "Allow",
        "Resource": "*"
    }
  ]
}
```

# Amazon WorkDocs 入门

Abstract

启动和运行 Amazon WorkDocs。

Amazon WorkDocs 以组织为基础。这些组织包括属于该组织的用户，以及有关各用户的文件夹和文档的信息。组织信息存储在 AWS Directory Service 目录中。这可以是 Simple AD 目录或 AD Connector 目录。您可以启用 Amazon WorkDocs 来处理现有目录，也可以让 Amazon WorkDocs 为您创建目录。

Topics



# 启用现有 AWS Directory Service 目录

如果您的当前区域中有一个 AWS Directory Service 目录，则可以将 Amazon WorkDocs 连接到您的现有目录。这可以是 Simple AD 目录或 AD Connector 目录。要连接到现有 AWS Directory Service 目录，请执行以下步骤。

连接到现有目录

1. 开启 Amazon WorkDocs 控制台，使用 https://console.aws.amazon.com/zocalo/ 。
2. 在 Manage Your WorkDocs Sites 页面上，单击 Create a New WorkDocs Site。
3. 在 Select a Directory 页面上，从 Available Directories 列表中选择您的 AWS Directory Service 目录，然后单击 Enable Directory。
4. 在 Set WorkDocs Administrator 页面上，输入 AWS Directory Service 目录中将成为您的 Amazon WorkDocs 管理员的用户名称，然后单击 Select Administrator。

   成功启用目录之后，站点的 Status 值将更改为 `Active`。

# 创建 Simple AD 目录

Amazon WorkDocs 使用 AWS Directory Service Simple AD 目录存储云中的用户信息。您可以通过两种方式之一创建 Simple AD 目录。快速启动过程 (p. 7)用于快速完成设置，适用于小型组织。快速启动过程创建并配置与目录一起使用的 VPC，另外还创建管理员账户。在特定区域中创建目录之后，“Quick Start”选项不再可用。

如果您需要更进一步地控制目录配置，则可以选择标准设置 (p. 8)，使用它可以指定您自己的目录域名，以及与目录一起使用的现有 VPC 之一。还提供了一个选项，可以让 Amazon WorkDocs 为您创建和配置 VPC。

Topics



## Simple AD 目录设置详细信息

创建 Simple AD 目录时，Amazon WorkDocs 代表您执行以下任务：

- 在 VPC 中设置用于存储用户信息的 Simple AD 目录。
- 使用管理员电子邮件地址作为用户名称来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。您可以使用此账户管理您的目录。

## 使用快速启动创建 Simple AD 目录

要使用快速启动过程创建 Simple AD 目录，请执行以下步骤。

使用快速启动创建 Simple AD 目录

1. 开启 Amazon WorkDocs 控制台，使用 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 页。
2. 如果您在 Amazon WorkDocs 起始页上，请执行以下步骤：

   1. 单击 Get Started Now。
   2. 在 Get Started with WorkDocs 页上，单击 Quick Start 下方的 Launch。

   如果您在 Manage Your WorkDocs Sites 页上，请执行下列步骤：

   1. 单击 Create a New WorkDocs Site。
   2. 在 Get Started with WorkDocs 页上，单击 Quick Start 下方的 Launch。
3. 输入以下值，然后单击 Complete Setup。

   在 Access Point 部分中输入以下值：

   区域
   : 验证区域。

Site URL
输入您的 Amazon WorkDocs 站点的 URL。

在 Set WorkDocs Administrator 部分中输入以下值：

电子邮件
目录管理员的电子邮件地址。注册电子邮件将发送到该电子邮件地址。

名
目录管理员的名字。

姓
目录管理员的姓氏。

创建目录和 Amazon WorkDocs 站点需要几分钟的时间。成功创建目录之后，站点的 Status 值将更改为 `Active`。

# 使用标准设置创建 Simple AD 目录

要创建 Simple AD 目录，您必须满足 *AWS Directory Service Administration Guide* 的 Simple AD 先决条件 中标识的先决条件。

要使用标准设置创建 Amazon WorkDocs 云目录，请执行以下步骤。

创建云目录

1. 开启 Amazon WorkDocs 控制台，使用 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 页。
2. 如果您在 Amazon WorkDocs 起始页上，请执行以下步骤：

