aws

Guia de administração

Amazon WorkDocs

Amazon WorkDocs: Guia de administração

Table of Contents

Você deve ser um administrador de WorkDocs sistema da Amazon para concluir as etapas deste guia. Se precisar de ajuda para usar a Amazon WorkDocs, consulte Introdução à Amazon WorkDocs no Guia do WorkDocs usuário da Amazon.

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 Amazon 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.

Pré-requisitos do Amazon WorkDocs

Para configurar novas organizações ou gerenciar organizações existentes do Amazon WorkDocs, você deve concluir as tarefas a seguir.

Cadastrar-se em uma Conta da AWS

Se você ainda não tem Conta da AWS, siga as etapas a seguir para criar um.

Para se cadastrar em uma Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
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 cadastra em uma Conta da AWS, um Usuário raiz da conta da AWS é criado. O usuário raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua acesso administrativo a um usuário administrativo e use somente o usuário raiz para realizar as tarefas que exigem acesso do usuário raiz.

A AWS envia um e-mail de confirmação depois que o processo de cadastramento é concluído. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando My Account (Minha conta).

Criar um usuário administrador

Depois de se inscrever em uma Conta da AWS, crie um usuário administrativo para não usar o usuário raiz em tarefas cotidianas.

Proteger seu Usuário raiz da conta da AWS

1. Faça login no AWS Management Console como o proprietário da conta ao escolher a opção Root user (Usuário raiz) e inserir o endereço de e-mail da Conta da AWS. Na próxima página, insira sua senha.

Para obter ajuda ao fazer login usando o usuário raiz, consulte Signing in as the root user (Fazer login como usuário raiz) no Guia do usuário do Início de Sessão da AWS.

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

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

Criar um usuário administrador

- Para suas tarefas administrativas diárias, conceda acesso administrativo a um usuário administrativo no AWS IAM Identity Center.

  Para obter instruções, consulte Getting started (Introdução) no Manual do usuário do AWS IAM Identity Center.

Fazer login como usuário administrador

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

  Para obter ajuda com o login utilizando um usuário do Centro de Identidade do IAM, consulte Fazer login no portal de acesso da AWS, no Guia do usuário do Início de Sessão da AWS.

Segurança no Amazon WorkDocs

A segurança para com a nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se contará com um datacenter e uma arquitetura de rede criados para atender aos requisitos das organizações com as maiores exigências de segurança.

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

- Segurança da nuvem: a AWS é responsável pela proteção da infraestrutura que executa produtos da AWS na Nuvem AWS. A AWS também fornece serviços que podem ser usados 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 ao Amazon WorkDocs, consulte Serviços da AWS no escopo pelo programa de conformidade.
- Segurança na nuvem: os serviços da AWS 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. O tópico desta seção ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Amazon WorkDocs.

> **Note**
>
> Os usuários de uma determinada organização do WorkDocs podem colaborar com usuários de fora dessa organização enviando um link ou convite para um arquivo. Revise 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 o Amazon WorkDocs para atender aos seus objetivos de segurança e compatibilidade. Você também aprenderá como usar outros serviços da AWS que ajudam você a monitorar e proteger os recursos do Amazon WorkDocs.

Tópicos

- Resiliência no Amazon WorkDocs
- Segurança da infraestrutura no Amazon WorkDocs

Gerenciamento de identidade e acesso para o Amazon WorkDocs

O AWS Identity and Access Management (IAM) é um serviço da AWS service (Serviço da AWS) que ajuda a controlar o acesso aos recursos da AWS de forma segura. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (ter permissões) para utilizar os recursos do Amazon WorkDocs. O IAM é um AWS service (Serviço da AWS) que pode ser usado sem custo adicional.

