



Guia de administração

Amazon WorkDocs



Amazon WorkDocs: Guia de administração

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestígie a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

.....	vi
O que é o Amazon WorkDocs?	1
Acessar o Amazon WorkDocs	1
Preços	2
Como começar a usar	2
Migração de dados de WorkDocs	3
Método 1: Baixar arquivos em massa	3
Baixando arquivos da web	4
Baixando pastas da web	5
Usando o WorkDocs Drive para baixar arquivos e pastas	5
Método 2: Usar a ferramenta de migração	6
Pré-requisitos	6
Limitações	9
Executando a ferramenta de migração	10
Baixando dados migrados do Amazon S3	14
Solução de problemas de migrações	15
Visualizando seu histórico de migração	15
Pré-requisitos	17
Inscreva-se para um Conta da AWS	17
Criar um usuário com acesso administrativo	17
Segurança	19
Gerenciamento de identidade e acesso	20
Público	20
Autenticando com identidades	21
Gerenciando acesso usando políticas	24
Como a Amazon WorkDocs trabalha com IAM	27
Exemplos de políticas baseadas em identidade	30
Solução de problemas	34
Logging e monitoramento	36
Exportação do feed de atividades de todo o site	36
CloudTrail registro	37
Validação de conformidade	41
Resiliência	42
Segurança da infraestrutura	42

Conceitos básicos	44
Criação de um site do Amazon WorkDocs	45
Antes de começar	45
Criação de um site do Amazon WorkDocs	45
Habilitar o logon único	47
Habilitar a autenticação multifator	48
Promover um usuário a administrador	48
Gerenciar o Amazon WorkDocs no Console da AWS	50
Configurando administradores do site	50
Reenvio de um e-mail de convite	50
Como gerenciar a autenticação multifator	51
Configurando URLs do site	51
Gerenciar notificações	52
Excluir um site	53
Gerenciando WorkDocs a Amazon a partir do painel de controle do administrador do site	55
Implantação do Amazon WorkDocs Drive em vários computadores	64
Convidar e gerenciar usuários	65
Perfis de usuário	66
Iniciando o painel de controle administrativo	67
Desativar a ativação automática	68
Gerenciando o compartilhamento de links	68
Controle de convites de usuários com ativação automática ativada	69
Convidar novos usuários	70
Editar usuários	71
Desabilitar usuários	72
Excluindo usuários pendentes	72
Transferir propriedade do documento	73
Fazer download das listas de usuários	73
Compartilhamento e colaboração	75
Compartilhar links	75
Compartilhar por convite	76
Compartilhamento externo	76
Permissões	77
Perfis de usuário	77
Permissões para pastas compartilhadas	78
Permissões para arquivos em pastas compartilhadas	79

Permissões para arquivos que não estão em pastas compartilhadas	82
Habilitar edição colaborativa	83
Habilitar o Hancom ThinkFree	84
Habilitação da opção de abrir com o Office Online	84
Migrar arquivos	86
Etapa 1: Preparar conteúdo para a migração	87
Etapa 2: Carregar arquivos para o Amazon S3	88
Etapa 3: Programar uma migração	88
Etapa 4: Rastrear uma migração	90
Etapa 5: Limpar recursos	91
Solução de problemas	93
Não é possível configurar meu site do Amazon WorkDocs em uma região específica da AWS	93
Desejo configurar meu site do Amazon WorkDocs em uma Amazon VPC existente	93
O usuário precisa redefinir a senha dele	93
O usuário compartilhou acidentalmente um documento confidencial	94
O usuário deixou a organização e não transferiu a propriedade do documento	94
Preciso implantar o Drive do Amazon WorkDocs ou o Companion do Amazon WorkDocs para vários usuários	94
A edição online não está funcionando	55
Gerenciando o Amazon WorkDocs para Amazon Business	95
Endereços IP e domínios para adicionar à sua lista de permissões	97
Histórico do documento	98

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 da Amazon 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 o Amazon WorkDocs?

O Amazon WorkDocs é um serviço de armazenamento e compartilhamento empresarial seguro e totalmente gerenciado, com sólidos controles administrativos e recursos de feedback que aprimoram a produtividade dos usuários. 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 cliente do Amazon WorkDocs podem ser usados para visualizar vários tipos diferentes de arquivos, dependendo do tipo de mídia do arquivo na internet. O Amazon WorkDocs oferece suporte a 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](#).

Acessar o Amazon WorkDocs

Os administradores usam o [console do Amazon WorkDocs](#) para criar e desativar os sites do Amazon 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 do Amazon WorkDocs](#).

Os usuários não administrativos usam os aplicativos cliente para acessar seus arquivos. Eles nunca usam o console do Amazon WorkDocs ou o painel de administração. O Amazon 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.
- Amazon WorkDocs Drive, um aplicativo que sincroniza uma pasta no seu desktop macOS ou Windows com seus arquivos do Amazon WorkDocs.

Para obter mais informações sobre como os usuários podem baixar clientes do Amazon WorkDocs e editar seus arquivos e sobre os tipos de arquivo compatíveis, consulte:

- [Conceitos básicos do Amazon WorkDocs](#)
- [Editar arquivos](#)
- [Tipos de arquivos com suporte](#)

Preços

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

Como começar a usar

Para começar a usar o Amazon WorkDocs, consulte [Criação de um site do Amazon WorkDocs](#).

Migração de dados para fora da Amazon WorkDocs

WorkDocs A Amazon 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](#)
- [Método 2: Usar a ferramenta de migração](#)

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 Amazon 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 feedback](#), no Guia WorkDocs do usuário da Amazon.
- Você deve usar o Amazon WorkDocs Drive para baixar arquivos maiores que 5 GB.
- Quando você usa o Amazon WorkDocs Drive para baixar arquivos e pastas, suas estruturas de diretórios, nomes de arquivos e conteúdo de 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:

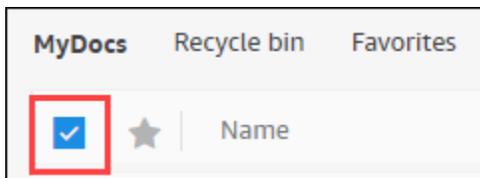
- Você só quer baixar alguns dos arquivos de um site.
- Você deseja baixar documentos do Word com comentários e fazer com que esses comentários permaneçam com seus respectivos documentos. A ferramenta de migração baixa todos os comentários, mas os grava em um arquivo XML separado. Os usuários do site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

Para baixar arquivos da web

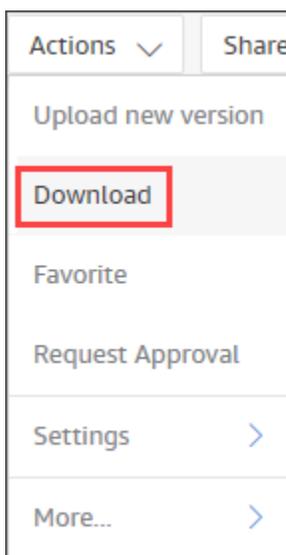
1. Faça login na Amazon WorkDocs.
2. Conforme necessário, abra a pasta que contém os arquivos que você deseja baixar.
3. Marque a caixa de seleção ao lado dos arquivos que você deseja baixar.

