管理指南

Amazon WorkDocs

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon WorkDocs: 管理指南

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

..... vi
什么是亚马逊 WorkDocs？ 1
正在访问 WorkDocs 1
定价 1
如何开始 2
将数据迁出 WorkDocs 3
方法 1：批量下载文件 3
从网络下载文件 3
从 Web 下载文件夹 4
使用 WorkDocs 云端硬盘下载文件和文件夹 5
方法 2：使用迁移工具 5
先决条件 6
限制 9
运行迁移工具 9
从 Amazon S3 下载迁移的数据 13
迁移疑难解答 14
查看您的迁移历史记录 14
先决条件 15
注册获取 AWS 账户 15
创建具有管理访问权限的用户 15
安全性 17
身份和访问管理 18
受众 18
使用身份进行身份验证 18
使用策略管理访问 20
亚马逊如何 WorkDocs 使用 IAM 23
基于身份的策略示例 25
故障排除 29
日志记录和监控 30
导出站点范围活动源 31
CloudTrail 日志记录 31
合规性验证 34
恢复能力 35
基础结构安全性 35

入门 ... 37
创建 WorkDocs 网站 ... 37
开始前的准备工作 ... 38
创建 WorkDocs 网站 ... 38
启用单点登录 ... 40
启用多重验证 ... 40
将用户提升为管理员 ... 41
通过 AWS 控制 WorkDocs 台进行管理 ... 42
设置站点管理员 ... 42
重新发送邀请电子邮件 ... 42
管理多重身份验证 ... 43
设置网站 URLs ... 43
管理通知 ... 44
删除站点 ... 45
WorkDocs 从站点管理员控制面板进行管理 ... 47
将 WorkDocs 云端硬盘部署到多台计算机 ... 54
邀请和管理用户 ... 55
用户角色 ... 55
启动管理员控制面板 ... 57
关闭自动激活功能 ... 57
管理链接共享 ... 58
在启用自动激活功能的情况下控制用户邀请 ... 59
邀请新用户 ... 59
编辑用户 ... 60
禁用用户 ... 61
删除待处理用户 ... 62
移交文档所有权 ... 62
下载用户列表 ... 63
共享与协作 ... 64
共享链接 ... 64
通过邀请共享 ... 64
外部共享 ... 65
权限 ... 65
用户角色 ... 65
共享文件夹的权限 ... 66
共享文件夹中的文件的权限 ... 67

不在共享文件夹中的文件的权限 70
允许协作编辑 72
启用 Hancom ThinkFree 72
启用“使用 Office Online 打开”功能 73
迁移文件 74
步骤 1：准备要迁移的内容。 75
步骤 2：将文件上传到 Amazon S3 75
步骤 3：计划迁移 76
步骤 4：跟踪迁移 78
步骤 5：清理资源 78
故障排除 80
无法在特定 AWS 地区设置我的 WorkDocs 网站 80
想在现有 Amazon VPC 中设置我的 WorkDocs 网站 80
用户需要重置密码 80
用户意外共享了一个敏感文档 80
用户离开了组织，没有移交文档所有权 80
需要将 WorkDocs 云端硬盘或 WorkDocs 配套部署给多个用户 81
在线编辑不起作用 47
管理亚马逊 WorkDocs 企业采购商城 82
要添加到允许列表的 IP 地址和域 84
文档历史记录 85

注意：亚马逊 WorkDocs不再提供新买家注册和账户升级服务。在此处了解迁移步骤：如何从中迁移数据 WorkDocs。

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。

什么是亚马逊 WorkDocs？

Amazon WorkDocs 是一项完全托管、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，可提高用户的工作效率。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。 WorkDocs 客户端应用程序可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。 WorkDocs 支持所有常见的文档和图像格式，并且不断添加对其他媒体类型的支持。

有关更多信息，请参阅 Amazon WorkDocs。

正在访问 WorkDocs

管理员使用WorkDocs 控制台创建和停用 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 WorkDocs 从站点管理员控制面板进行管理 和邀请和管理 WorkDocs 用户。

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 WorkDocs 控制台或管理仪表板。WorkDocs 提供了几种不同的客户端应用程序和实用程序：

- 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。
- WorkDocs 云端硬盘，一款将 macOS 或 Windows 桌面上的文件夹与 WorkDocs 文件同步的应用程序。

有关用户如何下载 WorkDocs 客户端、编辑其文件和使用文件夹的更多信息，请参阅《WorkDocs 用户指南》中的以下主题：

- 入门 WorkDocs
- 处理文件
- 使用文件夹

定价

使用 WorkDocs，无需预付费用或承诺。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 WorkDocs，请参阅创建 WorkDocs 网站。

将数据迁出 WorkDocs

WorkDocs 提供了两种将数据迁出 WorkDocs 站点的方法。本节概述了这些方法，并提供了有关运行、故障排除和优化每种迁移方法的详细步骤的链接。

客户将有两种选择将其数据从亚马逊上移出 WorkDocs：现有的批量下载功能（方法 1）或我们新的数据迁移工具（方法 2）。以下主题说明如何使用这两种方法。

主题

- 方法 1：批量下载文件
- 方法 2：使用迁移工具

方法 1：批量下载文件

如果您想控制要迁移哪些文件，可以手动批量下载它们。此方法允许您只选择所需的文件并将其下载到其他位置，例如本地驱动器。您可以从 WorkDocs 网站或 WorkDocs 云端硬盘下载文件和文件夹。

请记住以下事项：

- 您的网站用户可以按照下面列出的步骤下载文件。如果你愿意，你可以设置一个共享文件夹，让用户将文件移到该文件夹，然后将该文件夹下载到其他位置。您也可以将所有权转让给自己并进行下载。
- 要下载带注释的 Microsoft Word 文档，请参阅《WorkDocs 用户指南》中的 “下载带有反馈的 Word 文档”。
- 您必须使用 WorkDocs 云端硬盘下载大于 5 GB 的文件。
- 当您使用 WorkDocs 云端硬盘下载文件和文件夹时，您的目录结构、文件名和文件内容将保持不变。不保留文件所有权、权限和版本。

从网络下载文件

在以下情况下，您可以使用此方法下载文件：

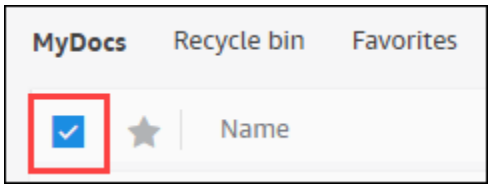
- 您只想从网站下载部分文件。
- 你想下载带有注释的 Word 文档，并将这些评论留在各自的文档中。迁移工具会下载所有注释，但会将其写入单独的 XML 文件中。然后，网站用户可能无法将评论与其 Word 文档关联起来。

从 Web 下载文件

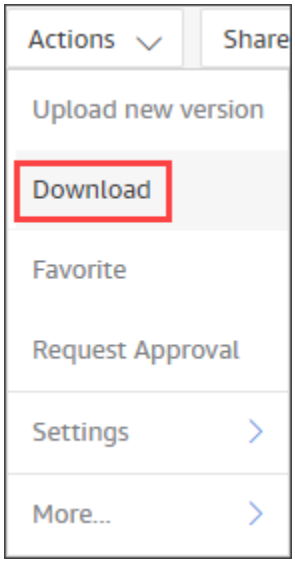
1. 登录到 WorkDocs。
2. 根据需要，打开包含要下载的文件的文件夹。
3. 选中要下载的文件旁边的复选框。

   -或-

   选中列表顶部的复选框以选择该文件夹中的所有文件。



4. 打开 “操作” 菜单并选择 “下载”。 。



在 PC 上，默认情况下，下载的文件以 Downl oadsWorkDocsDownloads//文件夹名称存放。在 Macintosh 上，默认情况下，文件以硬盘驱动器名称 /Users/ 用户名/存放。WorkDocsDownloads

从 Web 下载文件夹

> **Note**
>
> 当你下载文件夹时，你还会下载文件夹中的所有文件。如果您只想下载某个文件夹中的某些文件，请将不需要的文件移到其他位置或回收站，然后下载该文件夹。

从 Web 下载文件夹

1. 登录到 WorkDocs
2. 选中要下载的每个文件夹旁边的复选框。

   -或-

   打开文件夹，然后选中要下载的任何子文件夹旁边的复选框。
3. 打开 “操作” 菜单并选择 “下载”。 。

   在 PC 上，默认情况下，下载的文件夹以 Downl oadsWorkDocsDownloads//文件夹名称存放。在 Macintosh 上，默认情况下，文件以硬盘驱动器名称 /Users/ 用户名/存放。WorkDocsDownloads

使用 WorkDocs 云端硬盘下载文件和文件夹

> **Note**
>
> 您必须安装 WorkDocs 云端硬盘才能完成以下步骤。有关更多信息，请参阅《WorkDocs 云端硬盘用户指南》中的 “安装WorkDocs 云端硬盘”。

从 WorkDocs 云端硬盘下载文件和文件夹

1. 启动 “文件资源管理器” 或 “访达”，然后打开 W: 驱动器。
2. 选择要下载的文件夹或文件。
3. 点击并按住（右键单击）所选项目并选择 “复制”，然后将复制的项目粘贴到新位置。

   -或-

   将所选项目拖到其新位置。
4. 从 WorkDocs 云端硬盘中删除原始文件。

方法 2：使用迁移工具

当你想将 WorkDocs 所有数据迁出 WorkDocs 站点时，你可以使用迁移工具。

迁移工具将数据从站点移动到 Amazon 简单存储服务存储桶。该工具为每个用户创建一个压缩的 ZIP 文件。压缩文件包括您 WorkDocs 站点上每个最终用户的所有文件和文件夹、版本、权限、评论和注释。

主题

- 先决条件
- 限制
- 运行迁移工具
- 从 Amazon S3 下载迁移的数据
- 迁移疑难解答
- 查看您的迁移历史记录

先决条件

要使用迁移工具，必须具备以下物品。

- Amazon S3 存储桶。有关创建 Amazon S3 存储桶的信息，请参阅 Amazon S3 用户指南中的创建存储桶。您的存储桶必须使用相同的 IAM 账户，并且与您的 WorkDocs 网站位于同一区域。此外，您还必须阻止对存储桶的公开访问。有关执行此操作的更多信息，请参阅 Amazon S3 用户指南中的阻止公众访问您的 Amazon S3 存储。

  要授予上传文件的 WorkDocs 权限，请配置存储桶策略，如以下示例所示。该策略使用`aws:SourceAccount`和`aws:SourceArn`条件键来缩小策略的范围，这是一种安全最佳实践。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowWorkDocsFileUpload",
            "Effect": "Allow",
            "Principal": {
                "Service": "workdocs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::BUCKET-NAME/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "AWS-ACCOUNT-ID"
                },
```

```
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:workdocs:REGION:AWS-ACCOUNT-
ID:organization/WORKDOCS-DIRECTORY-ID"
                }
            }
        }
    ]
}
```

> **Note**
>
> - *WORKDOCS-DIRECTORY-ID*是您 WorkDocs 网站的组织 ID。这可以在 AWS WorkDocs 控制台的 “我的网站” 表中找到
> - 有关配置存储桶策略的更多信息，请参阅使用 Amazon S3 控制台添加存储桶策略

- IAM 策略。要在 WorkDocs 控制台上开始迁移，IAM 调用委托人的权限集必须附加以下策略：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowStartWorkDocsMigration",
            "Effect": "Allow",
            "Action": [
                "workdocs:StartInstanceExport"
            ],
            "Resource": [
                "arn:aws:workdocs:REGION:AWS-ACCOUNT-ID:organization/WORKDOCS-
DIRECTORY-ID"
            ]
        },
        {
            "Sid": "AllowDescribeWorkDocsMigrations",
            "Effect": "Allow",
            "Action": [
                "workdocs:DescribeInstanceExports",
                "workdocs:DescribeInstances"
            ],
            "Resource": [
                "*"
            ]
        },
```

```
        {
            "Sid": "AllowS3Validations",
            "Effect": "Allow",
            "Action": [
                "s3:HeadBucket",
                "s3:ListBucket",
                "s3:GetBucketPublicAccessBlock",
                "kms:ListAliases"
            ],
            "Resource": [
                "arn:aws:s3:::BUCKET-NAME"
            ]
        },
        {
            "Sid": "AllowS3ListMyBuckets",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

- 或者，您可以使用 AWS KMS 密钥对存储桶中的静态数据进行加密。如果您不提供密钥，则应用存储桶的标准加密设置。有关更多信息，请参阅《密AWS 钥管理服务开发人员指南》中的创建密钥。

  要使用 AWS KMS 密钥，请在 IAM 策略中添加以下语句。必须使用 SYMMETRIC_DEFAULT 类型的活动密钥。

