aws

Guia de administração

Amazon WorkDocs

Amazon WorkDocs: Guia de administração

Table of Contents

Aviso: novas inscrições de clientes e atualizações de conta não estão mais disponíveis para a Amazon. WorkDocs Saiba mais sobre as etapas de migração aqui: Como migrar dados de WorkDocs.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.

O que é a Amazon WorkDocs?

WorkDocs A Amazon é um serviço corporativo de armazenamento e compartilhamento totalmente gerenciado e seguro, com fortes controles administrativos e recursos de feedback que melhoram a produtividade do usuário. Os arquivos são armazenados na nuvem com segurança. Os arquivos dos usuários ficam visíveis apenas para eles, seus colaboradores e visualizadores designados. Outros membros da sua organização não têm acesso a arquivos de outros usuários a não ser que você conceda o acesso a eles especificamente.

Os usuários podem compartilhar seus arquivos com outros membros da organização para colaboração ou revisão. Os aplicativos WorkDocs cliente podem ser usados para visualizar vários tipos diferentes de arquivos, dependendo do tipo de mídia da Internet do arquivo. WorkDocs suporta todos os formatos comuns de documentos e imagens, e o suporte para outros tipos de mídia é constantemente adicionado.

Para obter mais informações, consulte Amazon WorkDocs.

Acessando WorkDocs

Os administradores usam o WorkDocs console para criar e desativar sites WorkDocs . No painel de controle do administrador, eles podem gerenciar configurações de usuários, armazenamento e segurança. Para obter mais informações, consulte Gerenciando WorkDocs a partir do painel de controle do administrador do site e Convidar e gerenciar usuários WorkDocs .

Os usuários não administrativos usam os aplicativos cliente para acessar seus arquivos. Eles nunca usam o WorkDocs console ou o painel de administração. WorkDocs oferece vários aplicativos e utilitários clientes diferentes:

- Aplicativo web usado para gerenciamento e análise de documentos.
- Aplicativos nativos para dispositivos móveis usados para análise de documentos.
- WorkDocs Drive, um aplicativo que sincroniza uma pasta na área de trabalho do macOS ou do Windows com WorkDocs seus arquivos.

Para obter mais informações sobre como os usuários podem baixar WorkDocs clientes, editar seus arquivos e usar pastas, consulte os tópicos a seguir no Guia do WorkDocs usuário:

- Começando com WorkDocs

- Trabalhando com arquivos
- Trabalhando com pastas

Preços

Com WorkDocs, não há taxas ou compromissos iniciais. Você paga somente pelas contas de usuário ativas e pelo armazenamento que você usa. Para obter mais informações, consulte Definição de preço.

Como começar

Para começar WorkDocs, consulteCriação de um WorkDocs site.

Migração de dados de WorkDocs

WorkDocs fornece dois métodos para migrar dados de um WorkDocs site. Esta seção fornece uma visão geral desses métodos e links para etapas detalhadas para executar, solucionar problemas e otimizar cada método de migração.

Os clientes terão duas opções para transferir seus dados da Amazon WorkDocs: a funcionalidade existente de download em massa (método 1) ou nossa nova ferramenta de migração de dados (método 2). Os tópicos a seguir explicam como usar os dois métodos.

Tópicos

Método 1: Baixar arquivos em massa

Se quiser controlar quais arquivos você migra, você pode baixá-los manualmente em massa. Esse método permite selecionar apenas os arquivos desejados e baixá-los para outro local, como sua unidade local. Você pode baixar arquivos e pastas do seu WorkDocs site ou do WorkDocs Drive.

Lembre-se do seguinte:

- Os usuários do seu site podem baixar arquivos seguindo as etapas listadas abaixo. Se preferir, você pode configurar uma pasta compartilhada, fazer com que seus usuários movam os arquivos para essa pasta e, em seguida, baixá-la para outro local. Você também pode transferir a propriedade para si mesmo e realizar os downloads.
- Para baixar documentos do Microsoft Word com comentários, consulte Baixar documentos do Word com comentários, no Guia WorkDocs do usuário.
- Você deve usar o WorkDocs Drive para baixar arquivos maiores que 5 GB.
- Quando você usa o WorkDocs Drive para baixar arquivos e pastas, as estruturas de diretórios, os nomes dos arquivos e o conteúdo dos arquivos permanecem intactos. A propriedade, as permissões e as versões do arquivo não são mantidas.

Baixando arquivos da web

Você usa esse método para baixar arquivos quando:

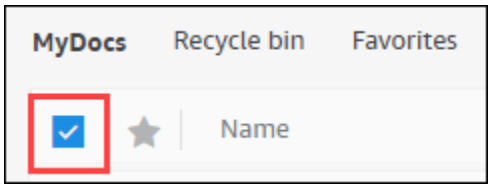
- Você só quer baixar alguns dos arquivos de um site.
- Você deseja baixar documentos do Word com comentários e fazer com que esses comentários permaneçam com seus respectivos documentos. A ferramenta de migração baixa todos os comentários, mas os grava em um arquivo XML separado. Os usuários do site podem então ter problemas para associar comentários a seus documentos do Word.

Para baixar arquivos da web

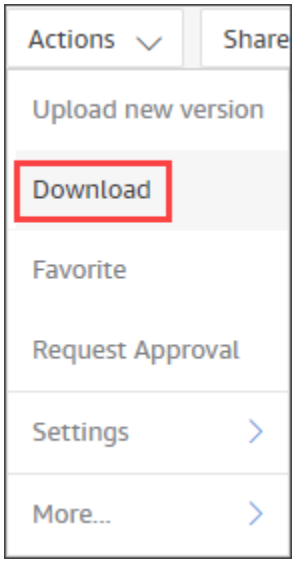
1. Faça login em WorkDocs.
2. Conforme necessário, abra a pasta que contém os arquivos que você deseja baixar.
3. Marque a caixa de seleção ao lado dos arquivos que você deseja baixar.

   —OU—

   Marque a caixa de seleção na parte superior da lista para escolher todos os arquivos na pasta.



4. Abra o menu Ações e escolha Baixar. .



   Em um PC, os arquivos baixados aparecem, por padrão, no nome da pasta WorkDocsDownloads Downloads//. Em um Macintosh, os arquivos chegam por padrão no nome do disco rígido /Usuários/nome de usuário/. WorkDocsDownloads

Baixando pastas da web

> **Note**
>
> Ao baixar pastas, você também baixa todos os arquivos nas pastas. Se você quiser baixar apenas alguns dos arquivos em uma pasta, mova os arquivos indesejados para outro local ou para a Lixeira e, em seguida, baixe a pasta.

Para baixar pastas da web

1. Faça login em WorkDocs
2. Marque a caixa de seleção ao lado de cada uma das pastas que você deseja baixar.

   —OU—

   Abra as pastas e marque as caixas de seleção ao lado das subpastas que você deseja baixar.
3. Abra o menu Ações e escolha Baixar. .

   Em um PC, as pastas baixadas aparecem, por padrão, em Downloads/WorkDocsDownloads/ nome da pasta. Em um Macintosh, os arquivos chegam por padrão no nome do disco rígido / Usuários/nome de usuário/. WorkDocsDownloads

Usando o WorkDocs Drive para baixar arquivos e pastas

> **Note**
>
> Você deve instalar o WorkDocs Drive para concluir as etapas a seguir. Para obter mais informações, consulte Instalando o WorkDocs Drive, no Guia do usuário do WorkDocs Drive.

Para baixar arquivos e pastas do WorkDocs Drive

1. Inicie o Explorador de Arquivos ou o Finder e abra sua unidade W:.
2. Selecione as pastas ou os arquivos que você deseja baixar.
3. Toque e segure (clique com o botão direito do mouse) nos itens selecionados e escolha Copiar e cole os itens copiados em seu novo local.

—OU—

Arraste os itens selecionados para o novo local.

4. Exclua os arquivos originais do WorkDocs Drive.

Método 2: Usar a ferramenta de migração

Você usa a ferramenta de WorkDocs migração quando deseja migrar todos os dados de um WorkDocs site.

A ferramenta de migração move os dados de um site para um bucket do Amazon Simple Storage Service. A ferramenta cria um arquivo ZIP compactado para cada usuário. O arquivo compactado inclui todos os arquivos e pastas, versões, permissões, comentários e anotações de cada um dos usuários finais do seu site. WorkDocs

Tópicos

Pré-requisitos

Você deve ter os seguintes itens para usar a ferramenta de migração.

- Um bucket do Amazon S3. Para obter informações sobre a criação de um bucket do Amazon S3, consulte Criação de um bucket, no Guia do usuário do Amazon S3. Seu bucket deve usar a mesma conta do IAM e residir na mesma região do seu WorkDocs site. Além disso, você deve bloquear o acesso público ao bucket. Para obter mais informações sobre como fazer isso, consulte Bloquear o acesso público ao seu armazenamento do Amazon S3, no Guia do usuário do Amazon S3.

  Para conceder WorkDocs permissão para carregar seus arquivos, configure a política de bucket conforme mostrado no exemplo a seguir. A política usa as chaves de `aws:SourceArn` condição

`aws:SourceAccount` e para reduzir o escopo da política, uma prática recomendada de segurança.

```
{
    "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*é o ID da organização do seu WorkDocs site. Isso pode ser encontrado na tabela “Meus sites” no WorkDocs console da AWS
> - Para obter mais informações sobre como configurar uma política de bucket, consulte Adicionar uma política de bucket usando o console do Amazon S3

- Uma política do IAM. Para iniciar uma migração no WorkDocs console, o responsável pela chamada do IAM deve ter a seguinte política anexada ao conjunto de permissões:

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

```
    ]
}
```

- Opcionalmente, você pode usar uma AWS KMS chave para criptografar os dados em repouso no seu bucket. Se você não fornecer uma chave, a configuração de criptografia padrão do bucket se aplica. Para obter mais informações, consulte Criação de chaves, no Guia do desenvolvedor do AWS Key Management Service.

  Para usar uma AWS KMS chave, adicione as seguintes declarações à política do IAM. Você deve usar uma chave ativa do tipo SYMMETRIC_DEFAULT.

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

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

Limitações

A ferramenta de migração tem as seguintes limitações:

- A ferramenta grava todas as permissões, comentários e anotações do usuário em arquivos CSV separados. Você deve mapear esses dados para os arquivos correspondentes manualmente.
- Você só pode migrar sites ativos.
- A ferramenta está limitada a uma migração bem-sucedida por site para cada período de 24 horas.
- Você não pode executar migrações simultâneas do mesmo site, mas pode executar migrações simultâneas para sites diferentes.
- Cada arquivo zip terá no máximo 50 GB. Usuários com mais de 50 GB de dados WorkDocs terão vários arquivos zip exportados para o Amazon S3.
- A ferramenta não exporta arquivos maiores que 50 GB. A ferramenta lista todos os arquivos maiores que 50 GB em um arquivo CSV que tenha o mesmo prefixo dos arquivos ZIP. Por

exemplo, ***site-alias***/workdocs///skippedFiles.csv. ***created-timestamp-UTC*** Você pode baixar os arquivos listados de forma programática ou manual. Para obter informações sobre o download programáticohttps://docs.aws.amazon.com/workdocs/latest/developerguide/download-documents.html, consulte o Guia do WorkDocs desenvolvedor. Para obter informações sobre como baixar os arquivos manualmente, consulte as etapas do Método 1, descritas anteriormente neste tópico.

- O arquivo zip de cada usuário conterá somente and/or pastas de arquivos de sua propriedade. Todas and/or as pastas de arquivos que foram compartilhadas com o usuário estarão no arquivo zip do usuário que possui as and/or pastas de arquivos.
- Se uma pasta estiver vazia (não contiver arquivos/pastas aninhados) WorkDocs, ela não será exportada.
- Não é garantido que quaisquer dados (arquivos, pastas, versões, comentários, anotações) criados após o início da tarefa de migração sejam incluídos nos dados exportados no S3.
- Você pode migrar vários sites para um bucket do Amazon S3. Você não precisa criar um bucket por site. No entanto, você deve garantir que suas políticas de IAM e bucket permitam vários sites.
- A migração aumenta seus custos do Amazon S3, dependendo da quantidade de dados que você migra para o bucket. Para obter mais informações, consulte a página de preços do Amazon S3.

Executando a ferramenta de migração

As etapas a seguir explicam como executar a ferramenta de WorkDocs migração.

Para migrar um site

1. Abra o WorkDocs console em https://console.aws.amazon.com/zocalo/.
2. No painel de navegação, escolha Meus sites e selecione o botão de opção ao lado do site que você deseja migrar.
3. Abra a lista de ações e escolha Migrar dados.
4. Na página do nome do site do Migrate Data, insira o URI do seu bucket do Amazon S3.

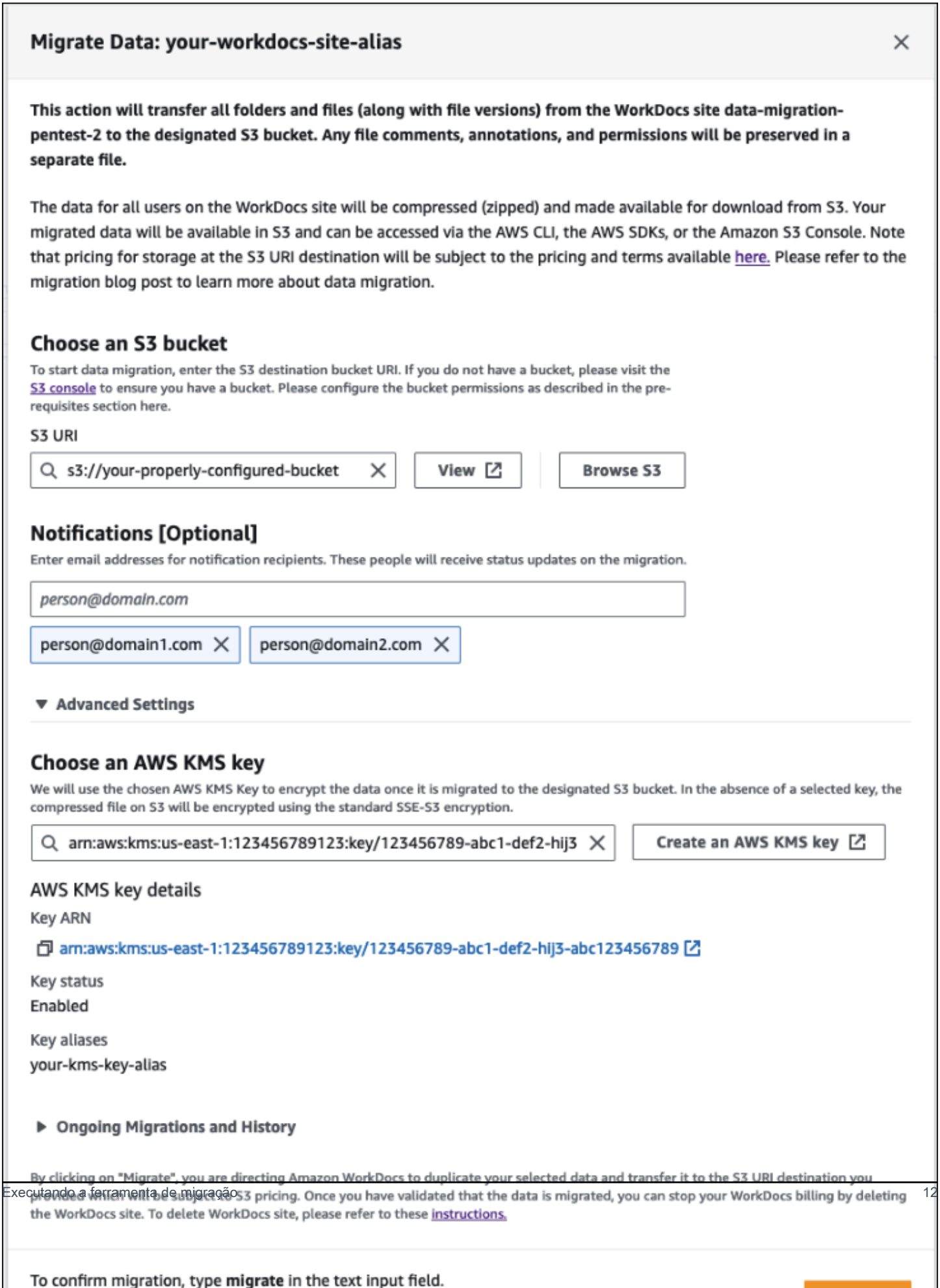
   —OU—

   Escolha Browse S3 e siga estas etapas:

   a. Conforme necessário, procure o balde.
   b. Selecione o botão de opção ao lado do nome do bucket e, em seguida, selecione Escolher.

5. (Opcional) Em Notificações, insira no máximo cinco endereços de e-mail. A ferramenta envia e-mails de status de migração para cada destinatário.
6. (Opcional) Em Configurações avançadas, selecione uma chave KMS para criptografar seus dados armazenados.
7. Digite **`migrate`** na caixa de texto para confirmar a migração e escolha Iniciar migração.

   Um indicador aparece e exibe o status da migração. Os tempos de migração variam, dependendo da quantidade de dados em um site.


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.

Quando a migração terminar:

- A ferramenta envia e-mails de “sucesso” para os endereços inseridos durante a configuração, se houver.
- Seu bucket do Amazon S3 conterá uma pasta /workdocs///*site-alias*. *created-timestamp-UTC* Essa pasta contém uma pasta compactada para cada usuário que tinha dados no site. Cada pasta compactada contém as pastas e os arquivos do usuário, incluindo as permissões e os comentários que mapeiam os arquivos CSV.
- Se um usuário remover todos os seus arquivos antes da migração, nenhuma pasta compactada será exibida para esse usuário.
- Versões — Documentos com várias versões têm um identificador de carimbo de data/hora de criação _ versão _. O carimbo de data/hora usa milissegundos de época. Por exemplo, um documento chamado “TestFile.txt” com duas versões aparece da seguinte forma:

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

- Permissões — O exemplo a seguir mostra o conteúdo de um arquivo CSV de permissões típico.