—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 Downloads/WorkDocsDownloads/. 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 na Amazon 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 Amazon WorkDocs Drive para concluir as etapas a seguir. Para obter mais informações, consulte [Instalando o Amazon WorkDocs Drive](#), no Guia do usuário do Amazon 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 Amazon WorkDocs Drive.

Método 2: Usar a ferramenta de migração

Você usa a ferramenta de WorkDocs migração da Amazon quando quer 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](#)
- [Limitações](#)
- [Executando a ferramenta de migração](#)
- [Baixando dados migrados do Amazon S3](#)
- [Solução de problemas de migrações](#)
- [Visualizando seu histórico de migração](#)

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 à Amazon para fazer upload de 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 site. WorkDocs 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": "AllowKSMigration",
  "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, `/workdocs/ site-alias/created-timestamp-utc /skippedFiles.csv`.** Você pode baixar os arquivos listados de forma programática ou manual. Para obter informações sobre o download programático <https://docs.aws.amazon.com/workdocs/latest/developerguide/download-documents.html>, consulte o Amazon WorkDocs Developer Guide. Para obter informações sobre como baixar os arquivos manualmente, consulte as etapas do Método 1, anteriormente neste tópico.
- O arquivo zip de cada usuário conterá apenas arquivos e/ou pastas de sua propriedade. Todos os arquivos e/ou pastas que foram compartilhados com o usuário estarão no arquivo zip do usuário que possui os arquivos e/ou pastas.
- 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 da Amazon.

Para migrar um site

1. Abra o WorkDocs console da Amazon 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 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 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 prerequisites section here.

S3 URI

 ✕ View [↗](#) Browse S3

Notifications [Optional]

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

 ✕ ✕

▼ 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.

 ✕ 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 provide 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 instância do EC2 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 da Amazon 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
✔ Succeeded	Feb 1, 2024, 18:01 EST	Feb 1, 2024, 12:01 EST	workdocs-data-migration-tool-test-bu
✔ Succeeded	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 da Amazon ou gerenciar sites existentes, você deve concluir as seguintes tarefas.

Inscreva-se para um Conta da AWS

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

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 chamada telefônica 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 AWS é criado. O usuário root tem acesso a todos 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, habilitar AWS IAM Identity Center 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 no [AWS Management Console](#) como proprietário da conta, escolhendo o usuário root e inserindo seu Conta da AWS endereço de e-mail. Na próxima página, insira sua senha.

Para obter ajuda para fazer login usando o usuário root, consulte [Como fazer login como usuário root](#) no Início de Sessão da AWS Guia do usuário.

2. Ative a autenticação multifator (MFA) para seu usuário root.

Para obter instruções, consulte [Habilitar um MFA dispositivo virtual para seu Conta da AWS usuário root \(console\)](#) no Guia do IAM usuário.

Criar um usuário com acesso administrativo

1. Ative o IAM Identity Center.

Para obter instruções, consulte [Habilitando AWS IAM Identity Center](#) no AWS IAM Identity Center Guia do usuário.

2. No IAM Identity Center, conceda acesso administrativo a um usuário.

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

Iniciar sessão como o usuário com acesso administrativo

- Para entrar com seu usuário do IAM Identity Center, use o login URL que foi enviado ao seu endereço de e-mail quando você criou o usuário do IAM Identity Center.

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

Atribuir acesso a usuários adicionais

1. No IAM Identity Center, crie um conjunto de permissões que siga as melhores práticas de aplicação de permissões com privilégios mínimos.

Para obter instruções, consulte [Criar um conjunto de permissões](#) no AWS IAM Identity Center Guia do usuário.

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

Para obter instruções, consulte [Adicionar grupos](#) no AWS IAM Identity Center Guia do usuário.

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 a Amazon 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 a Amazon WorkDocs para atender aos seus objetivos de segurança e conformidade. Você também aprende a usar outros AWS serviços que ajudam você a monitorar e proteger seus WorkDocs recursos da Amazon.

Tópicos

- [Gerenciamento de identidade e acesso para a Amazon WorkDocs](#)
- [Registro e monitoramento na Amazon WorkDocs](#)
- [Validação de conformidade para a Amazon WorkDocs](#)

- [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. IAMos administradores controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) para usar os recursos da Amazon WorkDocs . IAMé um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- [Público](#)
- [Autenticando com identidades](#)
- [Gerenciando acesso usando políticas](#)
- [Como a Amazon WorkDocs trabalha com 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 na Amazon WorkDocs.

Usuário do serviço — Se você usa o WorkDocs serviço da Amazon para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais WorkDocs recursos da Amazon para fazer seu trabalho, você pode precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se você não conseguir acessar um recurso na Amazon WorkDocs, consulte [Solução de problemas de WorkDocs identidade e acesso da Amazon](#).

Administrador de serviços — Se você é responsável pelos WorkDocs recursos da Amazon em sua empresa, provavelmente tem acesso total à Amazon WorkDocs. É seu trabalho determinar quais WorkDocs recursos e recursos da Amazon seus usuários do serviço devem acessar. Em seguida, você deve enviar solicitações ao IAM administrador para alterar as permissões dos usuários do

serviço. Revise as informações nesta página para entender os conceitos básicos do IAM. Para saber mais sobre como sua empresa pode usar IAM com a Amazon WorkDocs, consulte [Como a Amazon WorkDocs trabalha com IAM](#).

IAM administrador — Se você for IAM administrador, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso à Amazon WorkDocs. Para ver exemplos de políticas WorkDocs baseadas em identidade da Amazon que você pode usar IAM, consulte [Exemplos de políticas WorkDocs baseadas em identidade da Amazon](#)

Autenticando com identidades

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

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Os usuários (do 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 entra como uma identidade federada, seu administrador configurou previamente a federação de identidades usando IAM funções. 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 você mesmo assinar solicitações, consulte [AWS Signature versão 4 para API solicitações](#) no Guia IAM do usuário.

Independente do método de autenticação usado, também pode ser exigido que você forneça 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 AWS IAM Identity Center usuário e [Autenticação AWS multifator IAM no Guia do IAM usuário](#).

Grupos e usuários do IAM

Um [IAMusuário](#) é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos confiar em credenciais temporárias em vez de criar IAM usuários que tenham 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 IAM os usuários, recomendamos que você alterne as chaves de acesso. Para obter mais informações, consulte [Altere as chaves de acesso regularmente para casos de uso que exigem credenciais de longo prazo](#) no Guia do IAMusuário.

Um [IAMgrupo](#) é uma identidade que especifica uma coleção de IAM usuários. 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 IAM recursos.

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 IAM usuários](#) no Guia IAM do usuário.