```
{
    "Sid": "AllowKMSMigration",
     "Effect": "Allow",
     "Action": [
         "kms:CreateGrant",
         "kms:DescribeKey"
     ],
     "Resource": [

         "arn:aws:kms:REGION:AWS-ACCOUNT-ID:key/KEY-RESOURCE-ID"
     ]
```

```
}
```

限制

迁移工具有以下限制：

- 该工具将所有用户权限、评论和注释写入单独的 CSV 文件中。您必须手动将该数据映射到相应的文件。
- 您只能迁移活动站点。
- 该工具限制每个站点每 24 小时成功迁移一次。
- 您不能运行同一个站点的并行迁移，但可以为不同的站点运行并行迁移。
- 每个 zip 文件的最大容量为 50GB。数据量超过 50GB 的用户 WorkDocs 将有多个 zip 文件导出到 Amazon S3 中。
- 该工具不会导出大于 50 GB 的文件。该工具会列出与 ZIP 文件具有相同前缀的 CSV 文件中所有大于 50 GB 的文件。例如，/workdocs///skippedFiles.csv ***site-alias***。***created-timestamp-UTC***您可以通过编程或手动方式下载列出的文件。有关以编程方式下载的信息https://docs.aws.amazon.com/workdocs/latest/developerguide/download-documents.html，请参阅《WorkDocs 开发人员指南》中的。有关手动下载文件的信息，请参阅本主题前面的 “方法 1” 中的步骤。
- 每个用户的 zip 文件将仅包含他们拥有 and/or 的文件文件夹。与用户共享的所有文件 and/or 文件夹都将位于拥有这些文件 and/or 文件夹的用户的 zip 文件中。
- 如果中的某个文件夹为空（不包含嵌套文件/文件夹） WorkDocs，则不会将其导出。
- 不能保证在迁移任务启动后创建的任何数据（文件、文件夹、版本、注释、注释）都将包含在 S3 的导出数据中。
- 您可以将多个站点迁移到一个 Amazon S3 存储桶。您无需为每个站点创建一个存储桶。但是，您必须确保您的 IAM 和存储桶策略允许多个站点。
- 迁移会增加 Amazon S3 的成本，具体取决于您迁移到存储桶的数据量。有关更多信息，请参阅 Amazon S3 定价页面。

运行迁移工具

以下步骤说明了如何运行 WorkDocs 迁移工具。

迁移站点

1. 打开 WorkDocs 控制台，网址为https://console.aws.amazon.com/zocalo/。
2. 在导航窗格中，选择我的站点，然后选择要迁移的站点旁边的单选按钮。
3. 打开操作列表并选择迁移数据。
4. 在迁移数据站点名称页面上，输入您的 Amazon S3 存储桶的 URI。

   -或-

   选择 “浏览 S3”，然后按照以下步骤操作：

   a. 根据需要，搜索存储桶。
   b. 选择存储桶名称旁边的单选按钮，然后选择选择。
5. （可选）在 “通知” 下，最多输入五个电子邮件地址。该工具向每个收件人发送迁移状态电子邮件。
6. （可选）在 “高级设置” 下，选择 KMS 密钥来加密您存储的数据。
7. **`migrate`**在文本框中输入以确认迁移，然后选择开始迁移。

   将出现一个指示器，显示迁移的状态。迁移时间会有所不同，具体取决于站点中的数据量。

Migrate Data: your-workdocs-site-alias

This action will transfer all folders and files (along with file versions) from the WorkDocs site data-migration-pentest-2 to the designated S3 bucket. Any file comments, annotations, and permissions will be preserved in a separate file.

The data for all users on the WorkDocs site will be compressed (zipped) and made available for download from S3. Your migrated data will be available in S3 and can be accessed via the AWS CLI, the AWS SDKs, or the Amazon S3 Console. Note that pricing for storage at the S3 URI destination will be subject to the pricing and terms available here. Please refer to the migration blog post to learn more about data migration.

Choose an S3 bucket

To start data migration, enter the S3 destination bucket URI. If you do not have a bucket, please visit the S3 console to ensure you have a bucket. Please configure the bucket permissions as described in the pre-requisites section here.

S3 URI

s3://your-properly-configured-bucket | View | Browse S3

Notifications [Optional]

Enter email addresses for notification recipients. These people will receive status updates on the migration.

person@domain.com

person@domain1.com | person@domain2.com

▼ **Advanced Settings**

Choose an AWS KMS key

We will use the chosen AWS KMS Key to encrypt the data once it is migrated to the designated S3 bucket. In the absence of a selected key, the compressed file on S3 will be encrypted using the standard SSE-S3 encryption.

arn:aws:kms:us-east-1:123456789123:key/123456789-abc1-def2-hij3 | Create an AWS KMS key

AWS KMS key details

Key ARN

arn:aws:kms:us-east-1:123456789123:key/123456789-abc1-def2-hij3-abc123456789

Key status

Enabled

Key aliases

your-kms-key-alias

▶ **Ongoing Migrations and History**

By clicking on "Migrate", you are directing Amazon WorkDocs to duplicate your selected data and transfer it to the S3 URI destination you provided which will be subject to S3 pricing. Once you have validated that the data is migrated, you can stop your WorkDocs billing by deleting the WorkDocs site. To delete WorkDocs site, please refer to these instructions.

To confirm migration, type **migrate** in the text input field.

迁移完成后：

- 该工具会向设置期间输入的地址发送 “成功” 电子邮件（如果有）。
- 您的亚马逊 S3 存储桶将包含一个 /workdocs***site-alias***///***created-timestamp-UTC***文件夹。该文件夹包含每个在网站上有数据的用户的压缩文件夹。每个压缩文件夹都包含用户的文件夹和文件，包括映射 CSV 文件的权限和注释。
- 如果用户在迁移之前删除了所有文件，则不会显示该用户的压缩文件夹。
- 版本-具有多个版本的文档具有 _ 版本 _ 创建时间戳标识符。时间戳使用纪元毫秒。例如，名为 “TestFile.txt” 且有两个版本的文档如下所示：

```
TestFile.txt (version 2 - latest version)
TestFile_version_1707437230000.txt
```

- 权限-以下示例显示了典型权限 CSV 文件的内容。

```
PathToFile,PrincipalName,PrincipalType,Role
/mydocs/Projects,user1@domain.com,USER,VIEWER
/mydocs/Personal,user2@domain.com,USER,VIEWER
/mydocs/Documentation/Onboarding_Guide.xml,user2@domain.com,USER,CONTRIBUTOR
/mydocs/Documentation/Onboarding_Guide.xml,user1@domain.com,USER,CONTRIBUTOR
/mydocs/Projects/Initiative,user2@domain.com,USER,CONTRIBUTOR
/mydocs/Notes,user2@domain.com,USER,COOWNER
/mydocs/Notes,user1@domain.com,USER,COOWNER
/mydocs/Projects/Initiative/Structures.xml,user3@domain.com,USER,COOWNER
```

- 评论-以下示例显示了典型评论 CSV 文件的内容。

```
PathToFile,PrincipalName,PostedTimestamp,Text
/mydocs/Documentation/
Onboarding_Guide.xml,user1@domain.com,2023-12-28T20:57:40.781Z,TEST ANNOTATION 1
/mydocs/Documentation/
Onboarding_Guide.xml,user2@domain.com,2023-12-28T22:18:09.812Z,TEST ANNOTATION 2
/mydocs/Documentation/
Onboarding_Guide.xml,user3@domain.com,2023-12-28T22:20:04.099Z,TEST ANNOTATION 3
/mydocs/Documentation/
Onboarding_Guide.xml,user1@domain.com,2023-12-28T20:56:27.390Z,TEST COMMENT 1
/mydocs/Documentation/
Onboarding_Guide.xml,user2@domain.com,2023-12-28T22:17:10.348Z,TEST COMMENT 2
```

```
/mydocs/Documentation/
Onboarding_Guide.xml,user3@domain.com,2023-12-28T22:19:42.821Z,TEST COMMENT 3
/mydocs/Projects/Agora/
Threat_Model.xml,user1@domain.com,2023-12-28T22:21:09.930Z,TEST ANNOTATION 4
/mydocs/Projects/Agora/
Threat_Model.xml,user1@domain.com,2023-12-28T20:57:04.931Z,TEST COMMENT 4
```

- 跳过的文件-以下示例显示了典型的跳过文件 CSV 文件的内容。为了提高可读性，我们缩短了 ID 并跳过了原因值。