```
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
```

- Comentários — O exemplo a seguir mostra o conteúdo de um arquivo CSV de comentários típico.

```
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
```

- Arquivos ignorados — O exemplo a seguir mostra o conteúdo de um arquivo CSV típico de arquivos ignorados. Reduzimos o ID e ignoramos os valores do motivo para melhor legibilidade.

```
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...
```

Baixando dados migrados do Amazon S3

Como a migração aumenta seus custos do Amazon S3, você pode baixar os dados migrados do Amazon S3 para outra solução de armazenamento. Este tópico explica como baixar seus dados migrados e fornece sugestões para fazer o upload de dados em uma solução de armazenamento.

> **Note**
>
> As etapas a seguir explicam como baixar um arquivo ou pasta por vez. Para obter informações sobre outras formas de baixar arquivos, consulte Download de objetos no Guia do usuário do Amazon S3.

Para baixar dados

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Selecione o bucket de destino e navegue até o alias do site.
3. Marque a caixa de seleção ao lado da pasta compactada.

   —OU—

Abra a pasta compactada e marque a caixa de seleção ao lado do arquivo ou pasta de um usuário individual.

4. Escolha Baixar.

Sugestões para soluções de armazenamento

Para sites grandes, recomendamos provisionar uma EC2 instância usando uma Amazon Machine Image compatível com Linux para baixar programaticamente seus dados do Amazon S3, descompactar os dados e enviá-los para seu provedor de armazenamento ou disco local.

Solução de problemas de migrações

Experimente estas etapas para garantir que você tenha configurado seu ambiente corretamente:

- Se a migração falhar, uma mensagem de erro será exibida na guia Histórico de migração no WorkDocs console. Examine a mensagem de erro.
- Verifique as configurações do bucket do Amazon S3.
- Execute novamente a migração.

Se o problema persistir, entre em contato com AWS Support. Inclua o URL do WorkDocs site e o ID do Job de Migração, localizados na tabela do histórico de migração.

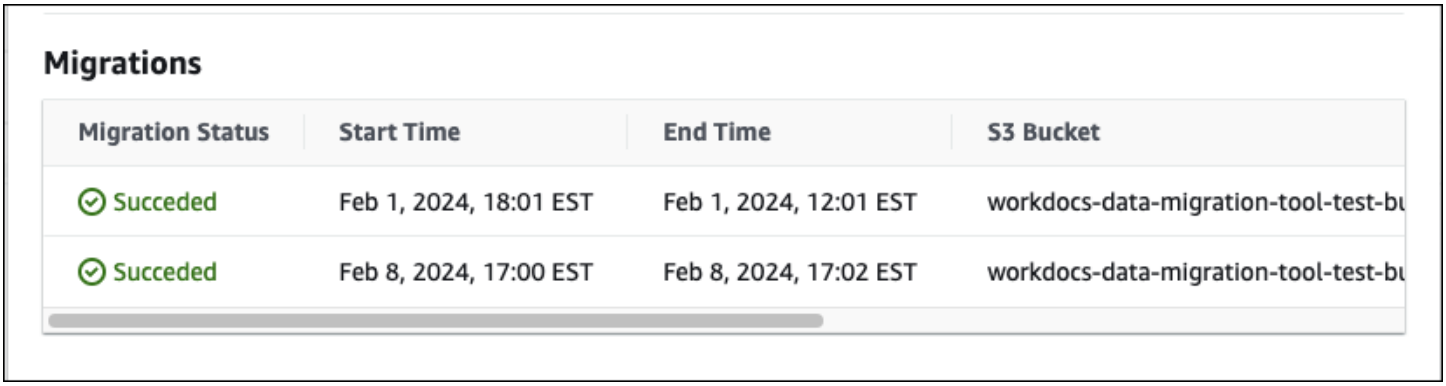
Visualizando seu histórico de migração

As etapas a seguir explicam como visualizar seu histórico de migração.

Para ver seu histórico

1. Abra o WorkDocs console em https://console.aws.amazon.com/zocalo/.
2. Selecione o botão de rádio ao lado do WorkDocs site desejado.
3. Abra a lista de ações e escolha Migrar dados.
4. Na página do nome do site do Migrate Data, escolha Histórico e migrações em andamento.

O histórico de migração aparece em Migrações. A imagem a seguir mostra uma história típica.


Migrations
Migration Status
Start Time
End Time
S3 Bucket
Succeded
Feb 1, 2024, 18:01 EST
Feb 1, 2024, 12:01 EST
workdocs-data-migration-tool-test-bu
Succeded
Feb 8, 2024, 17:00 EST
Feb 8, 2024, 17:02 EST
workdocs-data-migration-tool-test-bu

Pré-requisitos para a Amazon WorkDocs

Para configurar novos WorkDocs sites ou gerenciar sites existentes, você deve concluir as tarefas a seguir.

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra a https://portal.aws.amazon.com/billing/inscrição.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma ligação ou mensagem de texto e inserir um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando https://aws.amazon.com/e escolhendo Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.

Para obter ajuda ao fazer login usando o usuário-raiz, consulte Fazer login como usuário-raiz no Guia do usuário do Início de Sessão da AWS .

2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilita o Centro de Identidade do IAM.

   Para obter instruções, consulte Habilitar o AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .

2. No Centro de Identidade do IAM, conceda o acesso administrativo a um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com o seu usuário do Centro de Identidade do IAM, use o URL de login enviado ao seu endereço de e-mail quando o usuário do Centro de Identidade do IAM foi criado.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

   Para obter instruções, consulte Criar um conjunto de permissões no Guia do usuário do AWS IAM Identity Center .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

Para obter instruções, consulte Adicionar grupos no Guia do usuário do AWS IAM Identity Center .

Segurança na Amazon WorkDocs

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isto como segurança da nuvem e segurança na nuvem.

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam à Amazon WorkDocs, consulte AWS Services in Scope by Compliance Program.
- Segurança na nuvem — O AWS serviço que você usa determina sua responsabilidade. Você também é responsável por outros fatores, incluindo a confidencialidade dos dados, os requisitos da empresa e as leis e regulamentos aplicáveis. Os tópicos desta seção ajudam você a entender como aplicar o modelo de responsabilidade compartilhada ao usar WorkDocs.

> **Note**
>
> Os usuários de uma WorkDocs organização podem colaborar com usuários de fora dessa organização enviando um link ou convite para um arquivo. No entanto, isso só se aplica a sites que usam um conector do Active Directory. Veja as configurações de links compartilhados do seu site e selecione a opção que melhor atenda aos requisitos da sua empresa.

Os tópicos a seguir mostram como configurar para atender WorkDocs aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus WorkDocs recursos.

Tópicos

- Resiliência na Amazon WorkDocs
- Segurança da infraestrutura na Amazon WorkDocs

Gerenciamento de identidade e acesso para a Amazon WorkDocs

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar WorkDocs os recursos. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- Público
- Autenticação com identidades
- Gerenciar o acesso usando políticas
- Como a Amazon WorkDocs trabalha com o IAM
- Exemplos de políticas WorkDocs baseadas em identidade da Amazon
- Solução de problemas de WorkDocs identidade e acesso da Amazon

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz WorkDocs.

Usuário do serviço — Se você usar o WorkDocs serviço para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais WorkDocs recursos para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudá-lo a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um recurso no WorkDocs, consulte Solução de problemas de WorkDocs identidade e acesso da Amazon.

Administrador de serviços — Se você é responsável pelos WorkDocs recursos da sua empresa, provavelmente tem acesso total WorkDocs a. É seu trabalho determinar quais WorkDocs recursos e recursos seus usuários do serviço devem acessar. Envie as solicitações ao administrador do IAM para alterar as permissões dos usuários de serviço. Revise as informações nesta página para

compreender os conceitos básicos do IAM. Para saber mais sobre como sua empresa pode usar o IAM com WorkDocs, consulteComo a Amazon WorkDocs trabalha com o IAM.

Administrador do IAM: se você for um administrador do IAM, talvez queira saber detalhes sobre como pode gravar políticas para gerenciar o acesso ao WorkDocs. Para ver exemplos de políticas WorkDocs baseadas em identidade que você pode usar no IAM, consulte. Exemplos de políticas WorkDocs baseadas em identidade da Amazon

Autenticação com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login em AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para designar solicitações por conta própria, consulte Versão 4 do AWS Signature para solicitações de API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser necessário fornecer informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação multifator no Guia do usuário do AWS IAM Identity Center e Usar a autenticação multifator da AWS no IAM no Guia do usuário do IAM.

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, é recomendável contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, é recomendável alternar as chaves de acesso. Para obter mais informações, consulte Alternar as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdminse conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Casos de uso para usuários do IAM no Guia do usuário do IAM.

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Para assumir temporariamente uma função do IAM no AWS Management Console, você pode alternar de um usuário para uma função do IAM (console). Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para usar perfis, consulte Métodos para assumir um perfil no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, é possível criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas por ele. Para ter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidade de terceiros (federação) no Guia do usuário do IAM. Se usar o Centro de Identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de Identidade do IAM correlaciona o conjunto de permissões a

um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Guia do Usuário do AWS IAM Identity Center .

- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos na Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões da entidade principal da chamada, usando um perfil de serviço ou um perfil vinculado ao serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.
  - Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.
  - Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir o perfil para executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados a serviço.
- Aplicativos em execução na Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância

e fazendo solicitações AWS CLI de AWS API. Isso é preferível a armazenar chaves de acesso na EC2 instância. Para atribuir uma AWS função a uma EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que os programas em execução na EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte Usar uma função do IAM para conceder permissões a aplicativos executados em EC2 instâncias da Amazon no Guia do usuário do IAM.

Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e perfis não têm permissões. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação independentemente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Listas de controle de acesso

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o AWS WAF Amazon VPC são exemplos de serviços que oferecem suporte. ACLs Para saber mais ACLs, consulte a visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um recurso avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade

do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.

- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre Organizations e SCPs, consulte Políticas de controle de serviços no Guia AWS Organizations do Usuário.
- Políticas de controle de recursos (RCPs) — RCPs são políticas JSON que você pode usar para definir o máximo de permissões disponíveis para recursos em suas contas sem atualizar as políticas do IAM anexadas a cada recurso que você possui. O RCP limita as permissões para recursos nas contas dos membros e pode afetar as permissões efetivas para identidades, incluindo a Usuário raiz da conta da AWS, independentemente de pertencerem à sua organização. Para obter mais informações sobre Organizations e RCPs, incluindo uma lista Serviços da AWS desse suporte RCPs, consulte Políticas de controle de recursos (RCPs) no Guia AWS Organizations do usuário.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recursos. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

> **Note**
>
> WorkDocs não oferece suporte às políticas de controle de serviços para organizações do Slack.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como a Amazon WorkDocs trabalha com o IAM

Antes de usar o IAM para gerenciar o acesso WorkDocs, você precisa entender quais recursos do IAM estão disponíveis para uso WorkDocs. Para ter uma visão de alto nível de como WorkDocs e outros AWS serviços funcionam com o IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

Tópicos

- Políticas baseadas em identidade do WorkDocs
- Políticas baseadas em recursos do WorkDocs
- Autorização baseada em tags do WorkDocs
- WorkDocs Funções do IAM

Políticas baseadas em identidade do WorkDocs

Com as políticas baseadas em identidade do IAM, você pode especificar ações permitidas ou negadas. WorkDocs suporta ações específicas. Para saber mais sobre os elementos usados em uma política JSON, consulte Referência de elementos de política JSON do IAM no Manual do usuário do IAM.

Ações

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

As ações políticas WorkDocs usam o seguinte prefixo antes da ação:`workdocs:`. Por exemplo, para conceder permissão a alguém para executar a operação da WorkDocs `DescribeUsers` API, você inclui a `workdocs:DescribeUsers` ação na política dessa pessoa. As declarações de política devem incluir um elemento `Action` ou WorkDocs . O `NotAction` define seu próprio conjunto de ações que descrevem as tarefas que podem ser executadas com esse serviço.