IAMfunções

Uma [IAMfunção](#) é uma identidade dentro da sua Conta da AWS que tem permissões específicas. É semelhante a um IAM usuário, mas não está associado a uma pessoa específica. Para assumir temporariamente uma IAM função no AWS Management Console, você pode [alternar de um usuário para uma IAM função \(console\)](#). Você pode assumir uma função chamando uma AWS API operação AWS CLI or ou usando uma personalizadaURL. Para obter mais informações sobre métodos de uso de funções, consulte [Métodos para assumir uma função](#) no Guia IAM do usuário.

IAMfunções com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode 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 pelo mesmo. Para obter informações sobre funções para federação, consulte [Criar uma função para um provedor de identidade terceirizado \(federação\)](#) no Guia IAM do usuário. Se você usa o IAM Identity Center, configura um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a uma função em.

IAM Para obter informações sobre conjuntos de permissões, consulte [Conjuntos de Permissões](#) no Manual do Usuário do AWS IAM Identity Center .

- Permissões temporárias IAM de IAM usuário — Um usuário ou função pode assumir uma IAM função para assumir temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas — Você pode usar uma IAM função para permitir que alguém (um diretor confiável) em uma conta diferente 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 saber a diferença entre funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a [recursos entre contas IAM no Guia](#) do IAM usuário.
- 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 do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.
- Sessões de acesso direto (FAS) — Quando você usa um IAM usuário ou uma função para realizar ações em AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. 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. FAS as solicitações 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 FAS solicitações, consulte [Encaminhar sessões de acesso](#).
- Função de serviço — Uma função de serviço é uma [IAM função](#) que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função de serviço internamente IAM. Para obter mais informações, consulte [Criar uma função para delegar permissões a um AWS service \(Serviço da AWS\)](#) no Guia do IAM usuário.
- 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 a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões das funções vinculadas ao serviço.
- Aplicativos em execução na Amazon EC2 — Você pode usar uma IAM função para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância

e fazendo AWS CLI AWS API solicitações. Isso é preferível ao armazenamento de 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 IAM função para conceder permissões a aplicativos executados em EC2 instâncias da Amazon](#) no Guia IAM do usuário.

Gerenciando 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 JSON documentos. Para obter mais informações sobre a estrutura e o conteúdo dos documentos de JSON política, consulte [Visão geral das JSON políticas](#) no Guia IAM do usuário.

Os administradores podem usar AWS JSON políticas 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 funções não têm permissões. Para conceder permissão aos usuários para realizar ações nos recursos de que precisam, um IAM administrador pode criar IAM políticas. O administrador pode então adicionar as IAM políticas às funções e os usuários podem assumir as funções.

IAMas políticas definem permissões para uma ação, independentemente do método usado para realizar 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 do AWS Management Console AWS CLI, do ou do AWS API.

Políticas baseadas em identidade

Políticas baseadas em identidade são documentos de políticas de JSON permissões que você pode anexar a uma identidade, como um IAM usuário, grupo de usuários ou função. 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 IAM permissões personalizadas com políticas gerenciadas pelo cliente no Guia](#) do IAM usuário.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente 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 IAMusuário.

Políticas baseadas no recurso

Políticas baseadas em recursos são documentos JSON de política que você anexa a um recurso. Exemplos de políticas baseadas em recursos são políticas de confiança de IAM funções e políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso 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 de uma política baseada IAM 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 JSON de política.

Amazon S3, AWS WAF, e 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 as permissões máximas que uma política baseada em identidade pode conceder a uma IAM entidade

(IAMusuário ou função). 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 IAM entidades](#) no Guia IAM do usuário.

- Políticas de controle de serviço (SCPs) — SCPs são JSON políticas 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. Os SCP limites de permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre Organizations eSCPs, consulte [Políticas de controle de serviços](#) 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 atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte [Políticas de sessão](#) no Guia IAM do usuário.

Note

A Amazon 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 política estão envolvidos, consulte [Lógica de avaliação](#) de políticas no Guia IAM do usuário.

Como a Amazon WorkDocs trabalha com IAM

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

Tópicos

- [Políticas baseadas em WorkDocs identidade da Amazon](#)
- [Políticas baseadas em WorkDocs recursos da Amazon](#)
- [Autorização com base nas WorkDocs tags da Amazon](#)
- [WorkDocs IAM Funções na Amazon](#)

Políticas baseadas em WorkDocs identidade da Amazon

Com políticas IAM baseadas em identidade, você pode especificar ações permitidas ou negadas. A Amazon WorkDocs oferece suporte a ações específicas. Para saber mais sobre os elementos que você usa em uma JSON política, consulte a [referência aos elementos da IAM JSON política](#) no Guia IAM do usuário.

Ações

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

O `Action` elemento de uma JSON política descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da AWS API operação associada. Há algumas exceções, como ações somente de permissão que não têm uma operação 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 na Amazon WorkDocs usam o seguinte prefixo antes da ação: `workdocs:`. Por exemplo, para conceder permissão a alguém para executar a `WorkDocs DescribeUsers` API operação da Amazon, você inclui a `workdocs:DescribeUsers` ação na política dessa pessoa. As instruções de política devem incluir um elemento `Action` ou `NotAction`. A Amazon WorkDocs

define seu próprio conjunto de ações que descrevem as tarefas que você pode realizar 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 da Amazon, consulte [Ações definidas pela Amazon WorkDocs](#) no Guia IAM do usuário.

Recursos

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

Chaves de condição

WorkDocs A Amazon 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 IAM do usuário.

Exemplos

Para ver exemplos de políticas WorkDocs baseadas em identidade da Amazon, consulte. [Exemplos de políticas WorkDocs baseadas em identidade da Amazon](#)

Políticas baseadas em WorkDocs recursos da Amazon

A Amazon WorkDocs não oferece suporte a políticas baseadas em recursos.

Autorização com base nas WorkDocs tags da Amazon

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

WorkDocs IAMFunções na Amazon

Uma [IAMfunção](#) é uma entidade dentro da sua AWS conta que tem permissões específicas.

Usando credenciais temporárias com a Amazon WorkDocs

É altamente recomendável usar credenciais temporárias para entrar com a federação, assumir uma IAM função ou assumir uma função entre contas. Você obtém credenciais de segurança temporárias ligando para AWS STS API operações como [AssumeRole](#) ou [GetFederationToken](#).

A Amazon WorkDocs oferece suporte ao uso de credenciais temporárias.

Funções vinculadas a serviço

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

A Amazon 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. As funções de serviço aparecem na sua IAM conta e são de propriedade da conta. Isso significa que um IAM administrador pode alterar as permissões para essa função. Porém, fazer isso pode alterar a funcionalidade do serviço.

A Amazon 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 IAM usuários sempre que possível.

Por padrão, IAM usuários e funções não têm permissão para criar ou modificar WorkDocs recursos da Amazon. Eles também não podem realizar tarefas usando o AWS Management Console, AWS CLI, ou AWS API. Um IAM administrador deve criar IAM políticas que concedam aos usuários e funções permissão para realizar API operações específicas nos recursos especificados de que precisam. O administrador deve então anexar essas políticas aos IAM usuários ou grupos 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 IAM baseada em identidade usando esses exemplos de documentos JSON de política, consulte [Criação de políticas na JSON guia](#) do IAMusuário.

