aws

Guia de administração

Amazon WorkSpaces

Amazon WorkSpaces: Guia de administração

Table of Contents

O que é a Amazon WorkSpaces?

A Amazon WorkSpaces permite que você provisione desktops Microsoft Windows, Amazon Linux ou Ubuntu Linux virtuais baseados em nuvem para seus usuários, conhecidos como. WorkSpaces WorkSpaces elimina a necessidade de adquirir e implantar hardware ou instalar software complexo. Você pode rapidamente adicionar ou remover usuários à medida que suas necessidades mudarem. Os usuários podem acessar suas áreas de trabalho virtuais de vários dispositivos ou navegadores da web.

Para obter mais informações, consulte Amazon WorkSpaces.

Atributos

- Escolha seu sistema operacional (Windows, Amazon Linux, Ubuntu Linux) e selecione entre diversas configurações de hardware, configurações de software e regiões da AWS. Para obter mais informações, consulte Amazon WorkSpaces Bundles e. the section called “Criar uma imagem e um pacote personalizados”
- Escolha seu protocolo: PCoIP ou WorkSpaces Streaming Protocol (WSP). Para ter mais informações, consulte Protocolos para a Amazon WorkSpaces.
- Conecte-se ao seu WorkSpace e continue exatamente de onde você parou. WorkSpacesfornece uma experiência de desktop persistente.
- WorkSpaces fornece a flexibilidade do faturamento mensal ou por hora para WorkSpaces. Para obter mais informações, consulte WorkSpaces Preços.
- Para áreas de trabalho do Windows, você pode trazer as suas próprias licenças e aplicações ou comprá-las no AWS Marketplace for Desktop Apps.
- Crie um diretório gerenciado autônomo para seus usuários ou conecte-o WorkSpaces ao seu diretório local para que eles possam usar suas credenciais existentes para obter acesso contínuo aos recursos corporativos. Para ter mais informações, consulte Diretórios.
- Use as mesmas ferramentas de gerenciamento WorkSpaces que você usa para gerenciar desktops locais.
- Use a Multi-Factor Authentication (MFA) para segurança adicional.
- Use o AWS Key Management Service (AWS KMS) para criptografar dados em repouso, E/S de disco e snapshots de volumes.
- Controle os endereços IP a partir dos quais os usuários podem acessar seus WorkSpaces.

Arquitetura

Para Windows e Linux WorkSpaces, cada um WorkSpace está associado a uma nuvem privada virtual (VPC) e a um diretório para armazenar e gerenciar informações para você WorkSpaces e para os usuários. Para ter mais informações, consulte the section called “Requisitos da VPC”. Os diretórios são gerenciados por meio do AWS Directory Service, que oferece as seguintes opções: Simple AD, AD Connector ou AWS Directory Service para Microsoft Active Directory, também conhecido como Microsoft AD gerenciado pela AWS. Para obter mais informações, consulte o Guia do administrador do AWS Directory Service.

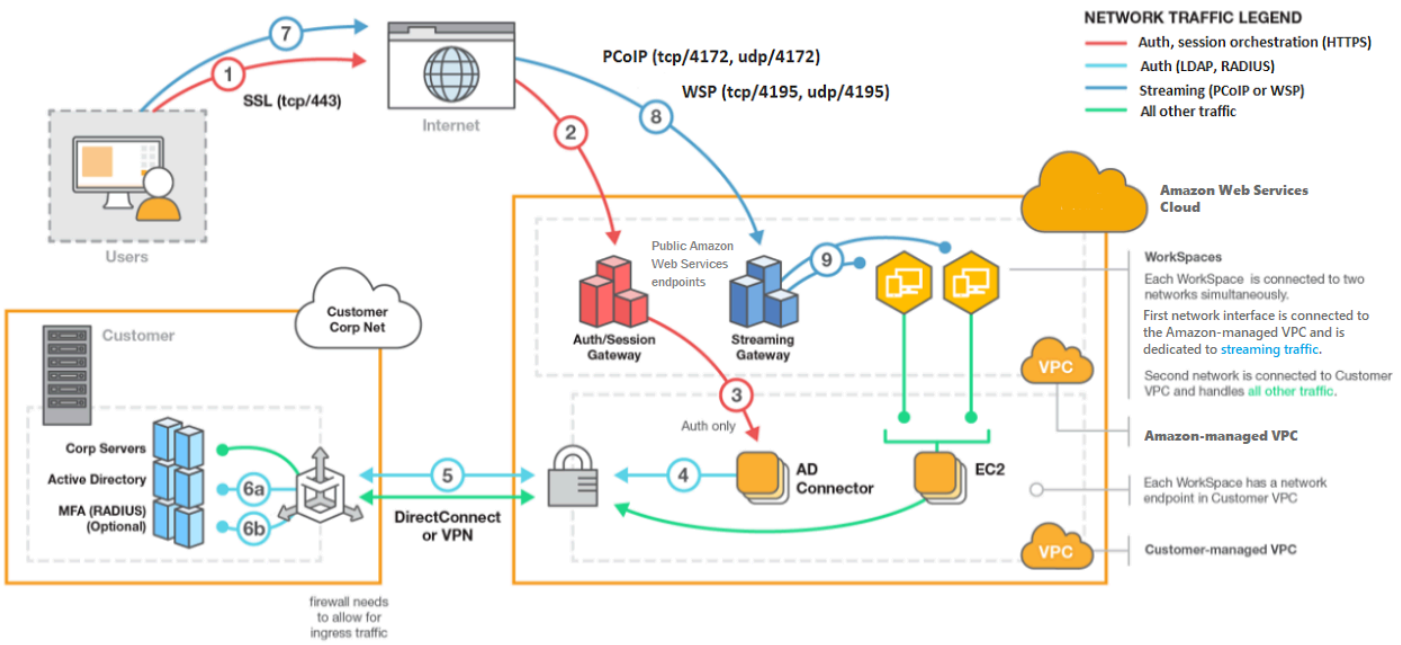
WorkSpaces usa seu diretório Simple AD, AD Connector ou AWS Managed Microsoft AD para autenticar usuários. Os usuários os acessam WorkSpaces usando um aplicativo cliente de um dispositivo compatível ou, para Windows WorkSpaces, de um navegador da Web e fazem login usando suas credenciais de diretório. As informações de login são enviadas para um gateway de autenticação, que encaminha o tráfego para o diretório do WorkSpace. Depois que o usuário é autenticado, o tráfego de streaming é iniciado por meio do gateway de streaming.

Os aplicativos clientes usam HTTPS na porta 443 para todas as informações relacionadas a autenticação e sessão. Os aplicativos cliente usam a porta 4172 (PCoIP) e a porta 4195 (WSP) para streaming de pixels para a e as portas 4172 WorkSpace e 4195 para verificações de integridade da rede. Para ter mais informações, consulte Portas para aplicações cliente.

Cada uma WorkSpace tem duas interfaces de rede elástica associadas: uma interface de rede para gerenciamento e streaming (eth0) e uma interface de rede primária (eth1). A interface de rede primária tem um endereço IP fornecido pela VPC, das mesmas sub-redes usadas pelo diretório. Isso garante que o tráfego do seu WorkSpace possa chegar facilmente ao diretório. O acesso a recursos na VPC é controlado pelos grupos de segurança atribuídos à interface de rede primária. Para ter mais informações, consulte Interfaces de rede.

O diagrama a seguir mostra a arquitetura do WorkSpaces.

Amazon WorkSpaces Architectural Diagram



Acesse seu WorkSpace

Você pode se conectar ao seu WorkSpaces usando o aplicativo cliente de um dispositivo compatível usando um navegador da Web compatível em um sistema operacional compatível.

> **Note**
>
> Você não pode usar um navegador da web para se conectar ao Amazon Linux WorkSpaces.

Há aplicativos clientes para os seguintes dispositivos:

- Computadores Windows
- Computadores macOS
- Computadores Ubuntu Linux 18.04
- Chromebooks
- iPads
- Dispositivos Android
- Tablets Fire

- Dispositivos cliente zero (dispositivos cliente zero do Teradici são compatíveis somente com PCoIP.)

Em PCs com Windows, macOS e Linux, você pode usar os seguintes navegadores da Web para se conectar ao Windows e ao Ubuntu Linux: WorkSpaces

- Chrome 53 e posterior (somente Windows e macOS)
- Firefox 49 e superior

Para obter mais informações, consulte WorkSpaces Clientes no Guia WorkSpaces do usuário da Amazon.

Definição de preço

Depois de se inscreverAWS, você pode começar a usar WorkSpaces gratuitamente a oferta de nível WorkSpaces gratuito. Para obter mais informações, consulte WorkSpaces Preços.

Com WorkSpaces, você paga apenas pelo que usa. Você é cobrado com base no pacote e no número do WorkSpaces que você lança. O preço WorkSpaces inclui o uso do Simple AD e do AD Connector, mas não o uso do AWS Managed Microsoft AD.

WorkSpaces fornece faturamento mensal ou por hora para WorkSpaces. Com o faturamento mensal, você paga uma taxa fixa pelo uso ilimitado, o que é melhor para usuários que usam em tempo WorkSpaces integral. Com o faturamento por hora, você paga uma pequena taxa mensal fixa por WorkSpace, além de uma taxa horária baixa para cada hora em execução. WorkSpace Para obter mais informações, consulte WorkSpaces Preços.

Para obter informações sobre as regiões suportadas, consulte WorkSpaces Preços.

Como começar a usar

Para criar um WorkSpace, experimente um dos seguintes tutoriais:

- Conceitos básicos de configuração rápida do WorkSpaces
- Inicializar um WorkSpace usando o AWS Managed Microsoft AD
- Inicializar um WorkSpace usando o Simple AD
- Inicializar um WorkSpace usando o AD Connector

- Inicializar um WorkSpace usando um domínio confiável

Talvez você também queira explorar esses recursos para saber mais sobre a Amazon WorkSpaces:

- Provision Desktops in the Cloud
- Melhores práticas para implantar a Amazon WorkSpaces
- WorkSpaces Recursos da Amazon — incluem whitepapers, publicações em blogs, webinars e sessões do re:Invent
- WorkSpaces Perguntas frequentes da Amazon

Conceitos básicos de configuração rápida do WorkSpaces

Neste tutorial, você aprenderá a provisionar uma área de trabalho virtual e baseada na nuvem do Microsoft Windows, do Amazon Linux ou do Ubuntu Linux, que é conhecida como WorkSpace, usando o WorkSpaces e o AWS Directory Service.

Este tutorial usa a opção de configuração rápida para iniciar o WorkSpace. Essa opção estará disponível somente se nunca tiver ativado um WorkSpace. Como alternativa, consulte Inicializar uma área de trabalho virtual usando WorkSpaces.

> **Note**
>
> A configuração rápida é compatível com as seguintes regiões da AWS:
>
> - Leste dos EUA (N. da Virgínia)
> - Oeste dos EUA (Oregon)
> - Europa (Irlanda)
> - Ásia-Pacífico (Singapura)
> - Ásia-Pacífico (Sydney)
> - Ásia-Pacífico (Tóquio)
>
> Para alterar a região, consulte Escolher uma região.

Tarefas

Antes de começar

Antes de começar, certifique-se de que os seguintes requisitos são atendidos:

- É necessário ter uma conta da AWS para criar ou administrar um WorkSpace. Os usuários não precisam de uma conta da AWS para se conectar e usar os WorkSpaces.
- O WorkSpaces não está disponível em todas as regiões. Verifique as regiões compatíveis e selecione uma região para os WorkSpaces. Para obter mais informações sobre as regiões compatíveis, consulte os preços do WorkSpaces por região da AWS.

É importante também analisar e compreender os seguintes conceitos antes de continuar:

- Ao ativar um WorkSpace, você deve selecionar um pacote do WorkSpace. Para obter mais informações, consulte Pacotes do Amazon WorkSpaces e Preço do Amazon WorkSpaces.
- Ao iniciar um WorkSpace, você deve selecionar qual protocolo (PCoIP ou WorkSpaces Streaming Protocol [WSP]) deseja usar com seu pacote. Para obter mais informações, consulte Protocolos para a Amazon WorkSpaces.
- Ao executar um WorkSpace, você deve especificar as informações de perfil do usuário, incluindo um nome de usuário e o endereço de e-mail. Os usuários concluem o perfil ao especificar uma senha. As informações sobre o WorkSpaces e os usuários são armazenadas em um diretório. Para obter mais informações, consulte Diretórios.

Funções da configuração rápida

A configuração rápida executa as seguintes tarefas em seu nome:

- Cria um perfil do IAM para permitir que o serviço WorkSpaces crie interfaces de rede elásticas e liste os diretórios de seus WorkSpaces. Essa função tem o nome `workspaces_DefaultRole`.
- Cria uma nuvem privada virtual (VPC). Se você preferir usar uma VPC existente, garanta que ela atenda aos requisitos indicados em Configurar uma VPC para WorkSpaces e siga as etapas em um dos tutoriais listados em Inicializar uma área de trabalho virtual usando WorkSpaces. Escolha o tutorial correspondente ao tipo do Active Directory que deseja usar.
- Configura um diretório do Simple AD na VPC e o habilita para o Amazon WorkDocs. Esse diretório do Simple AD é usado para armazenar informações do usuário e do WorkSpace. A primeira Conta da AWS criada pela configuração rápida é sua Conta da AWS de administrador. † O diretório

também tem uma conta de administrador. Para obter mais informações, consulte What gets created no Guia de administração do AWS Directory Service.

- Cria as Contas da AWS especificadas e as adiciona ao diretório.
- Cria Workspaces. Cada WorkSpace recebe um endereço IP público para fornecer acesso à Internet. O modo de execução é AlwaysOn. Para obter mais informações, consulte Gerenciar o modo de execução do WorkSpace.
- Envia convites por e-mail para os usuários especificados. Se os usuários não receberem os convites por e-mail, consulte Enviar um convite por e-mail.