```
FileOwner,PathToFile,DocumentId,VersionId,SkippedReason
user1@domain.com,/mydocs/LargeFile1.mp4,45e433b5469...,170899345...,The file is too
 large. Please notify the document owner...
user2@domain.com,/mydocs/LargeFile2.pdf,e87f725898c1...,170899696...,The file is too
 large. Please notify the document owner...
```

从 Amazon S3 下载迁移的数据

由于迁移会增加您的 Amazon S3 成本，因此您可以将迁移的数据从 Amazon S3 下载到其他存储解决方案。本主题介绍如何下载已迁移的数据，并提供了将数据上传到存储解决方案的建议。

> **Note**
>
> 以下步骤说明如何一次下载一个文件或文件夹。有关下载文件的其他方式的信息，请参阅 Amazon S3 用户指南中的下载对象。

要下载数据

1. 打开 Amazon S3 控制台，网址为 https://console.aws.amazon.com/s3/。
2. 选择目标存储桶并导航到网站别名。
3. 选中压缩文件夹旁边的复选框。

   -或-

   打开压缩文件夹，然后为单个用户选中该文件或文件夹旁边的复选框。
4. 选择下载。

存储解决方案建议

对于大型站点，我们建议使用合规的基于 Linux 的 Amazon 系统映像配置 EC2 实例，以编程方式从 Amazon S3 下载数据，解压缩数据，然后将其上传到存储提供商或本地磁盘。

迁移疑难解答

请尝试以下步骤以确保您的环境配置正确：

- 如果迁移失败，则 WorkDocs 控制台的 “迁移历史记录” 选项卡上会显示一条错误消息。查看错误消息。
- 检查您的亚马逊 S3 存储桶设置。
- 重新运行迁移。

如果问题仍然存在，请联系 AWS Support。包括位于迁移历史记录表中的 WorkDocs 站点 URL 和迁移 Job ID。

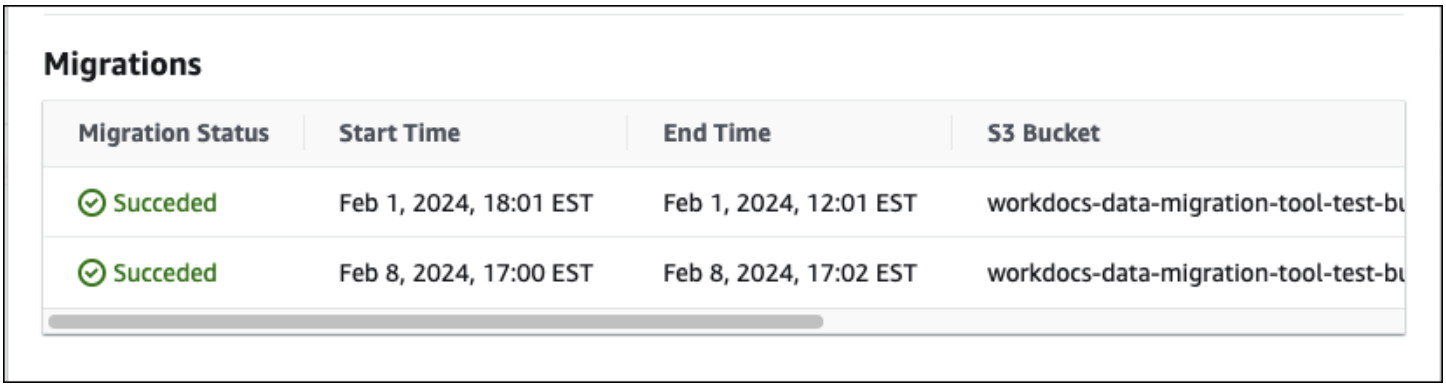
查看您的迁移历史记录

以下步骤说明了如何查看您的迁移历史记录。

查看您的历史记录

1. 打开 WorkDocs 控制台，网址为https://console.aws.amazon.com/zocalo/。
2. 选择所需 WorkDocs 站点旁边的单选按钮。
3. 打开操作列表并选择迁移数据。
4. 在 “迁移数据” 站点名称页面上，选择 “正在进行的迁移和历史记录”。

迁移历史记录显示在 “迁移” 下。下图显示了典型的历史记录。



Amazon 的先决条件 WorkDocs

要设置新 WorkDocs 站点或管理现有站点，必须完成以下任务。

注册获取 AWS 账户

如果您没有 AWS 账户，请完成以下步骤来创建一个。

要注册 AWS 账户

1. 打开https://portal.aws.amazon.com/billing/注册。
2. 按照屏幕上的说明操作。

   注册过程的一部分涉及接听电话或短信，并在电话键盘上输入验证码。

   当您注册时 AWS 账户，就会创建AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务 和资源。作为最佳安全实践，请为用户分配管理访问权限，并且只使用根用户来执行需要根用户访问权限的任务。

AWS 注册过程完成后会向您发送一封确认电子邮件。您可以随时前往 https://aws.amazon.com/并选择“我的账户”，查看当前账户活动并管理您的账户。

创建具有管理访问权限的用户

注册后，请保护您的安全 AWS 账户 AWS 账户根用户 AWS IAM Identity Center，启用并创建管理用户，这样您就不会使用 root 用户执行日常任务。

保护你的 AWS 账户根用户

1. 选择 Root 用户并输入您的 AWS 账户 电子邮件地址，以账户所有者的身份登录。AWS Management Console在下一页上，输入您的密码。

   要获取使用根用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的 Signing in as the root user。
2. 为您的根用户启用多重身份验证（MFA）。

   有关说明，请参阅 I A M 用户指南中的为 AWS 账户 根用户启用虚拟 MFA 设备（控制台）。

创建具有管理访问权限的用户

1. 启用 IAM Identity Center。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 Enabling AWS IAM Identity Center。

2. 在 IAM Identity Center 中，为用户授予管理访问权限。

   有关使用 IAM Identity Center 目录 作为身份源的教程，请参阅《用户指南》 IAM Identity Center 目录中的使用默认设置配置AWS IAM Identity Center 用户访问权限。

以具有管理访问权限的用户身份登录

- 要使用您的 IAM Identity Center 用户身份登录，请使用您在创建 IAM Identity Center 用户时发送到您的电子邮件地址的登录网址。

  有关使用 IAM Identity Center 用户登录的帮助，请参阅AWS 登录 用户指南中的登录 AWS 访问门户。

将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个权限集，该权限集遵循应用最低权限的最佳做法。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 Create a permission set。

2. 将用户分配到一个组，然后为该组分配单点登录访问权限。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 Add groups。

Amazon 的安全 WorkDocs

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 AWS 的责任。责任共担模式将其描述为云的 安全性和云中 的安全性：

- 云安全 — AWS 负责保护在 AWS 云中运行 AWS 服务的基础架构。 AWS 还为您提供可以安全使用的服务。作为 AWS 合规性计划的一部分，第三方审核人员将定期测试和验证安全性的有效性。要了解适用于亚马逊的合规计划 WorkDocs，请参阅合规计划范围内的AWS 服务。
- 云端安全 — 您使用的 AWS 服务决定了您的责任。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。本节中的主题可帮助您了解在使用分担责任模型时如何应用 WorkDocs。

> **Note**
>
> WorkDocs 组织中的用户可以通过发送文件链接或邀请来与该组织外部的用户协作。但是，这仅适用于使用 Active Directory 连接器的站点。查看您网站的共享链接设置，然后选择最符合贵公司要求的选项。

以下主题向您介绍如何进行配置 WorkDocs 以满足您的安全和合规性目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 WorkDocs 资源。

主题

- Amazon 的身份和访问管理 WorkDocs
- 在 Amazon 中记录和监控 WorkDocs
- Amazon 合规性验证 WorkDocs
- Amazon 的弹性 WorkDocs
- Amazon 的基础设施安全 WorkDocs

Amazon 的身份和访问管理 WorkDocs

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以进行身份验证（登录）和授权（有权限）使用 WorkDocs 资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- 亚马逊如何 WorkDocs 使用 IAM
- Amazon WorkDocs 基于身份的政策示例
- 对 Amazon WorkDocs 身份和访问进行故障排除

受众

您的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于您所做的工作 WorkDocs。

服务用户-如果您使用 WorkDocs 服务完成工作，则管理员会为您提供所需的凭证和权限。当你使用更多 WorkDocs 功能来完成工作时，你可能需要额外的权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 WorkDocs 中的特征，请参阅 对 Amazon WorkDocs 身份和访问进行故障排除。

服务管理员-如果您负责公司的 WorkDocs 资源，则可能拥有完全访问权限 WorkDocs。您的工作是确定您的服务用户应访问哪些 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。要详细了解您的公司如何将 IAM 与配合使用 WorkDocs，请参阅亚马逊如何 WorkDocs 使用 IAM。

IAM 管理员：如果您是 IAM 管理员，您可能希望了解如何编写策略以管理对 WorkDocs 的访问权限的详细信息。要查看您可以在 IAM 中使用的 WorkDocs 基于身份的策略示例，请参阅。Amazon WorkDocs 基于身份的政策示例

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 AWS 账户根用户任 IAM 角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （IAM Identity Center）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的如何登录到您 AWS 账户的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅《IAM 用户指南》中的用于签署 API 请求的AWS 签名版本 4。

无论使用何种身份验证方法，您都可能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《AWS IAM Identity Center 用户指南》中的多重身份验证和《IAM 用户指南》中的 IAM 中的AWS 多重身份验证。

IAM 用户和群组

I AM 用户是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的用例，应在需要时更新访问密钥。

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，您可以拥有一个名为的群组，IAMAdmins并向该群组授予管理 IAM 资源的权限。

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 IAM 用户的使用案例。

IAM 角色

I AM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。要在中临时担任 IAM 角色 AWS Management Console，您可以从用户切换到 IAM 角色（控制台）。您可以通过调用 AWS CLI 或 AWS API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的代入角色的方法。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问：要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关用于联合身份验证的角色的信息，请参阅《IAM 用户指南》中的针对第三方身份提供商创建角色（联合身份验证）。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的权限集。
- 临时 IAM 用户权限：IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取：您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）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，对于某些资源 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 中的跨账户资源访问。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在服务中拨打电话时，该服务通常会在 Amazon 中运行应用程序 EC2 或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两项操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。
  - 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分派的 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-服务相关角色是一种链接到的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 A@@ mazon 上运行的应用程序 EC2 — 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证书。这比在 EC2 实例中存储访问密钥更可取。要为 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建一个附加到该实例的实例配置文件。实例配置文件包含该角色，并允许在 EC2 实例上运行的程序获得临时证书。有关更多信息，请参阅 IAM 用户指南中的使用 IAM 角色向在 A mazon EC2 实例上运行的应用程序授予权限。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会

话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的结构和内容的更多信息，请参阅 IAM 用户指南中的 JSON 策略概览。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

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。拥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《IAM 用户指南》中的使用客户托管策略定义自定义 IAM 权限。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 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和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管策略与内联策略之间进行选择。

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，策略定义指定主体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主体。委托人可以包括账户、用户、角色、联合用户或 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 IAM 中的 AWS 托管策略。

访问控制列表

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。 ACLs 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 和 Amazon VPC 就是支持的服务示例 ACLs。 AWS WAF要了解更多信息 ACLs，请参阅《亚马逊简单存储服务开发者指南》中的访问控制列表 (ACL) 概述。

其他策略类型

AWS 支持其他不太常见的策略类型。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特征，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 (SCPs) — SCPs 是 JSON 策略，用于指定中组织或组织单位 (OU) 的最大权限 AWS Organizations。 AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果您启用组织中的所有功能，则可以将服务控制策略 (SCPs) 应用于您的任何或所有帐户。SCP 限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关 Organization SCPs s 和的更多信息，请参阅《AWS Organizations 用户指南》中的服务控制策略。
- 资源控制策略 (RCPs) — RCPs 是 JSON 策略，您可以使用它来设置账户中资源的最大可用权限，而无需更新附加到您拥有的每个资源的 IAM 策略。RCP 限制成员账户中资源的权限，并可能影响身份（包括身份）的有效权限 AWS 账户根用户，无论这些身份是否属于您的组织。有关 Organizations 的更多信息 RCPs，包括 AWS 服务 该支持的列表 RCPs，请参阅《AWS Organizations 用户指南》中的资源控制策略 (RCPs)。
- 会话策略：会话策略是当您以编程方式为角色或联合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 IAM 用户指南中的会话策略。

> **Note**
>
> WorkDocs 不支持 Slack 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。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

亚马逊如何 WorkDocs 使用 IAM

在使用 IAM 管理访问权限之前 WorkDocs，您需要了解哪些 IAM 功能可供使用 WorkDocs。要全面了解如何 WorkDocs 和其他 AWS 服务与 IAM 配合使用，请参阅 IAM 用户指南中的与 IAM 配合使用的 AWS 服务。

主题

- WorkDocs 基于身份的策略
- WorkDocs 基于资源的策略
- 基于 WorkDocs 标签的授权
- WorkDocs IAM 角色

WorkDocs 基于身份的策略

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

操作

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体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关联操作的权限。

正在执行的策略操作在操作前 WorkDocs 使用以下前缀:`workdocs:`. 例如，要向某人授予运行 WorkDocs `DescribeUsers` API 操作的权限，您需要将该`workdocs:DescribeUsers`操作包含在他们的策略中。策略语句必须包括 `Action` 或 `NotAction` 元素。 WorkDocs 定义了自己的一组操作，这些操作描述了可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**
>
> 为确保向后兼容性，请添加 zocalo 操作。例如：
>
> ```
> "Action": [
> "zocalo:*",
> "workdocs:*"
> ],
> ```

要查看 WorkDocs 操作列表，请参阅 IAM 用户指南 WorkDocs中定义的操作。

资源

WorkDocs 不支持在策略 ARNs 中指定资源。

条件键

WorkDocs 不提供任何特定于服务的条件密钥，但它确实支持使用某些全局条件密钥。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

示例

要查看 WorkDocs 基于身份的策略的示例，请参阅。Amazon WorkDocs 基于身份的政策示例

WorkDocs 基于资源的策略

WorkDocs 不支持基于资源的策略。

基于 WorkDocs 标签的授权

WorkDocs 不支持标记资源或基于标签控制访问权限。

WorkDocs IAM 角色

I AM 角色是您的 AWS 账户中具有特定权限的实体。

将临时凭证与 WorkDocs

强烈建议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AssumeRole或之类的 AWS STS API 操作来获取临时安全证书GetFederationToken。

WorkDocs 支持使用临时证书。

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 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。

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 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。

WorkDocs 不支持服务角色。

Amazon WorkDocs 基于身份的政策示例

> **Note**
>
> 为了提高安全性，请尽可能创建联合用户而不是 IAM 用户。

默认情况下，IAM 用户和角色没有创建或修改 WorkDocs 资源的权限。他们也无法使用 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**
>
> 为确保向后兼容性，请在策略中包含 `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
- 使用 WorkDocs 控制台
- 允许用户查看他们自己的权限
- 允许用户对 WorkDocs 资源进行只读访问
- 更多 WorkDocs 基于身份的策略示例

策略最佳实践

基于身份的策略决定了某人是否可以在您的账户中创建、访问或删除 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，请遵循以下指南和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略或工作职能的AWS 托管式策略。
- 应用最低权限：在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。

- 使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 AWS CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言（JSON）和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM Access Analyzer 验证策略。
- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的使用 MFA 保护 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅 IAM 用户指南中的 IAM 中的安全最佳实操。

使用 WorkDocs 控制台

要访问 Amazon WorkDocs 控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看 AWS 账户中 WorkDocs 资源的详细信息。如果您创建的基于身份的策略比所需的最低权限更严格，则无法为 IAM 用户或角色实体按预期运行此控制台。

为确保这些实体可以使用 WorkDocs 控制台，还要将以下 AWS 托管策略附加到这些实体。有关附加策略的更多信息，请参阅《IAM 用户指南》中的向用户添加权限。

- AmazonWorkDocsFullAccess
- AWSDirectoryServiceFullAccess
- AmazonEC2FullAccess

这些政策授予用户访问 WorkDocs 资源、 AWS Directory Service EC2 操作和亚马逊正常工作 WorkDocs 所需的亚马逊运营的完全访问权限。

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。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式策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

```
{
    "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 WorkDocs 资源进行只读访问