Tópicos

- [Melhores práticas de política](#)
- [Usando o WorkDocs console da Amazon](#)
- [Permitir que usuários visualizem suas próprias permissões](#)
- [Permita que os usuários tenham acesso somente para leitura aos recursos da Amazon WorkDocs](#)
- [Mais exemplos de políticas WorkDocs baseadas em identidade da Amazon](#)

Melhores práticas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir WorkDocs recursos da Amazon 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 AWS gerenciadas](#) ou [políticas AWS gerenciadas para funções de trabalho](#) no Guia IAM do usuário.
- Aplique permissões com privilégios mínimos — Ao definir permissões com IAM políticas, conceda somente as permissões necessárias para realizar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre IAM como usar para aplicar permissões, consulte [Políticas e permissões IAM no](#) Guia IAM do usuário.
- Use condições nas IAM políticas para restringir ainda mais o acesso — Você pode adicionar uma condição às suas 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 IAM JSON da política: Condição](#) no Guia IAM do usuário.
- Use o IAM Access Analyzer para validar suas IAM políticas e garantir permissões seguras e funcionais — o IAM Access Analyzer valida políticas novas e existentes para que as políticas sigam a linguagem da IAM política (JSON) e as melhores práticas. IAM IAMO Access Analyzer fornece mais de 100 verificações de políticas e recomendações práticas para ajudá-lo a criar

políticas seguras e funcionais. Para obter mais informações, consulte [Validar políticas com o IAM Access Analyzer](#) no Guia do IAMUsuário.

- Exigir autenticação multifatorial (MFA) — Se você tiver um cenário que exija IAM usuários ou um usuário root Conta da AWS, ative MFA para obter segurança adicional. Para exigir MFA quando API as operações são chamadas, adicione MFA condições às suas políticas. Para obter mais informações, consulte [APIAcesso seguro com MFA](#) no Guia IAM do usuário.

Para obter mais informações sobre as melhores práticas emIAM, consulte [as melhores práticas de segurança IAM no](#) Guia IAM do usuário.

Usando o WorkDocs console da Amazon

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 da Amazon em sua AWS conta. Se você criar uma política baseada em identidade que seja mais restritiva do que as permissões mínimas exigidas, o console não funcionará conforme planejado para entidades de IAM usuário ou função.

Para garantir que essas entidades possam usar o WorkDocs console da Amazon, 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 IAM usuário.

- AmazonWorkDocsFullAccess
- AWSDirectoryServiceFullAccess
- Amazon EC2FullAccess

Essas políticas concedem ao usuário acesso total aos WorkDocs recursos da Amazon, 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 AWS CLI o. ou AWS API o. Em vez disso, permita o acesso somente às ações que correspondam à API operação que você está tentando realizar.

Permitir que usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permita IAM aos usuários visualizar as políticas embutidas e gerenciadas que estão anexadas à identidade do usuário. Essa política inclui