Para especificar várias ações em uma única instrução, separe-as com vírgulas, como segue:

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

Você também pode especificar várias ações usando caracteres curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `Describe`, inclua a seguinte ação:

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

> **Note**
>
> Para garantir a compatibilidade com versões anteriores, inclua a ação `zocalo`. Por exemplo:
>
> ```
> "Action": [
> "zocalo:*",
> "workdocs:*"
> ],
> ```

Para ver uma lista de WorkDocs ações, consulte Ações definidas WorkDocs no Guia do usuário do IAM.

Recursos

WorkDocs não suporta a especificação de recursos ARNs em uma política.

Chaves de condição

WorkDocs não fornece nenhuma chave de condição específica do serviço, mas oferece suporte ao uso de algumas chaves de condição globais. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Exemplos

Para ver exemplos de políticas WorkDocs baseadas em identidade, consulte. Exemplos de políticas WorkDocs baseadas em identidade da Amazon

Políticas baseadas em recursos do WorkDocs

WorkDocs não oferece suporte a políticas baseadas em recursos.

Autorização baseada em tags do WorkDocs

WorkDocs não oferece suporte à marcação de recursos ou ao controle de acesso com base em tags.

WorkDocs Funções do IAM

Uma função do IAM é uma entidade dentro da sua AWS conta que tem permissões específicas.

Usando credenciais temporárias com WorkDocs

Recomendados fortemente usar credenciais temporárias para fazer login com federação, assumir um perfil do IAM ou assumir um perfil entre contas. Você obtém credenciais de segurança temporárias chamando operações de AWS STS API, como AssumeRoleou GetFederationToken.

WorkDocs suporta o uso de credenciais temporárias.

Perfis vinculados a serviço

As funções vinculadas ao serviço permitem que AWS os serviços acessem recursos em outros serviços para concluir uma ação em seu nome. Os perfis vinculados a serviço aparecem em sua conta do IAM e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados a serviço.

WorkDocs não oferece suporte a funções vinculadas a serviços.

Perfis de serviço

Esse atributo permite que um serviço assuma um perfil de serviço em seu nome. O perfil permite que o serviço acesse recursos em outros serviços para concluir uma ação em seu nome. Os perfis de serviço aparecem em sua conta do IAM e são de propriedade da conta. Isso significa que um administrador do IAM pode alterar as permissões para esse perfil. Porém, fazer isso pode alterar a funcionalidade do serviço.

WorkDocs não oferece suporte a funções de serviço.

Exemplos de políticas WorkDocs baseadas em identidade da Amazon

> **Note**
>
> Para maior segurança, crie usuários federados em vez de usuários do IAM sempre que possível.

Por padrão, os usuários e os perfis do IAM não têm permissão para criar ou modificar recursos do WorkDocs . Eles também não podem realizar tarefas usando a AWS API AWS Management Console AWS CLI, ou. Um administrador do IAM deve criar políticas do IAM que concedam aos usuários e perfis permissão para executarem operações de API específicas nos recursos especificados de que precisam. O administrador deve anexar essas políticas aos usuários ou grupos do IAM que exigem essas permissões.

> **Note**
>
> Para garantir a compatibilidade com versões anteriores, inclua a ação `zocalo` em suas políticas. Por exemplo:
>
> ```
> {
>     "Version": "2012-10-17",
>     "Statement": [
>         {
>             "Sid": "VisualEditor0",
>             "Effect": "Deny",
>             "Action": [
>             "zocalo:*",
>             "workdocs:*"
>             ],
>             "Resource": "*"
>         }
>     ]
> }
> ```

Para saber como criar uma política baseada em identidade do IAM utilizando esses exemplos de documentos de política JSON, consulte Criar políticas na guia JSON no Guia do usuário do IAM.

Tópicos

- Práticas recomendadas de política
- Usar o console do WorkDocs
- Permitir que os usuários visualizem suas próprias permissões
- Permita que os usuários tenham acesso somente para leitura aos recursos WorkDocs
- Mais exemplos de políticas WorkDocs baseadas em identidade

Práticas recomendadas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir WorkDocs recursos em sua conta. Essas ações podem incorrer em custos para sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte Elementos da política JSON do IAM: condição no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações práticas para ajudar a

criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.

- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Usar o console do WorkDocs

Para acessar o WorkDocs console da Amazon, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize os detalhes dos WorkDocs recursos em sua AWS conta. Se você criar uma política baseada em identidade mais restritiva do que as permissões mínimas requeridas, o console não funcionará conforme planejado para as entidades do usuário ou perfil do IAM.

Para garantir que essas entidades possam usar o WorkDocs console, anexe também as seguintes políticas AWS gerenciadas às entidades. Para obter mais informações sobre como anexar políticas, consulte Adicionar permissões a um usuário no Guia do usuário do IAM.

- AmazonWorkDocsFullAccess
- AWSDirectoryServiceFullAccess
- AmazonEC2FullAccess

Essas políticas concedem ao usuário acesso total aos WorkDocs recursos, às operações do AWS Directory Service e às EC2 operações da Amazon de que a Amazon WorkDocs precisa para funcionar adequadamente.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente às ações que correspondem à operação da API que você está tentando executar.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou AWS .

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

Permita que os usuários tenham acesso somente para leitura aos recursos WorkDocs

A AmazonWorkDocsReadOnlyAccesspolítica AWS gerenciada a seguir concede a um usuário do IAM acesso somente de leitura aos WorkDocs recursos. A política dá ao usuário acesso a todas as WorkDocs `Describe` operações. O acesso às duas EC2 operações da Amazon é necessário para que WorkDocs você possa obter uma lista das suas VPCs e das sub-redes. O acesso à AWS Directory Service `DescribeDirectories` operação é necessário para obter informações sobre seus AWS Directory Service diretórios.

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

Mais exemplos de políticas WorkDocs baseadas em identidade

Os administradores do IAM podem criar políticas adicionais para permitir que uma função ou usuário do IAM acesse a WorkDocs API. Para obter mais informações, consulte Controle de acesso e autenticação para aplicativos administrativos no Guia do desenvolvedor do WorkDocs .

Solução de problemas de WorkDocs identidade e acesso da Amazon

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com WorkDocs um IAM.

Tópicos

- Não estou autorizado a realizar uma ação em WorkDocs
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha AWS conta acessem meus WorkDocs recursos

Não estou autorizado a realizar uma ação em WorkDocs

Se isso AWS Management Console indicar que você não está autorizado a realizar uma ação, entre em contato com o administrador para obter ajuda. O administrador é a pessoa que forneceu o seu nome de usuário e senha.

Não estou autorizado a realizar iam: PassRole

Se você receber uma mensagem de erro informando que não está autorizado a executar a ação `iam:PassRole`, as suas políticas devem ser atualizadas para permitir que você passe uma função para o WorkDocs.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazê-lo, você deve ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta utilizar o console para executar uma ação no WorkDocs. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

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

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha AWS conta acessem meus WorkDocs recursos

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. É possível especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se é WorkDocs compatível com esses recursos, consulteComo a Amazon WorkDocs trabalha com o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Registro e monitoramento na Amazon WorkDocs

Os administradores WorkDocs do site da Amazon podem visualizar e exportar o feed de atividades de um site inteiro. Eles também podem ser usados AWS CloudTrail para capturar eventos do WorkDocs console.

Tópicos

Exportação do feed de atividades de todo o site

Os administradores podem visualizar e exportar o feed de atividade de uma organização inteira. Para usar esse recurso, você deve primeiro instalar o WorkDocs Companion. Para instalar o WorkDocs Companion, consulte Aplicativos e integrações para WorkDocs.

Para visualizar e exportar um feed de atividade de toda a organização

1. No aplicativo web, escolha Atividade.
2. Escolha Filtro e mova o controle deslizante de Atividades em todo o site para ativar o filtro.
3. Selecione filtros de Activity Type (Tipo de atividade), escolha as configurações de Date Modified (Data de modificação) de acordo com a necessidade e, em seguida, escolha Apply (Aplicar).

4. Quando os resultados filtrados de feed de atividade aparecerem, pesquise por arquivo, por pasta ou por nome de usuário para reduzir os resultados. Você também pode adicionar ou remover filtros conforme necessário.
5. Escolha Export (Exportar) para exportar o feed de atividade para arquivos `.csv` e `.json` em seu desktop. O sistema exporta os arquivos para um dos locais a seguir:

   - Windows — WorkDocsDownloadspasta na pasta Downloads do seu PC
   - macOS: `/users/username/WorkDocsDownloads/folder`

   O arquivo exportado reflete todos os filtros que você aplicar.

   > **Note**
   >
   > Os usuários que não são administradores podem visualizar e exportar o feed de atividade somente de seu próprio conteúdo. Para obter mais informações, consulte Visualizando o feed de atividades no Guia WorkDocs do usuário da Amazon.

Usando AWS CloudTrail para registrar chamadas de WorkDocs API da Amazon

Você pode usar AWS CloudTrail; para registrar chamadas de WorkDocs API da Amazon. CloudTrail fornece um registro das ações realizadas por um usuário, função ou AWS serviço em WorkDocs. CloudTrail captura todas as chamadas de API para eventos WorkDocs as, incluindo chamadas do WorkDocs console e de chamadas de código para o. WorkDocs APIs

Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para. WorkDocs Se você não criar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos.

As informações coletadas por CloudTrail incluem solicitações, os endereços IP dos quais as solicitações foram feitas, os usuários que fizeram as solicitações e as datas da solicitação.

Para obter mais informações sobre CloudTrail, consulte o Guia AWS CloudTrail do usuário.

WorkDocs informações em CloudTrail

CloudTrail é ativado em sua AWS conta quando você cria a conta. Quando a atividade ocorre em WorkDocs, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua AWS conta. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em sua AWS conta, incluindo eventos para WorkDocs, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, ao criar uma trilha no console, ela é aplicada a todas as regiões da . A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- CloudTrail serviços e integrações suportados
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

Todas WorkDocs as ações são registradas CloudTrail e documentadas na Amazon WorkDocs API Reference. Por exemplo, chamadas para as `UpdateDocument` seções`CreateFolder`, `DeactivateUser` e geram entradas nos arquivos de CloudTrail log.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário-raiz ou usuário do IAM.
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail .

Entendendo as entradas do arquivo de WorkDocs log

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

WorkDocs gera diferentes tipos de CloudTrail entradas, aquelas do plano de controle e aquelas do plano de dados. A diferença importante entre os dois é que a identidade do usuário para entradas do ambiente de gerenciamento é um usuário do IAM. A identidade do usuário para entradas do plano de dados é o usuário do WorkDocs diretório.

> **Note**
>
> Para maior segurança, crie usuários federados em vez de usuários do IAM sempre que possível.

As informações confidenciais, como senhas, tokens de autenticação, comentários de arquivos e o conteúdo do arquivo são redigidas nas entradas do registro. Eles aparecem como HIDDEN_DUE_TO_SECURITY_REASONS nos registros. CloudTrail Eles aparecem como HIDDEN_DUE_TO_SECURITY_REASONS nos registros. CloudTrail

O exemplo a seguir mostra duas entradas de CloudTrail registro para WorkDocs: o primeiro registro é para uma ação do plano de controle e o segundo é para uma ação do plano de dados.