   1. 单击 Get Started Now。
   2. 在 Get Started with WorkDocs 页上，单击 Standard Setup 下方的 Launch。

   如果您在 Manage Your WorkDocs Sites 页上，请执行下列步骤：

   1. 单击 Create a New WorkDocs Site。
   2. 在 Get Started with WorkDocs 页上，单击 Standard Setup 下方的 Launch。

3. 在 Set up a Directory 页上，单击 Create Simple AD。
4. 输入以下值，然后单击 Continue。

   在 Access Point 部分中输入以下值：

   区域
   验证区域。

   Site URL
   输入您的 Amazon WorkDocs 站点的 URL。

   在 Directory Details 部分中输入以下值：

   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。

在 Set WorkDocs Administrator 部分中输入以下值：

电子邮件
目录管理员的电子邮件地址。注册电子邮件将发送到该电子邮件地址。

名
目录管理员的名字。

姓
目录管理员的姓氏。

对于 VPC Details，您可以使用一个现有的 VPC，或者让 Amazon WorkDocs 为您创建和配置 VPC。要让 Amazon WorkDocs 为您创建 VPC，请选择 Set up a new VPC on my behalf。要使用现有 VPC，请选择 Select an existing VPC to use with WorkDocs，然后输入以下值。

VPC
在其中创建目录的 VPC。

Subnets
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。如果您选择 No Preference，则将随机选择两个不同的子网。

5. 查看目录信息并进行必要的更改。如果信息正确，请单击 Create Directory。

   创建目录和 Amazon WorkDocs 站点需要几分钟的时间。成功创建目录之后，站点的 Status 值将更改为 Active。

# 连接到您的本地目录

Amazon WorkDocs 使用 AWS Directory Service AD Connector 目录连接到您的本地目录。要使用 AD Connector 连接到您的本地目录，您必须满足在 *AWS Directory Service Administration Guide* 的 AD Connector 先决条件中标识的先决条件。

要连接到您的本地目录，请执行以下步骤。

连接到您的本地目录

1. 开启 Amazon WorkDocs 控制台，使用 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 页。
2. 如果您在 Amazon WorkDocs 起始页上，请执行以下步骤：

   1. 单击 Get Started Now。
   2. 在 Get Started with WorkDocs 页上，单击 Standard Setup 下方的 Launch。

   如果您在 Manage Your WorkDocs Sites 页上，请执行下列步骤：

   1. 单击 Create a New WorkDocs Site。
   2. 在 Get Started with WorkDocs 页上，单击 Standard Setup 下方的 Launch。

3. 在 Set up a Directory 页中，单击 Create AD Connector。

4. 输入以下值，然后单击 Continue。

   在 Directory Details 部分中输入以下值：

   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账户。用户账户不能包含在父目录中，例如 `example.com`。

   NetBIOS Name
   内部目录的 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。

   在 Access Point 部分中输入以下值：

   区域
   验证区域。

   Site URL
   输入您的 Amazon WorkDocs 站点的 URL。

   在 VPC Configuration 部分中输入以下值：

   VPC
   目录连接到的 VPC。

   Subnets
   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. 查看目录信息并进行必要的更改。如果信息正确，请单击 Connect Directory。

   连接目录和创建 Amazon WorkDocs 站点需要几分钟的时间。成功连接目录之后，站点的 Status 值将更改为 `Active`。

# Amazon WorkDocs 管理

大多数 Amazon WorkDocs 管理工作都是在 Amazon WorkDocs Web 应用程序的管理控制面板中执行的，而 Amazon WorkDocs 控制台用于管理 Amazon WorkDocs 目录和站点。

Topics



# Amazon WorkDocs 控制台

Amazon WorkDocs 控制台用于管理 Amazon WorkDocs 目录和站点。可以使用 Amazon WorkDocs 控制台执行以下操作：