permissões para concluir essa ação no console ou programaticamente usando o AWS CLI ou. AWS API

```
{
  "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 da Amazon WorkDocs

A AmazonWorkDocsReadOnlyAccess política AWS gerenciada a seguir concede IAM ao usuário acesso somente de leitura aos recursos da Amazon WorkDocs . A política dá ao usuário acesso a todas as WorkDocs Describe operações da Amazon. O acesso às duas EC2 operações da

Amazon é necessário para que a Amazon WorkDocs 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 da Amazon

IAMos administradores podem criar políticas adicionais para permitir que uma IAM função ou usuário acesse a Amazon WorkDocs API. Para obter mais informações, consulte [Autenticação e controle de acesso para aplicativos administrativos](#) no Amazon WorkDocs Developer Guide.

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 a Amazon WorkDocs e IAM

Tópicos

- [Não estou autorizado a realizar uma ação na Amazon WorkDocs](#)
- [Não estou autorizado a realizar iam: PassRole](#)
- [Quero permitir que pessoas fora da minha AWS conta acessem meus WorkDocs recursos da Amazon](#)

Não estou autorizado a realizar uma ação na Amazon 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 um erro informando que não está autorizado a realizar a `iam:PassRole` ação, suas políticas devem ser atualizadas para permitir que você passe uma função para a Amazon 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 fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando um IAM usuário chamado `marymajor` tenta usar o console para realizar uma ação na Amazon 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 da Amazon

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode 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 a Amazon WorkDocs oferece suporte a esses recursos, consulte [Como a Amazon WorkDocs trabalha com IAM](#).
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte [Fornecer acesso a um IAM usuário em outro Conta da AWS de sua propriedade](#) no Guia do IAM usuário.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte [Fornecer Contas da AWS acesso a terceiros](#) no Guia do IAM usuário.
- Para saber como fornecer acesso por meio da federação de identidades, consulte [Fornecendo acesso a usuários autenticados externamente \(federação de identidades\)](#) no Guia do IAM usuário.
- Para saber a diferença entre usar funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a [recursos entre contas IAM no Guia](#) do IAM usuário.

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 da Amazon.

Tópicos

- [Exportação do feed de atividades de todo o site](#)
- [Usando AWS CloudTrail para registrar WorkDocs API chamadas da Amazon](#)

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 Amazon WorkDocs Companion. Para instalar o Amazon WorkDocs Companion, consulte [Aplicativos e integrações para a Amazon 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 — WorkDocsDownloads pasta 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 [Visualização do feed de atividades](#) no Guia WorkDocs do usuário da Amazon.

Usando AWS CloudTrail para registrar WorkDocs API chamadas da Amazon

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

Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para a Amazon 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 da Amazon em CloudTrail

CloudTrail é ativado em sua AWS conta quando você cria a conta. Quando a atividade ocorre na Amazon 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 de eventos em sua AWS conta, incluindo eventos para a Amazon WorkDocs, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as regiões. 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 SNS notificações da Amazon para CloudTrail](#)
- [Recebendo arquivos de CloudTrail log de várias regiões](#) e [Recebendo arquivos de CloudTrail log de várias contas](#)

Todas as WorkDocs ações da Amazon são registradas CloudTrail e documentadas na [WorkDocs APIReferência da Amazon](#). Por exemplo, chamadas para as UpdateDocument seçõesCreateFolder, 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 o seguinte:

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

Para obter mais informações, consulte o [CloudTrail userIdentityelemento](#).

Entendendo as entradas do arquivo de WorkDocs log da Amazon

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 API chamadas públicas, portanto, eles não aparecem em nenhuma ordem específica.

WorkDocs A Amazon 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 as entradas do plano de controle é um IAM usuário. A identidade do usuário para entradas do plano de dados é o usuário do WorkDocs diretório Amazon.

Note

Para maior segurança, crie usuários federados em vez de IAM usuários 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 CloudTrail registros. Eles aparecem como `HIDDEN _ DUE _ TO _ SECURITY _ REASONS` nos CloudTrail registros.

O exemplo a seguir mostra duas entradas de CloudTrail registro para a Amazon 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:

- [Guias de início rápido sobre segurança e conformidade](#) — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- [Arquitetura para HIPAA segurança e conformidade na Amazon Web Services](#) — Este whitepaper descreve como as empresas podem usar AWS para criar HIPAA aplicativos qualificados.

Note

Nem todos Serviços da AWS são HIPAA elegíveis. Para obter mais informações, consulte a [Referência de serviços HIPAA elegíveis](#).

- 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, por exemplo PCIDSS, 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 em AWS Identity and Access Management](#) no Guia IAM do usuário e [Melhores práticas de segurança, identidade e conformidade](#) no AWS Architecture Center.

Você usa API chamadas AWS publicadas para acessar a Amazon WorkDocs pela rede. Os clientes devem oferecer suporte ao 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 uma ID de chave de acesso e uma chave de acesso secreta associada a um IAM principal. Ou você pode usar o [AWS Security Token Service](#) (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Conceitos básicos do Amazon WorkDocs

O Amazon WorkDocs usa um diretório para armazenar e gerenciar informações organizacionais para os usuários e seus documentos. Por sua vez, você anexa um diretório a um site ao provisionar esse site. Quando você faz isso, um recurso do Amazon WorkDocs 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 [Convidar e gerenciar usuários do Amazon WorkDocs](#), consulte 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.
- Permita que o Amazon WorkDocs trabalhe com um diretório existente da AWS.
- Faça com que o Amazon WorkDocs crie um diretório para você.

Também é possível criar uma relação de confiança entre o diretório do AD e um diretório do AWS Managed Microsoft AD.

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.

Índice

- [Criação de um site do Amazon WorkDocs](#)

- [Habilitar o logon único](#)
- [Habilitar a autenticação multifator](#)
- [Promover um usuário a administrador](#)

Criação de um site do Amazon WorkDocs

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

Tarefas

- [Antes de começar](#)
- [Criação de um site do Amazon WorkDocs](#)

Antes de começar

É necessário possuir os seguintes itens antes de criar um site do Amazon WorkDocs.

- Uma conta AWS para criar e administrar sites do Amazon WorkDocs. No entanto, os usuários não precisam de uma conta da AWS para se conectar e usar o Amazon 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 diretório AWS Managed Microsoft AD 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 site do Amazon WorkDocs

Siga essas etapas para criar um site do Amazon WorkDocs em minutos.

Para criar o site Amazon WorkDocs

1. Abra o console do Amazon WorkDocs em <https://console.aws.amazon.com/zocalo/>.
2. Na página inicial do console, em Criar um site do WorkDocs, escolha Get Started now.

—OU—

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

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 administrador do WorkDocs, 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.

O Amazon WorkDocs faz o seguinte:

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

Note

O Amazon 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

O AWS Directory Service permite que os usuários acessem o Amazon WorkDocs de um computador conectado ao mesmo diretório de registro do Amazon WorkDocs, sem precisar inserir as credenciais separadamente. Os administradores do Amazon WorkDocs podem habilitar a autenticação única

usando o console do AWS Directory Service. Para obter mais informações, consulte [Single Sign-On](#) no Guia de administração do AWS Directory Service.

Depois que o administrador do Amazon WorkDocs habilita a autenticação única, os usuários do site do Amazon WorkDocs também podem precisar modificar suas configurações do navegador da web para permitir a autenticação única. 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 protocolo de cliente/servidor padrão da indústria que fornece autenticação, autorização e gerenciamento de contas para que os usuários se conectem com 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

Use o console do Amazon WorkDocs para promover um usuário a administrador. Siga estas etapas.

Para promover um usuário a administrador

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

A página Gerenciar seus sites do WorkDocs é exibida.

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

A caixa de diálogo Definir administrador do WorkDocs 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 administrativo do site Amazon WorkDocs para rebaixar um administrador. Para obter mais informações, consulte [Editar usuários](#).

Gerenciar o Amazon WorkDocs no Console da AWS

Você usa essas ferramentas para gerenciar seus sites do Amazon WorkDocs:

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

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

Configurando 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 console do Amazon WorkDocs em <https://console.aws.amazon.com/zocalo/>.
2. No painel de navegação, selecione My sites.

A página Gerenciar seus sites do WorkDocs 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 administrador do WorkDocs é exibida.

5. Na caixa Nome de usuário, insira o nome do novo administrador e escolha Definir administrador.

Reenvio de 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 console do Amazon WorkDocs em <https://console.aws.amazon.com/zocalo/>.

2. No painel de navegação, selecione My sites.

A página Gerenciar seus sites do WorkDocs 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 site do Amazon WorkDocs. Para obter mais informações sobre a autenticação, consulte [Habilitar a autenticação multifator](#).

Configurando URLs do site

Note

Se você seguiu o processo de criação do site em [Conceitos básicos do Amazon WorkDocs](#), inseriu a URL do site. Como resultado, o Amazon WorkDocs torna o comando Set site URL indisponível, porque você só pode definir um URL uma vez. Você só segue essas etapas se implantar o Amazon WorkSpaces e integrá-lo ao Amazon WorkDocs. O processo de integração do Amazon WorkSpaces 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 do Amazon WorkSpaces e do Amazon WorkDocs, consulte [Integrar com WorkDocs](#) no Guia do usuário do Amazon WorkSpaces.

Para definir o URL de um site

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

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

3. Selecione o site que você integrou ao Amazon WorkSpaces. A URL contém o ID do diretório da sua instância do Amazon WorkSpaces, 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 a URL do site e escolha Definir URL do site.
6. Na página Gerenciar seus sites do WorkDocs, escolha Atualizar para ver a nova 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 perfis do IAM chamem a API [CreateNotificationSubscription](#), que você pode usar para definir seu próprio endpoint para processar as mensagens SNS enviadas pelo WorkDocs. Para obter mais informações sobre notificações, consulte [Configuração de notificações para um usuário ou função do IAM](#) no Guia do desenvolvedor do Amazon WorkDocs.

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

Criar uma notificação

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

A página Gerenciar seus sites do WorkDocs 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 caixa de diálogo Definir administrador do WorkDocs é exibida.

5. Na caixa Nome de usuário, insira o nome do novo administrador e escolha Definir administrador.

Para excluir uma notificação

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

A página Gerenciar seus sites do WorkDocs 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 administrador do WorkDocs é exibida.

5. Na caixa Nome de usuário, insira o nome do novo administrador e escolha Definir administrador.

Excluir um site

Use o console do Amazon WorkDocs para excluir um site.

Warning

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

Para excluir uma organização

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

A página Gerenciar seus sites do WorkDocs 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 do usuário.

Important

Quando você não fornece um diretório próprio para o Amazon WorkDocs, nós criamos um para você. Ao excluir o site do Amazon WorkDocs, você será cobrado pelo diretório que criamos, a menos que você exclua ou use o diretório 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 a URL do site e escolha Excluir.

A organização será imediatamente excluída e não estará mais disponível.

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

Você usa essas ferramentas para gerenciar seus WorkDocs sites da Amazon:

- O painel de controle do administrador do site, disponível para administradores em todos os WorkDocs sites da Amazon 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 [Gerenciar o Amazon WorkDocs no Console da AWS](#).

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 ter 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

Os administradores WorkDocs do site da Amazon podem adicionar configurações da Lista de IPs Permitidos para restringir o acesso ao site a uma faixa permitida de endereços IP. Você pode adicionar até 500 configurações da Lista de Permissões de IP por site.

Note

Atualmente, a IP Allow List (Lista de permissões de IP) funciona somente para endereços IPv4. 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.

- 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

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



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

Permita que os usuários criem links compartilháveis em todo o site, mas não permita que eles criem links compartilháveis públicos

Permita que os usuários criem links compartilháveis em todo o site, mas somente usuários avançados podem criar links compartilháveis públicos

Todos os usuários gerenciados podem criar links compartilháveis públicos e em todo o site

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

Permita que todos os usuários do seu diretório sejam ativados automaticamente no primeiro login WorkDocs no seu site.

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

Somente administradores podem convidar novos usuários.

Os usuários podem convidar novos usuários de qualquer lugar compartilhando arquivos ou pastas com elas.

Os usuários podem convidar novos usuários de alguns domínios específicos compartilhando arquivos ou pastas com elas.

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

Descrição

Limita o compartilhamento de links apenas aos membros do site. Usuários gerenciados podem criar esse tipo de link.

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.

Usuários gerenciados podem criar links públicos.

Ativa automaticamente os usuários quando eles acessam seu site pela primeira vez.

Somente administradores podem convidar novos usuários.

Permite que os usuários convidem novos usuários compartilhando arquivos ou pastas com esses usuários.

Os usuários podem convidar novas pessoas dos domínios específicos compartilhando arquivos ou pastas com elas.

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.

- 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

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



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

Configuração

Permita que os usuários criem links compartilháveis em todo o site, mas somente usuários avançados podem criar links compartilháveis públicos

Todos os usuários gerenciados podem criar links compartilháveis públicos e em todo o site

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

Permita que todos os usuários do seu diretório sejam ativados automaticamente no primeiro login WorkDocs no seu site.

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.

Os usuários podem ativar novos usuários de seu diretório compartilhando arquivos ou pastas com elas.

Os usuários podem ativar novos usuários de alguns domínios específicos compartilhando arquivos ou pastas com elas.

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

Descrição

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.

Usuários gerenciados podem criar links públicos.

Ativa automaticamente os usuários quando eles acessam seu site pela primeira vez.

Permite que somente administradores ativem novos usuários do diretório.

Permite que os usuários ativem os usuários do diretório compartilhando arquivos ou pastas com os usuários do diretório.

Os usuários só podem compartilhar arquivos ou pastas de usuários em domínios específicos. Ao escolher essa opção, você deve inserir os domínios.

Configuração

Share with external users (Compartilhamento com usuários externos)

Note

As opções abaixo só aparecem depois que você escolhe essa configuração.

Only administrators can invite new external users (Somente administradores podem convidar novos usuários externos)

Todos os usuários gerenciados podem convidar novos usuários

Somente usuários avançados podem convidar 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)

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))

Descrição

Enables administrators and users to invite new external users to your Amazon WorkDocs site.

Somente administradores podem convidar usuários externos.

Permite que usuários gerenciados convidem usuários externos.

Permite que somente usuários avançados convidem novos usuários externos.

Converte automaticamente novos usuários do seu diretório em usuários gerenciados.

Converte automaticamente novos usuários externos em usuários gerenciados.

- Quando terminar, escolha Salvar alterações.

Retenção da lixeira de recuperação

Quando um usuário exclui um arquivo, a Amazon WorkDocs armazena o arquivo na lixeira do usuário por 30 dias. Depois, a Amazon WorkDocs move os arquivos para um compartimento de recuperação temporário por 60 dias e depois 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 da lixeira de recuperação antes que a Amazon os WorkDocs exclua 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 ter mais informações, consulte [Convidar e gerenciar usuários do Amazon WorkDocs](#).

Implantação do Amazon WorkDocs Drive em vários computadores

Se você tiver uma frota de máquinas associada a um domínio, poderá usar o Group Policy Objects (GPO) ou o System Center Configuration Manager (SCCM) para instalar o cliente Amazon WorkDocs Drive. Você pode baixar o cliente em <https://amazonworkdocs.com/en/clients>.

Ao prosseguir, lembre-se de que o Amazon WorkDocs Drive requer acesso HTTPS na porta 443 para todos os endereços IP do AWS. Você também deve confirmar se seus sistemas de destino atendem aos requisitos de instalação do Amazon WorkDocs Drive. Para obter mais informações, consulte [Instalar o Amazon WorkDocs Drive](#) no Guia do usuário do Amazon WorkDocs.