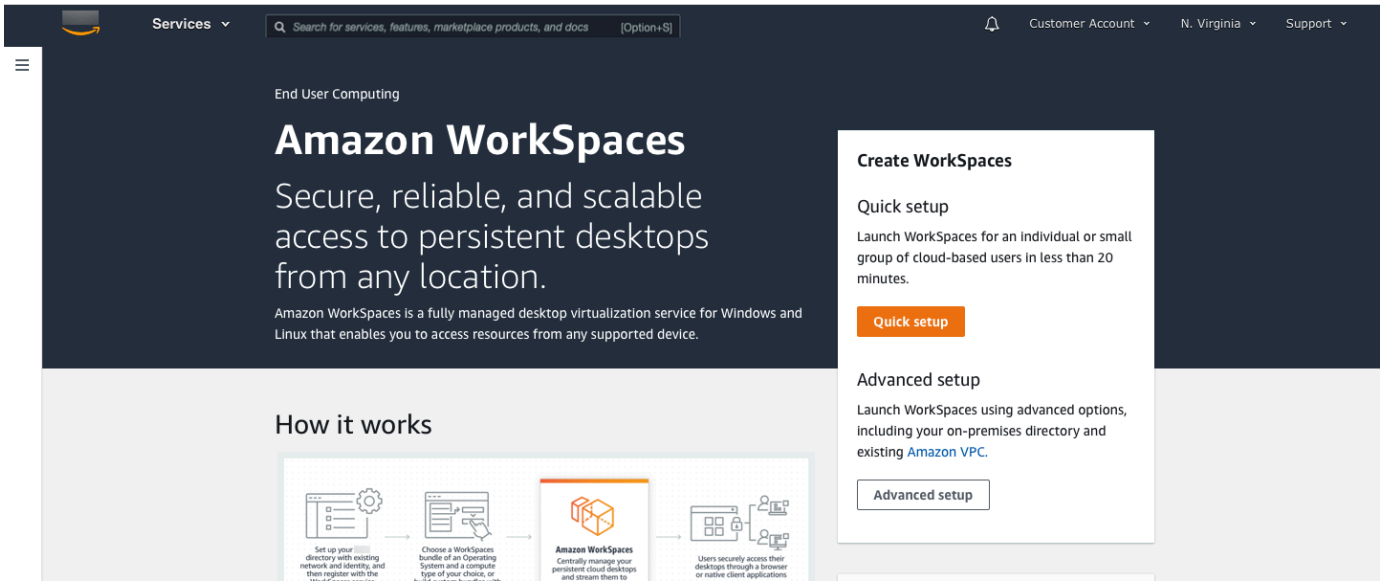
† A primeira Conta da AWS criada pela configuração rápida é sua Conta da AWS de administrador. Não é possível atualizar essa Conta da AWS no console do WorkSpaces. Não compartilhe as informações dessa conta com outras pessoas. Para convidar outros usuários a usar o WorkSpaces, crie novas Contas da AWS para eles.

Etapa 1: Ativar o WorkSpace

Usando a configuração rápida, você pode iniciar seu primeiro WorkSpace em minutos.

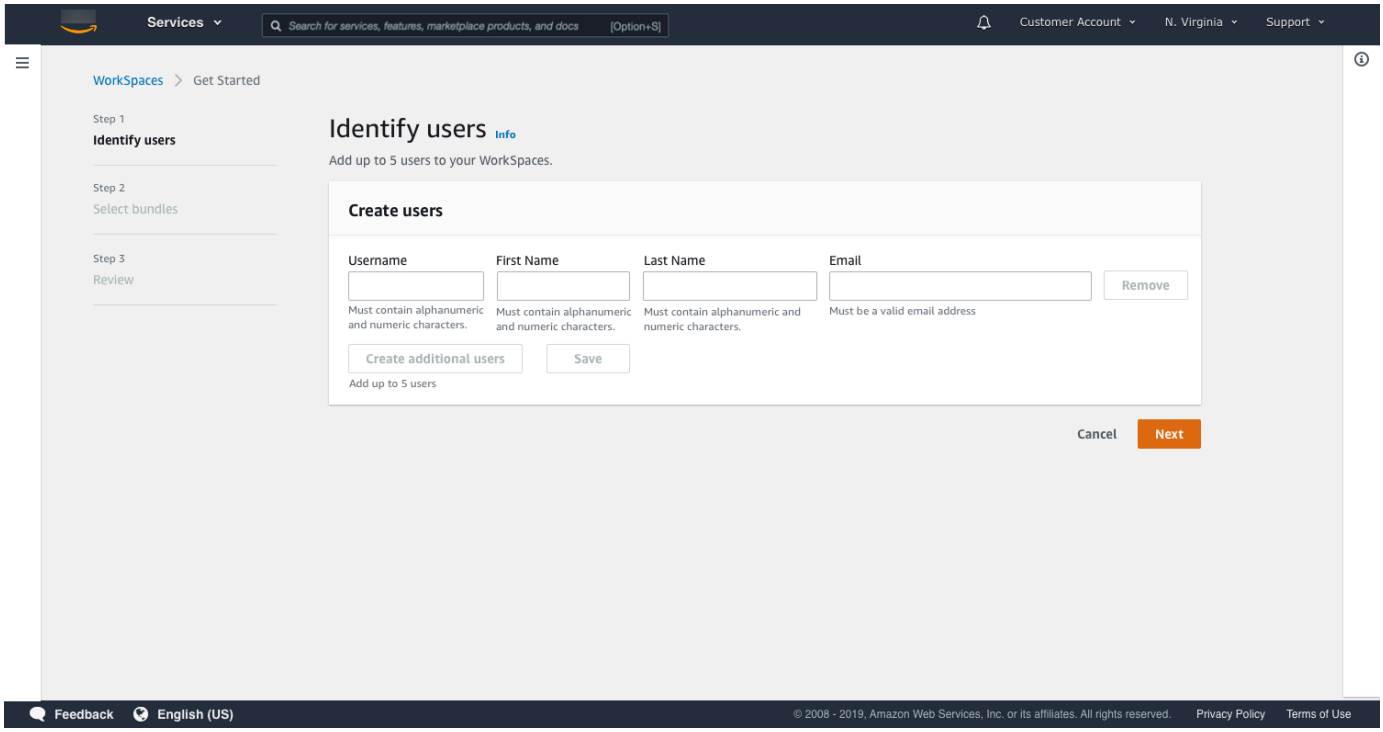
Para ativar um WorkSpace

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. Escolha Quick setup (Configuração rápida). Se esse botão não for exibido, ou você já iniciou um WorkSpace nessa região, ou você não está usando uma das regiões compatíveis com a configuração rápida. Nesse caso, consulte Inicializar uma área de trabalho virtual usando WorkSpaces.

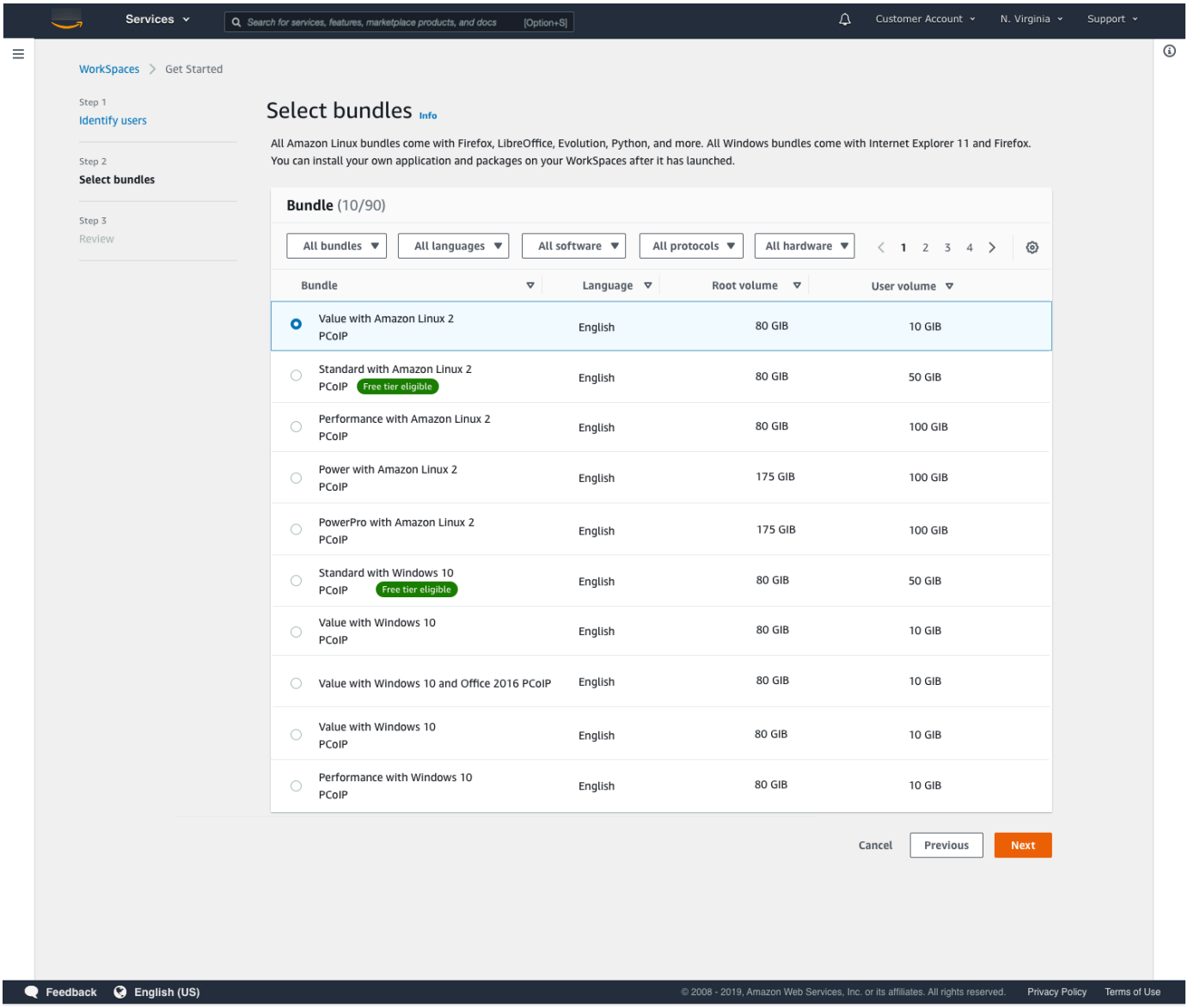


3. Em Identificar usuários, insira o Nome de usuário, o Nome, o Sobrenome e o E-mail. Em seguida, escolha Next (Próximo).

> **Note**
>
> Se esta é a sua primeira vez usando WorkSpaces, recomendamos criar um usuário para você mesmo para fins de teste.



4. Em Pacotes, selecione um pacote (hardware e software) para o usuário com o protocolo apropriado (PCoIP ou WSP). Para obter mais informações sobre os vários pacotes públicos disponíveis para o Amazon WorkSpaces, consulte Pacotes do Amazon WorkSpaces.



5. Revise as informações. Em seguida, selecione Criar WorkSpace.
6. A inicialização do WorkSpace leva aproximadamente 20 minutos. Para monitorar o progresso, vá para o painel de navegação esquerdo e selecione Diretórios. Você verá um diretório sendo criado com o status inicial de `REQUESTED` e depois de `CREATING`.

   Depois que o diretório for criado e tiver o status de `ACTIVE`, você poderá selecionar WorkSpaces no painel de navegação esquerdo para monitorar o progresso do processo de inicialização do WorkSpace. O status inicial do WorkSpace é `PENDING`. Quando a inicialização for concluída, o status será de `AVAILABLE` e um convite será enviado para o endereço de e-mail que você especificou para cada usuário. Se os usuários não receberem os convites por e-mail, consulte Enviar um convite por e-mail.

Etapa 2: Conectar-se ao WorkSpace

Depois de receber o e-mail de convite, você pode se conectar ao WorkSpace usando o cliente de sua escolha. Depois de fazer login, o cliente exibe o desktop WorkSpace.

Para se conectar ao WorkSpace

1. Se você ainda não configurou credenciais para o usuário, abra o link no e-mail de convite e siga as instruções. Lembre-se da senha que você especificar, pois precisará dela para se conectar ao WorkSpace.

   > **Note**
   >
   > As senhas diferenciam maiúsculas de minúsculas e devem ter entre 8 e 64 caracteres. As senhas devem conter pelo menos um caractere de cada uma das seguintes categorias: letras minúsculas (a-z), letras maiúsculas (A-Z), números (0-9) e o conjunto ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/.

2. Consulte WorkSpaces Clients no Guia do usuário do Amazon WorkSpaces para obter mais informações sobre os requisitos de cada cliente e, em seguida, execute uma das seguintes opções:

   - Quando receber o prompt, faça download de uma das aplicações cliente ou inicie o Acesso via Web.
   - Se você não receber o prompt e ainda não tiver instalado uma aplicação cliente, abra https://clients.amazonworkspaces.com/ e faça download de uma das aplicações cliente ou inicialize o Acesso via Web.

   > **Note**
   >
   > Não é possível usar um navegador da web (Acesso via Web) para se conectar aos WorkSpaces do Amazon Linux.

3. Inicie o cliente, digite o código de registro do e-mail de convite e selecione Registrar.
4. Quando for necessário fazer login, insira as credenciais de login e clique em Fazer login.
5. (Opcional) Quando solicitado a salvar suas credenciais, escolha Sim.

Para obter mais informações sobre o uso das aplicações cliente, como configurar vários monitores ou usar dispositivos periféricos, consulte WorkSpaces Clients e Peripheral Device Support no Guia do usuário do Amazon WorkSpaces.

Etapa 3: Limpar (opcional)

Se você tiver terminado de trabalhar com o WorkSpace que criou neste tutorial, poderá excluí-lo. Para obter mais informações, consulte the section called “Excluir um WorkSpace”.