```
{
  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"
    }
  ]
}
```

Validação de conformidade para a Amazon WorkDocs

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Governança e conformidade de segurança: esses guias de implementação de solução abordam considerações sobre a arquitetura e fornecem etapas para implantar recursos de segurança e conformidade.
- Referência de serviços qualificados para HIPAA: lista os serviços qualificados para HIPAA. Nem todos Serviços da AWS são elegíveis para a HIPAA.
- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca

de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.

- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Resiliência na Amazon WorkDocs

A infraestrutura AWS global é construída em torno de AWS regiões e zonas de disponibilidade. AWS As regiões fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que executam o failover automaticamente entre as zonas de disponibilidade sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre AWS regiões e zonas de disponibilidade, consulte Infraestrutura AWS global.

Segurança da infraestrutura na Amazon WorkDocs

Como um serviço gerenciado, a Amazon WorkDocs é protegida pelos procedimentos AWS globais de segurança de rede. Para obter mais informações, consulte Segurança da infraestrutura no AWS Identity and Access Management no Guia do usuário do IAM e as melhores práticas de segurança, identidade e conformidade no AWS Architecture Center.

Você usa chamadas de API AWS publicadas para acessar WorkDocs pela rede. Os clientes devem ser compatíveis com o Transport Layer Security (TLS) 1.2 e recomendamos o uso do TLS 1.3. Os clientes também devem ter suporte a conjuntos de criptografia com perfect forward secrecy como Ephemeral Diffie-Hellman ou Ephemeral Elliptic Curve Diffie-Hellman. A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Começando com WorkDocs

WorkDocs usa um diretório para armazenar e gerenciar as informações da organização para seus usuários e seus documentos. Por sua vez, você anexa um diretório a um site ao provisionar esse site. Quando você faz isso, um WorkDocs recurso chamado Ativação automática adiciona os usuários no diretório do site como usuários gerenciados, o que significa que eles não precisam de credenciais separadas para fazer login no seu site e podem compartilhar e colaborar em arquivos. Cada usuário tem 1 TB de armazenamento, a menos que compre mais.

Você não precisa mais adicionar e ativar usuários manualmente, embora ainda possa. Você também pode alterar as funções e permissões do usuário sempre que precisar. Para obter mais informações sobre como fazer isso, consulte Convidar e gerenciar usuários WorkDocs mais adiante neste guia.

Se precisar criar diretórios, você pode:

- Crie um diretório do Simple AD.
- Crie um diretório AD Connector para conexão a um diretório on-premises.
- Habilite WorkDocs para trabalhar com um AWS diretório existente.
- WorkDocs Crie um diretório para você.

Você também pode criar uma relação de confiança entre seu diretório do AD e um AWS Managed Microsoft AD diretório.

> **Note**
>
> Se você fizer parte de um programa de conformidade, como a PCI, o FedRAMP ou o DoD, você deve configurar um diretório do AWS Managed Microsoft AD para atender aos requisitos de conformidade. As etapas desta seção explicam como usar um diretório existente do Microsoft AD. Para obter informações sobre a criação de um diretório do Microsoft AD, consulte AWS Managed Microsoft AD no Guia do administrador do AWS Directory Service.

Conteúdo

- Habilitar a autenticação multifator
- Promover um usuário a administrador

Criação de um WorkDocs site

As etapas nas seções a seguir explicam como configurar um novo WorkDocs site.

Tarefas

- Antes de começar
- Criação de um WorkDocs site

Antes de começar

Você deve ter os seguintes itens antes de criar um WorkDocs site.

- Uma AWS conta para criar e administrar WorkDocs sites. No entanto, os usuários não precisam de uma AWS conta para se conectar e usar WorkDocs. Para obter mais informações, consulte Pré-requisitos para a Amazon WorkDocs.
- Se você planeja usar o Simple AD, deve atender aos pré-requisitos identificados nos Pré-requisitos do Simple AD no Guia de administração do AWS Directory Service .
- Um AWS Managed Microsoft AD diretório se você pertencer a um programa de conformidade, como PCI, FedRAMP ou DoD. As etapas desta seção explicam como usar um diretório existente do Microsoft AD. Para obter informações sobre a criação de um diretório do Microsoft AD, consulte AWS Managed Microsoft AD no Guia do administrador do AWS Directory Service.
- Informações de perfil do administrador, incluindo o nome, o sobrenome e o endereço de e-mail.

Criação de um WorkDocs site

Siga estas etapas para criar um WorkDocs site em minutos.

Para criar o WorkDocs site

1. Abra o WorkDocs console em https://console.aws.amazon.com/zocalo/.
2. Na página inicial do console, em Criar um WorkDocs site, escolha Começar agora.

   —OU—

No painel de navegação, escolha Meus sites e, na página Gerenciar seus WorkDocs sites, escolha Criar um WorkDocs site.

O que acontece em seguida depende se você tem um diretório.

- Se você tiver um diretório, a página Selecionar um diretório será exibida e permitirá que você escolha um diretório existente ou crie um diretório.
- Se você não tiver um diretório, a página Configurar um tipo de diretório será exibida e permitirá que você crie um diretório Simple AD ou AD Connector

As etapas a seguir explicam como realizar as duas tarefas.

Para usar um diretório existente

1. Abra a lista de Diretórios disponíveis e escolha o diretório que você deseja usar.
2. Escolha Enable directory (Habilitar diretório).

Para criar um diretório do

1. Repita as etapas 1 e 2 acima.

   Nesse ponto, o que você faz depende se você deseja usar o Simple AD ou criar um AD Connector.

   Usar o Simple AD

   a. Escolha Simple AD, e em seguida, escolha Avançar.

      A página do site Create Simple AD é exibida.

   b. Em Ponto de acesso, na caixa URL do site, insira a URL do site.

   c. Em Definir WorkDocs administrador, insira o endereço de e-mail, nome e sobrenome do administrador.

   d. Conforme necessário, preencha as opções em Detalhes do diretório e configuração da VPC.

   e. Escolha Criar local do Simple AD.

Como criar um diretório AD Connector

a. Escolha AD Connector e, em seguida, escolha Avançar.

   A página do site Create AD Connector é exibida.

b. Preencha todos os campos em Detalhes do diretório.

c. Em Ponto de acesso, na caixa URL do site, insira a URL do seu site.

d. Conforme desejado, preencha os campos opcionais em Configuração de VPC.

e. Escolha Criar local do AD Connector.

WorkDocs faz o seguinte:

- Se você escolher Configurar uma VPC em meu nome na etapa 4 acima, WorkDocs criará uma VPC para você. Um diretório na VPC armazena informações do usuário e do WorkDocs site.
- Se você usou o Simple AD, WorkDocs cria um usuário de diretório e define esse usuário como WorkDocs administrador. Se você criou um diretório do AD Connector, WorkDocs define o usuário do diretório existente que você forneceu como WorkDocs administrador.
- Se você usou um diretório existente, WorkDocs solicita que você insira o nome de usuário do WorkDocs administrador. O usuário deve ser um membro do diretório.

> **Note**
>
> WorkDocs não notifica os usuários sobre o novo site. Você precisa comunicar a URL a eles e informá-los de que não precisam de um login separado para usar o site.

Habilitar o logon único

AWS Directory Service permite que os usuários acessem a Amazon a WorkDocs partir de um computador associado ao mesmo diretório no qual WorkDocs está registrado, sem inserir credenciais separadamente. WorkDocs os administradores podem habilitar o login único usando o console. AWS Directory Service Para obter mais informações, consulte Single Sign-On no Guia de administração do AWS Directory Service .

Depois que o WorkDocs administrador ativar o login único, talvez os usuários do WorkDocs site também precisem modificar as configurações do navegador da Web para permitir o login único. Para

obter mais informações, consulte Single sign-on for IE and Chrome e Single sign-on for Firefox no Guia de administração do AWS Directory Service .

Habilitar a autenticação multifator

Você usa o AWS Directory Services Console em https://console.aws.amazon.com/directoryservicev2/para habilitar a autenticação multifator para seu diretório AD Connector. Para habilitar a MFA, é necessário ter uma solução de MFA que seja um servidor Remote Authentication Dial-in User Service (RADIUS) ou MFA, ou ter um plug-in MFA para um servidor RADIUS já implementado na sua infraestrutura on-premises. A solução de MFA deve implementar Senhas únicas (OTP) que os usuários conseguem pelo dispositivo de hardware ou por um software em execução em um dispositivo, como telefone celular.

O RADIUS é um client/server protocolo padrão do setor que fornece gerenciamento de autenticação, autorização e contabilidade para permitir que os usuários se conectem aos serviços de rede. O AWS Managed Microsoft AD inclui um cliente RADIUS que se conecta ao servidor RADIUS em que você implementou sua solução de MFA. Seu servidor RADIUS valida o nome de usuário e código OTP. Se o seu servidor RADIUS validar o usuário com êxito, o AWS Managed Microsoft AD então autenticará o usuário no AD. Depois da autenticação bem-sucedida no AD, os usuários podem acessar o aplicativo da AWS. A comunicação entre o cliente do RADIUS do AWS Managed Microsoft AD e o servidor RADIUS exige que você configure grupos de segurança da AWS que permitam a comunicação pela porta 1812.

Para obter mais informações, consulte Como habilitar a autenticação multifator para AWS Managed Microsoft AD no Guia do administrador do AWS Directory Service.

> **Note**
>
> A autenticação multifator não está disponível para diretórios do Simple AD.

Promover um usuário a administrador

Você usa o WorkDocs console para promover um usuário a administrador. Siga estas etapas.

Para promover um usuário a administrador

1. Abra o WorkDocs console em https://console.aws.amazon.com/zocalo/.

2. No painel de navegação, selecione My sites.

   A página Gerenciar seus WorkDocs sites é exibida.

3. Selecione o botão ao lado do site desejado, escolha Ações e escolha Definir um administrador.

   A caixa de diálogo Definir WorkDocs administrador é exibida.

4. Na caixa Nome de usuário, insira o nome de usuário da pessoa que você deseja promover e escolha Definir administrador.

Você também pode usar o painel de controle do administrador do WorkDocs site para rebaixar um administrador. Para obter mais informações, consulte Editar usuários.

Gerenciando WorkDocs a partir do AWS console

Você usa essas ferramentas para gerenciar seus WorkDocs sites:

- O AWS console em https://console.aws.amazon.com/zocalo/.
- O painel de controle do administrador do site, disponível para administradores em todos os WorkDocs sites.

Cada uma dessas ferramentas fornece um conjunto diferente de ações, e os tópicos desta seção explicam as ações fornecidas pelo AWS console. Para obter informações sobre o painel de controle do administrador do site, consulte Gerenciando WorkDocs a partir do painel de controle do administrador do site.

Configurar administradores do site

Se você for administrador, poderá conceder aos usuários acesso ao painel de controle do site e às ações que ele fornece.

Para definir um administrador

1. Abra o WorkDocs console em https://console.aws.amazon.com/zocalo/.
2. No painel de navegação, selecione My sites.

   A página Gerenciar seus WorkDocs sites é exibida e exibe uma lista dos seus sites.
3. Selecione o botão ao lado do site cujo administrador você deseja definir.
4. Abra a lista de Ações e escolha Definir um administrador.

   A caixa de diálogo Definir WorkDocs administrador é exibida.
5. Na caixa Nome de usuário, insira o nome do novo administrador e escolha Definir administrador.

Reenviar um e-mail de convite

É possível reenviar um e-mail de convite a qualquer momento.

Reenviar um convite por e-mail

1. Abra o WorkDocs console em https://console.aws.amazon.com/zocalo/.

2. No painel de navegação, selecione My sites.

   A página Gerenciar seus WorkDocs sites é exibida e exibe uma lista dos seus sites.
3. Selecione o botão ao lado do site para o qual você deseja reenviar o e-mail.
4. Abra a lista de Ações e escolha Reenviar e-mail de convite.

   Uma mensagem de êxito em um banner verde é exibida na parte superior da página.

Como gerenciar a autenticação multifator

Você pode ativar a autenticação multifator depois de criar um WorkDocs site. Para obter mais informações sobre a autenticação, consulte Habilitar a autenticação multifator.

Configurando o site URLs

> **Note**
>
> Se você seguiu o processo de criação do site em Começando com WorkDocs, inseriu o URL do site. Como resultado, WorkDocs torna o comando Definir URL do site indisponível, pois você só pode definir um URL uma vez. Você só segue essas etapas se implantar a Amazon WorkSpaces e integrá-la à WorkDocs. O processo de WorkSpaces integração da Amazon faz com que você insira um número de série em vez de uma URL do site, então você precisa inserir uma URL depois de concluir a integração. Para obter mais informações sobre a integração da Amazon WorkSpaces , WorkDocs consulte Integrar com WorkDocs no Guia do WorkSpaces usuário da Amazon.

Para definir o URL de um site

1. Abra o WorkDocs console em https://console.aws.amazon.com/zocalo/.
2. No painel de navegação, selecione My sites.

   A página Gerenciar seus WorkDocs sites é exibida e exibe uma lista dos seus sites.
3. Selecione o site que você integrou com a Amazon WorkSpaces. O URL contém o ID do diretório da sua WorkSpaces instância da Amazon, como https://{directory_id}.awsapps.com.
4. Selecione o botão ao lado desse URL, abra a lista de Ações e escolha Definir URL do site.

A caixa de diálogo Definir URL do site é exibida.

5. Na caixa URL do site, insira o URL do site e escolha Definir URL do site.
6. Na página Gerenciar seus WorkDocs sites, escolha Atualizar para ver o novo URL.

Gerenciar notificações

> **Note**
>
> Para maior segurança, crie usuários federados em vez de usuários do IAM sempre que possível.

As notificações permitem que usuários ou funções do IAM chamem a CreateNotificationSubscriptionAPI, que você pode usar para definir seu próprio endpoint para processar as mensagens do SNS enviadas. WorkDocs Para obter mais informações sobre notificações, consulte Configurar notificações para um usuário ou função do IAM no Guia do WorkDocs desenvolvedor.

Você pode criar e excluir notificações, e as etapas a seguir explicam como realizar as duas tarefas.

> **Note**
>
> Para criar uma notificação, você precisa ter seu IAM ou ARN de função. Para encontrar seu ARN do IAM, faça o seguinte:
>
> 1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
> 2. Na barra de navegação, selecione Usuários.
> 3. Selecione seu nome de usuário.
> 4. Em Resumo, copie seu ARN.

Criar uma notificação

1. Abra o WorkDocs console em https://console.aws.amazon.com/zocalo/.
2. No painel de navegação, selecione My sites.

A página Gerenciar seus WorkDocs sites é exibida e exibe uma lista dos seus sites.

3. Selecione o botão ao lado do site desejado.
4. Abra a lista de Ações e escolha Gerenciar notificações.