Tópicos

- Público
- Como autenticar com identidades
- Gerenciamento do acesso usando políticas
- Como o Amazon WorkDocs funciona com o IAM
- Exemplos de políticas baseadas em identidade do Amazon WorkDocs
- Solução de problemas de identidade e acesso do Amazon WorkDocs

Público

A forma de usar o AWS Identity and Access Management (IAM) varia em função do trabalho realizado no Amazon WorkDocs.

Usuário do serviço: se você usar o serviço do Amazon WorkDocs para fazer seu trabalho, o administrador fornecerá as credenciais e as permissões necessárias. À medida que mais recursos do Amazon WorkDocs forem usados para realizar o trabalho, talvez sejam necessárias 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 atributo no Amazon WorkDocs, consulte Solução de problemas de identidade e acesso do Amazon WorkDocs.

Administrador do serviço: se você for o responsável pelos recursos do Amazon WorkDocs em sua empresa, provavelmente terá acesso total ao Amazon WorkDocs. Cabe a você determinar quais funcionalidades e recursos do Amazon WorkDocs os usuários do seu serviço devem acessar. Assim, é necessário enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de

seu serviço. Revise as informações nesta página para entender os conceitos básicos do IAM. Para saber mais sobre como a empresa pode usar o IAM com o Amazon WorkDocs, consulte Como o Amazon WorkDocs funciona com o IAM.

Administrador do IAM: se você for um administrador do IAM, talvez deseje saber detalhes sobre como escrever políticas para gerenciar o acesso ao Amazon WorkDocs. Para visualizar exemplos de políticas do Amazon WorkDocs baseadas em identidade que podem ser usadas no IAM, consulte Exemplos de políticas baseadas em identidade do Amazon WorkDocs.

Como autenticar com identidades

A autenticação é a forma como você faz login na AWS usando suas credenciais de identidade. É necessário ser autenticado (fazer login na AWS) como o usuário raiz da Usuário raiz da conta da AWS, como usuário do IAM ou assumindo um perfil do IAM.

Você pode fazer login na AWS como uma identidade federada usando credenciais fornecidas por uma fonte de identidades. AWS IAM Identity Center Os usuários do IAM Identity Center, a autenticação única da empresa e as suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como uma identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Quando você acessa a AWS usando a federação, está indiretamente assumindo um perfil.

É possível fazer login no AWS Management Console ou no portal de acesso da AWS dependendo do tipo de usuário que você é. Para obter mais informações sobre como fazer login na AWS, consulte How to sign in to your Conta da AWS (Como fazer login na conta da) no Início de Sessão da AWS User Guide (Guia do usuário do).

Se você acessar a AWS programaticamente, a AWS fornecerá um kit de desenvolvimento de software (SDK) e uma interface da linha de comando (CLI) para você assinar criptograficamente as solicitações usando as suas credenciais. Se você não utilizar as ferramentas da AWS, deverá assinar as solicitações por conta própria. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinar solicitações de API da AWS no Guia do usuário do IAM.

Independentemente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, a AWS recomenda o uso da autenticação multifator (MFA) para aumentar a segurança de sua conta. Para saber mais, consulte Autenticação multifator no GuiaAWS IAM Identity Center do usuário. Usar a autenticação multifator (MFA) naAWS no Guia do usuário do IAM.

Grupos e usuários do IAM

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

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

Usuários são diferentes de funções. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas uma função pode ser assumida por qualquer pessoa que precisar dela. Os usuários têm credenciais permanentes de longo prazo, mas as funções fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário do IAM (em vez de uma função) no Guia do usuário do IAM.

Funções do IAM

Um perfil do IAM é uma identidade dentro da Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. É possível assumir temporariamente um perfil do IAM no AWS Management Console alternando perfis. É possível assumir um perfil chamando uma operação de API da AWS CLI ou da AWS, ou usando um URL personalizado. Para obter mais informações sobre métodos para o uso de perfis, consulte Usar perfis do IAM no Guia do usuário do IAM.