> **Note**
>
> O Simple AD é disponibilizado gratuitamente para uso com os WorkSpaces. Se não houver WorkSpaces sendo usados com o diretório do Simple AD por 30 dias consecutivos, o registro desse diretório será automaticamente cancelado para uso com o Amazon WorkSpaces, e você será cobrado por esse diretório de acordo com os Preços do AWS Directory Service. Para excluir diretórios vazios, consulte Excluir o diretório dos WorkSpaces. Se você excluir o diretório do Simple AD, sempre poderá criar um novo quando quiser começar a usar o WorkSpaces novamente.

Próximas etapas

Você pode continuar a personalizar o WorkSpace que acabou de criar. Por exemplo, é possível instalar o software e, em seguida, criar um pacote personalizado do seu WorkSpace. Você também pode realizar várias tarefas administrativas nos WorkSpaces e em seu diretório de WorkSpaces. Para obter mais informações, consulte a documentação a seguir.

- Crie uma WorkSpaces imagem e um pacote personalizados
- Administre seu WorkSpaces
- Gerenciar diretórios para WorkSpaces

Para criar WorkSpaces adicionais, siga um destes procedimentos:

- Se você quiser continuar usando a VPC e o diretório do Simple AD criados pela configuração rápida, adicione WorkSpaces para outros usuários seguindo as etapas na seção Etapa 2: criar um WorkSpace do tutorial de inicialização de um WorkSpace usando o Simple AD.

- Se você precisar usar outro tipo de diretório ou um Active Directory existente, consulte o tutorial apropriado em Inicializar uma área de trabalho virtual usando WorkSpaces.

Para obter mais informações sobre o uso das aplicações cliente do WorkSpaces, como configurar vários monitores ou usar dispositivos periféricos, consulte WorkSpaces Clients e Peripheral Device Support no Guia do usuário do Amazon WorkSpaces.

Conceitos básicos de configuração avançada do WorkSpaces

Neste tutorial, você aprenderá a provisionar uma área de trabalho virtual e baseada na nuvem do Microsoft Windows ou do Amazon Linux, que é conhecida como WorkSpace, usando o WorkSpaces e o AWS Directory Service.

Este tutorial usa a opção de configuração avançada para iniciar o WorkSpace.

> **Note**
>
> A configuração avançada é compatível com WorkSpaces em todas as regiões.

Tarefas

- Antes de começar
- Usar a configuração avançada para iniciar seu WorkSpace

Antes de começar

Antes de começar, verifique se você tem uma conta da AWS que possa ser usada para criar ou administrar um WorkSpace. Os usuários não precisam de uma conta da AWS para se conectar e usar os WorkSpaces.

Analise e compreenda os seguintes conceitos antes de continuar:

- Ao ativar um WorkSpace, você deve selecionar um pacote do WorkSpace. Para obter mais informações, consulte Pacotes do Amazon WorkSpaces.
- Ao iniciar um WorkSpace, você deve selecionar qual protocolo (PCoIP ou WorkSpaces Streaming Protocol [WSP]) deseja usar com seu pacote. Para obter mais informações, consulte Protocolos para a Amazon WorkSpaces.
- Ao executar um WorkSpace, você deve especificar as informações de perfil do usuário, incluindo um nome de usuário e o endereço de e-mail. Os usuários concluem o perfil ao especificar uma senha. As informações sobre o WorkSpaces e os usuários são armazenadas em um diretório. Para obter mais informações, consulte Diretórios.

Usar a configuração avançada para iniciar seu WorkSpace

Para usar a configuração avançada para iniciar seu WorkSpace:

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. Escolha uma dos seguintes tipos de diretório e selecione Próximo:
   - AWS Managed Microsoft AD
   - Simple AD
   - AD Connector
3. Insira as informações do diretório.
4. Escolha duas sub-redes em uma VPC em duas zonas de disponibilidade diferentes. Para obter mais informações, consulte Configure a VPC with public subnets.
5. Revise as informações do seu diretório e escolha Criar diretório.

Redes e acesso para o WorkSpaces

Como administrador do WorkSpace, você deve compreender o seguinte sobre os recursos de redes e o acesso ao WorkSpaces.

Índice

Protocolos para a Amazon WorkSpaces

A Amazon WorkSpaces oferece suporte a dois protocolos: PCoIP e WorkSpaces Streaming Protocol (WSP). O protocolo escolhido depende de vários fatores, como o tipo de dispositivo a WorkSpaces partir do qual seus usuários acessarão, qual sistema operacional está em seu sistema WorkSpaces, quais condições de rede seus usuários enfrentarão e se seus usuários precisarão de suporte de vídeo bidirecional.

Requisitos

O WSP só WorkSpaces é suportado com os seguintes requisitos mínimos.

Requisitos do agente do host:

- Agente do host do Windows versão 2.0.0.312 ou superior
- Agente do host do Ubuntu versão 2.1.0.501 ou superior
- Agente do host do Amazon Linux 2 versão 2.0.0.596 ou superior

Requisitos do cliente:

- Cliente nativo do Windows versão 5.1.0.329 ou superior
- Cliente nativo do macOS versão 5.5.0 ou superior
- Web Access

Para obter mais informações sobre como verificar a versão WorkSpace do cliente e a versão do host agent, consulte as perguntas frequentes.

Quando usar o WSP

- Se você precisar de maior tolerância de perda/latência para oferecer suporte às condições de rede do usuário final. Por exemplo, você tem usuários que estão acessando suas redes em WorkSpaces distâncias globais ou usando redes não confiáveis.
- Se você precisar que os usuários se autentiquem com cartões inteligentes ou usem cartões inteligentes durante a sessão.
- Se você precisar de recursos de compatibilidade de webcam durante a sessão.
- Se você precisar usar o Web Access com o WorkSpaces pacote Windows Server 2019.
- Se você precisar usar o Ubuntu WorkSpaces.
- Se você precisar usar o Windows 11 BYOL WorkSpaces.
- Se você precisar usar pacotes baseados em GPU do Ubuntu (Graphics.g4dn e .g4dn). GraphicsPro
- Se você precisar que seus usuários se autentiquem em sessão com WebAuthn autenticadores como YubiKey o Windows Hello.

Quando usar o PCoIP

- Se você quiser usar o iPad ou os clientes Linux do Android.
- Se você usa dispositivos cliente zero do Teradici.
- Se você precisar usar pacotes baseados em GPU (Graphics.g4dn, .g4dn, Graphics ou). GraphicsPro GraphicsPro
- Se você precisar usar um pacote Linux para casos de uso que não necessitem de cartões inteligentes.
- Se você precisar usar WorkSpaces na região da China (Ningxia).

> **Note**
>
> - Um diretório pode ter uma mistura de PCoIP e WSP nele WorkSpaces .
> - Um usuário pode ter um PCoIP e um WSP, WorkSpace desde que os dois WorkSpaces estejam localizados em diretórios separados. O mesmo usuário não pode ter um PCoIP e um WSP WorkSpace no mesmo diretório. Para obter mais informações sobre a criação de vários WorkSpaces para um usuário, consulteCriar vários WorkSpaces para um usuário.
> - Você pode migrar um WorkSpace entre os dois protocolos usando o recurso de WorkSpaces migração, que requer uma reconstrução do. WorkSpace Para ter mais informações, consulte Migre um WorkSpace.
> - Se o seu WorkSpace foi criado com pacotes PCoIP, você pode modificar o protocolo de streaming para migrar entre os dois protocolos sem exigir uma reconstrução, mantendo o volume raiz. Para obter mais informações, consulte Modificar protocolos.
> - Para obter a melhor experiência com videoconferência, recomendamos usar somente Power ou PowerPro pacotes.

Configurar uma VPC para WorkSpaces

WorkSpaces lança o seu WorkSpaces em uma nuvem privada virtual (VPC).

Você pode criar uma VPC com duas sub-redes privadas para você WorkSpaces e um gateway NAT em uma sub-rede pública. Como alternativa, você pode criar uma VPC com duas sub-redes públicas para você WorkSpaces e associar um endereço IP público ou endereço IP elástico a cada uma. WorkSpace

Para obter mais informações sobre as considerações de design de VPC, consulte Melhores práticas para VPCs e redes em WorkSpaces implantações da Amazon e Melhores práticas para implantação - Design de VPC. WorkSpaces

Conteúdo

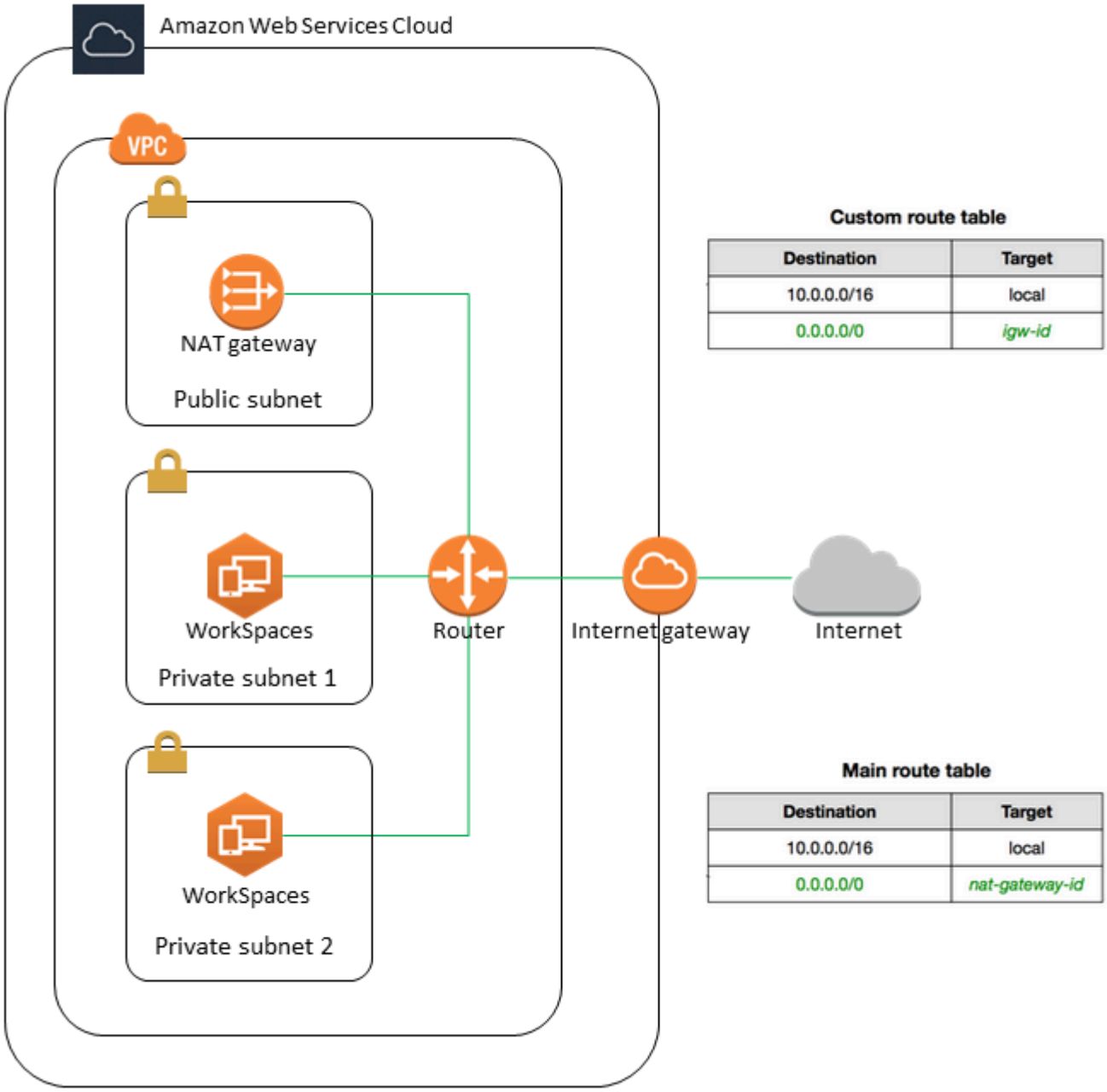
Requisitos

As sub-redes da sua VPC devem residir em diferentes zonas de disponibilidade na região em que você está lançando. WorkSpaces As zonas de disponibilidade são locais distintos projetados para serem isolados de falhas em outras zonas de disponibilidade. Ao iniciar as instâncias em zonas de disponibilidade separadas, você pode proteger seus aplicativos de falhas de um único local. Cada sub-rede deve residir inteiramente dentro de uma zona de disponibilidade e não pode abranger zonas.

> **Note**
>
> A Amazon WorkSpaces está disponível em um subconjunto das zonas de disponibilidade em cada região suportada. Para determinar quais zonas de disponibilidade você pode usar para as sub-redes da VPC que você está usando, consulte. WorkSpaces Zonas de disponibilidade para a Amazon WorkSpaces

Configurar uma VPC com sub-redes privadas e um gateway NAT

Se você usa AWS Directory Service para criar um Microsoft AWS gerenciado ou um Simple AD, recomendamos que você configure a VPC com uma sub-rede pública e duas sub-redes privadas. Configure seu diretório para iniciá-lo WorkSpaces nas sub-redes privadas. Para fornecer acesso à Internet WorkSpaces em uma sub-rede privada, configure um gateway NAT na sub-rede pública.



Como criar uma VPC com uma sub-rede pública e duas sub-redes privadas

1. Abra o console do Amazon VPC em https://console.aws.amazon.com/vpc/.
2. Escolha Criar VPC.
3. Em Recursos a serem criados, escolha VPC e mais.
4. Em Name tag auto-generation (Geração automática de tags de nome), insira um nome para a VPC.