Topics



## 创建或连接到目录

您可以使用 Amazon WorkDocs 控制台创建云目录或连接到本地目录。有关在云中创建目录的更多信息，请参阅创建 Simple AD 目录 (p. 7)。有关连接到本地目录的更多信息，请参阅连接到您的本地目录 (p. 9)。

## 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。用户必须是活动用户才能被提升。有关激活用户的更多信息，请参阅修改用户 (p. 18)。

将用户提升为管理员

1. 开启 Amazon WorkDocs 控制台，使用 https://console.aws.amazon.com/zocalo/ 。
2. 在 Manage Your WorkDocs Sites 页中，选择所需目录，选择 Actions 和 Set an Administrator。

3. 在 Set WorkDocs Administrator 页中，输入要提升的用户名并选择 Set Administrator。

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 修改用户 (p. 18)。

# 删除站点

使用 Amazon WorkDocs 控制台可以删除 Amazon WorkDocs 站点。

Warning

删除站点会导致丢失所有用户信息和所有文件。您只应在绝对确定不再需要此信息的情况下删除站点。

### 删除站点

1. 开启 Amazon WorkDocs 控制台，使用 https://console.aws.amazon.com/zocalo/ 。
2. 在 Manage Your WorkDocs Sites 页中，选择所需站点，选择 Actions 和 Delete WorkDocs Site。
3. 在 Delete Selected WorkDocs Site 对话框中，选择您是否还希望删除用户目录。这将删除用于存储 Amazon WorkDocs 用户信息的 AWS Directory Service Simple AD 或 AD Connector 目录。如果您希望删除目录，则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 *AWS Directory Service Administration Guide* 中的删除简单 AD 目录或删除 AD Connector 目录。
4. 确认您删除的是正确的站点，在确认字段中输入 `DELETE`，然后选择 Delete WorkDocs Site。

   站点将立即被删除且不再可用。

# 多重验证

您可以通过执行以下过程为 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. 开启 Amazon WorkDocs 控制台，使用 https://console.aws.amazon.com/zocalo/ 。
2. 在 Manage Your WorkDocs Sites 页中，选择所需站点，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。可以输入多个 IP 地址（用逗号将其分隔开），例如 `192.0.0.0,192.0.0.12`。

   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）。此值必须介于 1 和 60 之间。

最大重试次数
将尝试与 RADIUS 服务器通信的次数。此值必须介于 0 和 10 之间。

当 RADIUS Status 更改为 Enabled 时，多重验证将可用。在设置多重验证的过程中，您的用户将无法登录到其 Amazon WorkDocs 站点。

## 单点登录

AWS Directory Service 使您的用户能够从已加入 Amazon WorkDocs 所注册到的相同目录的计算机来访问 Amazon WorkDocs，而无需单独输入其凭证。有关为您的目录启用单点登录的信息，请参阅 *AWS Directory Service Administration Guide* 中的单点登录。

您的 Amazon WorkDocs 用户可能需要修改其 Web 浏览器设置来启用单点登录。有关更多信息，请参阅 *Amazon WorkDocs User Guide* 中的启用单点登录。

# Amazon WorkDocs 管理控制面板

使用管理控制面板可以管理您的 Amazon WorkDocs 站点。该管理控制面板对 Amazon WorkDocs Web 应用程序中的 Amazon WorkDocs 管理员可用。要访问该管理控制面板，请打开您站点的 Amazon WorkDocs Web 应用程序，然后单击用户控制窗格中的 Administration。

根据您使用的是云目录还是已连接的目录，管理控制面板会有所不同。

Topics



## 用户角色

Amazon WorkDocs 定义以下用户角色。

WS 用户
具有已分配的 Amazon WorkSpaces 工作区的用户。
- 可访问所有 Amazon WorkDocs 功能
- 50 GB 存储限制
- 无月度费用

升级的 WS 用户
具有已分配的 Amazon WorkSpaces 工作区且已升级的用户。
- 可访问所有 Amazon WorkDocs 功能
- 200 GB 默认存储限制（200 GB 以外的存储按实际使用量付费）
- 需支付月度费用

Amazon WorkDocs 用户