以下 AWS 托管AmazonWorkDocsReadOnlyAccess策略授予 IAM 用户对 WorkDocs 资源的只读访问权限。该策略允许用户访问所有 WorkDocs `Describe`操作。必须访问这两个 Amazon EC2 操作，这样 WorkDocs 才能获得您的 VPCs 和子网的列表。需要访问该 AWS Directory Service `DescribeDirectories`操作才能获取有关您的 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 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 角色或用户访问该 WorkDocs API。有关更多信息，请参阅《WorkDocs 开发人员指南》中的管理应用程序的身份验证和访问控制。

对 Amazon WorkDocs 身份和访问进行故障排除

使用以下信息来帮助您诊断和修复在使用 WorkDocs 和 IAM 时可能遇到的常见问题。

主题

- 我无权在以下位置执行操作 WorkDocs
- 我无权执行 iam：PassRole
- 我想允许 AWS 账户之外的人访问我的 WorkDocs 资源

我无权在以下位置执行操作 WorkDocs

如果 AWS Management Console 告诉您您无权执行某项操作，则必须联系管理员寻求帮助。管理员是指提供用户名和密码的人员。

我无权执行 iam：PassRole

如果您收到一个错误，表明您无权执行 `iam:PassRole` 操作，则必须更新策略以允许您将角色传递给 WorkDocs。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的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 marymajor 的 IAM 用户尝试使用控制台在 WorkDocs 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。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，必须更新 Mary 的策略以允许她执行 iam:PassRole 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许 AWS 账户之外的人访问我的 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 (ACLs) 的服务，您可以使用这些策略向人们授予访问您的资源的权限。

要了解更多信息，请参阅以下内容：

- 要了解是否 WorkDocs 支持这些功能，请参阅亚马逊如何 WorkDocs 使用 IAM。
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（身份联合验证）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 中的跨账户资源访问。

在 Amazon 中记录和监控 WorkDocs

Amazon WorkDocs 网站管理员可以查看和导出整个网站的活动提要。它们还可以 AWS CloudTrail 用来从 WorkDocs 控制台捕获事件。

主题

- 导出站点范围活动源
- AWS CloudTrail 用于记录亚马逊 WorkDocs API 调用

导出站点范围活动源

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 C WorkDocs ompanion。要安装 C WorkDocs ompanion，请参阅应用程序和集成。 WorkDocs

查看和导出站点范围活动源

1. 在 Web 应用程序中，选择活动源。
2. 选择筛选器，然后移动站点范围活动滑块以启用筛选器。
3. 选择活动类型筛选条件，根据需要选择修改日期设置，然后选择应用。
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. 选择导出可将活动源导出为桌面上的 `.csv` 和 `.json` 文件。系统会将文件导出到以下位置之一：

   - Windows — 电脑下载WorkDocsDownloads文件夹中的文件夹
   - macOS – `/users/`**`username`**`/WorkDocsDownloads/folder`

   导出的文件中会反映您应用的任意筛选条件。

   > **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 Amazon WorkDocs 用户指南中的查看活动源。

AWS CloudTrail 用于记录亚马逊 WorkDocs API 调用

您可以使用 AWS CloudTrail; 来记录 Amazon WorkDocs API 调用。 CloudTrail 提供了用户、角色或 AWS 服务在中执行的操作的记录 WorkDocs。 CloudTrail 将所有 API 调用捕获 WorkDocs 为事件，包括来自 WorkDocs 控制台的调用和对的代码调用 WorkDocs APIs。

如果您创建了跟踪，则可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括的事件 WorkDocs。如果您不创建跟踪，您仍然可以在 CloudTrail 控制台的事件历史记录中查看最新的事件。

收集的信息 CloudTrail 包括请求、发出请求的 IP 地址、提出请求的用户以及请求日期。

有关的更多信息 CloudTrail，请参阅《AWS CloudTrail 用户指南》。

WorkDocs 信息在 CloudTrail

CloudTrail 在您创建 AWS 账户时已在您的账户上启用。当活动发生在中时 WorkDocs，该活动会与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在自己的 AWS 账户中查看、搜索和下载最近发生的事件。有关更多信息，请参阅使用事件历史查看 CloudTrail 事件。

要持续记录您 AWS 账户中的事件，包括的事件 WorkDocs，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 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。跟踪记录 AWS 分区中所有区域的事件，并将日志文件传送到您指定的 Amazon S3 存储桶。此外，您可以配置其他 AWS 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅：

- 创建跟踪概览
- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail
- 接收来自多个区域的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail 日志文件

所有 WorkDocs 操作均由 Amazon WorkDocs API 参考记录 CloudTrail 并记录在案。例如，调用`CreateFolder`、`DeactivateUser`和`UpdateDocument`节会在 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 WorkDocs 日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。事件代表来自任何来源的单个请求，包括有关请求的操作、操作的日期和时间、请求参数等的信息。 CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序出现。

WorkDocs 生成不同类型的 CloudTrail 条目，分别来自控制平面的条目和来自数据平面的条目。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。数据平面条目的用户身份是 WorkDocs 目录用户。

> **Note**
>
> 为了提高安全性，请尽可能创建联合用户而不是 IAM 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。这些在日志中显示为 HIDDEN_DUE_TO_SECURITY_REASON。 CloudTrail 这些在日志中显示为 HIDDEN_DUE_TO_SECURITY_REASON。 CloudTrail

以下示例显示了两个 CloudTrail 日志条目 WorkDocs：第一条记录用于控制平面操作，第二条记录用于数据平面操作。

```
{
  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",
      "awsRegion" : "region",
      "sourceIPAddress" : "ip_address",
      "userAgent" : "user_agent",
      "requestParameters" :
      {
        "AuthenticationToken" : "**-redacted-**"
      },
      "responseElements" : null,
      "requestID" : "request_id",
      "eventID" : "event_id"
    }
  ]
}
```

Amazon 合规性验证 WorkDocs

要了解是否属于特定合规计划的范围，请参阅AWS 服务 “按合规计划划分的范围” ”，然后选择您感兴趣的合规计划。 AWS 服务 有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。 AWS 提供了以下资源来帮助实现合规性：

- Security Compliance & Governance：这些解决方案实施指南讨论了架构考虑因素，并提供了部署安全性和合规性功能的步骤。

- 符合 HIPAA 要求的服务参考：列出符合 HIPAA 要求的服务。并非所有 AWS 服务 人都符合 HIPAA 资格。
- AWS 合规资源AWS — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- AWS 客户合规指南 — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践， AWS 服务并将指南映射到跨多个框架（包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO)）的安全控制。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- AWS Security Hub— 这 AWS 服务 可以全面了解您的安全状态 AWS。Security Hub 通过安全控制措施评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控制措施的列表，请参阅 Security Hub 控制措施参考。
- Amazon GuardDuty — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务检测您的工作负载、容器和数据面临的潜在威胁。 GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。
- AWS Audit Manager— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

Amazon 的弹性 WorkDocs

AWS 全球基础设施是围绕 AWS 区域和可用区构建的。 AWS 区域提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络相连。利用可用区，您可以设计和操作在可用区之间无中断地自动实现失效转移的应用程序和数据库。与传统的单个或多个数据中心基础架构相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域和可用区的更多信息，请参阅AWS 全球基础设施。

Amazon 的基础设施安全 WorkDocs

作为一项托管服务， WorkDocs Amazon 受 AWS 全球网络安全程序的保护。有关更多信息，请参阅 IA M 用户指南中的 AWS Identity and Access Management 中的基础设施安全以及 AWS 架构中心中的安全、身份和合规最佳实践。

您可以使用 AWS 已发布的 API 调用 WorkDocs 通过网络进行访问。客户端必须支持传输层安全性协议 (TLS) 1.2，我们建议使用 TLS 1.3。客户端还必须支持具有完全向前保密的密码套件，例如 Ephemeral Diffie-Hellman 或 Elliptic Curve Ephemeral Diffie-Hellman。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 主体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。

入门 WorkDocs

WorkDocs 使用目录来存储和管理用户及其文档的组织信息。然后，在预置站点时，您可以将目录附加到该站点。当您这样做时，一项名为 “自动激活” 的 WorkDocs 功能会将目录中的用户作为托管用户添加到站点，这意味着他们无需单独的凭据即可登录您的站点，并且可以共享和协作处理文件。除非购买更多存储空间，否则每个用户都有 1 TB 的存储空间。

您不再需要手动添加和激活用户，但仍然具备该权限。您还可以根据需要更改用户角色和权限。有关执行此操作的更多信息，请参阅本指南后面的邀请和管理 WorkDocs 用户。

如果需要创建目录，您可以：

- 创建 Simple AD 目录。
- 创建 AD Connector 目录，连接到本地目录。
- 启用 WorkDocs 此选项可使用现有 AWS 目录。
- WorkDocs 为你创建一个目录。

您还可以在您的 AD 目录和目录之间创建信任关系。 AWS Managed Microsoft AD

> **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 目录以满足合规性要求。本部分中的步骤介绍了如何使用现有的 Microsoft AD Directory。有关创建 Microsoft AD Directory 的信息，请参阅《AWS Directory Service 管理指南》中的 AWS Managed Microsoft AD。

内容

- 创建 WorkDocs 网站
- 启用单点登录
- 启用多重验证
- 将用户提升为管理员

创建 WorkDocs 网站

以下各节中的步骤说明了如何设置新 WorkDocs 站点。

任务

- 开始前的准备工作
- 创建 WorkDocs 网站

开始前的准备工作

在创建 WorkDocs 网站之前，您必须具备以下物品。

- 用于创建和管理 WorkDocs 网站的 AWS 帐户。但是，用户不需要 AWS 帐户即可连接和使用 WorkDocs。有关更多信息，请参阅 Amazon 的先决条件 WorkDocs。
- 如果您计划使用 Simple AD，则必须满足《AWS Directory Service 管理指南》中 Simple AD 先决条件中确定的先决条件。
- 如果您属于合规计划（例如 PCI、FedRAMP 或 DoD），则为 AWS Managed Microsoft AD 目录。本部分中的步骤介绍了如何使用现有的 Microsoft AD Directory。有关创建 Microsoft AD Directory 的信息，请参阅《AWS Directory Service 管理指南》中的 AWS Managed Microsoft AD。
- 管理员的配置文件信息，包括名字和姓氏以及电子邮件地址。

创建 WorkDocs 网站

按照以下步骤在几分钟内创建一个 WorkDocs 网站。

创建 WorkDocs 网站

1. 打开 WorkDocs 控制台，网址为https://console.aws.amazon.com/zocalo/。
2. 在主机主页上的 “创建 WorkDocs 站点” 下，选择 “立即开始”。

   -或-

   在导航窗格中，选择我的站点，然后在管理您的 WorkDocs 网站页面上，选择创建 WorkDocs 网站。

   接下来的操作因您是否有目录而异。

   - 如果您有目录，系统将显示选择目录页面，您可以在此页面选择现有目录或创建目录。
   - 如果您没有目录，系统会显示设置目录类型页面，您可以在此页面创建 Simple AD 或 AD Connector 目录。

以下步骤说明了如何完成这两项任务。

使用现有目录

1. 打开可用目录列表，并选择要使用的目录。
2. 选择启用目录。

创建目录

1. 重复上述第 1 步和第 2 步。

   接下来的操作取决于您是要使用 Simple AD 还是要创建 AD Connector，

   使用 Simple AD

   a. 选择 Simple AD，然后选择下一步。

      系统将显示创建 Simple AD 站点页面。

   b. 在接入点下的站点 URL 框中，输入站点的 URL。
   c. 在 “设置 WorkDocs 管理员” 下，输入管理员的电子邮件地址、名字和姓氏。
   d. 根据需要填写目录详细信息和 VPC 配置下的选项。
   e. 选择创建 Simple AD 站点。

   创建 AD Connector 目录

   a. 选择 AD Connector，然后选择下一步。

      系统将显示创建 AD Connector 站点页面。

   b. 填写目录详细信息下的所有字段。
   c. 在接入点下的站点 URL 框中，输入站点的 URL。
   d. 根据需要填写 VPC 配置下的可选字段。
   e. 选择创建 AD Connector 站点。

WorkDocs 执行以下操作：

- 如果您在上面的步骤 4 中选择了代表我设置 VPC，则会为您 WorkDocs 创建一个 VPC。VPC 中的目录存储用户和 WorkDocs 站点信息。
- 如果您使用的是 Simple AD，则 WorkDocs 会创建一个目录用户并将该用户设置为 WorkDocs管理员。如果您创建了 AD Connector 目录，则 WorkDocs 设置您作为 WorkDocs 管理员提供的现有目录用户。
- 如果您使用的是现有目录，则 WorkDocs 会提示您输入 WorkDocs 管理员的用户名。用户必须是目录的成员。