5. Para configurar as sub-redes, faça o seguinte:

    a. Em Number of Availability Zones (Número de zonas de disponibilidade), escolha 1 ou 2 dependendo das suas necessidades.

    b. Expanda Personalizar AZs e escolha as zonas de disponibilidade. Caso contrário, AWS seleciona-os para você. Para fazer uma seleção adequada, consulte Zonas de disponibilidade para a Amazon WorkSpaces.

    c. Em Number of public subnets (Número de sub-redes públicas), verifique se você tem uma sub-rede pública por zona de disponibilidade.

    d. Em Número de sub-redes privadas, verifique se você tem pelo menos uma sub-rede privada por zona de disponibilidade.

    e. Insira um bloco CIDR para cada sub-rede. Para obter mais informações, consulte Dimensionamento de sub-rede no Guia do usuário da Amazon VPC.

6. Em Gateways NAT, escolha 1 por AZ.

7. Escolha Criar VPC.

Blocos CIDR IPv6

É possível associar blocos CIDR IPv6 à VPC e às sub-redes. No entanto, se você configurar suas sub-redes para atribuir automaticamente endereços IPv6 a instâncias executadas na sub-rede, não será possível usar pacotes Graphics. (No entanto, você pode usar Graphics.g4dn, GraphicsPro .g4dn e pacotes.) GraphicsPro Essa restrição surge de uma limitação de hardware de tipos de instância da geração anterior que não oferecem suporte ao IPv6.

Para contornar esse problema, você pode desativar temporariamente a configuração de atribuição automática de endereços IPv6 nas WorkSpaces sub-redes antes de iniciar os pacotes gráficos e, em seguida, reativar essa configuração (se necessário) após iniciar os pacotes gráficos para que outros pacotes recebam os endereços IP desejados.

Por padrão, a configuração de auto-assign IPv6 addresses (atribuição automática de endereços IPv6) está desabilitada. Para verificar essa configuração no console do Amazon VPC, no painel de navegação, escolha Sub-redes. Selecione a sub-rede e escolha Actions (Ações), Modify auto-assign IP settings (Modificar configurações de IP de atribuição automática).

Configurar uma VPC com sub-redes públicas

Se preferir, você poderá criar uma VPC com duas sub-redes públicas. Para fornecer acesso à Internet WorkSpaces em sub-redes públicas, configure o diretório para atribuir endereços IP elásticos automaticamente ou atribuir manualmente um endereço IP elástico a cada um. WorkSpace

Tarefas

- Etapa 1: Criar uma VPC
- Etapa 2: atribuir endereços IP públicos ao seu WorkSpaces

Etapa 1: Criar uma VPC

Crie uma VPC com uma sub-rede pública da maneira indicada a seguir.

Como criar a VPC

1. Abra o console do Amazon VPC em https://console.aws.amazon.com/vpc/.
2. Escolha Criar VPC.
3. Em Recursos a serem criados, escolha VPC e mais.
4. Em Name tag auto-generation (Geração automática de tags de nome), insira um nome para a VPC.
5. Para configurar as sub-redes, faça o seguinte:
    a. Em Número de zonas de disponibilidade, escolha 2.
    b. Expanda Personalizar AZs e escolha as zonas de disponibilidade. Caso contrário, AWS seleciona-os para você. Para fazer uma seleção adequada, consulte Zonas de disponibilidade para a Amazon WorkSpaces.
    c. Em Number of public subnets (Número de sub-redes públicas), escolha 2.
    d. Para Number of private subnets (Número de sub-redes privadas), escolha 0.
    e. Insira um bloco CIDR para cada sub-rede pública. Para obter mais informações, consulte Dimensionamento de sub-rede no Guia do usuário da Amazon VPC.
6. Escolha Criar VPC.

Blocos CIDR IPv6

É possível associar um bloco CIDR IPv6 à VPC e às sub-redes. No entanto, se você configurar suas sub-redes para atribuir automaticamente endereços IPv6 a instâncias executadas na sub-rede, não será possível usar pacotes Graphics. (No entanto, você pode usar GraphicsPro pacotes.) Essa restrição surge de uma limitação de hardware de tipos de instância da geração anterior que não oferecem suporte ao IPv6.

Para contornar esse problema, você pode desativar temporariamente a configuração de atribuição automática de endereços IPv6 nas WorkSpaces sub-redes antes de iniciar os pacotes gráficos e, em seguida, reativar essa configuração (se necessário) após iniciar os pacotes gráficos para que outros pacotes recebam os endereços IP desejados.

Por padrão, a configuração de auto-assign IPv6 addresses (atribuição automática de endereços IPv6) está desabilitada. Para verificar essa configuração no console do Amazon VPC, no painel de navegação, escolha Sub-redes. Selecione a sub-rede e escolha Actions (Ações), Modify auto-assign IP settings (Modificar configurações de IP de atribuição automática).

Etapa 2: atribuir endereços IP públicos ao seu WorkSpaces

Você pode atribuir endereços IP públicos aos seus de WorkSpaces forma automática ou manual. Para usar a atribuição automática, consulte the section called “Configurar endereços IP públicos automáticos”. Para atribuir endereços IP públicos manualmente, use o procedimento a seguir.

Para atribuir WorkSpace manualmente um endereço IP público a um

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, escolha WorkSpaces.
3. Expanda a linha (escolha o ícone de seta) para o WorkSpace e anote o valor de WorkSpace IP. Esse é o endereço IP privado primário do WorkSpace.
4. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
5. No painel de navegação, escolha Elastic IPs. Se você não tiver um endereço IP elástico disponível, selecione Alocar endereço IP elástico, escolha Grupo da Amazon de endereços IPv4 ou Grupo de endereços IPv4 de propriedade do cliente e selecione Alocar. Anote o novo endereço IP.
6. No painel de navegação, selecione Network Interfaces.
7. Selecione a interface de rede para o seu WorkSpace. Para encontrar a interface de rede para você WorkSpace, insira o valor do WorkSpace IP (que você anotou anteriormente) na caixa de pesquisa e pressione Enter. O valor WorkSpace IP corresponde ao endereço IPv4 privado

primário da interface de rede. Observe que o ID da VPC da interface de rede corresponde ao ID da sua WorkSpaces VPC.

8. Escolha Ações, Gerenciar endereços IP. Escolha Assign new IP (Atribuir novo IP) e Yes, Update (Sim, atualizar). Anote o novo endereço IP.
9. Escolha Actions (Ações), Associate Address (Associar endereço).
10. Na página Associate Elastic IP Address (Associar endereço IP elástico), escolha um endereço IP elástico em Address (Endereço). Em Associate to private IP address (Associar ao endereço IP privado), especifique um novo endereço IP privado e selecione Associate Address (Associar endereço).

Zonas de disponibilidade para a Amazon WorkSpaces

Ao criar uma nuvem privada virtual (VPC) para uso com a Amazon WorkSpaces, as sub-redes da sua VPC devem residir em diferentes zonas de disponibilidade na região em que você está lançando. WorkSpaces As zonas de disponibilidade são locais distintos projetados para serem isolados de falhas em outras zonas de disponibilidade. Ao iniciar as instâncias em zonas de disponibilidade separadas, você pode proteger seus aplicativos de falhas de um único local. Cada sub-rede deve residir inteiramente dentro de uma zona de disponibilidade e não pode abranger zonas.

Uma zona de disponibilidade é representada por um código de região seguido por um identificador de letra, por exemplo, `us-east-1a`. Para garantir que os recursos sejam distribuídos pelas zonas de disponibilidade de uma região, mapeamos as zonas de disponibilidade de forma independente para os nomes de cada AWS conta. Por exemplo, a zona de disponibilidade da `us-east-1a` sua AWS conta pode não estar no mesmo local `us-east-1a` de outra AWS conta.

Para coordenar as zonas de disponibilidade entre contas, use o ID da AZ que é um identificador exclusivo e consistente para uma zona de disponibilidade. Por exemplo, `use1-az2` é uma ID AZ para a `us-east-1` região e tem a mesma localização em todas as AWS contas.

A visualização de IDs de AZs permite determinar o local de recursos em uma conta em relação aos recursos em outra conta. Por exemplo, se você compartilhar uma sub-rede na zona de disponibilidade com o ID de AZ `use1-az2` com outra conta, essa sub-rede estará disponível para essa conta na zona de disponibilidade cujo ID de AZ também é `use1-az2`. O ID da AZ de cada VPC e sub-rede é exibido no console da Amazon VPC.

A Amazon só WorkSpaces está disponível em um subconjunto das zonas de disponibilidade para cada região suportada. A tabela a seguir lista os IDs de AZ que você pode usar para cada região.

Para ver o mapeamento de IDs de AZ para zonas de disponibilidade em sua conta, consulte IDs de AZ para seus recursos no Guia do usuário do AWS RAM .

Nome da região	Código da região	IDs de AZ compatíveis
Leste dos EUA (Norte da Virgínia)	us-east-1	use1-az2, use1-az4, use1-az6
Oeste dos EUA (Oregon)	us-west-2	usw2-az1, usw2-az2, usw2-az3
Asia Pacific (Mumbai)	ap-south-1	aps1-az1, aps1-az2, aps1-az3
Ásia-Pacífico (Seul)	ap-northeast-2	apne2-az1 , apne2-az3
Ásia-Pacífico (Singapura)	ap-southeast-1	apse1-az1 , apse1-az2
Ásia-Pacífico (Sydney)	ap-southeast-2	apse2-az1 , apse2-az3
Ásia-Pacífico (Tóquio)	ap-northeast-1	apne1-az1 , apne1-az4
Canadá (Central)	ca-central-1	cac1-az1, cac1-az2
Europa (Frankfurt)	eu-central-1	euc1-az2, euc1-az3
Europa (Irlanda)	eu-west-1	euw1-az1, euw1-az2, euw1-az3
Europa (Londres)	eu-west-2	euw2-az2, euw2-az3
América do Sul (São Paulo)	sa-east-1	sae1-az1, sae1-az3
África (Cidade do Cabo)	af-south-1	afs1-az1, afs1-az2, afs1-az3
Israel (Tel Aviv)	il-central-1	ilc1-az1, ilc1-az2, ilc1-az3

Nome da região	Código da região	IDs de AZ compatíveis
AWS GovCloud (Oeste dos EUA)	`us-gov-west-1`	`usgw1-az1` , `usgw1-az2` , `usgw1-az3`
AWS GovCloud (Leste dos EUA)	`us-gov-east-1`	`usge1-az1` , `usge1-az2` , `usge1-az3`

Para obter mais informações sobre Zonas de disponibilidade e IDs de AZ, consulte Regiões, Zonas de disponibilidade e Zonas Locais no Guia do usuário do Amazon EC2.

Requisitos de endereço IP e porta para WorkSpaces

Para se conectar à sua WorkSpaces, a rede à qual seus WorkSpaces clientes estão conectados deve ter determinadas portas abertas para os intervalos de endereços IP dos vários AWS serviços (agrupados em subconjuntos). Esses intervalos de endereços variam de acordo com a região AWS. Essas mesmas portas também devem estar abertas em qualquer firewall em execução no cliente. Para obter mais informações sobre os intervalos de endereços IP em diferentes regiões AWS, consulte os AWS Intervalos de Endereços IP em Referência geral da Amazon Web Services.

Para obter um diagrama de arquitetura, consulte WorkSpaces Arquitetura. Para diagramas de arquitetura adicionais, consulte Melhores práticas para implantar a Amazon. WorkSpaces

Portas para aplicações cliente

O aplicativo WorkSpaces cliente requer acesso de saída nas seguintes portas:

Porta 53 (UDP)

> Essa porta é usada para acessar servidores DNS. Ela deve estar aberta para seus endereços IP do servidor DNS para que o cliente possa resolver nomes de domínio público. Esse requisito de porta é opcional se você não estiver usando servidores DNS para resolução de nomes de domínio.

Porta 443 (TCP)

> Essa porta é usada para atualizações, registros e autenticações da aplicação cliente. As aplicações clientes de desktop dão suporte ao uso de um servidor de proxy para o tráfego da

porta 443 (HTTPS). Para habilitar o uso de um servidor proxy, abra o aplicativo cliente, escolha Configurações avançadas, selecione Usar servidor de proxy, especifique o endereço e a porta do servidor proxy e escolha Salvar.

Essa porta deve estar aberta para os seguintes intervalos de endereços IP:

- O subconjunto `AMAZON` na região `GLOBAL`.
- O `AMAZON` subconjunto na região em que o WorkSpace está.
- O subconjunto `AMAZON` na região `us-east-1`.
- O subconjunto `AMAZON` na região `us-west-2`.
- O subconjunto `S3` na região `us-west-2`.

Porta 4172 (UDP e TCP)

Essa porta é usada para transmitir o WorkSpace desktop e verificar a integridade do PCoIP WorkSpaces. Essa porta deve estar aberta para o gateway PCoIP e para os servidores de verificação de integridade na região em que o WorkSpace está. Para obter mais informações, consulte Servidores de gateway PCoIP e Servidores de verificação de integridade.

Para PCoIP WorkSpaces, os aplicativos cliente de desktop não suportam o uso de um servidor proxy nem a decodificação e inspeção de TLS para tráfego da porta 4172 em UDP (para tráfego de desktop). Elas exigem uma conexão direta com as portas 4172.

Porta 4195 (UDP e TCP)

Essa porta é usada para streaming da WorkSpace área de trabalho e verificações de integridade do Protocolo de WorkSpaces Streaming (WSP) WorkSpaces. Essa porta deve estar aberta para os intervalos de endereços IP do WSP Gateway e para os servidores de verificação de integridade na região em que o WorkSpace está. Para obter mais informações, consulte Servidores de gateway do WSP e Servidores de verificação de integridade.

Para o WSP WorkSpaces, o aplicativo cliente WorkSpaces Windows (versão 5.1 e superior) e o aplicativo cliente macOS (versão 5.4 e superior) oferecem suporte ao uso de servidores proxy HTTP para tráfego TCP da porta 4195, mas o uso de um proxy não é recomendado. A descriptografia e a inspeção de TLS não são compatíveis. Para obter mais informações, consulte Definir as configurações do servidor proxy do dispositivo para acesso à Internet para Windows WorkSpaces WorkSpaces, Amazon Linux e Ubuntu WorkSpaces.