Os perfis do IAM 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, ela é associada ao perfil e recebe as permissões definidas pelo perfil. Para obter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidades de terceiros no Guia do usuário do IAM. Se você usar o IAM Identity Center, configure 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 um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Permission sets (Conjuntos de permissões) no Guia do usuário do AWS IAM Identity Center.

- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode assumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (um principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, alguns Serviços da AWS permitem que você anexe uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recurso para acesso entre contas, consulte Como as funções do IAM diferem das políticas baseadas em recurso no Guia do usuário do IAM.
- Acesso entre serviços: alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando uma função de serviço ou uma função vinculada ao serviço.
  - Permissões de principal: ao usar um usuário ou um perfil do IAM para executar ações na AWS, você é considerado um principal. As políticas concedem permissões a uma entidade principal. Quando você usa alguns serviços, pode executar uma ação que, em seguida, aciona outra ação em outro serviço. Nesse caso, você deve ter permissões para executar ambas as ações. Para ver se uma ação requer ações dependentes adicionais em uma política, consulte a Referência de autorização de serviço.
  - Função de serviço: uma função de serviço é uma função do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do IAM.
  - Função vinculada a serviço: uma função vinculada a serviço é um tipo de função de serviço vinculada a um AWS service (Serviço da AWS). O serviço pode assumir a função de executar uma ação em seu nome. Os perfis vinculados ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para funções vinculadas ao serviço.
- Aplicações em execução no Amazon EC2: é possível usar uma função do IAM para gerenciar credenciais temporárias para aplicações em execução em uma instância do EC2 e fazer solicitações da AWS CLI ou da AWS API. É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma função da AWS a uma instância do EC2 e disponibilizá-

la para todas as suas aplicações, crie um perfil de instância que esteja anexado a ela. Um perfil de instância contém a função e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Uso de uma função do IAM para conceder permissões a aplicações em execução em instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar as funções do IAM, consulte Quando criar uma função do IAM (em vez de um usuário) no Guia do usuário do IAM.

Gerenciamento do acesso usando políticas

Você controla o acesso na AWS criando políticas e anexando-as a identidades ou recursos da AWS. Uma política é um objeto na AWS que, quando associado a uma identidade ou recurso, define suas permissões. A AWS avalia essas políticas quando uma entidade 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 são armazenadas na AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

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

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

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

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou função do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda mais como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou função. As políticas gerenciadas são políticas independentes que podem ser anexadas a vários usuários, grupos e funções na Conta da AWS. As políticas gerenciadas incluem políticas gerenciadas pela AWS e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recurso são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de função do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o 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 um principal em uma política baseada em recursos. As entidades principais podem incluir contas, usuários, funções, usuários federados ou Serviços da AWS.

Políticas baseadas em recursos são políticas em linha que estão localizadas nesse serviço. Não é possível usar as políticas gerenciadas da AWS do IAM em uma política baseada em recursos.

Listas de controle de acesso

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

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

Outros tipos de política

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

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

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

- Políticas de controle de serviço (SCPs): SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (UO) no AWS Organizations. O AWS Organizations é um serviço para agrupar e gerenciar centralmente várias Contas da AWS pertencentes à sua empresa. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades em contas-membro, incluindo cada Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizations e SCPs, consulte Como os SCPs funcionam no Guia do usuário do AWS Organizations.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para uma função ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou da função e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recurso. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

> **Note**
>
> O 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 a AWS determina se deve permitir uma solicitação quando há vários tipos de política envolvidos, consulte Lógica da avaliação de políticas no Guia do usuário do IAM.

Como o Amazon WorkDocs funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao Amazon WorkDocs, você deve entender quais recursos do IAM estão disponíveis para uso com o Amazon WorkDocs. Para obter uma visualização de alto nível de como o Amazon WorkDocs e outros serviços da AWS funcionam com o IAM, consulte Serviços da AWS compatíveis com o IAM no Guia do usuário do IAM.