> **Note**
>
> WorkDocs 不会通知用户有关新网站的信息。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站点。

启用单点登录

AWS Directory Service 允许用户通过加入注册目录 WorkDocs 的计算机访问 Amazon，无需单独输入凭证。 WorkDocs WorkDocs 管理员可以使用 AWS Directory Service 控制台启用单点登录。有关更多信息，请参阅《AWS Directory Service 管理指南》中的单点登录。

WorkDocs 管理员启用单点登录后， WorkDocs 站点用户可能还需要修改其 Web 浏览器设置以允许单点登录。有关更多信息，请参阅《AWS Directory Service 管理指南》中的 IE 和 Chrome 的单点登录以及 Firefox 的单点登录。

启用多重验证

您可以使用位于的 AWS 目录服务控制台为 A https://console.aws.amazon.com/directoryservicev2/D Connector 目录启用多因素身份验证。要启用 MFA，您必须具有属于远程身份验证拨入用户服务 (RADIUS) 服务器的 MFA 解决方案，或已在本地基础设施中实现的 RADIUS 服务器必须具有 MFA 插件。您的 MFA 解决方案应实施一次性密码 (OTP)，用户可从硬件设备或在设备（如手机）上运行的软件来获取此密码。

RADIUS 是一种行业标准 client/server 协议，它提供身份验证、授权和记账管理，使用户能够连接到网络服务。AWS Managed Microsoft AD 包括一个 RADIUS 客户端，此客户端将连接到您在其上已实现 MFA 解决方案的 RADIUS 服务器。您的 RADIUS 服务器将验证用户名和 OTP 代码。如果您的 RADIUS 服务器成功验证用户，之后 AWS Managed Microsoft AD 将针对 AD 对用户进行身份验

证。AD 身份验证成功后，用户之后可访问 AWS 应用程序。AWS Managed Microsoft AD RADIUS 客户端与 RADIUS 服务器之间的通信需要您配置 AWS 安全组，以允许通过端口 1812 通信。

有关更多信息，请参阅《AWS Directory Service 管理指南》中的为 AWS Managed Microsoft AD 启用多重身份验证。

> **Note**
>
> 多重身份验证不适用于 Simple AD 目录。

将用户提升为管理员

您可以使用 WorkDocs 控制台将用户提升为管理员。执行以下步骤。

将用户提升为管理员

1. 打开 WorkDocs 控制台，网址为https://console.aws.amazon.com/zocalo/。
2. 在导航窗格中，选择我的站点。

   将出现 “管理您的 WorkDocs 网站” 页面。
3. 选择所需站点旁边的按钮，接着选择操作，然后选择设置管理员。

   将出现 “设置 WorkDocs 管理员” 对话框。
4. 在用户名框中，输入要提升的人员的用户名，然后选择设置管理员。

您也可以使用 WorkDocs 站点管理员控制面板将管理员降级。有关更多信息，请参阅 编辑用户。

通过 AWS 控制 WorkDocs 台进行管理

您可以使用以下工具来管理您的 WorkDocs 网站：

- AWS 控制台位于https://console.aws.amazon.com/zocalo/。
- 站点管理员控制面板，可供所有 WorkDocs 站点的管理员使用。

这些工具中的每一个都提供了一组不同的操作，本节中的主题解释了 AWS 控制台提供的操作。有关站点管理员控制面板的信息，请参阅 WorkDocs 从站点管理员控制面板进行管理。

设置站点管理员

如果您是管理员，则可以授权用户访问站点控制面板及其提供的操作。

设置管理员

1. 打开 WorkDocs 控制台，网址为https://console.aws.amazon.com/zocalo/。
2. 在导航窗格中，选择我的站点。

   将出现 “管理您的 WorkDocs 站点” 页面，并显示您的网站列表。
3. 选择要设置管理员的站点旁边的按钮。
4. 打开操作列表，然后选择设置管理员。

   将出现 “设置 WorkDocs 管理员” 对话框。
5. 在用户名框中，输入新管理员的姓名，然后选择设置管理员。

重新发送邀请电子邮件

您可以随时重新发送邀请电子邮件。

重新发送邀请电子邮件

1. 打开 WorkDocs 控制台，网址为https://console.aws.amazon.com/zocalo/。
2. 在导航窗格中，选择我的站点。

   将出现 “管理您的 WorkDocs 站点” 页面，并显示您的网站列表。

3. 选择要为其重新发送电子邮件的站点旁边的按钮。
4. 打开操作列表，然后选择重新发送邀请电子邮件。

   页面顶部会显示一条绿色横幅消息。

管理多重身份验证

创建 WorkDocs 网站后，您可以启用多因素身份验证。有关身份验证的更多信息，请参阅 启用多重验证。

设置网站 URLs

> **Note**
>
> 如果您按照 入门 WorkDocs中的站点创建流程进行操作，则已经输入了站点 URL。因此，WorkDocs 会使 “设置站点 URL” 命令不可用，因为您只能设置一次 URL。只有在部署 Amazon 并将其 WorkSpaces 与集成后，您才可以按照以下步骤操作 WorkDocs。Amazon WorkSpaces 集成流程要求您输入序列号而不是网站 URL，因此您必须在完成集成后输入 URL。有关集成 Amazon WorkSpaces 的更多信息， WorkDocs 请参阅亚马逊 WorkSpaces 用户指南 WorkDocs中的与集成。

设置站点 URL

1. 打开 WorkDocs 控制台，网址为https://console.aws.amazon.com/zocalo/。
2. 在导航窗格中，选择我的站点。

   将出现 “管理您的 WorkDocs 站点” 页面，并显示您的网站列表。
3. 选择您与 Amazon 集成的网站 WorkSpaces。URL 包含您的 Amazon WorkSpaces 实例的目录 ID，例如https://{directory_id}.awsapps.com。
4. 选择该 URL 旁边的按钮，打开操作列表，然后选择设置站点 URL。

   系统将显示设置站点 URL 对话框。
5. 在站点 URL 框中，输入站点的 URL，然后选择设置站点 URL。
6. 在 “管理您的 WorkDocs 网站” 页面上，选择 “刷新” 以查看新 URL。

管理通知

> **Note**
>
> 为了提高安全性，请尽可能创建联合用户而不是 IAM 用户。

通知允许 IAM 用户或角色调用 CreateNotificationSubscriptionAPI，您可以使用它来设置自己的终端节点来处理 WorkDocs 发送的 SNS 消息。有关通知的更多信息，请参阅WorkDocs 开发人员指南中的为 IAM 用户或角色设置通知。

您可以创建和删除通知，以下步骤说明了如何完成这两项任务。

> **Note**
>
> 要创建通知，您必须拥有自己的 IAM 或角色 ARN。要查找您的 IAM ARN，请执行以下操作：
>
> 1. 使用 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
> 2. 在导航栏中，选择 “用户”。
> 3. 选择您的用户名。
> 4. 在 “摘要” 下，复制您的 ARN。

创建通知

1. 打开 WorkDocs 控制台，网址为https://console.aws.amazon.com/zocalo/。
2. 在导航窗格中，选择我的站点。

   将出现 “管理您的 WorkDocs 站点” 页面，并显示您的网站列表。
3. 选择所需站点旁边的按钮。
4. 打开操作列表，然后选择管理通知。

   将出现 “管理通知” 页面。
5. 选择 Create notification（创建通知）。
6. 在新建通知对话框中，输入您的 IAM 或角色 ARN，然后选择创建通知。

删除通知

1. 打开 WorkDocs 控制台，网址为https://console.aws.amazon.com/zocalo/。
2. 在导航窗格中，选择我的站点。

   将出现 “管理您的 WorkDocs 站点” 页面，并显示您的网站列表。
3. 选择包含您要删除的通知的网站旁边的按钮。
4. 打开操作列表，然后选择管理通知。
5. 在管理通知页面上，选择要删除的通知旁边的按钮，然后选择删除通知。

删除站点

您可以使用 WorkDocs 控制台删除站点。

> **Warning**
> 删除站点时会丢失所有文件。只有在确定不再需要这些信息的情况下，才删除站点。

删除站点

1. 打开 WorkDocs 控制台，网址为https://console.aws.amazon.com/zocalo/。
2. 在导航窗格中，选择我的站点。

   将出现 “管理您的 WorkDocs 网站” 页面。
3. 选择要删除的站点旁边的按钮，然后选择删除。

   系统将显示删除站点 URL 对话框。
4. （可选）选择同时删除用户目录。

   > **Important**
   > 如果您没有为提供自己的目录 WorkDocs，我们会为您创建一个。删除 WorkDocs 网站时，您需要为我们创建的目录付费，除非您删除该目录或将其用于其他 AWS 应用程序。有关定价信息，请参阅 AWS Directory Service 定价。
5. 在站点 URL 框中，输入站点 URL，然后选择删除。

该站点会立即删除，并且不再可用。

WorkDocs 从站点管理员控制面板进行管理

您可以使用以下工具来管理您的 WorkDocs 网站：

- 站点管理员控制面板，可供所有 WorkDocs 站点的管理员使用，并在以下主题中进行了介绍。
- AWS 控制台位于https://console.aws.amazon.com/zocalo/。

上述每个工具都提供了一组不同的操作。本部分中的主题说明了站点管理员控制面板提供的操作。有关控制台中可用任务的信息，请参阅通过 AWS 控制 WorkDocs 台进行管理。

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. 在我的账户下，选择打开管理员控制面板。
2. 对于语言设置偏好，选择您的首选语言。

Hancom 在线编辑和 Office Online

从管理员控制面板中启用或禁用 Hancom 在线编辑和 Office Online 设置。有关更多信息，请参阅 允许协作编辑。

存储

指定新用户接收的存储量。

更改存储设置

1. 在我的账户下，选择打开管理员控制面板。
2. 对于存储，选择更改。
3. 在存储限制对话框中，选择为新用户提供无限存储空间还是有限存储空间。
4. 选择保存更改。

更改存储设置只会对更改设置后添加的用户造成影响。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。

IP 白名单

WorkDocs 站点管理员可以添加 IP 允许列表设置，将站点访问限制在允许的 IP 地址范围内。每个站点最多可以添加 500 个 IP 允许列表设置。

> **Note**
>
> IP 允许列表目前仅适用于 IPv4 地址。目前不支持 IP 地址拒绝名单。

将 IP 范围添加到 IP 白名单

1. 在我的账户下，选择打开管理员控制面板。
2. 对于 IP 白名单，选择更改。
3. 对于输入 CIDR 值，输入 IP 地址范围的无类别域间路由 (CIDR) 块，然后选择添加。
   - 要允许从单个 IP 地址访问，请将 /32 指定为 CIDR 前缀。
4. 选择保存更改。
5. 允许通过 IP 白名单中的 IP 地址连接到站点的用户进行访问。试图通过未经授权的 IP 地址连接到站点的用户会收到“未授权”响应。

> **Warning**
>
> 如果您输入的 CIDR 值阻止您使用当前 IP 地址访问站点，系统会显示一条警告消息。如果您选择继续使用当前 CIDR 值，系统将阻止您使用当前 IP 地址访问该站点。只能通过联系 AWS Support 来撤消此操作。

安全 — 简单的 ActiveDirectory网站

本主题介绍了 Simple ActiveDirectory 网站的各种安全设置。如果您管理使用 ActiveDirectory 连接器的站点，请参阅下一节。

使用安全设置

1. 选择客户端右上角的配置文件图标。 WorkDocs

2. 在管理员下，选择打开管理员控制面板。
3. 向下滚动到安全，然后选择更改。

系统将显示策略设置对话框。下表列出了 Simple ActiveDirectory 站点的安全设置。

设置	描述
在选择可共享链接的设置下，选择以下选项之一：	
不允许站点范围或公共可共享链接	为所有用户禁用链接共享。
允许用户创建站点范围可共享链接，但不允许他们创建公共可共享链接	将链接共享限制为仅限站点成员。托管用户可以创建此类链接。
允许用户创建站点范围可共享链接，但只有高级用可以创建公共可共享链接	托管用户可以创建站点范围可共享链接，但只有高级用可以创建公共链接。互联网上的任何人都可以访问公共链接。
所有托管用户都可以创建站点范围和公共可共享链接	托管用户可以创建公共链接。
在自动激活下，选中或清除以下复选框。	
允许您目录中的所有用户在首次登录您的 WorkDocs 网站时自动激活。	在用户首次登录您的站点时自动激活他们。
在应允许谁邀请新用户访问您的 WorkDocs 网站下，选择以下选项之一：	
只有管理员可以邀请新用户。	只有管理员可以邀请新用户。
用户可以通过与位于任何位置的新用户共享文件或文件夹来邀请这些新用户。	允许用户通过与新用户共享文件或文件夹来邀请这些新用户。