> **Note**
>
> - Se o firewall usar filtragem com estado, as portas efêmeras (também conhecidas como portas dinâmicas) serão abertas automaticamente para permitir a comunicação de retorno. Se o firewall usar filtragem sem estado, será necessário abrir as portas efêmeras explicitamente para permitir a comunicação de retorno. O intervalo de portas efêmeras necessário que você deve abrir variará dependendo da configuração.
> - A função de servidor proxy não é compatível com tráfego UDP. Se você optar por usar um servidor proxy, as chamadas de API que o aplicativo cliente faz para os WorkSpaces serviços da Amazon também serão enviadas por proxy. Tanto as chamadas de API quanto o tráfego de área de trabalho devem passar pelo mesmo servidor proxy.

Portas para o Web Access

WorkSpaces O Web Access requer acesso de saída para as seguintes portas:

Porta 53 (UDP)

Essa porta é usada para acessar servidores DNS. Ela deve estar aberta para seus endereços IP do servidor DNS para que o cliente possa resolver nomes de domínio público. Esse requisito de porta é opcional se você não estiver usando servidores DNS para resolução de nomes de domínio.

Porta 80 (UDP e TCP)

Esta porta é usada para conexões iniciais ao `https://clients.amazonworkspaces.com`, que migra posteriormente para HTTPS. Ele deve estar aberto a todos os intervalos de endereços IP no `EC2` subconjunto da região em que o WorkSpace está.

Porta 443 (UDP e TCP)

Essa porta é usada para registros e autenticações usando HTTPS. Ele deve estar aberto a todos os intervalos de endereços IP no `EC2` subconjunto da região em que o WorkSpace está.

Porta 4195 (UDP e TCP)

Para WorkSpaces que estejam configurados para o WorkSpaces Streaming Protocol (WSP), essa porta é usada para transmitir o tráfego do WorkSpaces desktop. Essa porta deve estar aberta para os intervalos de endereços IP do gateway do WSP. Para ter mais informações, consulte Servidores de gateway do WSP.

O Acesso via Web com WSP é compatível com o uso de um servidor proxy para o tráfego TCP na porta 4195, mas não é recomendado. Para obter mais informações, consulte Definir as configurações do servidor proxy do dispositivo para acesso à Internet para Windows WorkSpaces WorkSpaces, Amazon Linux e Ubuntu WorkSpaces.

> **Note**
>
> Se o firewall usar filtragem com estado, as portas efêmeras (também conhecidas como portas dinâmicas) serão abertas automaticamente para permitir a comunicação de retorno. Se o firewall usar filtragem sem estado, será necessário abrir as portas efêmeras explicitamente para permitir a comunicação de retorno. O intervalo de portas efêmeras necessário que você deve abrir varia dependendo da sua configuração.

Normalmente, o navegador seleciona aleatoriamente uma porta de origem na faixa alta para usar no tráfego de streaming. WorkSpaces O Web Access não tem controle sobre a porta que o navegador seleciona. Você deve garantir que o tráfego de retorno para essa porta seja permitido.

Domínios e endereços IP para adicionar à sua lista de permissões

Para que o aplicativo WorkSpaces cliente possa acessar o WorkSpaces serviço, você deve adicionar os seguintes domínios e endereços IP à lista de permissões na rede da qual o cliente está tentando acessar o serviço.

Domínios e endereços IP para adicionar à sua lista de permissões

Categoria	Domínio ou endereço IP
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Atualização automática do cliente	• https://d2td7dqidlhjx7.cloudfront.net/ • Na região AWS GovCloud (Oeste dos EUA): https://d2td7dqidlhjx7.cloudfront.net/prod/pdt/windows/ WorkSpacesAppCastx 64.xml
Verificação de conectividade	https://connectivity.amazonworkspaces.com/

Categoria	Domínio ou endereço IP
Métricas do cliente (para mais de 3.0 aplicativos de WorkSpaces clientes)	Domínios: • skylight-client-dshttps://.us-east-1.amazonaws.com • skylight-client-dshttps://.us-west-2.amazonaws.com • skylight-client-dshttps://.ap-south-1.amazonaws.com • skylight-client-dshttps://.ap-northeast-2.amazonaws.com • skylight-client-dshttps://.ap-southeast-1.amazonaws.com • skylight-client-dshttps://.ap-southeast-2.amazonaws.com • skylight-client-dshttps://.ap-northeast-1.amazonaws.com • skylight-client-dshttps://.ca-central-1.amazonaws.com • skylight-client-dshttps://.eu-central-1.amazonaws.com • skylight-client-dshttps://.eu-west-1.amazonaws.com • skylight-client-dshttps://.eu-west-2.amazonaws.com • skylight-client-dshttps://.sa-east-1.amazonaws.com • skylight-client-dshttps://.af-south-1.amazonaws.com • skylight-client-dshttps://.il-central-1.amazonaws.com • Na região AWS GovCloud (Oeste dos EUA):

Categoria	Domínio ou endereço IP
	https://skylight-client-ds. us-gov-west-1.amazonaws.com • Na região AWS GovCloud (Leste dos EUA): https://skylight-client-ds. us-gov-east-1.amazonaws.com

Categoria	Domínio ou endereço IP
Serviço de mensagens dinâmicas (para mais de 3.0 aplicativos WorkSpaces clientes)	Domínios: • ws-client-servicehttps://.us-east-1.amazonaws.com • ws-client-servicehttps://.us-west-2.amazonaws.com • ws-client-servicehttps://.ap-south-1.amazonaws.com • ws-client-servicehttps://.ap-northeast-2.amazonaws.com • ws-client-servicehttps://.ap-southeast-1.amazonaws.com • ws-client-servicehttps://.ap-southeast-2.amazonaws.com • ws-client-servicehttps://.ap-northeast-1.amazonaws.com • ws-client-servicehttps://.ca-central-1.amazonaws.com • ws-client-servicehttps://.eu-central-1.amazonaws.com • ws-client-servicehttps://.eu-west-1.amazonaws.com • ws-client-servicehttps://.eu-west-2.amazonaws.com • ws-client-servicehttps://.sa-east-1.amazonaws.com • ws-client-servicehttps://.af-south-1.amazonaws.com • ws-client-servicehttps://.il-central-1.amazonaws.com • Na região AWS GovCloud (Oeste dos EUA):

Categoria	Domínio ou endereço IP
	https://ws-client-service. us-gov-west-1.amazonaws.com • Na região AWS GovCloud (Leste dos EUA): https://ws-client-service. us-gov-east-1.amazonaws.com

Categoria	Domínio ou endereço IP
Configurações de diretório	Autenticação do cliente no diretório de clientes antes de fazer login no WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/*<região>*/*<ID do diretório>* Conexões de clientes macOS: • https://d32i4gd7pg4909.cloudfront.net/ Configurações de diretório do cliente: • https://d21ui22avrxoh6.cloudfront.net/prod/<região>/<ID do diretório> Gráficos da página de login para marcas conjuntas no nível de diretório do cliente: • Herdado: https://d1cbg795sa4g1u.cloudfront.net/prod/<região>/<ID do diretório> • Leste dos EUA (N. da Virgínia): https://d2h1yryv1jxiq.cloudfront.net/ • Oeste dos EUA (Oregon): https://d1fq42e1gi7rtq.cloudfront.net/ • Ásia-Pacífico (Mumbai): https://d1ctsk4u02kky7.cloudfront.net/ • Ásia-Pacífico (Seul): https://dyoj3cw6iktvg.cloudfront.net • Ásia-Pacífico (Singapura): https://d1525ef92caquk.cloudfront.net/ • Ásia-Pacífico (Sydney): https://dodwxjr2amr8p.cloudfront.net/

Categoria	Domínio ou endereço IP
	• Ásia-Pacífico (Tóquio): https://d3v7kcib8ir2e1.cloudfront.net/ • Canadá (Central): https://d1ebdk07rro1qy.cloudfront.net/ • Europa (Frankfurt): https://d39q4y7cndearu.cloudfront.net/ • Europa (Irlanda): https://d2127w6wvrc6l3.cloudfront.net/ • Europa (Londres): https://df4ahgpxbxqy2.cloudfront.net/ • América do Sul (São Paulo): https://d2nezqurrjvain.cloudfront.net/ • África (Cidade do Cabo): https://dr6ry0pwaoy23.cloudfront.net • Israel (Tel Aviv) — https://d2kmf63k5sit88.cloudfront.net Arquivo CSS para estilizar as páginas de login: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript arquivo para as páginas de login: • Leste dos EUA (N. da Virgínia): https://d32i4gd7pg4909.cloudfront.net/ • Oeste dos EUA (Oregon): https://d18af777lco7lp.cloudfront.net/ • Ásia-Pacífico (Mumbai): https://d78hovzzqqtsb.cloudfront.net/ • Ásia-Pacífico (Seul): https://dtyv4uwoh7ynt.cloudfront.net/

Categoria	Domínio ou endereço IP
	• Ásia-Pacífico (Singapura): https://d3qzmd7y07pz0i.cloudfront.net/ • Ásia-Pacífico (Sydney): https://dwcpoxuuza83q.cloudfront.net/ • Ásia-Pacífico (Tóquio): https://d2c2t8mxjhq5z1.cloudfront.net/ • Canadá (Central): https://d2wfbsypmqjmog.cloudfront.net/ • Europa (Frankfurt): https://d1whcm49570jjw.cloudfront.net/ • Europa (Irlanda): https://d3pgffbf39h4k4.cloudfront.net/ • Europa (Londres): https://d16q6638mh01s7.cloudfront.net/ • América do Sul (São Paulo): https://d2lh2qc5bdoq4b.cloudfront.net/ • África (Cidade do Cabo): https://di5ygl2cs0mrh.cloudfront.net/ • Israel (Tel Aviv) — https://d1a3pnge9on3sx.cloudfront.net Na região AWS GovCloud (Oeste dos EUA): • Configurações de diretório do cliente: https://s3.amazonaws.com/ workspaces-client-properties /prod/pdt/ <directory ID> • Gráficos da página de login para marcas conjuntas no nível de diretório do cliente: workspace-client-assets-pdthttps://.s3--1.amazonaws.com us-gov-west

Categoria	Domínio ou endereço IP
	• Arquivo CSS para estilizar as páginas de login: https://s3.amazonaws.com/ workspaces-clients-css /workspaces_v2.css • JavaScript arquivo para as páginas de login: Não aplicável Na região AWS GovCloud (Leste dos EUA): • Configurações de diretório do cliente: https://s3.amazonaws.com/ workspaces-client-properties /prod/osu/ <directory ID> • Gráficos da página de login para marcas conjuntas no nível de diretório do cliente: workspace-client-assets-pdthttps://.s3--1.amazonaws.com us-gov-east • Arquivo CSS para estilizar as páginas de login: https://s3.amazonaws.com/ workspaces-clients-css /workspaces_v2.css • JavaScript arquivo para as páginas de login: Não aplicável
Serviço de registro Forrester	https://fls-na.amazon.com/
Servidores de Verificação de Integridade (DRP)	Servidores de verificação de integridade

Categoria	Domínio ou endereço IP
Endpoints de autenticação de cartão inteligente pré-sessão	• https://smartcard.us-east-1.signin.aws • https://smartcard.us-west-2.signin.aws • https://smartcard.ap-southeast-2.signin.aws • https://smartcard.ap-northeast-1.signin.aws • https://smartcard.eu-west-1.signin.aws • https://smartcard.signin. amazonaws-us-gov.com
Páginas de login do usuário	https://<ID do diretório>.awsapps.com/ (em que <ID do diretório> é o domínio do cliente) Nas regiões AWS GovCloud (Oeste dos EUA) e AWS GovCloud (Leste dos EUA): https://login. us-gov-home<directory id>.awsapps.com/directory/<directory id>/(onde está o domínio do cliente)

Categoria	Domínio ou endereço IP
WS Broker	Domínios: • ws-broker-servicehttps://.us-east-1.amazonaws.com • ws-broker-service-fipshttps://.us-east-1.amazonaws.com • ws-broker-servicehttps://.us-west-2.amazonaws.com • ws-broker-service-fipshttps://.us-west-2.amazonaws.com • ws-broker-servicehttps://.ap-south-1.amazonaws.com • ws-broker-servicehttps://.ap-northeast-2.amazonaws.com • ws-broker-servicehttps://.ap-southeast-1.amazonaws.com • ws-broker-servicehttps://.ap-southeast-2.amazonaws.com • ws-broker-servicehttps://.ap-northeast-1.amazonaws.com • ws-broker-servicehttps://.ca-central-1.amazonaws.com • ws-broker-servicehttps://.eu-central-1.amazonaws.com • ws-broker-servicehttps://.eu-west-1.amazonaws.com • ws-broker-servicehttps://.eu-west-2.amazonaws.com • ws-broker-servicehttps://.sa-east-1.amazonaws.com • ws-broker-servicehttps://.af-south-1.amazonaws.com

Categoria	Domínio ou endereço IP
	• ws-broker-servicehttps://.il-central-1.amazonaws.com • https://ws-broker-service. us-gov-west-1.amazonaws.com • https://ws-broker-service-fips. us-gov-west-1.amazonaws.com • https://ws-broker-service. us-gov-east-1.amazonaws.com • https://ws-broker-service-fips. us-gov-east-1.amazonaws.com