: 未分配有 Amazon WorkSpaces 工作区的任何活动 Amazon WorkDocs 用户。
  - 可访问所有 Amazon WorkDocs 功能
  - 200 GB 默认存储限制（200 GB 以外的存储按实际使用量付费）
  - 需支付月度费用

有关升级或降级 Amazon WorkSpaces 用户的更多信息，请参阅云目录用户 (p. 18)和已连接目录用户 (p. 20)。

# 协作权限

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。

Topics



## 角色

文件夹权限和文件权限均根据用户角色来授予。以下是 Amazon WorkDocs 定义的、适用于文件夹的角色：

- 文件夹所有者 – 文件夹或文件的所有者。
- 文件夹共有者 – 由所有者指定为文件夹或文件共有者的用户或群组。
- 文件夹参与者 – 与之共享文件夹的某个用户，对文件夹访问权限没有限制。
- 文件夹查看者 – 与之共享文件夹的某个用户，但是向其提供对文件夹的有限访问权限（仅查看）。

以下角色适用于文件：

- 所有者 – 文件的所有者。
- 共有者 – 由所有者指定为文件共有者的用户或群组。
- 参与者 – 要求其提供有关文件的反馈的某个用户。
- 查看者 – 与之共享文件的某个用户，但是向其提供了对文件的有限访问权限（仅查看）。
- 匿名查看者–组织之外的非注册用户，可以查看通过外部查看链接共享的文件。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

以下是 Amazon WorkDocs 为共享文件夹定义的权限：

- 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 – 查看与之共享文件夹的其他用户。
- 添加子文件夹 – 添加子文件夹。
- 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 |
| 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 | | | |

## 文件权限

以下是 Amazon WorkDocs 为不在共享文件夹中的文件定义的权限：

- 查看 – 查看文件。
- 删除 – 删除文件。
- 注释 – 可以向文件添加反馈。
- 查看共享 – 查看与之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。可以在文件属性中允许或拒绝下载共享文件的能力。
- 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 | | |
| 查看活动 | X | X | | |

| 许可 | 所有者/共有者 | 贡献者 | 查看者 | 匿名查看者 |
|---|---|---|---|---|
| 查看版本 | X | X | | |
| 上传 | X | X | | |
| 删除 | X | | | |
| 禁止下载 | X | | | |
| 共享 | X | | | |
| 撤销共享 | X | | | |

## 共享文件权限

以下是 Amazon WorkDocs 为不在共享文件夹中的文件定义的权限：

- 查看 – 查看共享文件夹中的文件。
- 查看共享 – 查看与之共享文件的其他用户。
- 下载 – 下载文件。
- 注释 – 可以向文件添加反馈。
- 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。

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 | | |
| 删除 | X | X | X | | |
| 禁止下载 | 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 |
|---|---|---|---|---|---|
| 共享 | X | X | | | |
| 撤销共享 | X | X | | | |

* - 文件所有者，在这种情况下是将文件原始版本上传到与其他用户共享的文件夹中的人员。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。

# 匿名查看者

您可以配置您的组织，以便邀请匿名用户查看文件。匿名查看者无法下载文件，也不能对文件提供反馈。

要支持匿名查看者，必须满足以下条件：

- 组织的 External Share Settings 必须设置为 Users can send external view links to anyone。有关 Simple AD 目录，请参阅安全性 (p. ?)。有关 AD Connector 目录，请参阅安全性 (p. ?)。
- 组织的 Invite Settings 必须设置为 Only administrators can invite new users。

如果满足上述所有条件，Amazon WorkDocs 用户便能邀请匿名查看者查看文档，方式是在该用户发送邀请时输入匿名查看者的电子邮件地址。

# 云目录

在云目录的管理控制面板中，可以管理以下各项：

Topics

- 存储 (p. 17)
- 安全性 (p. 17)
- 云目录用户 (p. 18)

## 存储

在 Storage 部分中，可以指定新用户接收的存储量。要更改此设置，请选择 Storage 部分中的 Change。在 Storage Limit 对话框中，为新用户提供无限量存储或限制用户仅可使用特定量的存储。此设置仅影响在设置发生更改后添加的用户。它不会更改已分配给现有用户的存储量。要更改现有用户的存储限制，请参阅修改用户 (p. 18)。