Tópicos

Políticas baseadas em identidade do Amazon WorkDocs

Com políticas do IAM baseadas em identidade, é possível especificar ações permitidas ou negadas. O Amazon WorkDocs oferece suporte a ações específicas. Para saber mais sobre os elementos usados em uma política JSON, consulte Referência de elementos de política JSON do IAM no Manual do usuário do IAM.

Ações

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

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

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

As ações de política no Amazon WorkDocs usam o seguinte prefixo antes da ação: `workdocs:`. Por exemplo, para conceder a alguém permissão para executar a operação de API Amazon WorkDocs do `DescribeUsers`, inclua a ação `workdocs:DescribeUsers` na política da pessoa. As instruções de política devem incluir um elemento `Action` ou `NotAction`. O Amazon WorkDocs

define seu próprio conjunto de ações que descrevem as tarefas que você pode executar com esse serviço.

Para especificar várias ações em uma única declaração, separe-as com vírgulas, conforme o seguinte:

```
"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 das ações do Amazon WorkDocs, consulte Ações definidas pelo Amazon WorkDocs no Manual do usuário do IAM.

Recursos

O Amazon WorkDocs não oferece suporte à especificação de ARNs de recursos em uma política.

Chaves de condição

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

Exemplos

Para visualizar exemplos de políticas baseadas em identidade do Amazon WorkDocs, consulte Exemplos de políticas baseadas em identidade do Amazon WorkDocs.

Políticas baseadas em recursos do Amazon WorkDocs

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

Autorização baseada em tags do Amazon WorkDocs

O Amazon WorkDocs não é compatível com recursos de marcação ou de controle de acesso com base em tags.

Perfis do IAM do Amazon WorkDocs

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

Usar credenciais temporárias com o Amazon WorkDocs

Recomendados fortemente usar credenciais temporárias para fazer login com federação, assumir um perfil do IAM ou assumir um perfil entre contas. As credenciais de segurança temporárias são obtidas chamando AWS STS operações da API como AssumeRole ou GetFederationToken.

O Amazon WorkDocs oferece suporte ao uso de credenciais temporárias.

Funções vinculadas ao serviço

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

O Amazon WorkDocs não oferece suporte às funções vinculadas ao serviço.

Perfis de serviço

Esse recurso permite que um serviço assuma um perfil de serviço em seu nome. A função permite que o serviço acesse recursos em outros serviços para concluir uma ação em seu nome. As funções de serviço aparecem em sua conta do IAM e são de propriedade da conta. Isso significa que um administrador do IAM pode alterar as permissões para essa função. Porém, fazer isso pode alterar a funcionalidade do serviço.

O Amazon WorkDocs não é compatível com perfis de serviço.

Exemplos de políticas baseadas em identidade do Amazon WorkDocs

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

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

> **Note**
>
> Para garantir a compatibilidade com versões anteriores, inclua a ação `zocalo` em suas políticas. Por exemplo:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": [
            "zocalo:*",
            "workdocs:*"
            ],
            "Resource": "*"
        }
    ]
}
```

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

Tópicos

Práticas recomendadas de políticas

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

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

Analyzer oferece mais de 100 verificações de política e recomendações acionáveis para ajudar você a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do usuário do IAM.

- Require multi-factor authentication (MFA) (Exigir autenticação multifator (MFA)): se houver um cenário que exija usuários do IAM ou um usuário raiz em sua Conta da AWS, ative a MFA para obter segurança adicional. Para exigir a MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do usuário do IAM.

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

Usar o console do Amazon WorkDocs

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

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

- AmazonWorkDocsFullAccess
- AWSDirectoryServiceFullAccess
- AmazonEC2FullAccess

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

Não é necessário conceder permissões mínimas do console para usuários que fazem chamadas somente à AWS CLI ou à API do AWS. Em vez disso, permita o acesso somente às ações que correspondem à operação da API que você está tentando executar.