设置	描述
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。	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。
在为新用户配置角色下，选中或清除以下复选框。	
您目录中的新用户将为托管用户（默认情况下，他们为访客用户）	自动将目录中的新用户转换为托管用户。

4. 完成后，选择保存更改。

安全- ActiveDirectory 连接器站点

本主题介绍 ActiveDirectory 连接器站点的各种安全设置。如果您管理使用 Simple 的网站 ActiveDirectory，请参阅上一节。

使用安全设置

1. 选择客户端右上角的配置文件图标。 WorkDocs

2. 在管理员下，选择打开管理员控制面板。
3. 向下滚动到安全，然后选择更改。

   系统将显示策略设置对话框。下表列出并描述了 ActiveDirectory连接器站点的安全设置。

设置	描述
在选择可共享链接的设置下，选择以下选项之一：	
不允许站点范围或公共可共享链接	选中后，将为所有用户禁用链接共享。
允许用户创建站点范围可共享链接，但不允许他们创建公共可共享链接	将链接共享限制为仅限站点成员。托管用户可以创建此类链接。

设置	描述
允许用户创建站点范围可共享链接，但只有高级用可以创建公共可共享链接	托管用户可以创建站点范围可共享链接，但只有高级用可以创建公共链接。互联网上的任何人都可以访问公共链接。
所有托管用户都可以创建站点范围和公共可共享链接	托管用户可以创建公共链接。

在自动激活下，选中或清除以下复选框。

允许您目录中的所有用户在首次登录您的 WorkDocs 网站时自动激活。	在用户首次登录您的站点时自动激活他们。

在“应该允许谁在您的 WorkDocs 站点中激活目录用户？”，请选择以下选项之一：

只有管理员可以激活目录中的新用户。	只允许管理员激活目录中的新用户。
用户可以通过与目录中的新用户共享文件或文件夹来激活这些新用户	允许用户通过与目录中的用户共享文件或文件夹来激活这些用户。
用户可以通过与一些指定域中的新用户共享文件或文件夹来激活这些新用户。	用户只能与指定域中的用户共享文件或文件夹。选择此选项后，必须输入域。

在“应允许谁邀请新用户访问您的 WorkDocs 网站？”，请选择以下选项之一：

与外部用户共享	使管理员和用户能够邀请新的外部用户访问您的 WorkDocs 站点。

> **Note**
>
> 以下选项仅在您选择此设置后才会显示。

只有管理员可以邀请新的外部用户	只有管理员可以邀请外部用户。
所有托管用户都可以邀请新用户	允许托管用户邀请外部用户。
只有高级用户才能邀请新的外部用户。	只允许高级用户邀请新的外部用户。

在为新用户配置角色下，选择一个或两个选项。

设置	描述
您目录中的新用户将为托管用户（默认情况下，他们为访客用户）	自动将目录中的新用户转换为托管用户。
新的外部用户将为托管用户（默认情况下，他们为访客用户）	自动将新的外部用户转换为托管用户。

4. 完成后，选择保存更改。

恢复站保留

当用户删除文件时，会将该文件 WorkDocs 存储在用户的回收站中 30 天。之后， WorkDocs 将文件移到临时恢复箱中 60 天，然后将其永久删除。只有管理员才能看到临时恢复站。通过更改站点范围的数据留存策略，站点管理员可以将恢复站的保留期更改为最短零天，最长 365 天。

更改恢复站保留期

1. 在我的账户下，选择打开管理员控制面板。
2. 在恢复站保留旁边，选择更改。
3. 输入在恢复站中保留文件的天数，然后选择保存。

> **Note**
>
> 默认保留期为 60 天。您可以自行选择保留期，最短 0 天，最长 365 天。

管理员可以在永久 WorkDocs 删除用户文件之前将其从恢复箱中恢复。

恢复用户文件

1. 在我的账户下，选择打开管理员控制面板。
2. 在管理用户下，选择用户的文件夹图标。
3. 在恢复站下，选择要恢复的文件，然后选择恢复图标。
4. 对于恢复文件，选择要将文件恢复到的位置，然后选择恢复。

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 WorkDocs 用户。

将 WorkDocs 云端硬盘部署到多台计算机

如果您有加入域的计算机队列，则可以使用组策略对象 (GPO) 或系统中心配置管理器 (SCCM) 来安装云端硬盘客户端。 WorkDocs 您可以从客户端下载 https://amazonworkdocs.com/en/客户端。

在使用过程中，请记住，云端 WorkDocs 硬盘要求所有 AWS IP 地址通过端口 443 访问 HTTPS。您还需要确认您的目标系统是否满足 WorkDocs 云端硬盘的安装要求。有关更多信息，请参阅《Amazon WorkDocs 用户指南》中的 “安装 WorkDocs 云端硬盘”。

> **Note**
>
> 使用 GPO 或 SCCM 时，最佳做法是在用户登录后安装 WorkDocs 云端硬盘客户端。

适用于 WorkDocs 云端硬盘的 MSI 安装程序支持以下可选安装参数：

- **`SITEID`**— 在注册期间为用户预先填充 WorkDocs 网站信息。例如 `SITEID=`*`site-name`*。
- **`DefaultDriveLetter`**— 预先填充用于安装 WorkDocs 驱动器的驱动器号。例如 `DefaultDriveLetter=`*`W`*。请记住，每个用户必须有不同的驱动器号。此外，用户在首次启动云端硬盘后，可以更改驱动器名称，但不能更改 WorkDocs 驱动器号。

以下示例部署了没有用户界面且不重启的 WorkDocs 云端硬盘。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 WorkDocs 用户

默认情况下，当您在网站创建期间附加目录时，中的自动激活功能会将该目录中的所有用户作为托管用户 WorkDocs 添加到新站点。

在中 WorkDocs，托管用户无需使用单独的凭据登录。他们可以共享和协作处理文件，而且自动拥有 1 TB 的存储空间。但是，当您只想添加目录中的部分用户时，可以关闭自动激活功能，后续部分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。有关提升用户的更多信息，请参阅将用户提升为管理员。

您可以在 WorkDocs Web 客户端的管理控制面板中执行这些任务，以下各节中的步骤说明了如何执行这些任务。但是，如果您不熟悉 WorkDocs，请花几分钟时间了解各种用户角色，然后再深入研究管理任务。

内容

- 用户角色概述
- 启动管理员控制面板
- 关闭自动激活功能
- 管理链接共享
- 在启用自动激活功能的情况下控制用户邀请
- 邀请新用户
- 编辑用户
- 禁用用户
- 移交文档所有权
- 下载用户列表

用户角色概述

WorkDocs 定义了以下用户角色。您可以通过编辑用户的用户配置文件来更改他们的角色。有关更多信息，请参阅 编辑用户。

- 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。

- 高级用户：管理员可授予其一组专用权限的付费用户。有关如何为高级用户设置权限的更多信息，请参阅安全 — 简单的 ActiveDirectory网站和安全- ActiveDirectory 连接器站点。
- 用户：付费用户，可以保存文件并与 WorkDocs 网站中的其他人协作。
- 访客用户：只能查看文件的未付费用户。您可以将访客用户升级为用户、高级用户或管理员角色。

> **Note**
>
> 当您更改访客用户的角色时，您执行的是无法撤销的一次性操作。

WorkDocs 还定义了这些其他用户类型。

WS 用户

已分配的用户 WorkSpaces WorkSpace。

- 访问所有 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

已分配 WorkSpaces WorkSpace 和升级存储空间的用户。

- 访问所有 WorkDocs 功能
- 默认存储空间为 1 TB（额外存储空间视情况而 pay-as-you-go定）
- 需支付月度费用

WorkDocs 用户

未分配的活跃 WorkDocs 用户 WorkSpaces WorkSpace。

- 访问所有 WorkDocs 功能
- 默认存储空间为 1 TB（额外存储空间视情况而 pay-as-you-go定）
- 需支付月度费用

启动管理员控制面板

您可以使用 WorkDocs Web 客户端中的管理控制面板来关闭和打开自动激活，以及更改用户角色和设置。

打开管理员控制面板

1. 选择客户端右上角的配置文件图标。 WorkDocs

2. 在管理员下，选择打开管理员控制面板。

> **Note**
>
> 某些控制面板选项在云目录和连接目录之间有所不同。

关闭自动激活功能

如果您不想将目录中的所有用户添加到新站点，并且想要为邀请访问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功能。关闭自动激活功能后，您还可以决定谁能够邀请新用户访问该站点，包括当前用户、高级用户或管理员。以下步骤说明了如何完成这两项任务。

关闭自动激活功能

1. 选择客户端右上角的配置文件图标。 WorkDocs

2. 在管理员下，选择打开管理员控制面板。
3. 向下滚动到安全，然后选择更改。

   系统将显示策略设置对话框。
4. 在 “自动激活” 下，清除 “允许目录中的所有用户在首次登录您的 WorkDocs 网站时自动激活” 旁边的复选框。

“应允许谁激活您 WorkDocs 站点中的目录用户” 下的选项发生了变化。您可以让当前用户邀请新用户，也可以将该权限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。

重复第 1 步到第 4 步以重新启用自动激活功能。

管理链接共享

本主题介绍如何管理链接共享。 WorkDocs 用户可以通过共享文件和文件夹的链接来共享文件和文件夹。他们可以在组织内部和外部共享文件链接，但只能在内部共享文件夹链接。作为管理员，您可以管理谁能够共享链接。

启用链接共享

1. 选择客户端右上角的配置文件图标。 WorkDocs

2. 在管理员下，选择打开管理员控制面板。
3. 向下滚动到安全，然后选择更改。

   系统将显示策略设置对话框。
4. 在选择可共享链接的设置下，选择一个选项：
   - 不允许站点范围或公共可共享链接 – 为所有用户禁用链接共享。
   - 允许用户创建站点范围可共享链接，但不允许他们创建公共可共享链接 – 将链接共享限制为仅限站点成员。托管用户可以创建此类链接。
   - 允许用户创建站点范围可共享链接，但只有高级用户才能创建公共可共享链接 – 托管用户可以创建站点范围链接，但只有高级用户才能创建公共链接。互联网上的任何人都可以访问公共链接。
   - 所有托管用户都可以创建站点范围和公共可共享链接 – 托管用户可以创建公共链接。
5. 选择保存更改。

在启用自动激活功能的情况下控制用户邀请

启用自动激活功能（请记住，该功能默认处于开启状态）后，您可以授予用户邀请其他用户的权限。您可以向以下任何一类用户授予权限：

- 所有用户
- 高级用户
- 管理员

您也可以完全禁用权限，以下步骤说明了具体方法。

设置邀请权限

1. 选择客户端右上角的配置文件图标。 WorkDocs

2. 在管理员下，选择打开管理员控制面板。
3. 向下滚动到安全，然后选择更改。

   系统将显示策略设置对话框。
4. 在 “应允许谁在您的 WorkDocs站点中激活目录用户” 下，选中 “与外部用户共享” 复选框，选择复选框下方的选项之一，然后选择保存更改。

   -或-

   如果您不想让任何人邀请新用户，可以清除该复选框，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，请参阅本指南中的安全— 简单的 ActiveDirectory网站和安全- ActiveDirectory 连接器站点。

邀请新用户

1. 选择客户端右上角的配置文件图标。 WorkDocs

2. 在管理员下，选择打开管理员控制面板。
3. 在管理用户下，选择邀请用户。
4. 在邀请用户对话框中，对于您想邀请谁？，输入受邀者的电子邮件地址，然后选择发送。对每个邀请重复此步骤。

WorkDocs 向每位收件人发送一封邀请电子邮件。该邮件包含有关如何创建 WorkDocs 帐户的链接和说明。邀请链接将在 30 天后到期。

编辑用户

您可以更改用户信息和设置。

编辑用户

1. 选择客户端右上角的配置文件图标。 WorkDocs

2. 在管理员下，选择打开管理员控制面板。
3. 在管理用户下，选择用户姓名旁边的铅笔图标 (✎)。
4. 在编辑用户对话框中，您可以编辑以下选项：

   名字（仅限 Cloud Directory）

   用户的名字。

   姓氏（仅限 Cloud Directory）

   用户的姓氏。

   状态

   指定用户是活动还是非活动。有关更多信息，请参阅 禁用用户。

角色

指定某人是用户还是管理员。您也可以升级或降级已 WorkSpaces WorkSpace分配给他们的用户。有关更多信息，请参阅 用户角色概述。

存储

指定现有用户的存储限制。

5. 选择保存更改。

禁用用户

您可以通过将用户的状态更改为非活动来禁用其访问权限。

将用户状态更改为非活动

1. 选择客户端右上角的配置文件图标。 WorkDocs

2. 在管理员下，选择打开管理员控制面板。
3. 在管理用户下，选择用户姓名旁边的铅笔图标 (✎)。
4. 选择非活动，然后选择保存更改

已停用的用户无法访问您的 WorkDocs 网站。

> **Note**
>
> 将用户更改为 “非活动” 状态并不会从您的 WorkDocs 站点中删除其文件、文件夹或反馈。不过，您可以将非活动用户的文件和文件夹移交给活动的用户。有关更多信息，请参阅 移交文档所有权。