## 安全性

在 Security 部分中，您可以指定以下内容：

Topics

- 外部共享设置 (p. 17)
- 邀请设置 (p. 18)

### 外部共享设置

指定用户是否能将文件查看链接发送给组织外部人员。从以下设置中进行选择：

Users can send external view links to anyone
: 用户可以将链接发送给组织外部的任何人员。

Users can send external view links to a few specific domains
: 用户可以将链接发送给作为指定域成员的人员。

Users cannot send external view links
: 用户无法将查看链接发送给组织外部的任何人。

### 邀请设置

指定用户如何将新用户邀请到云组织（如果适用）。对于云目录，请从以下设置进行选择：

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新成员共享文件或文件夹来邀请这些新成员。

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。

Only administrators can invite new users
: 用户无法邀请新用户。

## 云目录用户

在云目录的 Manage Users 部分中，您可以执行以下任务：

Topics



### 邀请新用户

对于云目录，您可以邀请新用户加入您的目录。要将新用户邀请到云目录，请执行以下步骤：

1. 在 Manage Users 部分中，选择 Invite Users。
2. 在 Invite Users 对话框的 Who would you like to invite 字段中输入要邀请的人员的电子邮件地址，然后按 Enter。对要邀请的每个人员重复此步骤。
3. 输入自定义主题和消息正文（如果需要），然后选择 Send。将向每个收件人发送邀请电子邮件，其中包含有关如何创建其 Amazon WorkDocs 账户的说明。

### 修改用户

您可以通过单击用户名称旁边的铅笔图标（ ）来修改现有用户。

在 Edit User 对话框中，您可以更改以下设置：

名
: 用户的名字。

姓
: 用户的姓氏。

状态
: 指定用户是活动的还是不活动的。

角色
: 指定该用户是用户还是管理员。您也可以升级或降级已分配有 Amazon WorkSpaces 工作区的用户。有关更多信息，请参阅 用户角色 (p. 13)。

存储
: 指定现有用户的存储限制。

### 删除用户

使用 Amazon WorkDocs 管理控制面板，您只能删除尚未创建其 Amazon WorkDocs 账户的云用户。要删除这些用户之一，请选择用户名旁边的垃圾桶图标（ ）。

建议您不要删除已注册用户。相反，您应该停用用户，使其无法访问您的 Amazon WorkDocs 站点。有关停用用户的更多信息，请参阅修改用户 (p. 18)。

您的 Amazon WorkDocs 站点必须始终具有至少一名活动用户。如果要删除所有用户，必须删除整个 Amazon WorkDocs 站点。

## 连接的目录

在连接的目录的管理控制面板中，可以管理以下各项：

Topics

- 存储 (p. 19)
- 安全性 (p. 19)
- 已连接目录用户 (p. 20)

## 存储

在 Storage 部分中，可以指定新用户接收的存储量。要更改此设置，请选择 Storage 部分中的 Change。在 Storage Limit 对话框中，为新用户提供无限量存储或限制用户仅可使用特定量的存储。此设置仅影响在设置发生更改后启用的用户。它不会更改已分配给当前启用的用户的存储量。要更改已启用的用户的存储限制，请参阅修改用户 (p. 20)。

## 安全性

在 Security 部分中，您可以指定以下内容：

Topics

- 外部共享设置 (p. 19)
- 邀请设置 (p. 20)

### 外部共享设置

指定用户是否能将文件查看链接发送给组织外部人员。从以下设置中进行选择：

Users can send external view links to anyone
: 用户可以将链接发送给组织外部的任何人员。

Users can send external view links to a few specific domains
: 用户可以将链接发送给作为指定域成员的人员。

Users cannot send external view links
: 用户无法将查看链接发送给组织外部的任何人。

### 邀请设置

对于连接的目录，您不能邀请新用户加入您的目录，而只能启用目录中现有的用户来使用 Amazon WorkDocs。对于连接的目录，请从以下设置进行选择：

Users can enable new people from your directory by sharing files or folders with them
: 用户可以允许您的目录中已存在的人员使用 Amazon WorkDocs，方式是与这些人员共享文件或文件夹。

Only administrators can enable new users
: 只有 Amazon WorkDocs 管理员才能允许新用户使用 Amazon WorkDocs。

## 已连接目录用户

在已连接目录的 Manage Users 部分中，您可以执行以下任务：

Topics

- 启用用户 (p. 20)