Permitir que os usuários visualizem suas próprias permissões

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

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

Permitir aos usuários acesso somente leitura aos recursos do Amazon WorkDocs

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

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

Mais exemplos de políticas baseadas em identidade do Amazon WorkDocs

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

Solução de problemas de identidade e acesso do Amazon WorkDocs

Use as informações a seguir para ajudar a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o Amazon WorkDocs e o IAM.

Tópicos

- Não tenho autorização para executar uma ação no Amazon WorkDocs
- Não estou autorizado a executar iam:PassRole

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

Não tenho autorização para executar uma ação no Amazon WorkDocs

Se o AWS Management Console informar que você não está autorizado a executar uma ação, você deverá entrar em contato com o administrador para obter assistência. O administrador é a pessoa que forneceu a você o seu nome de usuário e senha.

Não estou autorizado a executar iam:PassRole

Caso receba uma mensagem de erro informando que você não tem autorização para executar a ação `iam:PassRole`, as políticas deverão ser atualizadas para permitir a transmissão de um perfil ao Amazon WorkDocs.

Alguns Serviços da AWS permitem que você transmita um perfil existente para o serviço, em vez de criar um perfil de serviço ou um perfil vinculado ao serviço. Para fazer isso, um usuário deve ter permissões para passar o perfil para o serviço.

O erro exemplificado a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta usar o console para executar uma ação no Amazon WorkDocs. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar a função 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 você precisar de ajuda, entre em contato com seu administrador da AWS. Seu administrador é a pessoa que forneceu a você suas credenciais de login.

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

Você pode criar uma função 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 a

função. 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 o seguinte:

- Para saber se o Amazon WorkDocs é compatível com esses recursos, consulte Como o Amazon WorkDocs funciona com o IAM.
- Para saber como conceder acesso a seus recursos em todas as Contas da AWS pertencentes a você, consulte Fornecimento de acesso a um usuário do IAM em outra Conta da AWS pertencente a você no Guia de usuário do IAM.
- Para saber como conceder acesso a seus recursos para terceiros Contas da AWS, consulte Fornecimento de acesso a Contas da AWS pertencentes a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre usar perfis e políticas baseadas em recursos para acesso entre contas, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

Registrar em log e monitorar no Amazon WorkDocs

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

Tópicos

Exportação do feed de atividades de todo o site

Os administradores podem visualizar e exportar o feed de atividade de uma organização inteira. Para usar esse recurso, você deve primeiro instalar o aplicativo Amazon WorkDocs Companion. Para instalar o Amazon WorkDocs Companion, consulte Aplicativos e integrações para o 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: pasta WorkDocsDownloads na pasta Downloads do seu computador
   - 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 do usuário do Amazon WorkDocs.

Usar o AWS CloudTrail para log de chamadas de API do Amazon WorkDocs

Você pode usar o AWS CloudTrail para registrar chamadas de API do Amazon WorkDocs. O CloudTrail fornece um registro de ações executadas por um usuário, uma função ou um serviço da AWS no Amazon WorkDocs. O CloudTrail captura todas as chamadas de API para o Amazon WorkDocs como eventos, incluindo chamadas do console do Amazon WorkDocs e chamadas de código para as APIs do Amazon WorkDocs.

Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para o Amazon WorkDocs. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history.

As informações coletadas pelo 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 o CloudTrail, consulte o Guia do usuário do AWS CloudTrail.

Informações sobre o Amazon WorkDocs no CloudTrail

O CloudTrail é habilitado em sua conta da AWS quando ela é criada. Quando ocorre uma atividade no Amazon WorkDocs, essa atividade é registrada em um evento do CloudTrail junto com outros eventos de serviço da AWS no Histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua conta da AWS. Para obter mais informações, consulte Visualizar eventos com o histórico de eventos do CloudTrail.