删除待处理用户

你可以删除处于 “待定” 状态的 Simple AD、Microsoft AWS 托管和 AD Connector 用户。要删除这些用户之一，请选择用户姓名旁边的垃圾桶图标 (🗑)。

您的 WorkDocs 网站必须始终至少有一个非访客用户的活跃用户。如果您需要删除所有用户，可以删除整个站点。

建议您不要删除已注册用户。相反，您应该将用户从 “活动” 状态切换为 “非活动” 状态，以防止他们访问您的 WorkDocs 网站。

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。

> **Warning**
>
> 您不能撤消此操作。

移交文档所有权

1. 选择客户端右上角的配置文件图标。 WorkDocs

2. 在管理员下，选择打开管理员控制面板。
3. 在管理用户下，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. 选择移交文档所有权，然后输入新所有者的电子邮件地址。
6. 选择保存更改。

下载用户列表

要从管理员控制面板下载用户列表，必须安装 C WorkDocs ompanion。要安装 C WorkDocs ompanion，请参阅应用程序和集成。 WorkDocs

下载用户列表

1. 选择客户端右上角的配置文件图标。 WorkDocs

2. 在管理员下，选择打开管理员控制面板。
3. 在管理用户下，选择下载用户。
4. 对于下载用户，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
   - 用户
   - 高级用户
   - Admin
5. WorkDocs 将文件保存到以下位置之一：
   - Windows – `Downloads/WorkDocsDownloads`
   - macOS – *`hard drive`*`/users/`*`username`*`/WorkDocsDownloads/folder`

> **Note**
>
> 下载可能需要一些时间。此外，下载的文件不会存放在您的 `/~users` 文件夹中。

有关这些用户角色的更多信息，请参阅用户角色概述。

共享与协作

您的用户可以通过发送链接或邀请来共享内容。如果您启用外部共享，用户还可以与外部用户协作。

WorkDocs 通过使用权限来控制对文件夹和文件的访问。系统根据用户的角色来应用权限。

内容

- 共享链接
- 通过邀请共享
- 外部共享
- 权限
- 允许协作编辑

共享链接

用户可以选择 “共享链接”，快速复制 WorkDocs 内容的超链接，并与组织内外的同事和外部用户共享内容。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：

- 该 WorkDocs 网站的所有成员都可以搜索、查看和评论该文件。
- 任何有链接的人，甚至不是 WorkDocs 网站成员的人，都可以查看该文件。此链接选项会将权限限制为“仅查看”。

具有查看权限的接收者只能查看文件。具有评论权限的用户可以发表评论和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，请从管理员控制面板更新安全设置。有关更多信息，请参阅 WorkDocs 从站点管理员控制面板进行管理。

通过邀请共享

启用“通过邀请共享”后，站点用户可以通过发送邀请电子邮件与个人用户或组共享文件或文件夹。邀请中包含指向共享内容的链接，受邀者可以打开共享的文件或文件夹。受邀者还可与其他站点成员或外部用户共享这些文件或文件夹。

您可以为每位受邀用户设置权限级别。您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。

> **Note**
>
> 共享邀请不包括嵌套组的成员。要将这些成员包括在内，必须将其添加到通过邀请共享列表中。

有关更多信息，请参阅 WorkDocs 从站点管理员控制面板进行管理。

外部共享

外部共享允许 WorkDocs 站点的托管用户共享文件和文件夹，并与外部用户协作，而不会产生额外费用。网站用户可以与外部用户共享文件和文件夹，而无需要求收件人必须是 WorkDocs 网站的付费用户。启用外部共享后，用户可以输入要与之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，只能设置仅查看者权限，无法设置其他权限。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。选择该链接会将外部用户带到该站点，在那里他们输入要登录的凭据 WorkDocs。他们可以在与我共享视图中查看文件或文件夹。

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。站点管理员必须为站点启用外部共享，然后托管用户才能与外部用户共享内容。访客用户要成为贡献者或共有者，必须由站点管理员将其升级到用户级别。有关更多信息，请参阅 用户角色概述。

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，请从管理员控制面板更新安全设置。有关更多信息，请参阅 WorkDocs 从站点管理员控制面板进行管理。

权限

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

内容

- 用户角色
- 共享文件夹的权限
- 共享文件夹中的文件的权限
- 不在共享文件夹中的文件的权限

用户角色

用户角色控制着文件夹和文件权限。您可以在文件夹一级应用以下用户角色：

- 文件夹拥有者 – 文件夹或文件的拥有者。
- 文件夹共有者 – 由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 – 对文件夹有无限访问权限的人员。
- 文件夹查看者 – 对文件夹有部分访问权限（只读权限）的人员。

您可以在单个文件夹一级应用以下用户角色：

- 拥有者 – 文件的拥有者。
- 共有者 – 由拥有者指定为文件共有者的用户或组。
- 贡献者* — 允许有人在档案中提供反馈。
- 查看者-对文件具有有限访问权限（只读权限和查看活动权限）的人。
- 匿名查看者 – 组织外部的非注册用户，可以通过外部查看链接查看共享的文件。除非另有说明，否则匿名查看者具有与查看者相同的只读权限。匿名查看者无法查看文件活动。

* 贡献者无法重命名现有文件版本。但是，他们可以上传具有不同名称的文件的新版本。

共享文件夹的权限

以下权限适用于共享文件夹的用户角色：

> **Note**
>
> 对文件夹应用的权限也会应用于此文件夹中的子文件夹和文件。

- 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 – 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。
- 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。

	查看	查看子文件夹	查看共享	下载文件夹	添加子文件夹	共享	撤销共享	删除子文件夹	删除顶级文件夹
文件夹所有者	✓	✓	✓	✓	✓	✓	✓	✓	✓
文件夹共有者	✓	✓	✓	✓	✓	✓	✓	✓	✓
文件夹贡献者	✓	✓	✓	✓	✓				
文件夹查看者	✓	✓	✓	✓					

共享文件夹中的文件的权限

以下权限适用于共享文件夹中文件的用户角色：

- 注释 – 可以向文件添加反馈。
- 删除 – 删除共享文件夹中的文件。
- 重命名 – 重命名文件。
- 上传 – 上传文件的新版本。
- 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能力。
- 禁止下载 – 禁止下载文件。

> **Note**
>
> - 选择此选项后，具有查看权限的用户仍然可以下载文件。为防止出现这种情况，请打开共享文件夹，然后为不希望这些用户下载的每个文件清除允许下载设置。
> - 当文件的所有者或共同所有者不允许下载该 MP4 文件时，贡献者和查看者将无法在 Amazon WorkDocs 网络客户端中播放该文件。

- 共享 – 与其他用户共享文件。
- 撤销共享 – 撤销文件的共享。

- 查看 – 查看共享文件夹中的文件。
- 查看共享 – 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 – 查看文件的先前版本。
- 删除版本 – 删除文件的一个或多个版本。
- 恢复版本 – 恢复文件的一个或多个已删除版本。
- 查看所有私有评论 – 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。

	注释	删除	重命名	上传	下载	禁止下载	共享	撤销共享	视图	查看共享	查看注释	查看活动	查看版本	删除版本	恢复版本	查看所有私有评论**
文件所有者*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
文件夹所有者*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

	注释	删除	重命名	上传	下载	禁止下载	共享	撤销共享	视图	查看共享	查看注释	查看活动	查看版本	删除版本	恢复版本	查看所有私有评论**
文件夹共同所有者**	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
文件夹贡献者***	✓			✓	✓				✓	✓	✓	✓	✓			
文件夹查看者					✓				✓	✓		✓				

	注释	删除	重命名	上传	下载	禁止下载	共享	撤销共享	视图	查看共享	查看注释	查看活动	查看版本	删除版本	恢复版本	查看所有私有评论 **
匿名查看者									✓	✓						

* 在这种情况下，文件所有者是将文件的原始版本上传到共享文件夹的人。此角色的权限仅适用于所拥有的文件，不适用于共享文件夹中的所有文件。

** 所有者和共同所有者可以查看所有私人评论。贡献者只有回复评论之后才能看到私有评论。

*** 贡献者无法重命名现有文件版本。但是，他们可以上传具有不同名称的文件的新版本。

不在共享文件夹中的文件的权限

以下权限适用于不在共享文件夹中文件的用户角色：

- 注释 – 可以向文件添加反馈。
- 删除 – 删除文件。
- 重命名 – 重命名文件。
- 上传 – 上传文件的新版本。
- 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能力。
- 禁止下载 – 禁止下载文件。

> **Note**
>
> 当文件的所有者或共同所有者不允许下载该 MP4 文件时，贡献者和查看者将无法在 Amazon WorkDocs 网络客户端中播放该文件。

- 共享 – 与其他用户共享文件。
- 撤销共享 – 撤销文件的共享。
- 查看 – 查看文件。
- 查看共享 – 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 – 查看文件的先前版本。
- 删除版本 – 删除文件的一个或多个版本。
- 恢复版本 – 恢复文件的一个或多个已删除版本。

	注释	删除	重命名	上传	下载	禁止下载	共享	撤销共享	视图	查看共享	查看注释	查看活动	查看版本	删除版本	恢复版本
所有者*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
共同所有者*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
贡献者**	✓			✓	✓				✓	✓	✓	✓	✓		

	注释	删除	重命名	上传	下载	禁止下载	共享	撤销共享	视图	查看共享	查看注释	查看活动	查看版本	删除版本	恢复版本
查看者					✓				✓	✓		✓			
匿名查看者									✓	✓					

* 文件所有者和共同所有者可以查看所有私人评论。贡献者只有回复评论之后才能看到私有评论。

** 贡献者无法重命名现有文件版本。但是，他们可以上传具有不同名称的文件的新版本。

允许协作编辑

您可以使用管理员控制面板中的在线编辑设置部分来启用协作编辑选项。

内容

- 启用 Hancom ThinkFree
- 启用“使用 Office Online 打开”功能

启用 Hancom ThinkFree

你可以 ThinkFree 为你的 WorkDocs 网站启用 Hancom，这样用户就可以通过 WorkDocs Web 应用程序创建和协作编辑 Microsoft Office 文件。如需了解更多信息，请参阅使用 Hancom ThinkFree 编辑。

WorkDocs 用户无需支付额外费用即可使用Hancom ThinkFree 。无需其他许可或软件安装。

启用 Hancom ThinkFree

从管理员控制面板启用 Hancom ThinkFree 编辑。

1. 在我的账户下，选择打开管理员控制面板。
2. 对于 Hancom 在线编辑，选择更改。
3. 选择启用 Hancom 在线编辑特征，查看使用条款，然后选择保存。

禁用 Hancom ThinkFree

在管理员控制面板中禁用 Hancom ThinkFree 编辑。

1. 在我的账户下，选择打开管理员控制面板。
2. 对于 Hancom 在线编辑，选择更改。
3. 清除启用 Hancom 在线编辑特征复选框，然后选择保存。

启用“使用 Office Online 打开”功能

为你的 WorkDocs 网站启用 Office Online 打开，这样用户就可以通过 WorkDocs Web 应用程序协作编辑 Microsoft Office 文件。

对于同时拥有 Microsoft Office 365 Work 或 S chool 帐户并获得 Office Online 编辑许可证的 WorkDocs 用户，可以免费使用 Office Online 打开。有关更多信息，请参阅使用 Office Online 打开。

启用“使用 Office Online 打开”

从管理员控制面板启用“使用 Office Online 打开”。

1. 在我的账户下，选择打开管理员控制面板。
2. 对于 Office Online，选择更改。
3. 选择启用 Office Online，然后选择保存。

禁用“使用 Office Online 打开”

从管理员控制面板中禁用“使用 Office Online 打开”。

1. 在我的账户下，选择打开管理员控制面板。
2. 对于 Office Online，选择更改。
3. 清除启用 Office Online 复选框，然后选择保存。