Categoria	Domínio ou endereço IP
WorkSpaces Endpoints da API	Domínios: • https://workspaces.us-east-1.amazonaws.com • https://workspaces-fips.us-east-1.amazonaws.com • https://workspaces.us-west-2.amazonaws.com • https://workspaces-fips.us-west-2.amazonaws.com • https://workspaces.ap-south-1.amazonaws.com • https://workspaces.ap-northeast-2.amazonaws.com • https://workspaces.ap-southeast-1.amazonaws.com • https://workspaces.ap-southeast-2.amazonaws.com • https://workspaces.ap-northeast-1.amazonaws.com • https://workspaces.ca-central-1.amazonaws.com • https://workspaces.eu-central-1.amazonaws.com • https://workspaces.eu-west-1.amazonaws.com • https://workspaces.eu-west-2.amazonaws.com • https://workspaces.sa-east-1.amazonaws.com • https://workspaces.af-south-1.amazonaws.com

Categoria	Domínio ou endereço IP
	• https://workspaces.il-central-1.amazonaws.com • https://workspaces. us-gov-west-1.amazonaws.com • https://workspaces-fips. us-gov-west-1.amazonaws.com • https://workspaces. us-gov-east-1.amazonaws.com • https://workspaces-fips. us-gov-east-1.amazonaws.com

Categoria	Domínio ou endereço IP
WorkSpaces Endpoints para SAML Single Sign-On (SSO)	Domínios: • euc-sso-smhttps://.us-east-1.amazonaws.com/v1/report-heartbeat • euc-sso-sm-fipshttps://.us-east-1.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.us-west-2.amazonaws.com/v1/report-heartbeat • euc-sso-sm-fipshttps://.us-west-2.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.ap-south-1.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.ap-northeast-2.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.ap-southeast-1.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.ap-southeast-2.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.ap-northeast-1.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.eu-central-1.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.eu-west-2.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.af-south-1.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.il-central-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm. us-gov-west-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm-fips. us-gov-west-1.amazonaws.com/v1/report-heartbeat

Categoria	Domínio ou endereço IP
	• https://euc-sso-sm. us-gov-east-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm-fips. us-gov-east-1.amazonaws.com/v1/report-heartbeat

Domínios e endereços IP para adicionar à sua lista de permissões para PCoIP

Categoria	Domínio ou endereço IP
Gateway de sessão PCoIP (PSG)	Servidores de gateway PCoIP
Agente de sessão (PCM)	Domínios: • https://skylight-cm.us-east-1.amazonaws.com • skylight-cm-fipshttps://.us-east-1.amazonaws.com • https://skylight-cm.us-west-2.amazonaws.com • skylight-cm-fipshttps://.us-west-2.amazonaws.com • https://skylight-cm.ap-south-1.amazonaws.com • https://skylight-cm.ap-northeast-2.amazonaws.com • https://skylight-cm.ap-southeast-1.amazonaws.com • https://skylight-cm.ap-southeast-2.amazonaws.com • https://skylight-cm.ap-northeast-1.amazonaws.com • https://skylight-cm.ca-central-1.amazonaws.com

Categoria	Domínio ou endereço IP
	• https://skylight-cm.eu-central-1.amazonaws.com • https://skylight-cm.eu-west-1.amazonaws.com • https://skylight-cm.eu-west-2.amazonaws.com • https://skylight-cm.sa-east-1.amazonaws.com • https://skylight-cm.af-south-1.amazonaws.com • https://skylight-cm.il-central-1.amazonaws.com • https://skylight-cm. us-gov-west-1.amazonaws.com • https://skylight-cm-fips. us-gov-west-1.amazonaws.com • https://skylight-cm. us-gov-east-1.amazonaws.com • https://skylight-cm-fips. us-gov-east-1.amazonaws.com

Categoria	Domínio ou endereço IP
Servidores TURN do Acesso via Web para PCoIP	Servidores: • turn:*.us-east-1.rdn.amazonaws.com • turn:*.us-west-2.rdn.amazonaws.com • O Acesso via Web ainda não está disponível na região Ásia-Pacífico (Mumbai). • turn:*.ap-northeast-2.rdn.amazonaws.com • turn:*.ap-southeast-1.rdn.amazonaws.com • turn:*.ap-southeast-2.rdn.amazonaws.com • turn:*.ap-northeast-1.rdn.amazonaws.com • turn:*.ca-central-1.rdn.amazonaws.com • turn:*.eu-central-1.rdn.amazonaws.com • turn:*.eu-west-1.rdn.amazonaws.com • turn:*.eu-west-2.rdn.amazonaws.com • turn:*.sa-east-1.rdn.amazonaws.com • No momento, o Web Access não está disponível na região África (Cidade do Cabo) • No momento, o Web Access não está disponível na região de Israel (Tel Aviv).

Domínios e endereços IP para adicionar à sua lista de permissões do WorkSpaces Streaming Protocol (WSP)

Categoria	Domínio ou endereço IP
Gateway de sessão WSP (WSG)	Servidores de gateway do WSP
Servidores TURN do Acesso via Web para WSP	Servidores de gateway do WSP

Servidores de verificação de integridade

Os aplicativos WorkSpaces cliente realizam verificações de integridade nas portas 4172 e 4195. Essas verificações validam se o tráfego TCP ou UDP é transmitido dos WorkSpaces servidores para os aplicativos clientes. Para que essas verificações sejam concluídas com sucesso, as políticas do seu firewall devem permitir o tráfego de saída para os endereços IP dos seguintes servidores de verificação de integridade regionais.

Região	Nome do host de verificação de integridade	Endereços IP
Leste dos EUA (Norte da Virgínia)	drp-iad.amazonworkspaces.com	3.209.215.252 3.212.50.30 3.225.55.35 3.226.24.234 34.200.29.95 52.200.219.150
Oeste dos EUA (Oregon)	drp-pdx.amazonworkspaces.com	34.217.248.177 52.34.160.80 54.68.150.54 54.185.4.125 54.188.171.18 54.244.158.140
Ásia-Pacífico (Mumbai)	drp-bom.amazonworkspaces.com	13.127.57,82 13.234.250.73
Ásia-Pacífico (Seul)	drp-icn.amazonworkspaces.com	13.124.44.166 13.124.203.105

Região	Nome do host de verificação de integridade	Endereços IP
		52.78.44.253 52.79.54.102
Ásia-Pacífico (Singapura)	drp-sin.amazonworkspaces.com	3.0.212.144 18.138.99.116 18.140.252.123 52.74.175.118
Ásia-Pacífico (Sydney)	drp-syd.amazonworkspaces.com	3.24.11.127 13.237.232.125
Ásia-Pacífico (Tóquio)	drp-nrt.amazonworkspaces.com	18.178.102.247 54.64.174.128
Canadá (Central)	drp-yul.amazonworkspaces.com	52.60.69.16 52.60.80.237 52.60.173.117 52.60.201.0
Europa (Frankfurt)	drp-fra.amazonworkspaces.com	52.59.191.224 52.59.191.225 52.59.191.226 52.59.191.227

Região	Nome do host de verificação de integridade	Endereços IP
Europa (Irlanda)	drp-dub.amazonworkspaces.com	18.200.177.86 52.48.86.38 54.76.137.224
Europa (Londres)	drp-lhr.amazonworkspaces.com	35.176.62.54 35.177.255.44 52.56.46.102 52.56.111.36
América do Sul (São Paulo)	drp-gru.amazonworkspaces.com	18.231.0.105 52.67.55.29 54.233.156.245 54.233.216.234
África (Cidade do Cabo)	drp-cpt.amazonworkspaces.com/	13.24.128.155 13.245.205.255 13.245.216.116
Israel (Tel Aviv)	drp-tlv.amazonworkspaces.com/	51.17.52.90 51.17.109.231 51.16.190.43

Região	Nome do host de verificação de integridade	Endereços IP
AWS GovCloud (Oeste dos EUA)	drp-pdt.amazonworkspaces.com	52.61.60.65 52.61.65.14 52.61.88.170 52.61.137.87 52.61.155.110 52.222.20.88
AWS GovCloud (Leste dos EUA)	drp-osu.amazonworkspaces.com	18.253.251.70 18.254.0.118

Servidores de gateway PCoIP

WorkSpaces usa PCoIP para transmitir a sessão do desktop aos clientes pela porta 4172. Para seus servidores de gateway PCoIP, WorkSpaces usa uma pequena variedade de endereços IPv4 públicos do Amazon EC2. Isso permite que você defina políticas de firewall mais granulares para dispositivos que acessam o WorkSpaces. Observe que os WorkSpaces clientes não oferecem suporte a endereços IPv6 como opção de conectividade no momento.

Região	Intervalo de endereços IP públicos
Leste dos EUA (Norte da Virgínia)	3.217.228.0 - 3.217.231.255 3.235.112.0 - 3.235.119.255 52.23.61.0 - 52.23.62.255
Oeste dos EUA (Oregon)	35.80.88.0 - 35.80.95.255 44.234.54.0 - 44.234.55.255 54.244.46.0 - 54.244.47.255

Região	Intervalo de endereços IP públicos
Ásia-Pacífico (Mumbai)	13.126.243.0 - 13.126.243.255
Ásia-Pacífico (Seul)	3.34.37.0 - 3.34.37.255 3.34.38.0 - 3.34.39.255 13.124.247.0 - 13.124.247.255
Ásia-Pacífico (Singapura)	18.141.152.0 - 18.141.152.255 18.141.154.0 - 18.141.155.255 52.76.127.0 - 52.76.127.255
Ásia-Pacífico (Sydney)	3.25.43.0 - 3.25.43.255 3.25.44.0 - 3.25.45.255 54.153.254.0 - 54.153.254.255
Ásia-Pacífico (Tóquio)	18.180.178.0 - 18.180.178.255 18.180.180.0 - 18.180.181.255 54.250.251.0 - 54.250.251.255
Canadá (Central)	15.223.100.0 - 15.223.100.255 15.223.102.0 - 15.223.103.255 35.183.255.0 - 35.183.255.255
Europa (Frankfurt)	18.156.52.0 - 18.156.52.255 18.156.54.0 - 18.156.55.255 52.59.127.0 - 52.59.127.255
Europa (Irlanda)	3.249.28.0 - 3.249.29.255 52.19.124.0 - 52.19.125.255

Região	Intervalo de endereços IP públicos
Europa (Londres)	18.132.21.0 - 18.132.21.255 18.132.22.0 - 18.132.23.255 35.176.32.0 - 35.176.32.255
América do Sul (São Paulo)	18.230.103.0 - 18.230.103.255 18.230.104.0 - 18.230.105.255 54.233.204.0 - 54.233.204.255
África (Cidade do Cabo)	13.246.120.0 - 13.246.123.255
Israel (Tel Aviv)	51.17.28.0-51.17.31.255
AWS GovCloud (Oeste dos EUA)	52.61.193.0 - 52.61.193.255
AWS GovCloud (Leste dos EUA)	18.254.140.0 - 18.254.143.255

Servidores de gateway do WSP

> **Important**
>
> A partir de junho de 2020, WorkSpaces transmite a sessão de desktop do WSP WorkSpaces para clientes pela porta 4195 em vez da porta 4172. Se você quiser usar o WSP WorkSpaces, verifique se a porta 4195 está aberta ao tráfego.

WorkSpaces usa uma pequena variedade de endereços IPv4 públicos do Amazon EC2 para seus servidores de gateway WSP. Isso permite que você defina políticas de firewall mais granulares para dispositivos que acessam o WorkSpaces. Observe que os WorkSpaces clientes não oferecem suporte a endereços IPv6 como opção de conectividade no momento.

Região	Intervalo de endereços IP públicos
Leste dos EUA (Norte da Virgínia)	• 3.227.4.0/22

Região	Intervalo de endereços IP públicos
	• 44.209.84.0/22
Oeste dos EUA (Oregon)	34.223.96.0/22
Ásia-Pacífico (Mumbai)	65.1.156.0/22
Ásia-Pacífico (Seul)	3.35.160.0/22
Ásia-Pacífico (Singapura)	13.212.132.0/22
Ásia-Pacífico (Sydney)	3.25.248.0/22
Ásia-Pacífico (Tóquio)	3.14.164.0/22
Canadá (Central)	3.97.20.0/22
Europa (Frankfurt)	18.192.216.0/22
Europa (Irlanda)	3.248.176.0/22
Europa (Londres)	18.134.68.0/22
América do Sul (São Paulo)	15.228.64.0/22
África (Cidade do Cabo)	13.246.108.0/22
Israel (Tel Aviv)	51.17.72.0/22
AWS GovCloud (Oeste dos EUA)	• 3.32.139.0/24 • 3.30.129.0/24 • 3.30.130.0/23
AWS GovCloud (Leste dos EUA)	18.254.148.0/22

Nomes de domínio do gateway WSP

A tabela a seguir lista os nomes de domínio do WorkSpace gateway WSP. Esses domínios devem ser contatáveis para que o aplicativo WorkSpaces cliente possa acessar o serviço WorkSpace WSP.

Região	Domínio
Leste dos EUA (Norte da Virgínia)	*.prod.us-east-1.highlander.aws.a2z.com
Oeste dos EUA (Oregon)	*.prod.us-west-2.highlander.aws.a2z.com
Ásia-Pacífico (Mumbai)	*.prod.ap-south-1.highlander.aws.a2z.com
Ásia-Pacífico (Seul)	*.prod.ap-northeast-2.highlander.aws.a2z.com
Ásia-Pacífico (Singapura)	*.prod.ap-southeast-1.highlander.aws.a2z.com
Ásia-Pacífico (Sydney)	*.prod.ap-southeast-2.highlander.aws.a2z.com
Ásia-Pacífico (Tóquio)	*.prod.ap-northeast-1.highlander.aws.a2z.com
Canadá (Central)	*.prod.ca-central-1.highlander.aws.a2z.com
Europa (Frankfurt)	*.prod.eu-central-1.highlander.aws.a2z.com
Europa (Irlanda)	*.prod.eu-west-1.highlander.aws.a2z.com
Europa (Londres)	*.prod.eu-west-2.highlander.aws.a2z.com
América do Sul (São Paulo)	*.prod.sa-east-1.highlander.aws.a2z.com
África (Cidade do Cabo)	*.prod.af-south-1.highlander.aws.a2z.com
Israel (Tel Aviv)	*.prod.il-central-1.highlander.aws.a2z.com
AWS GovCloud (Oeste dos EUA)	*.prod. us-gov-west-1.highlander.aws.a2z.com
AWS GovCloud (Leste dos EUA)	*.prod. us-gov-east-1.highlander.aws.a2z.com

Interfaces de rede

Cada WorkSpace uma tem as seguintes interfaces de rede:

- A interface de rede primária (eth1) fornece conectividade aos recursos em sua VPC e na Internet e é usada para unir WorkSpace os ao diretório.