Para obter um registro de eventos em andamento na sua conta da AWS, incluindo eventos do Amazon WorkDocs, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as regiões. A trilha registra em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, é possível configurar outros serviços da AWS para analisar mais ainda mais e agir com base nos dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- Serviços e integrações compatíveis com o CloudTrail
- Configurar notificações do Amazon SNS para o CloudTrail
- Receber arquivos de log do CloudTrail de várias regiões e Receber arquivos de log do CloudTrail de várias contas

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

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

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

Para obter mais informações, consulte Elemento userIdentity do CloudTrail.

Noções básicas sobre entradas de arquivos de log do Amazon WorkDocs

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer origem e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada das chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

Há dois tipos de entrada do CloudTrail geradas pelo Amazon WorkDocs: do ambiente de gerenciamento e do plano de dados. A diferença importante entre os dois é que a identidade do usuário para entradas do ambiente de gerenciamento é um usuário do IAM. A identidade do usuário para entradas do plano de dados é o usuário do diretório do Amazon WorkDocs.

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

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

O exemplo a seguir mostra duas entradas de registro do CloudTrail para o Amazon WorkDocs: o primeiro registro é para uma ação do ambiente de gerenciamento, 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 compatibilidade para o Amazon WorkDocs

Para saber se um AWS service (Serviço da AWS) está no escopo de programas de conformidade específicos, consulte Serviços da AWS no escopo por programa de conformidade e selecione o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de conformidade da AWS.

É possível fazer download de relatórios de auditoria de terceiros usando o AWS Artifact. Para obter mais informações, consulte Downloading Reports in AWS Artifact.

Sua responsabilidade de conformidade ao usar o Serviços da AWS é determinada pela confidencialidade dos seus dados, pelos objetivos de conformidade da sua empresa e pelos regulamentos e leis aplicáveis. A AWS fornece os seguintes recursos para ajudar com a conformidade:

- Guias de início rápido de segurança e conformidade: estes guias de implantação discutem considerações sobre arquitetura e fornecem as etapas para a implantação de ambientes de linha de base focados em segurança e conformidade na AWS.
- Architecting for HIPAA Security and Compliance on Amazon Web Services (Arquitetura para segurança e conformidade com HIPAA no Amazon Web Services): esse whitepaper descreve como as empresas podem usar a AWS para criar aplicações adequadas aos padrões HIPAA.

  > **Note**
  >
  > Nem todos os Serviços da AWS estão qualificados pela HIPAA. Para mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- Recursos de conformidade da AWS: essa coleção de manuais e guias pode ser aplicada a seu setor e local.
- Avaliar recursos com regras no AWS Config Developer Guide (Guia do desenvolvedor do CCI): o serviço AWS Config avalia como as configurações de recursos estão em conformidade com práticas internas, diretrizes do setor e regulamentos.
- AWS Security Hub: este AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança na 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.

- AWS Audit Manager: esse AWS service (Serviço da AWS) ajuda a auditar continuamente seu uso da AWS para simplificar a forma como você gerencia os riscos e a conformidade com regulamentos e padrões do setor.

Resiliência no Amazon WorkDocs

A infraestrutura global da AWS é criada com base em regiões da AWS e zonas de disponibilidade. As regiões da AWS As regiões fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, as quais são conectadas com baixa latência, alto throughput e redes altamente redundantes. Com as zonas de disponibilidade, você pode 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 regiões e zonas de disponibilidade da AWS, consulte Infraestrutura global da AWS.

Segurança da infraestrutura no Amazon WorkDocs

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

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

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

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

- 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 do 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 uma 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.

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

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

Segurança — ActiveDirectory Sites simples

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

Para usar configurações de segurança

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

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

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

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

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

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

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

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

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

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

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

4. Quando terminar, escolha Salvar alterações.

Segurança — sites de ActiveDirectory conexão

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

Para usar configurações de segurança

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

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

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

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

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

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

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

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

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

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

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

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

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

4. Quando terminar, escolha Salvar alterações.

Retenção da lixeira de recuperação

Quando um usuário exclui um arquivo, 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

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

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

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

Índice

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.