   A página Gerenciar notificações é exibida.
5. Escolha Create Notification (Criar notificação).
6. Na caixa de diálogo Nova notificação, insira seu IAM ou ARN da função e escolha Criar notificações.

Para excluir uma notificação

1. Abra o WorkDocs console em https://console.aws.amazon.com/zocalo/.
2. No painel de navegação, selecione My sites.

   A página Gerenciar seus WorkDocs sites é exibida e exibe uma lista dos seus sites.
3. Escolha o botão ao lado do site que tem a notificação que você deseja excluir.
4. Abra a lista de Ações e escolha Gerenciar notificações.
5. Na página Gerenciar notificações, escolha o botão ao lado da notificação que você deseja excluir e, em seguida, escolha Excluir notificações.

Excluir um site

Você usa o WorkDocs console para excluir um site.

> **Warning**
>
> Você perde todos os arquivos quando exclui uma site. Exclua uma organização somente se tiver certeza de que essas informações não são mais necessárias.

Para excluir um site

1. Abra o WorkDocs console em https://console.aws.amazon.com/zocalo/.
2. Na barra de navegação, selecione Meus sites.

A página Gerenciar seus WorkDocs sites é exibida.

3. Escolha o botão Excluir ao lado da regra que deseja excluir.

   A caixa de diálogo Excluir URL do site é exibida.

4. Opcionalmente, escolha Também excluir o diretório de usuários.

   > **Important**
   >
   > Se você não fornecer seu próprio diretório para WorkDocs, criaremos um para você. Quando você exclui o WorkDocs site, você é cobrado pelo diretório que criamos, a menos que você exclua esse diretório ou o use para outro aplicativo da AWS. Para obter informações de definição de preço, consulte Definição de preço do AWS Directory Service.

5. Na caixa URL do site, insira o URL do site e escolha Excluir.

   A organização será imediatamente excluída e não estará mais disponível.

Gerenciando WorkDocs a partir do painel de controle do administrador do site

Você usa essas ferramentas para gerenciar seus WorkDocs sites:

- O painel de controle do administrador do site, disponível para administradores em todos os WorkDocs sites e descrito nos tópicos a seguir.
- O AWS console em https://console.aws.amazon.com/zocalo/.

Cada uma dessas ferramentas fornece um conjunto diferente de ações. Os tópicos nesta seção explicam as ações fornecidas pelo painel de controle do administrador do site. Para obter mais informações sobre tarefas disponíveis no console do, consulte Gerenciando WorkDocs a partir do AWS console.

Configurações do idioma de preferência

Você pode especificar o idioma das notificações por e-mail.

Como alterar as configurações de idioma

1. Em My Account (Minha conta), selecione Open admin control panel (Abrir painel de controle do administrador).
2. Em Definições de idioma preferido, selecione o idioma de sua preferência.

Office Online e edição online do Hancom

Habilite ou desabilite as configurações da Hancom Online Editing (Edição online do Hancom) e do Office Online no Admin control panel (Painel de controle do administrador). Para obter mais informações, consulte Habilitar edição colaborativa.

Armazenamento

Especifique a quantidade de armazenamento que os novos usuários recebem.

Como alterar as configurações de armazenamento

1. Em My Account (Minha conta), selecione Open admin control panel (Abrir painel de controle do administrador).
2. Em Armazenamento, selecione Alteração.
3. Na caixa de diálogo Limite de armazenamento, escolha se os novos usuários terão armazenamento limitado ou ilimitado.
4. Escolha Salvar alterações.

Alterar a configuração de armazenamento afeta somente os usuários adicionados após a alteração da configuração. Ela não altera a quantidade de armazenamento alocada aos usuários existentes. Para alterar o limite de armazenamento de um usuário existente, consulte Editar usuários.

Lista de permissões de IP

WorkDocs os administradores do site podem adicionar configurações da Lista de IPs Permitidos para restringir o acesso ao site a um intervalo permitido de endereços IP. Você pode adicionar até 500 configurações da Lista de Permissões de IP por site.

> **Note**
>
> Atualmente, a Lista de IPs Permitidos funciona somente para IPv4 endereços. Atualmente, a lista de negação de endereços IP não é suportada.

Para adicionar um intervalo de IP à IP Allow List (Lista de permissões de IP)

1. Em My Account (Minha conta), selecione Open admin control panel (Abrir painel de controle do administrador).
2. Para IP Allow List (Lista de permissões de IP), selecione Change (Alterar).
3. Em Inserir valor de CIDR, insira o bloco Encaminhamento Entre Domínios Sem Classificação (CIDR) para os intervalos de endereços IP e selecione Adicionar.
   - Para permitir o acesso de um único endereço IP, especifique `/32` como prefixo CIDR.
4. Escolha Salvar alterações.

5. Os usuários que se conectam ao site a partir de endereços IP da IP Allow List (Lista de permissões de IP) têm acesso permitido. Os usuários que tentam se conectar ao site a partir de um endereço IP não autorizado recebem uma resposta informando que não está autorizado.

> **Warning**
>
> Se você inserir um valor CIDR que bloqueia o uso do endereço IP atual para acessar o site, será exibida uma mensagem de aviso. Se você escolher continuar com o valor CIDR atual, terá o acesso ao site bloqueado com seu endereço IP atual. Esta ação só pode ser revertida entrando em contato com o AWS Support.

Segurança — ActiveDirectory Sites simples

Este tópico explica as várias configurações de segurança para ActiveDirectory sites simples. Se você gerencia sites que usam ActiveDirectory conector, consulte a próxima seção.

Para usar configurações de segurança

1. Escolha o ícone do perfil no canto superior direito do WorkDocs cliente.

2. Em Admin, selecione Abrir painel de controle do administrador.
3. Role para baixo até Segurança e escolha Alterar.

   A caixa de diálogo Configurações de políticas é exibida. A tabela a seguir lista as configurações de segurança para ActiveDirectory sites simples.

Configuração	Descrição
Em Escolha sua configuração para links compartilháveis, selecione uma das seguintes opções:	
Não permita links compartilháveis públicos ou em todo o site	Desativa o compartilhamento de links para todos os usuários.

Configuração	Descrição
Permita que os usuários criem links compartilháveis em todo o site, mas não permita que eles criem links compartilháveis públicos	Limita o compartilhamento de links apenas aos membros do site. Usuários gerenciados podem criar esse tipo de link.
Permita que os usuários criem links compartilháveis em todo o site, mas somente usuários avançados podem criar links compartilháveis públicos	Usuários gerenciados podem criar links para todo o site, mas somente usuários avançados podem criar links públicos. Os links públicos permitem o acesso de qualquer pessoa na internet.
Todos os usuários gerenciados podem criar links compartilháveis públicos e em todo o site	Usuários gerenciados podem criar links públicos.

Em Ativação automática, marque ou desmarque a caixa de seleção.

Permita que todos os usuários do seu diretório sejam ativados automaticamente após o primeiro login WorkDocs no seu site.	Ativa automaticamente os usuários quando eles acessam seu site pela primeira vez.

Em Quem deve ter permissão para convidar novos usuários para seu WorkDocs site, selecione uma das seguintes opções:

Somente administradores podem convidar novos usuários.	Somente administradores podem convidar novos usuários.
Os usuários podem convidar novos usuários de qualquer lugar compartilhando arquivos ou pastas com elas.	Permite que os usuários convidem novos usuários compartilhando arquivos ou pastas com esses usuários.
Os usuários podem convidar novos usuários de alguns domínios específicos compartilhando arquivos ou pastas com elas.	Os usuários podem convidar novas pessoas dos domínios específicos compartilhando arquivos ou pastas com elas.

Em Configurar função para novos usuários, marque ou desmarque a caixa de seleção.

Configuração	Descrição
Os novos usuários do diretório serão usuários gerenciados (por padrão, eles são usuários convidados)	Converte automaticamente novos usuários do seu diretório em usuários gerenciados.

4. Quando terminar, escolha Salvar alterações.

Segurança — sites de ActiveDirectory conexão

Este tópico explica as várias configurações de segurança para sites de ActiveDirectory conectores. Se você gerencia sites que usam o Simple ActiveDirectory, consulte a seção anterior.

Para usar configurações de segurança

1. Escolha o ícone do perfil no canto superior direito do WorkDocs cliente.

2. Em Admin, selecione Abrir painel de controle do administrador.
3. Role para baixo até Segurança e escolha Alterar.

   A caixa de diálogo Configurações de políticas é exibida. A tabela a seguir lista e descreve as configurações de segurança para sites de ActiveDirectory conectores.

Configuração	Descrição
Em Escolha sua configuração para links compartilháveis, selecione uma das seguintes opções:	
Não permita links compartilháveis públicos ou em todo o site	Quando selecionada, desativa o compartil hamento de links para todos os usuários.
Permita que os usuários criem links compartil háveis em todo o site, mas não permita que eles criem links compartilháveis públicos	Limita o compartilhamento de links apenas aos membros do site. Usuários gerenciados podem criar esse tipo de link.

Configuração	Descrição
Permita que os usuários criem links compartilháveis em todo o site, mas somente usuários avançados podem criar links compartilháveis públicos	Usuários gerenciados podem criar links para todo o site, mas somente usuários avançados podem criar links públicos. Os links públicos permitem o acesso de qualquer pessoa na internet.
Todos os usuários gerenciados podem criar links compartilháveis públicos e em todo o site	Usuários gerenciados podem criar links públicos.

Em Ativação automática, marque ou desmarque a caixa de seleção.

Permita que todos os usuários do seu diretório sejam ativados automaticamente após o primeiro login WorkDocs no seu site.	Ativa automaticamente os usuários quando eles acessam seu site pela primeira vez.

Em Quem deve ter permissão para ativar os usuários do diretório em seu WorkDocs site? , selecione uma das seguintes opções:

Somente administradores podem ativar novos usuários do seu diretório.	Permite que somente administradores ativem novos usuários do diretório.
Os usuários podem ativar novos usuários de seu diretório compartilhando arquivos ou pastas com elas.	Permite que os usuários ativem os usuários do diretório compartilhando arquivos ou pastas com os usuários do diretório.
Os usuários podem ativar novos usuários de alguns domínios específicos compartilhando arquivos ou pastas com elas.	Os usuários só podem compartilhar arquivos ou pastas de usuários em domínios específicos. Ao escolher essa opção, você deve inserir os domínios.

Em Quem deve ter permissão para convidar novos usuários para seu WorkDocs site? , selecione uma das seguintes opções:

Configuração	Descrição
Share with external users (Compartilhamento com usuários externos) **Note** As opções abaixo só aparecem depois que você escolhe essa configuração.	Permite que administradores e usuários convidem novos usuários externos para seu WorkDocs site.
Only administrators can invite new external users (Somente administradores podem convidar novos usuários externos)	Somente administradores podem convidar usuários externos.
Todos os usuários gerenciados podem convidar novos usuários	Permite que usuários gerenciados convidem usuários externos.
Somente usuários avançados podem convidar novos usuários externos.	Permite que somente usuários avançados convidem novos usuários externos.

Em Configurar função para novos usuários, selecione uma ou ambas as opções.

Os novos usuários do diretório serão usuários gerenciados (por padrão, eles são usuários convidados)	Converte automaticamente novos usuários do seu diretório em usuários gerenciados.
New external users will be Managed users (they are Guest users by default) (Os novos usuários externos serão usuários gerenciados (por padrão, eles são usuários convidados))	Converte automaticamente novos usuários externos em usuários gerenciados.

4. Quando terminar, escolha Salvar alterações.

Retenção da lixeira de recuperação

Quando um usuário exclui um arquivo, WorkDocs armazena o arquivo na lixeira do usuário por 30 dias. Depois, WorkDocs move os arquivos para um compartimento de recuperação temporário por 60 dias e os exclui permanentemente. Somente administradores podem ver o compartimento de recuperação temporário. Ao alterar a política de retenção de dados de toda a organização, os administradores da organização podem alterar o período de retenção do volume de recuperação em um mínimo de zero dias e máximo de 365 dias.

Para alterar o período de retenção do volume de recuperação

1. Em My Account (Minha conta), selecione Open admin control panel (Abrir painel de controle do administrador).
2. Na opção Recovery bin retention (Retenção do volume de recuperação), selecione Alteração.
3. Insira o número de dias durante os quais os arquivos devem ser mantidos na lixeira de recuperação e escolha Salvar.

> **Note**
>
> O período de retenção padrão é de 60 dias. Você pode usar um período de 0 a 365 dias.

Os administradores podem restaurar os arquivos do usuário do compartimento de recuperação antes de WorkDocs excluí-los permanentemente.

Para restaurar o arquivo de um usuário

1. Em My Account (Minha conta), selecione Open admin control panel (Abrir painel de controle do administrador).
2. Em Gerenciar usuários, selecione o ícone da pasta do usuário.
3. Em Recovery bin (Lixeira de recuperação), selecione os arquivos a serem restaurados e, então, selecione o ícone Recover (recuperação).
4. Para Restore file (Restaurar arquivo), escolha o local para o qual restaurar o arquivo e selecione Restore (Restaurar).

Gerenciar configurações do usuário

Você pode gerenciar as configurações dos usuários, incluindo alterar as funções do usuário, bem como convidar, habilitar ou desabilitar usuários. Para obter mais informações, consulte Convidar e gerenciar usuários WorkDocs .

Implantando o WorkDocs Drive em vários computadores

Se você tiver uma frota de máquinas associada ao domínio, poderá usar Objetos de Política de Grupo (GPO) ou o System Center Configuration Manager (SCCM) para instalar o cliente Drive. WorkDocs Você pode baixar o cliente dos https://amazonworkdocs.com/en/clientes.

À medida que você avança, lembre-se de que o WorkDocs Drive exige acesso HTTPS na porta 443 para todos os endereços IP da AWS. Você também deve confirmar se os sistemas de destino atendem aos requisitos de instalação do WorkDocs Drive. Para obter mais informações, consulte Instalando o WorkDocs Drive no Guia WorkDocs do usuário da Amazon.

> **Note**
>
> Como prática recomendada ao usar o GPO ou o SCCM, instale o cliente WorkDocs Drive depois que os usuários fizerem login.

O instalador MSI para o WorkDocs Drive suporta os seguintes parâmetros de instalação opcionais:

- **`SITEID`**— Preenche previamente as informações do WorkDocs site para os usuários durante o registro. Por exemplo, `.SITEID=`*`site-name`*