Note

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

O instalador MSI do Amazon WorkDocs oferece suporte aos seguintes parâmetros de instalação opcionais:

- **SITEID**: preenche previamente as informações do site do Amazon WorkDocs para os usuários durante o registro. Por exemplo, `SITEID=site-name`.
- **DefaultDriveLetter**: preenche previamente a letra de unidade a ser usada para a montagem do Amazon WorkDocs Drive. 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 do drive, mas não a letra do drive, depois de iniciarem o Amazon WorkDocs Drive pela primeira vez.

O exemplo a seguir implanta o Amazon 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 do Amazon WorkDocs

Por padrão, quando você anexa um diretório durante a criação do site, o recurso de ativação automática no Amazon WorkDocs adiciona todos os usuários desse diretório ao novo site como usuários gerenciados.

No WorkDocs, 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 web do Amazon WorkDocs, e as etapas nas seções a seguir explicam como. Mas, se você é novo no Amazon WorkDocs, dedique alguns minutos e aprenda sobre as várias funções de usuário antes de mergulhar nas tarefas administrativas.

Índice

- [Visão geral das funções de usuário](#)
- [Iniciando o painel de controle administrativo](#)
- [Desativar a ativação automática](#)
- [Gerenciando o compartilhamento de links](#)
- [Controle de convites de usuários com ativação automática ativada](#)
- [Convidar novos usuários](#)
- [Editar usuários](#)
- [Desabilitar usuários](#)
- [Transferir propriedade do documento](#)
- [Fazer download das listas de usuários](#)

Visão geral das funções de usuário

O Amazon 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 site do Amazon WorkDocs.
- **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.

O Amazon WorkDocs também define esses tipos adicionais de usuários.

Usuário do WS

Um usuário com um WorkSpaces Workspace atribuído.

- Acesso a todos os recursos do Amazon WorkDocs
- 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 WorkSpaces Workspace atribuído e armazenamento atualizado.

- Acesso a todos os recursos do Amazon WorkDocs
- Armazenamento padrão de 1 TB (armazenamento adicional disponível com pagamento conforme o uso)
- Cobranças mensais são aplicadas

Usuário do Amazon WorkDocs

Um usuário ativo do Amazon WorkDocs sem um WorkSpaces Workspace atribuído.

- Acesso a todos os recursos do Amazon WorkDocs
- Armazenamento padrão de 1 TB (armazenamento adicional disponível com pagamento conforme o uso)
- Cobranças mensais são aplicadas

Iniciando o painel de controle administrativo

Você usa o painel de controle administrativo no cliente web do Amazon WorkDocs 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 de perfil no canto superior direito do cliente WorkDocs.



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 de perfil no canto superior direito do cliente WorkDocs.



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 no site do WorkDocs.

As opções são alteradas em Quem deve ter permissão para ativar os usuários do diretório em seu site do WorkDocs. 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. Os usuários do Amazon WorkDocs 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 de perfil no canto superior direito do cliente WorkDocs.



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 Save Changes (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 de perfil no canto superior direito do cliente WorkDocs.



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 usuários do diretório em seu site do WorkDocs, 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 de perfil no canto superior direito do cliente WorkDocs.



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.

O Amazon WorkDocs envia um e-mail de convite para cada destinatário. O e-mail contém um link e instruções sobre como criar uma conta do Amazon WorkDocs. 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 de perfil no canto superior direito do cliente WorkDocs.



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](#).

Role (Função)

Especifica se alguém é usuário ou administrador. Também é possível fazer upgrade ou downgrade de um usuário que tiver um Workspace do WorkSpaces atribuído. Para obter mais informações, consulte [Visão geral das funções de usuário](#).

Storage (Armazenamento)

Especifica o limite de armazenamento de um usuário existente.

5. Escolha Save Changes (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 de perfil no canto superior direito do cliente WorkDocs.



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 site do Amazon WorkDocs.

Note

Alterar o status de um usuário para Inativo não exclui os arquivos, as pastas ou os comentários dele do seu site do Amazon WorkDocs. 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.

O site do Amazon WorkDocs deve sempre 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 evitar que ele acesse seu site do Amazon WorkDocs.

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 de perfil no canto superior direito do cliente WorkDocs.



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 Save Changes (Salvar alterações).

Fazer download das listas de usuários

Para fazer download de uma lista de usuários no Painel de controle do administrador, você deve instalar o Companion do Amazon WorkDocs. Para instalar o Amazon WorkDocs Companion, consulte [Aplicativos e integrações para o Amazon WorkDocs](#).

Para fazer download de uma lista de usuários

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



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
 - Admin
5. O 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.

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

Índice

- [Compartilhar links](#)
- [Compartilhar por convite](#)
- [Compartilhamento externo](#)
- [Permissões](#)
- [Habilitar edição colaborativa](#)

Compartilhar links

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

- Todos os membros do site do Amazon WorkDocs podem pesquisar, visualizar e comentar o arquivo.
- Qualquer pessoa com o link, mesmo pessoas que não são membros do site do Amazon WorkDocs, pode visualizar 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 Amazon 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 Amazon a partir do painel de controle do administrador do site](#).

Compartilhamento externo

O compartilhamento externo permite que os usuários gerenciados de um site do Amazon WorkDocs compartilhem arquivos e pastas e colaborem com usuários externos sem incorrer em custos extras. Os usuários do site podem compartilhar arquivos e pastas com destinatários externos não pagos do site do Amazon WorkDocs. 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. Ao escolher o link, os usuários externos são direcionados para o site, no qual eles digitam suas credenciais para fazer login no Amazon 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 Amazon a partir do painel de controle do administrador do site](#).

Permissões

A Amazon 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](#)
- [Permissões para pastas compartilhadas](#)
- [Permissões para arquivos em pastas compartilhadas](#)
- [Permissões para arquivos que não estão em pastas compartilhadas](#)

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 (permissões somente de leitura) 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 contrária, um visualizador anônimo tem as mesmas permissões que um visualizador.

* 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.

	Visão	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 arquivo MP4 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 compartilhamento	Visualizar anotações	Visualizar atividade	Visualizar versões	Excluir versões	Recuperar versões	Ver todos os comentários privados*
Proprietário	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

	Anotar	Deletar	Renomear	Carregar	Baixar	Imprimir	Compartilhar	Revogar compartilhamento	Visão geral	Visualizar comentários	Visualizar anotações	Visualizar atividades	Visualizar versões	Excluir versão	Recuperar versão	Ver todos os comentários privados*
do arquivo																
Proprietário da pasta	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Copista da pasta	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Colaborador da pasta	✓			✓	✓				✓	✓	✓	✓	✓			
Visualizador da pasta				✓					✓	✓						
Visualizador anônimo									✓	✓						

* 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 proprietário, 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 arquivo MP4 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	Deletar	Renomear	Carregar	Baixar	Impedir download	Compartilhar	Revogar compartilhamento	Visão	Visualizar comentários	Visualizar anotações	Visualizar atividades	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.

Índice

- [Habilitar o Hancom ThinkFree](#)
- [Habilitação da opção de abrir com o Office Online](#)

Habilitar o Hancom ThinkFree

Você pode habilitar o Hancom ThinkFree para seu site do Amazon WorkDocs para que os usuários possam criar e editar arquivos do Microsoft Office de maneira colaborativa no aplicativo web do Amazon WorkDocs. Para obter mais informações, consulte [Editar com o Hancom ThinkFree](#).

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

Para habilitar o Hancom ThinkFree

Habilite a edição do Hancom ThinkFree no Admin control panel (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 desabilitar o Hancom ThinkFree

Desabilite a edição do Hancom ThinkFree no Admin control panel (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 a opção de abrir com o Office Online para o seu site do Amazon WorkDocs, para que os usuários possam editar de maneira colaborativa os arquivos do Microsoft Office no aplicativo web Amazon WorkDocs.