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 do 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	Visão	Visualizar compartilhamento	Visualizar anotações	Visualizar atividade	Visualizar versões	Excluir versões	Recuperar versões	Ver todos os comentários privados**
Proprio	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

	Anota	Exclu	Re	nom	Carrega	Baixa	Impe	Ci	ompa	har	Revoga	compar	hament	Visã	Visualiz	r	compar	hament	Visualiz	r	anotaçã	Visualiz	r	ativida	Visualiz	r	versõe	Exclu	versõe	Recuper	versõe	Ver	todos	os	comentári	os	privados	*	*
do arqu																																							
Prop rio da past	✓	✓	✓		✓	✓	✓		✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Copı tário da past	✓	✓	✓		✓	✓	✓		✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cola or da past	✓				✓	✓								✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓												
Visu dor da past						✓								✓	✓																								
Visu dor anôr														✓	✓																								

* O proprietário do arquivo, neste caso, é a pessoa que carregou a versão original de um arquivo em uma pasta compartilhada. As permissões para essa função se aplicam apenas ao arquivo que tem proprietário, não a todos os arquivos que estão na pasta compartilhada.

** O proprietário/coproprietário do arquivo pode ver todos os comentários privados. Os colaboradores podem ver apenas comentários privados que sejam respostas aos comentários deles.

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 do Amazon WorkDocs.

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

	Anotar	Excluir	Renomear	Carregar	Baixar	Impedir download	Compartilhar	Revogar compartilhamento	Visão	Visualizar compartilhamento	Visualizar anotação	Visualizar atividade	Visualizar versões	Excluir versões	Recuperar versões
Proprietário	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Coproprietário	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Contributor (Colaborador)	✓			✓	✓				✓	✓	✓	✓	✓		
Visualizador					✓				✓	✓					
Visualizador anônimo									✓	✓					

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

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 o Amazon WorkDocs

Os administradores do Amazon WorkDocs podem usar o Amazon WorkDocs Migration Service para realizar uma migração em grande escala de vários arquivos e pastas para o site do Amazon WorkDocs. O Amazon WorkDocs Migration Service funciona com o Amazon Simple Storage Service (Amazon S3). Isso permite migrar os compartilhamentos de arquivos e unidade local do departamento ou os compartilhamentos arquivos do usuário para o Amazon WorkDocs.

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

- Ler e listar o bucket do Amazon S3 designado por você.
- Ler e gravar no site do Amazon WorkDocs designado por você.

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

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

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

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

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

Tarefas

Etapa 1: Preparar conteúdo para a migração

Para preparar o conteúdo para migração

1. No site do Amazon WorkDocs, em Meus documentos, crie uma pasta para a qual deseja migrar os arquivos e as 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 bucket do Amazon Simple Storage Service (Amazon S3) na conta da AWS na qual você deseja fazer upload de arquivos e pastas. O bucket do Amazon S3 deve estar na mesma conta AWS e região da AWS que o site do 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 o AWS DataSync para carregar arquivos e pastas no bucket do Amazon S3. O DataSync fornece recursos adicionais de rastreamento, geração de relatórios e sincronização. Para obter mais informações, consulte Como o AWS DataSync funciona e Como usar políticas baseadas em identidade (políticas do IAM) para o DataSync no Guia do usuário do AWS DataSync.

Etapa 3: Programar uma migração

Após 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 usuário do Amazon WorkDocs muda automaticamente para Ilimitado.

> **Note**
>
> A migração de arquivos que excederem o limite de armazenamento do Amazon WorkDocs poderá resultar em custos adicionais. Para obter mais informações, consulte Preços do Amazon WorkDocs.