- **`DefaultDriveLetter`**— Preenche previamente a letra da unidade a ser usada para montar WorkDocs a unidade. Por exemplo, `.DefaultDriveLetter=`*`W`* Lembre-se de que cada usuário deve ter uma letra de drive diferente. Além disso, os usuários podem alterar o nome da unidade, mas não a letra da unidade, depois de iniciarem o WorkDocs Drive pela primeira vez.

O exemplo a seguir implanta o WorkDocs Drive sem interfaces de usuário e sem reinicializações. Observe que ele usa o nome padrão do arquivo MSI:

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

Convidar e gerenciar usuários WorkDocs

Por padrão, quando você anexa um diretório durante a criação do site, o recurso de ativação automática WorkDocs adiciona todos os usuários desse diretório ao novo site como usuários gerenciados.

No WorkDocs sistema, os usuários gerenciados não precisam fazer login com credenciais separadas. Eles podem compartilhar e colaborar em arquivos e têm automaticamente 1 TB de armazenamento. No entanto, você pode desativar a ativação automática quando quiser adicionar apenas alguns usuários em um diretório, e as etapas nas próximas seções explicam como fazer isso.

Além disso, você pode convidar, ativar ou desativar usuários e alterar as funções e configurações do usuário. Também é possível promover um usuário a administrador. Para obter mais informações sobre como promover usuários, consulte Promover um usuário a administrador.

Você executa essas tarefas no painel de controle administrativo no cliente WorkDocs web, e as etapas nas seções a seguir explicam como. Mas, se você é novato WorkDocs, dedique alguns minutos e aprenda sobre as várias funções de usuário antes de mergulhar nas tarefas administrativas.

Conteúdo

Visão geral das funções de usuário

WorkDocs define as seguintes funções de usuário. É possível alterar as funções de usuários editando seus perfis. Para obter mais informações, consulte Editar usuários.

- Admin (Administrador): um usuário pago com permissões administrativas para todo o site, inclusive de configuração do site e de gerenciamento de usuários. Para obter mais informações sobre como promover um usuário a administrador, consulte Promover um usuário a administrador.
- Usuário avançado: usuário pago que tem um conjunto especial de permissões concedido pelo administrador. Para obter mais informações sobre como definir permissões para um usuário avançado, consulte Segurança — ActiveDirectory Sites simples e Segurança — sites de ActiveDirectory conexão.
- Usuário: um usuário pago que pode salvar arquivos e colaborar com outras pessoas em um WorkDocs site.
- Guest user (Usuário convidado): usuário não pago que só pode visualizar arquivos. Você pode fazer o upgrade de usuários convidados para as funções de Usuário, Usuário avançado ou Administrador.

> **Note**
>
> Ao alterar a função de um usuário convidado, você executa uma ação única que não pode ser revertida.

WorkDocs também define esses tipos de usuários adicionais.

Usuário do WS

Um usuário com um atribuído WorkSpaces WorkSpace.

- Acesso a todos os WorkDocs recursos
- Armazenamento padrão de 50 GB (passível de pagamento pelo upgrade de até 1 TB)
- Nenhuma cobrança mensal

Usuário do WS com upgrade

Um usuário com um armazenamento atribuído WorkSpaces WorkSpace e atualizado.

- Acesso a todos os WorkDocs recursos
- Armazenamento padrão de 1 TB (armazenamento adicional disponível em uma pay-as-you-go base)
- Cobranças mensais são aplicadas

WorkDocs usuário

Um WorkDocs usuário ativo sem um atribuído WorkSpaces WorkSpace.

- Acesso a todos os WorkDocs recursos
- Armazenamento padrão de 1 TB (armazenamento adicional disponível em uma pay-as-you-go base)
- Cobranças mensais são aplicadas

Iniciando o painel de controle administrativo

Você usa o painel de controle administrativo no cliente WorkDocs web para ativar e desativar a ativação automática e alterar as funções e configurações do usuário.

Para abrir o painel de controle do administrador

1. Escolha o ícone do perfil no canto superior direito do WorkDocs cliente.

2. Em Admin, selecione Abrir painel de controle do administrador.

> **Note**
>
> Algumas opções de painel de controle diferem entre diretórios na nuvem e diretórios conectados.

Desativar a ativação automática

Você desativa a ativação automática quando não deseja adicionar todos os usuários em um diretório a um novo site e quando deseja definir permissões e funções diferentes para os usuários que você convida para um novo site. Ao desativar a ativação automática, você também pode decidir quem tem a capacidade de convidar novos usuários para o site: usuários atuais, usuários avançados ou administradores. Estas etapas explicam como realizar ambas as tarefas.

Para desabilitar a ativação automática

1. Escolha o ícone do perfil no canto superior direito do WorkDocs cliente.

2. Em Admin, selecione Abrir painel de controle do administrador.
3. Role para baixo até Segurança e escolha Alterar.

   A caixa de diálogo Configurações de políticas é exibida.
4. Em Ativação automática, desmarque a caixa de seleção ao lado de Permitir que todos os usuários do seu diretório sejam ativados automaticamente no primeiro login WorkDocs no seu site.

   As opções são alteradas em Quem deve ter permissão para ativar os usuários do diretório em seu WorkDocs site. Você pode permitir que os usuários atuais convidem novos usuários, ou você pode dar essa capacidade para usuários avançados ou outros administradores.
5. Selecione uma opção e escolha Salvar alterações.

Repita as etapas de 1 a 4 para reativar a ativação automática.

Gerenciando o compartilhamento de links

Este tópico explica como gerenciar o compartilhamento de links. WorkDocs os usuários podem compartilhar seus arquivos e pastas compartilhando links para eles. Eles podem compartilhar links de arquivos dentro e fora da sua organização, mas só podem compartilhar links de pastas internamente. Como administrador, você gerencia quem pode compartilhar links.

Para ativar o compartilhamento de links

1. Escolha o ícone do perfil no canto superior direito do WorkDocs cliente.

2. Em Admin, selecione Abrir painel de controle do administrador.
3. Role para baixo até Segurança e escolha Alterar.

   A caixa de diálogo Configurações de políticas é exibida.
4. Em Escolha sua configuração para links compartilháveis, selecione uma opção:

   - Não permita links compartilháveis públicos ou em todo o site: desativa o compartilhamento de links para todos os usuários.
   - Permita que os usuários criem links compartilháveis em todo o site, mas não permita que eles criem links compartilháveis públicos: Limita o compartilhamento de links apenas aos membros do site. Usuários gerenciados podem criar esse tipo de link.
   - Permita que os usuários criem links compartilháveis em todo o site, mas somente usuários avançados podem criar links públicos compartilháveis: usuários gerenciados podem criar links para todo o site, mas somente usuários avançados podem criar links públicos. Os links públicos permitem o acesso de qualquer pessoa na internet.
   - Todos os usuários gerenciados podem criar links compartilháveis públicos e em todo o site: usuários gerenciados podem criar links públicos.
5. Escolha Salvar alterações.

Controle de convites de usuários com ativação automática ativada

Quando você ativa a ativação automática — e lembre-se de que ela está ativada por padrão — você pode dar aos usuários a capacidade de convidar outros usuários. Você pode conceder permissão a um dos seguintes itens:

- Todos os usuários
- Usuários avançados
- Administradores.

Você também pode desativar totalmente as permissões, e essas etapas explicam como.

Para definir permissões de convite

1. Escolha o ícone do perfil no canto superior direito do WorkDocs cliente.

2. Em Admin, selecione Abrir painel de controle do administrador.
3. Role para baixo até Segurança e escolha Alterar.

   A caixa de diálogo Configurações de políticas é exibida.
4. Em Quem deve ter permissão para ativar os usuários do diretório em seu WorkDocs site, marque a caixa de seleção Compartilhar com usuários externos, selecione uma das opções abaixo da caixa de seleção e escolha Salvar alterações.

   —OU—

   Desmarque a caixa de seleção se não quiser que ninguém convide novos usuários e escolha Salvar alterações.

Convidar novos usuários

Você pode convidar novos usuários para participar de um diretório. Você também pode permitir que usuários existentes convidem novos usuários. Para obter mais informações, consulte Segurança — ActiveDirectory Sites simples e Segurança — sites de ActiveDirectory conexão neste guia.

Como convidar novos usuários

1. Escolha o ícone do perfil no canto superior direito do WorkDocs cliente.

2. Em Admin, selecione Abrir painel de controle do administrador.
3. Em Manage Users (Gerenciar usuários), escolha Invite Users (Convidar usuários).
4. Na caixa de diálogo Convidar usuários, em Quem você deseja convidar?, insira o endereço de e-mail do convidado e selecione Enviar. Repita esta etapa para cada convite.

WorkDocs envia um e-mail de convite para cada destinatário. O e-mail contém um link e instruções sobre como criar uma WorkDocs conta. O link de convite expira após 30 dias.

Editar usuários

Você pode alterar as informações e configurações do usuário.

Como editar usuários

1. Escolha o ícone do perfil no canto superior direito do WorkDocs cliente.

2. Em Admin, selecione Abrir painel de controle do administrador.
3. Em Gerenciar usuários, selecione o ícone de lápis (✎) ao lado do nome do usuário.
4. Na caixa de diálogo Edit User (Editar usuário), é possível editar as seguintes opções:

   Name (Nome) (somente diretório na nuvem)

   O nome do usuário.

   Last Name (Sobrenome) (somente diretório na nuvem)

   O sobrenome do usuário.

   Status

   Especifique se o usuário está Ativo ou Inativo. Para obter mais informações, consulte Desabilitar usuários.

   Função

   Especifica se alguém é usuário ou administrador. Você também pode atualizar ou rebaixar os usuários que têm uma WorkSpaces WorkSpace atribuição atribuída a eles. Para obter mais informações, consulte Visão geral das funções de usuário.

   Armazenamento

   Especifica o limite de armazenamento de um usuário existente.
5. Escolha Salvar alterações.

Desabilitar usuários

Você desabilita o acesso de um usuário ao alterar o status dele para Inativo.

Como alterar o status do usuário para Inativo

1. Escolha o ícone do perfil no canto superior direito do WorkDocs cliente.

2. Em Admin, selecione Abrir painel de controle do administrador.
3. Em Gerenciar usuários, selecione o ícone de lápis (✎) ao lado do nome do usuário.
4. Selecione Inactive (Inativo) e Save Changes (Salvar alterações).

O usuário inativado não pode acessar seu WorkDocs site.

> **Note**
>
> Alterar um usuário para o status Inativo não exclui seus arquivos, pastas ou comentários do seu WorkDocs site. No entanto, é possível transferir arquivos e pastas de um usuário inativo para um usuário ativo. Para obter mais informações, consulte Transferir propriedade do documento.

Excluindo usuários pendentes

Você pode excluir usuários do Simple AD, AWS Managed Microsoft e AD Connector no status Pendente. Para excluir um daqueles usuários, selecione o ícone de lixeira (🗑) a lado do nome do usuário.

Seu WorkDocs site sempre deve ter pelo menos um usuário ativo que não seja um usuário convidado. Se você precisar excluir todos os usuários, exclua o site inteiro.

Não recomendamos a exclusão de usuários registrados. Em vez disso, você deve mudar um usuário do status Ativo para Inativo para impedir que ele acesse seu WorkDocs site.

Transferir propriedade do documento

É possível transferir arquivos e pastas de um usuário inativo para um usuário ativo. Para obter mais informações sobre como desativar um usuário, consulte Desabilitar usuários.

> **Warning**
>
> Não é possível desfazer essa ação.

Como transferir a propriedade do documento

1. Escolha o ícone do perfil no canto superior direito do WorkDocs cliente.

2. Em Admin, selecione Abrir painel de controle do administrador.
3. Em Gerenciar usuários, procure o usuário inativo.
4. Escolha o ícone de lápis
   (✎)
   ao lado do nome do usuário inativo.
5. Selecione Transferir propriedade do documento e insira o endereço de e-mail do novo proprietário.
6. Escolha Salvar alterações.

Fazer download das listas de usuários

Para baixar uma lista de usuários do painel de controle do administrador, você deve instalar o WorkDocs Companion. Para instalar o WorkDocs Companion, consulte Aplicativos e integrações para WorkDocs.

Para fazer download de uma lista de usuários

1. Escolha o ícone do perfil no canto superior direito do WorkDocs cliente.

2. Em Admin, selecione Abrir painel de controle do administrador.
3. Em Gerenciar usuários, selecione Fazer download do usuário.
4. Em Download user (Fazer download de usuário), escolha uma das seguintes opções para exportar uma lista de usuários como um arquivo `.json` para seu desktop:

   - Todos os usuários
   - Usuário convidado
   - Usuário do WS
   - Usuário
   - Usuário avançado
   - Administrador
5. WorkDocs salva o arquivo em um dos seguintes locais:

   - Windows: `Downloads/WorkDocsDownloads`
   - macOS: *`hard drive`*`/users/`*`username`*`/WorkDocsDownloads/folder`

   > **Note**
   >
   > Os downloads podem levar algum tempo. Além disso, os arquivos baixados não chegam à sua pasta da `/~users`.

Para obter mais informações sobre essas funções de usuário, consulte Visão geral das funções de usuário.

Compartilhamento e colaboração

Seus usuários podem compartilhar conteúdo ao enviar um link ou um convite. Os usuários também podem colaborar com usuários externos se você habilitar o compartilhamento externo.

WorkDocs controla o acesso a pastas e arquivos por meio do uso de permissões. O sistema aplica permissões com base na função do usuário.

Conteúdo

Compartilhar links

Os usuários podem escolher Compartilhar um link para copiar e compartilhar rapidamente hiperlinks de WorkDocs conteúdo com colegas de trabalho e usuários externos, dentro e fora da organização. Quando os usuários compartilham um link, eles podem configurá-lo para permitir uma das seguintes opções de acesso:

- Todos os membros do WorkDocs site podem pesquisar, visualizar e comentar o arquivo.
- Qualquer pessoa com o link, mesmo pessoas que não sejam membros do WorkDocs site, podem ver o arquivo. Essa opção de link restringe permissões somente para visualização.

Os destinatários com permissões de visualização só podem visualizar um arquivo. As permissões de comentário habilitam os usuários a comentar e a realizar operações de atualização e exclusão, como fazer upload de um novo arquivo ou excluir um arquivo existente.

Por padrão, todos os usuários gerenciados podem criar links públicos. Para alterar essa configuração, atualize as configurações de Security (Segurança) no painel de controle do administrador. Para obter mais informações, consulte Gerenciando WorkDocs a partir do painel de controle do administrador do site.

Compartilhar por convite

Quando você ativa o compartilhamento por convite, os usuários do seu site podem compartilhar arquivos ou pastas com usuários individuais e com grupos enviando e-mails de convite. Os convites contêm links para o conteúdo compartilhado, e os convidados podem abrir os arquivos ou pastas compartilhados. Os convidados podem compartilhar arquivos ou pastas com outros membros da organização e com usuários externos.