A opção de abrir com o Office Online é disponibilizada sem nenhum custo adicional para os usuários do Amazon WorkDocs que também têm uma conta corporativa ou de estudante do Microsoft Office

365 com uma licença para editar 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).

Migração de arquivos para a Amazon WorkDocs

WorkDocs Os administradores da Amazon podem usar o Amazon WorkDocs Migration Service para realizar uma migração em grande escala de vários arquivos e pastas para o site da Amazon WorkDocs . O Amazon WorkDocs Migration Service funciona com o Amazon Simple Storage Service (Amazon S3). Isso permite migrar compartilhamentos de arquivos departamentais e compartilhamentos de arquivos de unidades domésticas ou de usuários para a Amazon. WorkDocs

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

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

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

- Permissões de administrador para seu WorkDocs site da Amazon
- Permissões para criar uma função do IAM

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

- Não use Admin como nome de usuário da sua WorkDocs conta Amazon. Admin é uma função de usuário reservada na Amazon WorkDocs.
- Seu tipo de usuário WorkDocs administrador da Amazon deve ser Usuário WS atualizado. Para ter mais informações, consulte [Visão geral das funções de usuário](#) e [Editar usuários](#).

Note

A estrutura de diretórios, os nomes dos arquivos e o conteúdo dos arquivos são preservados durante a migração para a Amazon WorkDocs. A propriedade e as permissões dos arquivos não são preservadas.

Tarefas

- [Etapa 1: Preparar conteúdo para a migração](#)
- [Etapa 2: Carregar arquivos para o Amazon S3](#)
- [Etapa 3: Programar uma migração](#)
- [Etapa 4: Rastrear uma migração](#)
- [Etapa 5: Limpar recursos](#)

Etapa 1: Preparar conteúdo para a migração

Para preparar o conteúdo para migração

1. No seu WorkDocs site da Amazon, 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. O Amazon WorkDocs 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 site da Amazon WorkDocs . 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 carregar seus arquivos e pastas no 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 \(IAMpolíticas\) DataSync no Guia](#) do AWS DataSync usuário.

Etapa 3: Programar uma migração

Depois de concluir as etapas 1 e 2, use o Amazon WorkDocs Migration Service para programar 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 da Amazon muda automaticamente para Ilimitado.

Note

A migração de arquivos que excedem o limite WorkDocs de armazenamento da Amazon pode resultar em custos adicionais. Para obter mais informações, consulte [Amazon WorkDocs Pricing](#).

O Amazon WorkDocs Migration Service fornece uma política AWS Identity and Access Management (IAM) para você usar na migração. Com essa política, você cria uma nova IAM função que concede ao Amazon WorkDocs Migration Service acesso ao bucket do Amazon S3 e ao WorkDocs site da Amazon que você designar. Você também assina as notificações SNS por e-mail da Amazon para receber atualizações quando sua solicitação de migração está agendada e quando ela começa e termina.

Como programar uma migração:

1. No WorkDocs console da Amazon, escolha Apps, Migrations.
 - Se esta é a primeira vez que você acessa o Amazon WorkDocs Migration Service, você será solicitado a assinar as notificações SNS por e-mail da Amazon. 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. Para Fonte de dados e validação, em Política de exemplo, copie a IAM política fornecida.
6. Use a IAM política que você copiou na etapa anterior para criar uma nova IAM política e função, da seguinte maneira:
 - a. Abra o IAM console em <https://console.aws.amazon.com/iam/>.
 - b. Selecione Políticas (Políticas), Create policy (Criar política).
 - c. Escolha JSON e cole a IAM política que você copiou para sua área de transferência anteriormente.
 - d. Selecione Revisar política. Insira um nome e uma descrição para a política.
 - e. Escolha Criar política.
 - f. Selecione Roles (Funções), Create role (Criar função).

- g. Selecione Outra AWS conta. 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 função.
 - 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/sessão para 12 horas.
 - l. Copie a função ARN para sua área de transferência para usar na próxima etapa.
7. Retorne ao Amazon WorkDocs Migration Service. Em Fonte de dados e validação, em Função ARN, cole a função ARN da IAM função que você copiou 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 na Amazon 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 Amazon WorkDocs Migration Service. Para acessar a página inicial no WorkDocs site da Amazon, escolha Apps, Migrations. 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.

Failed (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 estiver concluída, exclua a política e a função de migração que você criou no IAM console.

Para excluir a IAM política e a função

1. Abra o IAM console 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 começa, a configuração de armazenamento da sua conta de WorkDocs usuário da Amazon 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 Amazon WorkDocs

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

Problemas

- [Não é possível configurar meu site do Amazon WorkDocs em uma região específica da AWS](#)
- [Desejo configurar meu site do Amazon WorkDocs em uma Amazon VPC existente](#)
- [O usuário precisa redefinir a senha dele](#)
- [O usuário compartilhou acidentalmente um documento confidencial](#)
- [O usuário deixou a organização e não transferiu a propriedade do documento](#)
- [Preciso implantar o Drive do Amazon WorkDocs ou o Companion do Amazon WorkDocs para vários usuários](#)
- [A edição online não está funcionando](#)

Não é possível configurar meu site do Amazon WorkDocs em uma região específica da AWS

Se você estiver configurando um novo site do Amazon WorkDocs, selecione a região da AWS durante a configuração. Para mais informações, consulte o tutorial para seu caso de uso específico em [Conceitos básicos do Amazon WorkDocs](#).

Desejo configurar meu site do Amazon WorkDocs em uma Amazon VPC existente

Ao configurar seu novo site do Amazon WorkDocs, crie um diretório usando a nuvem privada virtual (VPC) existente. O Amazon WorkDocs usa um 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](#).

Preciso implantar o Drive do Amazon WorkDocs ou o Companion do Amazon WorkDocs 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 do Amazon WorkDocs Drive para vários usuários, consulte [Implantação do Amazon WorkDocs Drive em vários computadores](#).

A edição online não está funcionando

Verifique se o Amazon WorkDocs Companion está instalado. Para instalar o Amazon WorkDocs Companion, consulte [Aplicativos e integrações para o Amazon WorkDocs](#).

Gerenciando o Amazon WorkDocs para Amazon Business

Se você for um administrador do Amazon WorkDocs for Amazon Business, será possível gerenciar usuários fazendo login em <https://workdocs.aws/> usando as credenciais do Amazon Business.

Para convidar um novo usuário para o Amazon WorkDocs for Amazon Business

1. Faça login com as credenciais do Amazon Business em <https://workdocs.aws/>.
2. Na página inicial do Amazon WorkDocs para 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. Escolha Done (Concluído).

Para pesquisar um usuário no Amazon WorkDocs para Amazon Business

1. Faça login com as credenciais do Amazon Business em <https://workdocs.aws/>.
2. Na página inicial do Amazon WorkDocs para 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 Amazon WorkDocs para Amazon Business

1. Faça login com as credenciais do Amazon Business em <https://workdocs.aws/>.
2. Na página inicial do Amazon WorkDocs para 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 Amazon WorkDocs para Amazon Business

1. Faça login com as credenciais do Amazon Business em <https://workdocs.aws/>.
2. Na página inicial do Amazon WorkDocs para 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 Delete (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 nos dispositivos que acessam o Amazon WorkDocs, adicione os endereços IP e domínios a seguir à sua lista de permissões. Isso permite que o Amazon WorkDocs e o Amazon WorkDocs Drive se conectem ao serviço WorkDocs.

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

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 DeleteDocumentVersion API.	29 de julho de 2022
WorkDocs Backup da Amazon	A documentação do Amazon WorkDocs Backup foi removida do Guia de WorkDocs Administração da Amazon porque o componente não é mais suportado.	24 de junho de 2021
Gerenciando a Amazon WorkDocs para Amazon Business	O Amazon WorkDocs for Amazon Business oferece suporte ao gerenciamento de usuários por administradores. Para obter mais informações, consulte Gerenciando a Amazon WorkDocs para Amazon Business no Guia de WorkDocs Administração da Amazon.	26 de março de 2020
Migração de arquivos para a Amazon WorkDocs	WorkDocs Os administradores da Amazon podem usar o Amazon WorkDocs Migration Service para realizar uma	8 de agosto de 2019

migração em grande escala de vários arquivos e pastas para o site da Amazon WorkDocs . Para obter mais informações, consulte [Migração de arquivos para a Amazon WorkDocs](#) no Guia de WorkDocs Administração da Amazon.

[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 da Amazon por faixa de endereços IP. Para obter mais informações, consulte [as configurações da lista de permissões de IP](#) no Amazon WorkDocs Administration 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 da Amazon. Para obter mais informações, 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 da Amazon. 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 informações, consulte [Solução de WorkDocs problemas da Amazon](#) 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