- A interface de rede de gerenciamento (eth0) é conectada a uma rede de gerenciamento segura do WorkSpaces. Ele é usado para streaming interativo do WorkSpace desktop para WorkSpaces clientes e para WorkSpaces permitir o gerenciamento do WorkSpace.

WorkSpaces seleciona o endereço IP para a interface da rede de gerenciamento de vários intervalos de endereços, dependendo da região em que foram WorkSpaces criados. Quando um diretório é registrado, WorkSpaces testa o CIDR da VPC e as tabelas de rotas na sua VPC para determinar se esses intervalos de endereços criam um conflito. Se um conflito é encontrado em todos os intervalos de endereços disponíveis na região, é exibida uma mensagem de erro e o diretório não é registrado. Se você alterar as tabelas de rotas em sua VPC depois do diretório ser registrado, poderá causar um conflito.

Warning

Não modifique nem exclua nenhuma das interfaces de rede conectadas a um WorkSpace. Isso pode fazer com que eles WorkSpace fiquem inacessíveis ou percam o acesso à Internet. Por exemplo, se você habilitou a atribuição automática de endereços IP elásticos no nível do diretório, um endereço IP elástico (do pool fornecido pela Amazon) será atribuído a você WorkSpace quando ele for lançado. No entanto, se você associar um endereço IP elástico de sua propriedade a um WorkSpace e depois desassociar esse endereço IP elástico do WorkSpace, ele WorkSpace perderá seu endereço IP público e não obterá automaticamente um novo do pool fornecido pela Amazon.
Para associar um novo endereço IP público do pool fornecido pela Amazon ao WorkSpace, você deve reconstruir o. WorkSpace Se você não quiser reconstruir o WorkSpace, deverá associar outro endereço IP elástico de sua propriedade ao WorkSpace.

Intervalos de IP de interface de gerenciamento

A tabela a seguir lista os intervalos de endereços IP usados para a interface de rede de gerenciamento.

Note

- Se você estiver usando o Windows Bring Your Own License (BYOL) WorkSpaces, os intervalos de endereços IP na tabela a seguir não se aplicam. Em vez disso, o PCoIP BYOL WorkSpaces usa o intervalo de endereços IP 54.239.224.0/20 para o tráfego

da interface de gerenciamento em todas as regiões. AWS Para Windows WSP BYOL WorkSpaces, os intervalos de endereços IP 54.239.224.0/20 e 10.0.0.0/8 se aplicam a todas as regiões. AWS (Esses intervalos de endereços IP são usados além do bloco CIDR /16 que você seleciona para gerenciar o tráfego do seu WorkSpaces BYOL.)

- Se você estiver usando o WSP WorkSpaces criado a partir de pacotes públicos, o intervalo de endereços IP 10.0.0.0/8 também se aplica ao tráfego da interface de gerenciamento em todas as AWS regiões, além dos intervalos PCoIP/WSP mostrados na tabela a seguir.

Região	Intervalo de endereços IP
Leste dos EUA (Norte da Virgínia)	PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16 WSP: 10.0.0.0/8
Oeste dos EUA (Oregon)	PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16 e 198.19.0.0/16 WSP: 10.0.0.0/8
Ásia-Pacífico (Mumbai)	PCoIP/WSP: 192.168.0.0/16 WSP: 10.0.0.0/8
Ásia-Pacífico (Seul)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
Ásia-Pacífico (Singapura)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
Ásia-Pacífico (Sydney)	PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16 e 198.19.0.0/16 WSP: 10.0.0.0/8
Ásia-Pacífico (Tóquio)	PCoIP/WSP: 198.19.0.0/16

Região	Intervalo de endereços IP
	WSP: 10.0.0.0/8
Canadá (Central)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
Europa (Frankfurt)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
Europa (Irlanda)	PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16 e 198.19.0.0/16 WSP: 10.0.0.0/8
Europa (Londres)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
América do Sul (São Paulo)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
África (Cidade do Cabo)	PCoIP/WSP: 172.31.0.0/16 e 198.19.0.0/16 WSP: 10.0.0.0/8
Israel (Tel Aviv)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
AWS GovCloud (Oeste dos EUA)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8 e 192.169.0.0/16
AWS GovCloud (Leste dos EUA)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8

Portas de interface de gerenciamento

As seguintes portas devem estar abertas na interface da rede de gerenciamento de todos WorkSpaces:

- TCP de entrada na porta 4172. Isso é usado para o estabelecimento da conexão de streaming no protocolo PCoIP.
- UDP de entrada na porta 4172. Isso é usado para transmitir a entrada do usuário no protocolo PCoIP.
- TCP de entrada na porta 4489. Isso é usado para acesso usando o cliente web.
- TCP de entrada na porta 8200. Isso é usado para gerenciamento e configuração do WorkSpace.
- TCP de entrada nas portas 8201-8250. Essas portas são usadas para estabelecer a conexão de streaming e para transmitir a entrada do usuário no protocolo WSP.
- UDP de entrada na porta 8220. Essa porta é usada para estabelecer a conexão de streaming e para transmitir a entrada do usuário no protocolo WSP.
- TCP de saída nas portas 8443 e 9997. Isso é usado para acesso usando o cliente web.
- UDP de saída nas portas 3478, 4172 e 4195. Isso é usado para acesso usando o cliente web.
- UDP de saída nas portas 50002 e 55002. Usada para o streaming. Se o seu firewall usa filtragem stateful, as portas efêmeras 50002 e 55002 são automaticamente abertas para permitir a comunicação de retorno. Se o firewall usar filtragem sem estado, será necessário abrir as portas efêmeras 49152 – 65535 para permitir a comunicação de retorno.
- TCP de saída na porta 80, conforme definido nos intervalos de IP da interface de gerenciamento, para o endereço IP 169.254.169.254 para acesso ao serviço de metadados do EC2. Qualquer proxy HTTP atribuído a você também WorkSpaces deve excluir 169.254.169.254.
- TCP de saída na porta 1688 para os endereços IP 169.254.169.250 e 169.254.169.251 para permitir o acesso ao KMS da Microsoft para ativação do Windows em Workspaces baseados em pacotes públicos. Se você estiver usando o Windows Bring Your Own License (BYOL) WorkSpaces, deverá permitir o acesso aos seus próprios servidores KMS para ativação do Windows.
- TCP de saída na porta 1688 para o endereço IP 54.239.236.220 para permitir acesso à ativação do Microsoft KMS para Office para BYOL. WorkSpaces

  Se você estiver usando o Office por meio de um dos pacotes WorkSpaces públicos, o endereço IP para ativação do Microsoft KMS for Office varia. Para determinar esse endereço IP, encontre o endereço IP da interface de gerenciamento do e WorkSpace, em seguida, substitua os dois

últimos octetos por. `64.250` Por exemplo, se o endereço IP da interface de gerenciamento for 192.168.3.5, o endereço IP do KMS da Microsoft para ativação do Office será 192.168.64.250.

- TCP de saída para o endereço IP 127.0.0.2 para WSP WorkSpaces quando o WorkSpace host está configurado para usar um servidor proxy.
- Comunicações originadas do endereço de loopback 127.0.01.

Em circunstâncias normais, o WorkSpaces serviço configura essas portas para você WorkSpaces. Se algum software de segurança ou firewall estiver instalado em um WorkSpace que bloqueie qualquer uma dessas portas, ele WorkSpace pode não funcionar corretamente ou estar inacessível.

Portas de interface primária

Independentemente do tipo de diretório que você tenha, as seguintes portas devem estar abertas na interface de rede principal de todas WorkSpaces:

- Para conectividade com a Internet, as seguintes portas devem estar abertas de saída para todos os destinos e de entrada da WorkSpaces VPC. Você precisa adicioná-los manualmente ao grupo de segurança do seu WorkSpaces se quiser que eles tenham acesso à Internet.
  - TCP 80 (HTTP)
  - TCP 443 (HTTPS)
- Para se comunicar com os controladores de diretório, as portas a seguir devem estar abertas entre sua WorkSpaces VPC e seus controladores de diretório. Para um diretório Simple AD, o grupo de segurança criado por AWS Directory Service terá essas portas configuradas corretamente. Para um diretório do AD Connector, talvez seja necessário ajustar o grupo de segurança padrão da VPC para abrir essas portas.
  - TCP/UDP 53 - DNS
  - TCP/UDP 88 - autenticação de Kerberos
  - UDP 123 - NTP
  - TCP 135 - RPC
  - UDP 137-138 - Netlogon
  - TCP 139 - Netlogon
  - TCP/UDP 389 - LDAP
  - TCP/UDP 445 - SMB
  - TCP/UDP 636 - LDAPS (LDAP sobre TLS/SSL)

- TCP 1024-65535 - Portas dinâmicas para o RPC

Se algum software de segurança ou firewall estiver instalado em um WorkSpace que bloqueie qualquer uma dessas portas, ele WorkSpace pode não funcionar corretamente ou estar inacessível.

Requisitos de endereço IP e porta por Região

Leste dos EUA (Norte da Virgínia)

Domínios e Endereços IP para adicionar à sua lista de permissões

Categoria	Detalhes
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Atualização automática do cliente	https://d2td7dqidlhjx7.cloudfront.net/
Verificação de conectividade	https://connectivity.amazonworkspaces.com/
Métricas do cliente (para mais de 3.0 aplicativos de WorkSpaces clientes)	Domínio: skylight-client-dshttps://.us-east-1.amazonaws.com
Serviço de mensagens dinâmicas (para mais de 3.0 aplicativos WorkSpaces clientes)	Domínio: ws-client-servicehttps://.us-east-1.amazonaws.com
Configurações de diretório	Autenticação do cliente no diretório de clientes antes de fazer login no WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<região>/<ID do diretório> Conexões de clientes macOS: • https://d32i4gd7pg4909.cloudfront.net/

Categoria	Detalhes
	Configurações de diretório do cliente: • https://d21ui22avrxoh6.cloudfront.net/prod/<região>/<ID do diretório> Gráficos da página de login para marcas conjuntas no nível de diretório do cliente: • https://d1cbg795sa4g1u.cloudfront.net/prod/<região>/<ID do diretório> Arquivo CSS para estilizar as páginas de login: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript arquivo para as páginas de login: • Leste dos EUA (N. da Virgínia): https://d32i4gd7pg4909.cloudfront.net/
Serviço de registro Forrester	https://fls-na.amazon.com/
Servidores de Verificação de Integridade (DRP)	Servidores de verificação de integridade
Endpoints de autenticação de cartão inteligente pré-sessão	https://smartcard.us-east-1.signin.aws
Dependência de registro (para Web Access e Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Páginas de login do usuário	https://<directory id>.awsapps.com/ (em que <directory id> é o domínio do cliente)

Categoria	Detalhes
WS Broker	Domínios: • ws-broker-servicehttps://.us-east-1.amazonaws.com • ws-broker-service-fipshttps://.us-east-1.amazonaws.com
WorkSpaces Endpoints da API	Domínios: https://workspaces.us-east-1.amazonaws.com
Agente de sessão (PCM)	Domínios: • https://skylight-cm.us-east-1.amazonaws.com • skylight-cm-fipshttps://.us-east-1.amazonaws.com
Servidores TURN do Acesso via Web para PCoIP	Servidor: • turn:*.us-east-1.rdn.amazonaws.com
Nome do host de verificação de integridade	drp-iad.amazonworkspaces.com
Endereços IP para verificação de integridade	• 3.209.215.252 • 3.212.50.30 • 3.225.55.35 • 3.226.24.234 • 34.200.29.95 • 52.200.219.150
Intervalos de endereços IP públicos dos servidores de gateway PCoIP	• 3.217.228.0 - 3.217.231.255 • 3.235.112.0 - 3.235.119.255 • 52.23.61.0 - 52.23.62.255

Categoria	Detalhes
Intervalo de endereços IP dos servidores de gateway do WSP	• 3.227.4.0/22 • 44.209.84.0/22
Nome de domínio do gateway WSP	*.prod.us-east-1.highlander.aws.a2z.com
Intervalos de endereço IP de interface de gerenciamento	• PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16 • WSP: 10.0.0.0/8

Oeste dos EUA (Oregon)

Domínios e Endereços IP para adicionar à sua lista de permissões

Categoria	Detalhes
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Atualização automática do cliente	https://d2td7dqidlhjx7.cloudfront.net/
Verificação de conectividade	https://connectivity.amazonworkspaces.com/
Métricas do cliente (para mais de 3.0 aplicativos de WorkSpaces clientes)	Domínio: skylight-client-dshttps://.us-west-2.amazonaws.com
Serviço de mensagens dinâmicas (para mais de 3.0 aplicativos WorkSpaces clientes)	Domínio: ws-client-servicehttps://.us-west-2.amazonaws.com
Configurações de diretório	Autenticação do cliente no diretório de clientes antes de fazer login no WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<região>/<ID do diretório>

Categoria	Detalhes
	Conexões de clientes macOS: • https://d32i4gd7pg4909.cloudfront.net/ Configurações de diretório do cliente: • https://d21ui22avrxoh6.cloudfront.net/prod/<região>/<ID do diretório> Gráficos da página de login para marcas conjuntas no nível de diretório do cliente: • https://d1cbg795sa4g1u.cloudfront.net/prod/<região>/<ID do diretório> Arquivo CSS para estilizar as páginas de login: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript arquivo para as páginas de login: • Oeste dos EUA (Oregon): https://d18af777lco7lp.cloudfront.net/
Serviço de registro Forrester	https://fls-na.amazon.com/
Servidores de Verificação de Integridade (DRP)	Servidores de verificação de integridade
Endpoints de autenticação de cartão inteligente pré-sessão	https://smartcard.us-west-2.signin.aws
Dependência de registro (para Web Access e Teradici PCoIP Zero Clients)	https://s3.amazonaws.com