Você pode definir níveis de permissão para cada usuário convidado. Você também pode criar pastas da equipe para compartilhar por convite com grupos de diretórios que você criar.

> **Note**
>
> Os convites de compartilhamento não incluem membros de grupos aninhados. Para incluir esses membros, você deve adicioná-los à lista Compartilhar por convite.

Para obter mais informações, consulte Gerenciando WorkDocs a partir do painel de controle do administrador do site.

Compartilhamento externo

O compartilhamento externo permite que usuários gerenciados de um WorkDocs site compartilhem arquivos e pastas e colaborem com usuários externos sem incorrer em custos adicionais. Os usuários do site podem compartilhar arquivos e pastas com usuários externos sem exigir que os destinatários sejam usuários pagos do WorkDocs site. Quando o compartilhamento externo estiver habilitado, os usuários podem digitar o endereço de e-mail do usuário externo com o qual desejam compartilhar e definir as permissões adequadas de compartilhamento de visualizador. Quando usuários externos são adicionados, as permissões são limitadas somente a visualizadores, e outras permissões não estão disponíveis. Os usuários externos recebem uma notificação por e-mail com um link para o arquivo ou pasta compartilhado. A escolha do link leva os usuários externos ao site, onde eles inserem suas credenciais para fazer login. WorkDocs É possível visualizar o arquivo ou pasta compartilhado na visualização Compartilhados comigo.

Os proprietários de arquivos podem modificar as permissões de compartilhamento ou remover o acesso do usuário externo a um arquivo ou pasta a qualquer momento. O compartilhamento externo com a organização deve ser habilitado pelo administrador dela para os usuários gerenciados

compartilharem o conteúdo com os usuários externos. Para que os usuários convidados se tornem colaboradores ou coproprietários, eles devem passar por upgrade para o nível de usuário pelo administrador da organização. Para obter mais informações, consulte Visão geral das funções de usuário.

Por padrão, compartilhamento externo é ativado, e todos os usuários podem convidar usuários externos. Para alterar essa configuração, atualize as configurações de Security (Segurança) no painel de controle do administrador. Para obter mais informações, consulte Gerenciando WorkDocs a partir do painel de controle do administrador do site.

Permissões

WorkDocs usa permissões para controlar o acesso a pastas e arquivos. As permissões são aplicadas com base nas funções do usuário.

Conteúdo

Perfis de usuário

As funções do usuário controlam as permissões de pastas e arquivos. É possível aplicar as seguintes funções de usuário no nível de pasta:

- Proprietário da pasta: o proprietário da pasta ou do arquivo.
- Coproprietário da pasta: um usuário ou grupo que o proprietário designa como o coproprietário de uma pasta ou arquivo.
- Colaborador da pasta: alguém com acesso ilimitado a uma pasta.
- Visualizador de pastas: alguém com acesso limitado (permissões somente para leitura) a uma pasta.

Você pode aplicar as seguintes funções de usuário no nível de arquivo individual:

- Proprietário: o proprietário do arquivo.

- Coproprietário: um usuário ou grupo que o proprietário designa como o coproprietário do arquivo.
- Colaborador* — Alguém autorizado a dar feedback sobre o arquivo.
- Visualizador — Alguém com acesso limitado (somente leitura e permissões de atividade de visualização) ao arquivo.
- Visualizador anônimo: um usuário não registrado de fora da organização que pode visualizar um arquivo que foi compartilhado por meio de um link de visualização externo. Salvo indicação em contrário, um visualizador anônimo tem as mesmas permissões de somente leitura que um visualizador. Visualizadores anônimos não podem ver a atividade do arquivo.

* Os colaboradores não podem renomear versões de arquivos existentes. No entanto, eles podem carregar uma nova versão de um arquivo com um nome diferente.

Permissões para pastas compartilhadas

As permissões a seguir se aplicam às funções de usuário das pastas compartilhadas:

> **Note**
>
> As permissões aplicadas a uma pasta também se aplicam às subpastas e arquivos dessa pasta.

- Visualizar: exibe o conteúdo de uma pasta compartilhada.
- Visualizar subpasta: exibe uma subpasta.
- Visualizar compartilhamentos: ver os outros usuários com os quais uma pasta foi compartilhada.
- Baixar pasta: faz o download de uma pasta.
- Adicionar subpasta: adiciona uma subpasta.
- Compartilhar: compartilha a pasta de nível superior com outros usuários.
- Revogar compartilhamento: revoga o compartilhamento da pasta de nível superior.
- Excluir subpasta: exclui uma subpasta.
- Excluir pasta de nível superior: exclui a pasta compartilhada de nível superior.

	Visualizar	Visualizar subpastas	Visualizar compartilhamentos	Baixar pasta	Adicionar subpasta	Compartilhar	Revogar compartilhamento	Excluir subpasta	Excluir pasta de nível superior
Proprietário da pasta	✓	✓	✓	✓	✓	✓	✓	✓	✓
Coproprietário da pasta	✓	✓	✓	✓	✓	✓	✓	✓	✓
Colaborador da pasta	✓	✓	✓	✓	✓				
Visualizador da pasta	✓	✓	✓	✓					

Permissões para arquivos em pastas compartilhadas

As permissões a seguir se aplicam às funções do usuário para arquivos em uma pasta compartilhada:

- Anotar: é possível adicionar feedback a um arquivo.
- Excluir: exclui um arquivo em uma pasta compartilhada.
- Renomear: renomeia arquivos.
- Upload: faz upload de novas versões de um arquivo.
- Download: baixa um arquivo. Essa é a permissão padrão. Você pode usar as propriedades do arquivo para permitir ou negar a capacidade de baixar os arquivos compartilhados.
- Impedir download: impede que o download de um arquivo seja feito.

> **Note**
>
> - Quando você seleciona essa opção, os usuários com permissões de Visualização ainda podem baixar arquivos. Para evitar isso, abra a pasta compartilhada e desmarque a configuração Permitir downloads para cada um dos arquivos que você não deseja que esses usuários baixem.
> - Quando o proprietário ou coproprietário de um MP4 arquivo proíbe o download desse arquivo, colaboradores e espectadores não podem reproduzi-lo no cliente web da Amazon WorkDocs .

- Compartilhar: compartilha um arquivo com outros usuários.
- Revogar compartilhamento: revoga o compartilhamento de um arquivo.
- Visualizar: exibe um arquivo em uma pasta compartilhada.
- Visualizar compartilhamentos: ver os outros usuários com os quais um arquivo foi compartilhado.
- Visualizar anotações: ver o feedback de outros usuários.
- Visualizar atividade: exibe o histórico de atividades de um arquivo.
- Visualizar versões: exibe as versões anteriores de um arquivo.
- Excluir versões: excluir uma ou mais versões de um arquivo.
- Recuperar versões: recuperar uma ou mais versões excluídas de um arquivo.
- Comentários privados: o proprietário/coproprietário pode ver todos os comentários privados de um documento, mesmo que não sejam respostas ao comentário dele.

	Anotar	Excluir	Renomear	Carregar	Baixar	Impedir download	Compartilhar	Revogar compartilhamento	Visualizar	Visualizar compartilhamento	Visualizar anotações	Visualizar atividade	Visualizar versões	Excluir versões	Recuperar versões	Ver todos os comentários privados**
Proprio	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

	Anota	Exclui	Renom	Carrega	Baixar	Impedir download	Compartilhar	Revogar compartilhamento	Visualizar	Visualizar compartilhamento	Visualizar anotações	Visualizar atividade	Visualizar versões	Excluir versões	Recuperar versões	Ver todos os comentários privados**
do arqu																
Prop rio da past	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Copı tário da past	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cola or da past	✓			✓	✓				✓	✓	✓	✓	✓			
Visu dor da past					✓				✓	✓		✓				
Visu dor anôr									✓	✓						

* Nesse caso, o proprietário do arquivo é a pessoa que carregou a versão original de um arquivo em uma pasta compartilhada. As permissões para essa função se aplicam somente ao arquivo de propriedade, não a todos os arquivos na pasta compartilhada.

** Proprietários e coproprietários podem ver todos os comentários privados. Os colaboradores podem ver apenas comentários privados que sejam respostas aos comentários deles.

*** Os colaboradores não podem renomear versões de arquivos existentes. No entanto, eles podem carregar uma nova versão de um arquivo com um nome diferente.

Permissões para arquivos que não estão em pastas compartilhadas

As permissões a seguir se aplicam às funções de usuário de arquivos que não residem em uma pasta compartilhada:

- Anotar: é possível adicionar feedback a um arquivo.
- Excluir: exclui um arquivo.
- Renomear: renomeia arquivos.
- Upload: faz upload de novas versões de um arquivo.
- Download: baixa um arquivo. Essa é a permissão padrão. Você pode usar as propriedades do arquivo para permitir ou negar a capacidade de baixar os arquivos compartilhados.
- Impedir download: impede que o download de um arquivo seja feito.

> **Note**
>
> Quando o proprietário ou coproprietário de um MP4 arquivo proíbe o download desse arquivo, colaboradores e espectadores não podem reproduzi-lo no cliente web da Amazon WorkDocs .

- Compartilhar: compartilha um arquivo com outros usuários.
- Revogar compartilhamento: revoga o compartilhamento de um arquivo.
- Visualizar: exibe um arquivo.
- Visualizar compartilhamentos: ver os outros usuários com os quais um arquivo foi compartilhado.
- Visualizar anotações: ver o feedback de outros usuários.
- Visualizar atividade: exibe o histórico de atividades de um arquivo.
- Visualizar versões: exibe as versões anteriores de um arquivo.
- Excluir versões: excluir uma ou mais versões de um arquivo.
- Recuperar versões: recuperar uma ou mais versões excluídas de um arquivo.

	Anotar	Excluir	Renomear	Carregar	Baixar	Impedir download	Compartilhar	Revogar compartilhamento	Visualizar	Visualizar compartilhamento	Visualizar anotações	Visualizar atividade	Visualizar versões	Excluir versões	Recuperar versões
Proprietário*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Coproprietário	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Colaborador**	✓			✓	✓				✓	✓	✓	✓	✓		
Visualizador					✓				✓	✓		✓			
Visualizador anônimo									✓	✓					

* Proprietários e coproprietários de arquivos podem ver todos os comentários privados. Os colaboradores podem ver apenas comentários privados que sejam respostas aos comentários deles.

** Os colaboradores não podem renomear versões de arquivos existentes. No entanto, eles podem carregar uma nova versão de um arquivo com um nome diferente.

Habilitar edição colaborativa

Você pode usar as Configurações de edição online no Painel de controle do administrador para habilitar as opções de edição colaborativa.

Conteúdo

Habilitando o Hancom ThinkFree

Você pode habilitar o Hancom em seu WorkDocs site, ThinkFree para que os usuários possam criar e editar de forma colaborativa arquivos do Microsoft Office a partir do aplicativo WorkDocs web. Para obter mais informações, consulte Editando com a Hancom. ThinkFree

O Hancom ThinkFree está disponível sem custo adicional para WorkDocs os usuários. Não é necessária nenhuma outra licença ou instalação de software.

Para habilitar o Hancom ThinkFree

Ative a ThinkFree edição Hancom no painel de controle do administrador.

1. Em My account (Minha conta), selecione Open admin control panel (Abrir painel de controle do administrador).
2. Em Hancom Online Editing (Edição online do Hancom), escolha Change (Alterar).
3. Selecione Enable Hancom Online Editing Feature (Recurso de edição online do Hancom), examine os termos de uso e escolha Save (Salvar).

Para desativar o Hancom ThinkFree

Desative a ThinkFree edição Hancom no painel de controle do administrador.

1. Em My account (Minha conta), selecione Open admin control panel (Abrir painel de controle do administrador).
2. Em Hancom Online Editing (Edição online do Hancom), escolha Change (Alterar).
3. Desmarque a caixa de seleção Enable Hancom Online Editing Feature (Habilitar recurso de edição online do Hancom) e escolha Save (Salvar).

Habilitação da opção de abrir com o Office Online

Habilite Abrir com o Office Online em seu WorkDocs site, para que os usuários possam editar de forma colaborativa os arquivos do Microsoft Office a partir do aplicativo WorkDocs web.

Abrir com o Office Online está disponível sem custo adicional para WorkDocs usuários que também têm uma conta do Microsoft Office 365 Work ou School com uma licença para edição no Office Online. Para obter mais informações, consulte o artigo sobre a opção de abrir com o Office Online.

Para habilitar a opção de abrir com o Office Online

Habilite a opção de abrir com o Office Online no Painel de controle do administrador.

1. Em My account (Minha conta), selecione Open admin control panel (Abrir painel de controle do administrador).
2. Em Office Online, escolha Change (Alterar).
3. Selecione Enable Office Online (Habilitar o Office Online) e escolha Save (Salvar).

Para desabilitar a opção de abrir com o Office Online

Desabilite a opção de abrir com o Office Online no Painel de controle do administrador.

1. Em My account (Minha conta), selecione Open admin control panel (Abrir painel de controle do administrador).
2. Em Office Online, escolha Change (Alterar).
3. Desmarque a caixa de seleção Enable Office Online (Habilitar o Office Online) e escolha Save (Salvar).

Migrando arquivos para WorkDocs

WorkDocs os administradores podem usar o Serviço de WorkDocs Migração para realizar uma migração em grande escala de vários arquivos e pastas para o WorkDocs site. O Serviço de WorkDocs Migração funciona com o Amazon Simple Storage Service (Amazon S3). Isso permite migrar compartilhamentos de arquivos departamentais e compartilhamentos de arquivos do drive doméstico ou do usuário para o. WorkDocs

Durante esse processo, WorkDocs fornece uma política AWS Identity and Access Management (IAM) para você. Use essa política para criar uma nova função do IAM que conceda acesso ao Serviço de WorkDocs Migração para fazer o seguinte:

- Ler e listar o bucket do Amazon S3 designado por você.
- Leia e escreva no WorkDocs site que você designar.

Conclua as tarefas a seguir para migrar arquivos e pastas para o WorkDocs. Antes de começar, verifique se você tem as seguintes permissões:

- Permissões de administrador para seu WorkDocs site
- Permissões para criar um perfil do IAM

Se seu WorkDocs site estiver configurado no mesmo diretório da sua WorkSpaces frota, você deverá seguir estes requisitos:

- Não use Admin como nome de usuário WorkDocs da sua conta. Admin é uma função de usuário reservada no WorkDocs.
- Seu tipo de usuário WorkDocs administrador deve ser Usuário WS atualizado. Para obter mais informações, consulte Visão geral das funções de usuário e Editar usuários.

> **Note**
>
> A estrutura do diretório, os nomes dos arquivos e o conteúdo do arquivo são preservados durante a migração para o. WorkDocs A propriedade e as permissões dos arquivos não são preservadas.

Tarefas

Etapa 1: Preparar conteúdo para a migração

Para preparar o conteúdo para migração

1. No seu WorkDocs site, em Meus documentos, crie uma pasta para a qual você deseja migrar seus arquivos e pastas.
2. Confirme o seguinte:
   - A pasta de origem não contém mais do que 100.000 arquivos e subpastas. As migrações falharão se você exceder esse limite.