将文件迁移到 WorkDocs

WorkDocs 管理员可以使用 WorkDocs 迁移服务将多个文件和文件夹大规模迁移到其 WorkDocs 站点。 WorkDocs 迁移服务可与亚马逊简单存储服务 (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 WorkDocs。

在此过程中， WorkDocs 为您提供 AWS Identity and Access Management (IAM) 策略。使用此策略创建新的 IAM 角色，该角色授予对 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 桶。
- 阅读并写入您指定的 WorkDocs 站点。

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

- 您 WorkDocs 网站的管理员权限
- 创建 IAM 角色的权限

如果您的 WorkDocs 站点设置在与您的 WorkSpaces 车队相同的目录中，则必须遵循以下要求：

- 请勿使用管理员作为您的 WorkDocs 账户用户名。Admin 是 WorkDocs 中的保留用户角色。
- 您的 WorkDocs 管理员用户类型必须为 “升级后的 WS 用户”。有关更多信息，请参阅用户角色概述和编辑用户。

> **Note**
>
> 迁移到时会保留目录结构、文件名和文件内容 WorkDocs。不保留文件所有权和权限。

任务

- 步骤 1：准备要迁移的内容。
- 步骤 2：将文件上传到 Amazon S3
- 步骤 3：计划迁移
- 步骤 4：跟踪迁移
- 步骤 5：清理资源

步骤 1：准备要迁移的内容。

准备要迁移的内容

1. 在您的 WorkDocs 网站的 “我的文档” 下，创建一个要将文件和文件夹迁移到的文件夹。
2. 请确认以下内容：
   - 源文件夹包含的文件和子文件夹不超过 100,000 个。如果超过该限制，迁移将会失败。
   - 任何文件都不超过 5 TB。
   - 每个文件名包含 255 个字符或更少字符。 WorkDocs 云端硬盘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。
- 开头或结尾的句点 – 例如：`.file`、`.file.ppt`、`.`、`..` 或 `file.`
- 开头或结尾的波浪号 – 例如：`file.doc~`、`~file.doc` 或 `~$file.doc`
- 以 **`.tmp`** 结尾的文件名 – 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 `Thumbnails`
- 包含以下任一字符的文件名 – `*`（星号）、`/`（正斜线）、`\`（反斜线）、`:`（冒号）、`<`（小于号）、`>`（大于号）、`?`（问号）、`|`（竖线）、`"`（双引号）或 `\202E`（字符代码 202E）。

步骤 2：将文件上传到 Amazon S3

将文件上传到 Amazon S3

1. 在 AWS 您的账户中创建一个新的亚马逊简单存储服务 (Amazon S3) 存储桶，您要将文件和文件夹上传到该存储桶。Amazon S3 存储桶必须与您的 WorkDocs 网站位于相同的 AWS 账户和 AWS

区域。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的 Amazon Simple Storage Service 入门。

2. 将文件上传到您在上一步中创建的 Amazon S3 桶。我们建议使用将您的文件和文件夹上传 AWS DataSync 到 Amazon S3 存储桶。 DataSync 提供了其他跟踪、报告和同步功能。有关更多信息，请参阅AWS DataSync 用户指南 DataSync中的AWS DataSync 工作原理和使用基于身份的策略（IAM 策略）。

步骤 3：计划迁移

完成步骤 1 和步骤 2 后，使用 WorkDocs 迁移服务安排迁移。迁移服务可能需要长达一周的时间来处理您的迁移请求，并会向您发送电子邮件，告知您可以开始迁移。如果您在收到电子邮件之前就开始迁移，管理控制台会显示一条消息，提示您等待一段时间。

安排迁移时，您的 WorkDocs 用户帐户存储空间设置会自动更改为 “无限制”。

> **Note**
>
> 迁移超过 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WorkDocs 定价。

WorkDocs 迁移服务提供了一个 AWS Identity and Access Management (IAM) 策略供您用于迁移。通过此策略，您可以创建一个新的 IAM 角色，该角色向 WorkDocs 迁移服务授予访问您指定的 Amazon S3 存储桶和 WorkDocs 站点的权限。您还订阅了 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 WorkDocs 控制台中，选择应用程序，迁移。
   - 如果这是您首次访问 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，然后选择继续。
2. 选择创建迁移。
3. 对于源类型，选择 Amazon S3。
4. 选择下一步。
5. 对于数据源和验证，在示例策略下，复制提供的 IAM 策略。

6. 使用您在上一步中复制的 IAM 策略来创建新的 IAM 策略和角色，如下所示：
   a. 使用 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
   b. 选择策略，然后选择创建策略。
   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. 依次选择角色和创建角色。
   g. 选择另一个 AWS 账户。对于账户 ID，输入以下内容之一：
      - 对于美国东部（弗吉尼亚州北部）区域，输入 899282061130
      - 对于美国西部（俄勒冈州）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
      - 对于欧洲地区（爱尔兰）区域，输入 191921258524
   h. 选择您创建的新策略，然后选择下一步：查看。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。选择创建角色。
   j. 在角色页面上的角色名称下，选择您创建的角色名称。
   k. 在摘要页面上，将最长 CLI/API 会话持续时间更改为 12 小时。
   l. 将角色 ARN 复制到剪贴板中以便在下一步中使用。
7. 返回到 WorkDocs 迁移服务。对于数据源和验证，在角色 ARN 下方，粘贴您在上一步中复制的 IAM 角色中的角色 ARN。
8. 对于桶，选择要从中迁移文件的 Amazon S3 桶。
9. 选择下一步。
10. 在 “选择目标 WorkDocs 文件夹” 中，选择要将文件迁移 WorkDocs 到的目标文件夹。
11. 选择下一步。
12. 在审核下，对于标题，输入迁移的名称。
13. 选择迁移的日期和时间。
14. 选择发送。

步骤 4：跟踪迁移

您可以从迁移服务登录页面中跟踪 WorkDocs 迁移情况。要从 WorkDocs 网站访问登录页面，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，也可以选择取消迁移，或选择更新以更新迁移的时间表。迁移完成后，您可以选择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。

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。

已取消

迁移已取消。

步骤 5：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. 使用 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 选择策略。
3. 搜索并选择您创建的策略。
4. 对于策略操作，选择删除。

5. 选择删除。
6. 选择角色。
7. 搜索并选择您创建的角色。
8. 依次选择删除角色和删除。

计划迁移开始时，您的 WorkDocs 用户帐户存储空间设置将自动更改为 “无限制”。迁移完成后，您可以使用管理控制面板更改该设置。有关更多信息，请参阅 编辑用户。

排查 WorkDocs 问题

以下信息可以帮助您解决问题 WorkDocs。

事务

- 无法在特定 AWS 地区设置我的 WorkDocs 网站
- 想在现有 Amazon VPC 中设置我的 WorkDocs 网站
- 用户需要重置密码
- 用户意外共享了一个敏感文档
- 用户离开了组织，没有移交文档所有权
- 需要将 WorkDocs 云端硬盘或 WorkDocs 配套部署给多个用户
- 在线编辑不起作用

无法在特定 AWS 地区设置我的 WorkDocs 网站

如果您要设置新 WorkDocs 站点，请在设置过程中选择 AWS 区域。有关详细信息，请参阅 入门 WorkDocs下的特定使用案例的教程。

想在现有 Amazon VPC 中设置我的 WorkDocs 网站

设置新 WorkDocs 站点时，请使用现有虚拟私有云 (VPC) 创建目录。 WorkDocs 使用此目录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。

需要将 WorkDocs 云端硬盘或 WorkDocs 配套部署给多个用户

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 Amazon 的身份和访问管理 WorkDocs。有关向多个用户部署 WorkDocs 云端硬盘的具体信息，请参阅将 WorkDocs 云端硬盘部署到多台计算机。

在线编辑不起作用

确认您已安装 WorkDocs 配套软件。要安装 C WorkDocs ompanion，请参阅 “应用程序和集成” WorkDocs。

管理亚马逊 WorkDocs 企业采购商城

如果您是亚马逊企业版 WorkDocs 的管理员，则可以使用亚马逊企业版凭证登录 https://workdocs.aws/ 来管理用户。

邀请新用户加入 Amazon Business WorkDocs

1. 在 https://workdocs.aws/ 上使用 Amazon Business 凭证进行登录。
2. 在 F WorkDocs or Amazon Business 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. 对于收件人，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 Amazon Busines WorkDocs s 上搜索用户

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

选择亚马逊企业版 WorkDocs 的用户角色

1. 在 https://workdocs.aws/ 上使用 Amazon Business 凭证进行登录。
2. 在 F WorkDocs or Amazon Business 主页上，打开左侧的导航窗格。
3. 选择管理员设置。
4. 在人员下，在用户旁边，选择要分配给用户的角色。

删除 Amazon Busines WorkDocs s 上的用户

1. 在 https://workdocs.aws/ 上使用 Amazon Business 凭证进行登录。
2. 在 F WorkDocs or Amazon Business 主页上，打开左侧的导航窗格。
3. 选择管理员设置。

4. 在人员下，选择用户旁边的省略号 (...)。
5. 选择删除。
6. 如果出现提示，请输入要接收用户文件的新用户，然后选择删除。

要添加到允许列表的 IP 地址和域

如果您对可访问的设备实施 IP 过滤 WorkDocs，请将以下 IP 地址和域名添加到允许列表中。这样做可以使 WorkDocs WorkDocs 云端硬盘连接到该 WorkDocs 服务。

- zocalo.ap-northeast-1.amazonaws.com
- zocalo.ap-southeast-2.amazonaws.com
- zocalo.eu-west-1.amazonaws.com
- zocalo.eu-central-1.amazonaws.com
- zocalo.us-east-1.amazonaws.com
- zocalo。 us-gov-west-1.amazonaws.com
- zocalo.us-west-2.amazonaws.com
- awsapps.com
- amazonaws.com
- cloudfront.net
- aws.amazon.com
- amazonworkdocs.com
- console.aws.amazon.com
- cognito-identity.us-east-1.amazonaws.com
- firehose.us-east-1.amazonaws.com

如果需要使用 IP 地址范围，请参阅《AWS 一般参考》中的 AWS IP 地址范围。

文档历史记录

下表描述了自 2018 年 2 月起对《亚马逊 WorkDocs 管理指南》所做的重要更改。如需有关此文档更新的通知，您可以订阅 RSS 源。

变更	说明	日期
新的文件所有者权限	管理员现在可以提供“删除版本”和“恢复版本”权限。这些权限是 DeleteDocumentVersionAPI 发布的一部分。	2022 年 7 月 29 日
WorkDocs 备份	已从《Amazon WorkDocs 管理指南》中删除 WorkDocs 备份文档，因为该组件不再受支持。	2021 年 6 月 24 日
管理亚马逊 WorkDocs 企业采购商城	WorkDocs 亚马逊企业版支持管理员管理用户。有关更多信息，请参阅《亚马逊管理 WorkDocs 指南》中的 “亚马逊企业 WorkDocs 管理”。	2020 年 3 月 26 日
将文件迁移到亚马逊 WorkDocs	WorkDocs 管理员可以使用 WorkDocs 迁移服务将多个文件和文件夹大规模迁移到其 WorkDocs 站点。有关更多信息，请参阅《Amazon WorkDocs 管理指南》WorkDocs中的将文件迁移到。	2019 年 8 月 8 日
IP 白名单设置	IP 允许列表设置可用于按 IP 地址范围筛选对您 WorkDocs 网站的访问权限。有关更多信息，请参阅《Amazon WorkDocs 管理指南》中的 IP 允许列表设置。	2018 年 10 月 22 日

Hancom ThinkFree	Hancom 可 ThinkFree 用。用户可以通过 WorkDocs Web 应用程序创建和协作编辑 Microsoft Office 文件。有关更多信息，请参阅《亚马逊 WorkDocs 管理指南》 ThinkFree中的 “启用 Hancom”。	2018 年 6 月 21 日
使用 Office Online 打开	开始提供“使用 Office Online 打开”功能。用户可以通过 WorkDocs Web 应用程序协作编辑微软 Office 文件。有关更多信息，请参阅《亚马逊 WorkDocs 管理指南》中的 “启用 Office Online 打开”。	2018 年 6 月 6 日
故障排除	增加了故障排除主题。有关更多信息，请参阅《Amazon WorkDocs 管理指南》中的 WorkDocs 问题疑难解答。	2018 年 5 月 23 日
更改恢复站保留期	可以修改恢复站保留期。有关更多信息，请参阅《Amazon WorkDocs 管理指南》中的恢复箱保留期设置。	2018 年 2 月 27 日