- 修改用户 (p. 20)

### 启用用户

对于连接的目录，您不能邀请新用户加入您的目录，但可以允许目录中现有的用户使用 Amazon WorkDocs。有关启用用户的更多信息，请参阅修改用户 (p. 20)。

### 修改用户

您可以通过选择用户名旁边的铅笔图标（ ）来修改现有用户。

在 Edit User 对话框中，您可以更改以下设置：

状态
: 指定用户是活动的还是不活动的。

角色
: 指定该用户是用户还是管理员。您也可以升级或降级已分配有 Amazon WorkSpaces 工作区的用户。有关更多信息，请参阅 用户角色 (p. 13)。

存储
: 指定现有用户的存储限制。

# Amazon WorkDocs 限制

Abstract

## Amazon WorkDocs 资源限制是什么？

下面是 Amazon WorkDocs 的默认限制。除非另有说明，否则每个区域具有各自的限制。

Amazon WorkDocs 限制

| 资源 | 默认限制 |
| --- | --- |
| Simple AD 目录 | 2 |
| AD Connector 目录 | 2 |

# 使用 AWS CloudTrail 记录 Amazon WorkDocs API 调用

Amazon WorkDocs 与 CloudTrail 集成，后者是一种服务，它在 AWS 账户中捕获 Amazon WorkDocs 或代表 Amazon WorkDocs 发出的 API 调用，并将日志文件提交到您指定的 &S3; 存储桶。CloudTrail 从 Amazon WorkDocs 控制台捕获 API 调用。通过使用 CloudTrail 收集的信息，您可以确定对 Amazon WorkDocs 发出了什么请求、发出请求的源 IP 地址、何人发出的请求以及发出请求的时间等。有关 CloudTrail 的更多信息，包括如何对其进行配置和启用，请参阅 *AWS CloudTrail User Guide*。

## CloudTrail 中的 Amazon WorkDocs 信息

在您的 AWS 账户中启用 CloudTrail 日志记录后，将在日志文件中跟踪对 Amazon WorkDocs 操作进行的 API 调用。Amazon WorkDocs 记录与其他 AWS 服务记录一起写入日志文件中。CloudTrail 基于时间段和文件大小来确定何时创建新文件并向其写入内容。

每个日志条目都包含有关生成请求的人员的信息。日志中的用户身份信息有助于确定发出的请求是否具有根或 IAM 用户证书，是否具有角色或联合用户的临时安全证书，或者是否是由其他 AWS 服务发出的。有关更多信息，请参阅 CloudTrail 事件参考中的 userIdentity 字段。

日志文件可以在存储桶中存储任意长时间，不过您也可以定义 Amazon S3 生命周期规则以自动存档或删除日志文件。默认情况下，将使用 Amazon S3 服务器端加密 (SSE) 对日志文件进行加密。

如果需要针对日志文件传输快速采取措施，可选择让 CloudTrail 在传输新日志文件时发布 Amazon SNS 通知。有关更多信息，请参阅配置 Amazon SNS 通知。

您也可以将多个 AWS 区域和多个 AWS 账户的 Amazon WorkDocs 日志文件聚合到单个 Amazon S3 存储桶中。有关更多信息，请参阅将 CloudTrail 日志文件聚合到单个 Amazon S3 存储桶中。

## 了解 Amazon WorkDocs 日志文件条目

CloudTrail 日志文件可包含一个或多个日志条目，每个条目由多个 JSON 格式的事件组成。一个日志条目表示来自任何源的一个请求，包括有关所请求的操作、所有参数以及操作的日期和时间等信息。日志条目不一定具有任何特定顺序。也就是说，它们不是公用 API 调用的有序堆栈跟踪。

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。二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，而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 的两个 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" : "<username>"
      },
      "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" : "<username>"
      },
      "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>"
    }
  ]
}
```

# 文档历史记录

Abstract

查找 Amazon WorkDocs 的文档的修订日期、相关版本和重要更改。

下表介绍了对 *Amazon WorkDocs 管理指南* 的重要补充。我们还经常更新文档来处理您发送给我们的反馈意见。

- 文档最新更新时间：2015 年 3 月 31 日

| 修改 | 描述 | 修改日期 |
| --- | --- | --- |
| 增加了单点登录支持 | 增加了用于支持单点登录的文档。有关更多信息，请参阅单点登录 (p. 13)。 | 2015 年 3 月 31 日 |
| 多重验证支持。 | 添加多重验证信息。 | 2014 年 11 月 3 日 |
| 首次发布 | *Amazon WorkDocs 管理指南*的初始版本。 | 2014 年 7 月 10 日 |