   - Nenhum arquivo individual excede 5 TB.
   - Cada nome de arquivo contém 255 caracteres ou menos. WorkDocs O Drive exibe somente arquivos com um caminho de diretório completo de 260 caracteres ou menos.

> **Warning**
>
> A tentativa de migrar arquivos ou pastas com nomes que contenham os caracteres a seguir pode causar erros e interromper o processo de migração. Se isso ocorrer, selecione Download report (Fazer download do relatório) para fazer download de um log listando os erros, os arquivos que apresentaram falha ao migrar e os arquivos que foram migrados com êxito.

- Espaços finais: por exemplo, um espaço adicional no final do nome do arquivo.
- Pontos no começo ou no final: por exemplo, `.file`, `.file.ppt`, `.`, `..` ou `file.`.
- Til no começo ou no final: por exemplo, `file.doc~`, `~file.doc` ou `~$file.doc`
- Nomes de arquivo terminando em **`.tmp`**: por exemplo, `file.tmp`

- Nomes de arquivo que correspondam exatamente a estes termos que diferenciam letras maiúsculas de minúsculas: `Microsoft User Data`, `Outlook files`, `Thumbs.db` ou `Thumbnails`
- Nomes de arquivo que contêm estes caracteres: `*` (asterisco), `/` (barra), `\` (barra invertida), `:` (dois-pontos), < (menor que), > (maior que), `?` (ponto de interrogação), `|` (barra vertical), `"` (aspas duplas) ou `\202E` (caractere código 202E).

Etapa 2: Carregar arquivos para o Amazon S3

Fazer upload de arquivos para o Amazon S3

1. Crie um novo bucket do Amazon Simple Storage Service (Amazon S3) em AWS sua conta para o qual você deseja carregar seus arquivos e pastas. O bucket do Amazon S3 deve estar na mesma AWS conta e AWS região do seu WorkDocs site. Para obter mais informações, consulte Conceitos básicos do Amazon Simple Storage Service no Guia do usuário do Amazon Simple Storage Service.
2. Faça upload de seus arquivos no bucket do Amazon S3 que você criou na etapa anterior. Recomendamos usar AWS DataSync para fazer upload de seus arquivos e pastas para o bucket do Amazon S3. DataSync fornece recursos adicionais de rastreamento, geração de relatórios e sincronização. Para obter mais informações, consulte Como AWS DataSync funciona e Como usar políticas baseadas em identidade (políticas do IAM) DataSync no Guia do AWS DataSync usuário.

Etapa 3: Programar uma migração

Depois de concluir as etapas 1 e 2, use o Serviço de WorkDocs Migração para agendar a migração. O Serviço de Migração pode levar até uma semana para processar sua solicitação de migração e enviar um e-mail informando que você pode começar a migração. Se você iniciar a migração antes de receber o e-mail, o console de gerenciamento exibirá uma mensagem solicitando que você espere.

Quando você agenda a migração, a configuração de armazenamento da sua conta de WorkDocs usuário muda automaticamente para Ilimitado.

> **Note**
>
> A migração de arquivos que excedem seu limite WorkDocs de armazenamento pode resultar em custos adicionais. Para obter mais informações, consulte WorkDocs Preço.

O Serviço de WorkDocs Migração fornece uma política AWS Identity and Access Management (IAM) para você usar na migração. Com essa política, você cria uma nova função do IAM que concede ao Serviço de WorkDocs Migração acesso ao bucket e ao WorkDocs site do Amazon S3 que você designar. Também é possível se inscrever em notificações de e-mail do Amazon SNS para receber atualizações quando a solicitação de migração for programada e quando ela for iniciada e finalizada.

Como programar uma migração:

1. No WorkDocs console, escolha Aplicativos, Migrações.
   - Se esta é a primeira vez que você acessa o Serviço de WorkDocs Migração, você será solicitado a assinar as notificações por e-mail do Amazon SNS. Inscreva-se, realize a confirmação na mensagem de e-mail que você receber e selecione Continue (Continuar).
2. Selecione Create Migration (Criar migração).
3. Em Source Type (Tipo de origem), selecione Amazon S3.
4. Escolha Próximo.
5. Em Validação e fonte de dados, em Exemplo de política, copie a política do IAM fornecida.
6. Use a política do IAM copiada na etapa anterior para criar uma função e política do IAM da seguinte maneira:
   a. Abra o console do IAM em https://console.aws.amazon.com/iam/.
   b. Selecione Policies (Políticas), Create policy (Criar política).
   c. Selecione JSON e cole a política do IAM copiada anteriormente para a área de transferência.
   d. Selecione Revisar política. Insira um nome e uma descrição para a política.
   e. Selecione Criar política.
   f. Selecione Roles (Funções), Create role (Criar função).
   g. Selecione Another AWS account (Outra conta da AWS). Em Account ID (ID da conta), insira uma das seguintes opções:

- Para a região Leste dos EUA (Norte da Virgínia), insira `899282061130`
- para a região Oeste dos EUA (Oregon)
- Para a região da Ásia-Pacífico (Singapura), insira `900469912330`
- Para a região da Ásia-Pacífico (Sydney), insira `031131923584`
- Para a região da Ásia-Pacífico (Tóquio), insira `178752524102`
- Para a região da Europa (Irlanda), insira `191921258524`

h. Selecione a política que você criou e escolha Next: Review (Próximo: revisar). Se a nova política não for exibida, selecione o ícone de atualização.

i. Insira um nome e uma descrição para a função. Selecione Criar perfil.

j. Na página Roles (Funções), em Role name (Nome da função), selecione o nome da função criada.

k. Na página Resumo, altere a duração máxima da CLI/API sessão para 12 horas.

l. Copie o Role ARN (ARN da função) para a área de transferência para usá-lo na próxima etapa.

7. Volte para o WorkDocs Migration Service. Em Validação e fonte de dados, em ARN da função, cole o ARN do perfil do IAM copiado na etapa anterior.
8. Em Bucket, selecione o bucket do Amazon S3 do qual migrar os arquivos.
9. Escolha Próximo.
10. Em Selecionar uma WorkDocs pasta de destino, selecione a pasta de destino WorkDocs para a qual migrar os arquivos.
11. Escolha Próximo.
12. Em Review (Revisar), em Title (Título), insira um nome para a migração.
13. Selecione a data e a hora da migração.
14. Selecione Enviar.

Etapa 4: Rastrear uma migração

Você pode acompanhar sua migração na página inicial do Serviço de WorkDocs Migração. Para acessar a página inicial a partir do WorkDocs site, escolha Aplicativos, Migrações. Selecione sua migração para visualizar os detalhes e acompanhar seu progresso. Também é possível selecionar Cancel Migration (Cancelar a migração), caso precise cancelá-la, ou selecionar Update (Atualizar) para atualizar a linha do tempo da migração. Depois que a migração for concluída, você poderá

selecionar Download report (Fazer download do relatório) para fazer download de um log dos arquivos migrados com êxito, de falhas ou erros.

Os seguintes estados de migração fornecem o status da sua migração:

Programado

A migração está programada, mas não foi iniciada. É possível cancelar migrações ou atualizar a hora de início da migração até cinco minutos antes da hora de início programada.

Migrating

A migração está em andamento.

Bem-sucedida

A migração foi concluída.

Partial Success (Parcialmente bem-sucedida)

A migração foi concluída parcialmente. Para obter mais detalhes, visualize o resumo da migração e faça download do relatório fornecido.

Falha

Ocorreu uma falha na migração. Para obter mais detalhes, visualize o resumo da migração e faça download do relatório fornecido.

Cancelado

A migração foi cancelada.

Etapa 5: Limpar recursos

Quando a migração for concluída, exclua a função e a política de migração criada no console do IAM.

Para excluir a política e o perfil do IAM

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. Selecione Políticas.
3. Pesquise e selecione a política que você criou.
4. Em Policy actions (Ações da política), selecione Delete (Excluir).

5. Escolha Excluir.
6. Escolha Perfis.
7. Pesquise e escolha a função que você criou.
8. Selecione Delete role (Excluir função), Delete (Excluir).

Quando uma migração programada é iniciada, a configuração de armazenamento da sua conta de WorkDocs usuário é automaticamente alterada para Ilimitado. Após a migração, você pode usar o painel de controle administrativo para alterar essa configuração. Para obter mais informações, consulte Editar usuários.

Solução de problemas do WorkDocs

As informações a seguir podem ajudá-lo a solucionar problemas com WorkDocs.

Problemas

Não consigo configurar meu WorkDocs site em uma AWS região específica

Se você estiver configurando um novo WorkDocs site, selecione a região da AWS durante a configuração. Para mais informações, consulte o tutorial para seu caso de uso específico em Começando com WorkDocs.

Quero configurar meu WorkDocs site em uma Amazon VPC existente?

Ao configurar seu novo WorkDocs site, crie um diretório usando a nuvem privada virtual (VPC) existente. WorkDocs usa esse diretório para autenticar usuários.

O usuário precisa redefinir a senha dele

Os usuários podem redefinir suas senhas selecionando Esqueceu a senha? na tela de login.

O usuário compartilhou acidentalmente um documento confidencial

Para revogar o acesso ao documento, selecione a opção Share by invite (Compartilhar por convite) ao lado do documento. Em seguida, remova os usuários que não devem mais ter acesso. Se

o documento foi compartilhado usando um link, selecione Share a link (Compartilhar um link) e desabilite o link.

O usuário deixou a organização e não transferiu a propriedade do documento

Transfira a propriedade do documento para outro usuário no painel de controle do administrador. Para obter mais informações, consulte Transferir propriedade do documento.

É necessário implantar o WorkDocs Drive ou o WorkDocs Companion para vários usuários

Faça a implementação para vários usuários em uma empresa usando as políticas de grupo. Para obter mais informações, consulte Gerenciamento de identidade e acesso para a Amazon WorkDocs. Para obter informações específicas sobre a implantação WorkDocs do Drive para vários usuários, consulteImplantando o WorkDocs Drive em vários computadores.

A edição online não está funcionando

Verifique se você tem o WorkDocs Companion instalado. Para instalar o WorkDocs Companion, consulte Aplicativos e integrações para WorkDocs.

Gerenciando WorkDocs para a Amazon Business

Se você WorkDocs for administrador do Amazon Business, poderá gerenciar usuários fazendo login em https://workdocs.aws/ usando suas credenciais da Amazon Business.

Para convidar um novo usuário WorkDocs para o Amazon Business

1. Faça login com as credenciais do Amazon Business em https://workdocs.aws/.
2. Na WorkDocs página inicial do Amazon Business, abra o painel de navegação à esquerda.
3. Escolha Configurações do administrador.
4. Escolha Adicionar pessoas.
5. Em Recipients (Destinatários), insira os endereços de e-mail ou os nomes de usuário dos usuários a serem convidados.
6. (Opcional) Personalize a mensagem de convite.
7. Selecione Concluído.

Para pesquisar um usuário no WorkDocs Amazon Business

1. Faça login com as credenciais do Amazon Business em https://workdocs.aws/.
2. Na WorkDocs página inicial do Amazon Business, abra o painel de navegação à esquerda.
3. Escolha Configurações do administrador.
4. Em Search users (Pesquisar usuários), digite o nome do usuário e pressione **`Enter`**.

Para selecionar funções de usuário no WorkDocs Amazon Business

1. Faça login com as credenciais do Amazon Business em https://workdocs.aws/.
2. Na WorkDocs página inicial do Amazon Business, abra o painel de navegação à esquerda.
3. Escolha Configurações do administrador.
4. Em People (Pessoas), ao lado do usuário, selecione a Role (Função) a ser atribuída ao usuário.

Para excluir um usuário no WorkDocs Amazon Business

1. Faça login com as credenciais do Amazon Business em https://workdocs.aws/.
2. Na WorkDocs página inicial do Amazon Business, abra o painel de navegação à esquerda.

3. Escolha Configurações do administrador.
4. Em People (Pessoas), escolha as reticências (...) ao lado do usuário.
5. Escolha Excluir.
6. Se solicitado, insira um novo usuário para o qual transferir os arquivos do usuário e escolha Delete (Excluir).

Endereços IP e domínios para adicionar à sua lista de permissões

Se você implementar a filtragem de IP em dispositivos que acessam WorkDocs, adicione os seguintes endereços IP e domínios à sua lista de permissões. Isso permite que WorkDocs o WorkDocs Drive se conecte ao WorkDocs serviço.

- 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
- zócalo. 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

Se você quiser usar intervalos de endereço IP, consulte Intervalos de endereço IP da AWS na Referência geral da AWS .

Histórico do documento

A tabela a seguir descreve mudanças importantes no Guia de WorkDocs Administração da Amazon, a partir de fevereiro de 2018. Para receber notificações sobre atualizações dessa documentação, assine um feed RSS.

Alteração	Descrição	Data
Novas permissões do proprietário do arquivo	Agora, os administradores podem fornecer as permissões Excluir versão e Recuperar versão. As permissões fazem parte do lançamento da DeleteDocumentVersionAPI.	29 de julho de 2022
WorkDocs Backup	A documentação de WorkDocs Backup foi removida do Amazon WorkDocs Administration Guide porque o componente não é mais suportado.	24 de junho de 2021
Gerenciando WorkDocs para a Amazon Business	WorkDocs for Amazon Business oferece suporte ao gerenciamento de usuários por administradores. Para obter mais informações, consulte Managing WorkDocs for Amazon Business no Amazon WorkDocs Administration Guide.	26 de março de 2020
Migração de arquivos para a Amazon WorkDocs	WorkDocs os administradores podem usar o Serviço de WorkDocs Migração para realizar uma migração em grande escala de vários	8 de agosto de 2019

	arquivos e pastas para o WorkDocs site. Para obter mais informações, consulte Como migrar arquivos para WorkDocs o Amazon WorkDocs Administration Guide.	
Configurações da lista de permissões de IP	As configurações da Lista de Permissões de IP estão disponíveis para filtrar o acesso ao seu WorkDocs site por faixa de endereços IP. Para obter mais informações, consulte as configurações da lista de permissões de IP no Amazon WorkDocs Administr ation Guide.	22 de outubro de 2018
Hancom ThinkFree	Hancom ThinkFree está disponível. Os usuários podem criar e editar de forma colaborativa arquivos do Microsoft Office a partir do aplicativo WorkDocs web. Para obter mais informaçõ es, consulte Habilitando o Hancom ThinkFree no Guia de WorkDocs Administração da Amazon.	21 de junho de 2018

Abrir com o Office Online	A opção de abrir com o Office Online está disponível. Os usuários podem editar de forma colaborativa os arquivos do Microsoft Office a partir do aplicativo WorkDocs web. Para obter mais informações, consulte Habilitando o Open with Office Online no Guia de WorkDocs Administração da Amazon.	6 de junho de 2018
Solução de problemas	Tópico de solução de problemas adicionado. Para obter mais informaçõ es, consulte Solução de WorkDocs problemas no Guia de WorkDocs administração da Amazon.	23 de maio de 2018
Alteração do período de retenção da lixeira de recuperação	O período de retenção da lixeira de recuperação pode ser alterado. Para obter mais informações, consulte Configurações de retenção da lixeira de recuperação no Guia de WorkDocs Administração da Amazon.	27 de fevereiro de 2018