O Amazon WorkDocs Migration Service fornece uma política do AWS Identity and Access Management (IAM) para ser usada para a migração. Com essa política, é possível criar um perfil do IAM que conceda ao Amazon WorkDocs Migration Service acesso ao bucket do Amazon S3 e ao site do Amazon WorkDocs designados por você. Também é possível se inscrever em notificações de e-mail do Amazon SNS para receber atualizações quando a solicitação de migração for programada e quando ela for iniciada e finalizada.

Como programar uma migração:

1. No console do Amazon WorkDocs, selecione Aplicativos, Migrações.
   - Se este for seu primeiro acesso ao Amazon WorkDocs Migration Service, será solicitado que você se inscreva nas notificações de e-mail do Amazon SNS. Inscreva-se, realize a confirmação na mensagem de e-mail que você receber e selecione Continue (Continuar).
2. Selecione Create Migration (Criar migração).
3. Em Source Type (Tipo de origem), selecione Amazon S3.
4. Escolha Next (Próximo).
5. Em Validação e fonte de dados, em Exemplo de política, copie a política do IAM fornecida.
6. Use a política do IAM copiada na etapa anterior para criar uma função e política do IAM da seguinte maneira:
   a. Abra o console do IAM em https://console.aws.amazon.com/iam/.
   b. Selecione Policies (Políticas), Create policy (Criar política).
   c. Selecione JSON e cole a política do IAM copiada anteriormente para a área de transferência.
   d. Escolha Review policy (Revisar política). Insira um nome e uma descrição para a política.
   e. Escolha Create policy (Criar política).
   f. Selecione Roles (Funções), Create role (Criar função).

g. Selecione Another AWS account (Outra conta da AWS). Em Account ID (ID da conta), insira uma das seguintes opções:

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

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

i. Insira um nome e uma descrição para a função. Selecione Create role (Criar função).

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

k. Na página Summary (Resumo), altere Maximum CLI/API session duration (Duração máxima da sessão de CLI/API) para 12 horas.

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

7. Retorne ao Amazon WorkDocs Migration Service. Em Validação e fonte de dados, em ARN da função, cole o ARN do perfil do IAM copiado na etapa anterior.
8. Em Bucket, selecione o bucket do Amazon S3 do qual migrar os arquivos.
9. Escolha Next (Próximo).
10. Em Selecionar uma pasta de destino do WorkDocs, selecione a pasta de destino no Amazon WorkDocs para a qual migrar os arquivos.
11. Escolha Next (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 Send (Enviar).

Etapa 4: Rastrear uma migração

É possível rastrear a migração na página inicial do Amazon WorkDocs Migration Service. Para acessar a página inicial do site do Amazon WorkDocs, selecione Aplicativos, Migrações. Selecione

sua migração para visualizar os detalhes e acompanhar seu progresso. Também é possível selecionar Cancel Migration (Cancelar a migração), caso precise cancelá-la, ou selecionar Update (Atualizar) para atualizar a linha do tempo da migração. Depois que a migração for concluída, você poderá selecionar Download report (Fazer download do relatório) para fazer download de um log dos arquivos migrados com êxito, de falhas ou erros.

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

Programado

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

Migrating

A migração está em andamento.

Bem-sucedida

A migração foi concluída.

Partial Success (Parcialmente bem-sucedida)

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

Reprovada

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

Canceled

A migração foi cancelada.

Etapa 5: Limpar recursos

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

Para excluir a política e o perfil do IAM

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. Escolha Policies (Políticas).

3. Pesquise e selecione a política que você criou.
4. Em Policy actions (Ações da política), selecione Delete (Excluir).
5. Escolha Delete (Excluir).
6. Escolha Roles.
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 usuário do Amazon WorkDocs é automaticamente alterada para Ilimitado. Após a migração, será possível escolher as configurações de Storage (Armazenamento) editando a conta do usuário no painel de controle do administrador. 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

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 o 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 DeleteDocumentVersionAPI.	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 informaçõ es, 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

Glossário da AWS

Para obter a terminologia mais recente da AWS, consulte o glossário da AWS na Referência do Glossário da AWS.