Categoria	Detalhes
Páginas de login do usuário	https://<directory id>.awsapps.com/ (em que <directory id> é o domínio do cliente)
WS Broker	Domínios: • ws-broker-servicehttps://.us-west-2.amazonaws.com • ws-broker-service-fipshttps://.us-west-2.amazonaws.com
WorkSpaces Endpoints da API	Domínios: • https://workspaces.us-west-2.amazonaws.com • https://workspaces-fips.us-west-2.amazonaws.com
Agente de sessão (PCM)	Domínios: • https://skylight-cm.us-west-2.amazonaws.com • skylight-cm-fipshttps://.us-west-2.amazonaws.com
Servidores TURN do Acesso via Web para PCoIP	Servidor: • turn:*.us-west-2.rdn.amazonaws.com
Nome do host de verificação de integridade	drp-pdx.amazonworkspaces.com
Endereços IP para verificação de integridade	• 34.217.248.177 • 52.34.160.80 • 54.68.150.54 • 54.185.4.125 • 54.188.171.18 • 54.244.158.140

Categoria	Detalhes
Intervalos de endereços IP públicos dos servidores de gateway PCoIP	• 35.80.88.0 - 35.80.95.255 • 44.234.54.0 - 44.234.55.255 • 54.244.46.0 - 54.244.47.255
Intervalo de endereços IP dos servidores de gateway do WSP	34.223.96.0/22
Nome de domínio do gateway WSP	*.prod.us-west-2.highlander.aws.a2z.com
Intervalos de endereço IP de interface de gerenciamento	• PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16 • WSP: 10.0.0.0/8

Ásia-Pacífico (Mumbai)

Domínios e Endereços IP para adicionar à sua lista de permissões

Categoria	Detalhes
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Atualização automática do cliente	https://d2td7dqidlhjx7.cloudfront.net/
Verificação de conectividade	https://connectivity.amazonworkspaces.com/
Métricas do cliente (para mais de 3.0 aplicativos de WorkSpaces clientes)	Domínio: skylight-client-dshttps://.ap-south-1.amazonaws.com
Serviço de mensagens dinâmicas (para mais de 3.0 aplicativos WorkSpaces clientes)	Domínio: ws-client-servicehttps://.ap-south-1.amazonaws.com
Configurações de diretório	Autenticação do cliente no diretório de clientes antes de fazer login no WorkSpace:

Categoria	Detalhes
	• https://d32i4gd7pg4909.cloudfront.net/prod/<região>/<ID do diretório> Conexões de clientes macOS: • https://d32i4gd7pg4909.cloudfront.net/ Configurações de diretório do cliente: • https://d21ui22avrxoh6.cloudfront.net/prod/<região>/<ID do diretório> Gráficos da página de login para marcas conjuntas no nível de diretório do cliente: • https://d1cbg795sa4g1u.cloudfront.net/prod/<região>/<ID do diretório> Arquivo CSS para estilizar as páginas de login: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript arquivo para as páginas de login: • Ásia-Pacífico (Mumbai): https://d78hovzzqqtsb.cloudfront.net/
Serviço de registro Forrester	https://fls-na.amazon.com/
Servidores de Verificação de Integridade (DRP)	Servidores de verificação de integridade
Dependência de registro (para Web Access e Teradici PCoIP Zero Clients)	https://s3.amazonaws.com

Categoria	Detalhes
Páginas de login do usuário	https://<directory id>.awsapps.com/ (em que <directory id> é o domínio do cliente)
WS Broker	Domínio: • ws-broker-servicehttps://.ap-south-1 .amazonaws.com
WorkSpaces Endpoints da API	Domínio: • https://workspaces.ap-south-1.amazon aws.com
Agente de sessão (PCM)	Domínio: • https://skylight-cm.ap-south-1.amazo naws.com
Servidores TURN do Acesso via Web para PCoIP	O Acesso via Web ainda não está disponível na região Ásia-Pacífico (Mumbai).
Nome do host de verificação de integridade	drp-bom.amazonworkspaces.com
Endereços IP para verificação de integridade	• 13.127.57,82 • 13.234.250.73
Intervalos de endereços IP públicos dos servidores de gateway PCoIP	13.126.243.0 - 13.126.243.255
Intervalo de endereços IP dos servidores de gateway do WSP	65.1.156.0/22
Nome de domínio do gateway WSP	*.prod.ap-south-1.highlander.aws.a2z.com
Intervalos de endereço IP de interface de gerenciamento	• PCoIP/WSP: 192.168.0.0/16 • WSP: 10.0.0.0/8

Ásia-Pacífico (Seul)

Domínios e Endereços IP para adicionar à sua lista de permissões

Categoria	Detalhes
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Atualização automática do cliente	https://d2td7dqidlhjx7.cloudfront.net/
Verificação de conectividade	https://connectivity.amazonworkspaces.com/
Device Metrics (para aplicativos clientes 1.0+ e 2.0+) WorkSpaces	device-metrics-ushttps://-2.amazon.com/
Métricas do cliente (para mais de 3.0 aplicativos de WorkSpaces clientes)	Domínio: skylight-client-dshttps://.ap-northeast-2.amazonaws.com
Serviço de mensagens dinâmicas (para mais de 3.0 aplicativos WorkSpaces clientes)	Domínio: ws-client-servicehttps://.ap-northeast-2.amazonaws.com
Configurações de diretório	Autenticação do cliente no diretório de clientes antes de fazer login no WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<região>/<ID do diretório> Conexões de clientes macOS: • https://d32i4gd7pg4909.cloudfront.net/ Configurações de diretório do cliente: • https://d21ui22avrxoh6.cloudfront.net/prod/<região>/<ID do diretório>

Categoria	Detalhes
	Gráficos da página de login para marcas conjuntas no nível de diretório do cliente: • https://d1cbg795sa4g1u.cloudfront.net/prod/<região>/<ID do diretório> Arquivo CSS para estilizar as páginas de login: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript arquivo para as páginas de login: • Ásia-Pacífico (Seul): https://dtyv4uwoh7ynt.cloudfront.net/
Serviço de registro Forrester	https://fls-na.amazon.com/
Servidores de Verificação de Integridade (DRP)	Servidores de verificação de integridade
Dependência de registro (para Web Access e Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Páginas de login do usuário	https://<directory id>.awsapps.com/ (em que <directory id> é o domínio do cliente)
WS Broker	Domínio: • ws-broker-servicehttps://.ap-northeast-2.amazonaws.com
WorkSpaces Endpoints da API	Domínio: • https://workspaces.ap-northeast-2.amazonaws.com

Categoria	Detalhes
Agente de sessão (PCM)	Domínio: • https://skylight-cm.ap-northeast-2.amazonaws.com
Servidores TURN do Acesso via Web para PCoIP	Servidor: • turn:*.ap-northeast-2.rdn.amazonaws.com
Nome do host de verificação de integridade	drp-icn.amazonworkspaces.com
Endereços IP para verificação de integridade	• 13.124.44.166 • 13.124.203.105 • 52.78.44.253 • 52.79.54.102
Intervalos de endereços IP públicos dos servidores de gateway PCoIP	• 3.34.37.0 - 3.34.37.255 • 3.34.38.0 - 3.34.39.255 • 13.124.247.0 - 13.124.247.255
Intervalo de endereços IP dos servidores de gateway do WSP	3.35.160.0/22
Nome de domínio do gateway WSP	*.prod.ap-northeast-2.highlander.aws.a2z.com
Intervalos de endereço IP de interface de gerenciamento	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

Ásia-Pacífico (Singapura)

Domínios e Endereços IP para adicionar à sua lista de permissões

Categoria	Detalhes
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/

Categoria	Detalhes
Atualização automática do cliente	https://d2td7dqidlhjx7.cloudfront.net/
Verificação de conectividade	https://connectivity.amazonworkspaces.com/
Métricas do cliente (para mais de 3.0 aplicativos de WorkSpaces clientes)	Domínio: skylight-client-dshttps://.ap-southeast-1.amazonaws.com
Serviço de mensagens dinâmicas (para mais de 3.0 aplicativos WorkSpaces clientes)	Domínio: https://ws-client-service.ap-southeast-1.amazonaws.com

Categoria	Detalhes
Configurações de diretório	Autenticação do cliente no diretório de clientes antes de fazer login no WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<região>/<ID do diretório> Conexões de clientes macOS: • https://d32i4gd7pg4909.cloudfront.net/ Configurações de diretório do cliente: • https://d21ui22avrxoh6.cloudfront.net/prod/<região>/<ID do diretório> Gráficos da página de login para marcas conjuntas no nível de diretório do cliente: • https://d1cbg795sa4g1u.cloudfront.net/prod/<região>/<ID do diretório> Arquivo CSS para estilizar as páginas de login: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript arquivo para as páginas de login: • Ásia-Pacífico (Singapura): https://d3qzmd7y07pz0i.cloudfront.net/
Serviço de registro Forrester	https://fls-na.amazon.com/
Servidores de Verificação de Integridade (DRP)	Servidores de verificação de integridade

Categoria	Detalhes
Dependência de registro (para Web Access e Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Páginas de login do usuário	https://<directory id>.awsapps.com/ (em que <directory id> é o domínio do cliente)
WS Broker	Domínio: • ws-broker-servicehttps://.ap-southeast-1.amazonaws.com
WorkSpaces Endpoints da API	Domínio: • https://workspaces.ap-southeast-1.amazonaws.com
Agente de sessão (PCM)	Domínio: • https://skylight-cm.ap-southeast-1.amazonaws.com
Servidores TURN do Acesso via Web para PCoIP	Servidor: • turn:*.ap-southeast-1.rdn.amazonaws.com
Nome do host de verificação de integridade	drp-sin.amazonworkspaces.com
Endereços IP para verificação de integridade	• 3.0.212.144 • 18.138.99.116 • 18.140.252.123 • 52.74.175.118
Intervalos de endereços IP públicos dos servidores de gateway PCoIP	• 18.141.152.0 - 18.141.152.255 • 18.141.154.0 - 18.141.155.255 • 52.76.127.0 - 52.76.127.255

Categoria	Detalhes
Intervalo de endereços IP dos servidores de gateway do WSP	13.212.132.0/22
Nome de domínio do gateway WSP	*.prod.ap-southeast-1.highlander.aws.a2z.com
Intervalos de endereço IP de interface de gerenciamento	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

Ásia-Pacífico (Sydney)

Domínios e Endereços IP para adicionar à sua lista de permissões

Categoria	Detalhes
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Atualização automática do cliente	https://d2td7dqidlhjx7.cloudfront.net/
Verificação de conectividade	https://connectivity.amazonworkspaces.com/
Métricas do cliente (para mais de 3.0 aplicativos de WorkSpaces clientes)	Domínio: skylight-client-dshttps://.ap-southeast-2.amazonaws.com
Serviço de mensagens dinâmicas (para mais de 3.0 aplicativos WorkSpaces clientes)	Domínio: ws-client-servicehttps://.ap-southeast-2.amazonaws.com
Configurações de diretório	Autenticação do cliente no diretório de clientes antes de fazer login no WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<região>/<ID do diretório> Conexões de clientes macOS:

Categoria	Detalhes
	• https://d32i4gd7pg4909.cloudfront.net/ Configurações de diretório do cliente: • https://d21ui22avrxoh6.cloudfront.net/prod/<região>/<ID do diretório> Gráficos da página de login para marcas conjuntas no nível de diretório do cliente: • https://d1cbg795sa4g1u.cloudfront.net/prod/<região>/<ID do diretório> Arquivo CSS para estilizar as páginas de login: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript arquivo para as páginas de login: • Ásia-Pacífico (Sydney): https://dwcpoxuuza83q.cloudfront.net/
Serviço de registro Forrester	https://fls-na.amazon.com/
Servidores de Verificação de Integridade (DRP)	Servidores de verificação de integridade
Endpoints de autenticação de cartão inteligente pré-sessão	https://smartcard.ap-southeast-2.signin.aws
Dependência de registro (para Web Access e Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Páginas de login do usuário	https://<directory id>.awsapps.com/ (em que <directory id> é o domínio do cliente)

Categoria	Detalhes
WS Broker	Domínio: • ws-broker-servicehttps://.ap-southeast-2.amazonaws.com
WorkSpaces Endpoints da API	Domínio: • https://workspaces.ap-southeast-2.amazonaws.com
Agente de sessão (PCM)	Domínio: • https://skylight-cm.ap-southeast-2.amazonaws.com
Servidores TURN do Acesso via Web para PCoIP	Servidor: • turn:*.ap-southeast-2.rdn.amazonaws.com
Nome do host de verificação de integridade	drp-syd.amazonworkspaces.com
Endereços IP para verificação de integridade	• 3.24.11.127 • 13.237.232.125
Intervalos de endereços IP públicos dos servidores de gateway PCoIP	• 3.25.43.0 - 3.25.43.255 • 3.25.44.0 - 3.25.45.255 • 54.153.254.0 - 54.153.254.255
Intervalo de endereços IP dos servidores de gateway do WSP	3.25.248.0/22
Nome de domínio do gateway WSP	*.prod.ap-southeast-2.highlander.aws.a2z.com
Intervalos de endereço IP de interface de gerenciamento	• PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16 e 198.19.0.0/16 • WSP: 10.0.0.0/8

Ásia-Pacífico (Tóquio)

Domínios e Endereços IP para adicionar à sua lista de permissões

Categoria	Detalhes
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Atualização automática do cliente	https://d2td7dqidlhjx7.cloudfront.net/
Verificação de conectividade	https://connectivity.amazonworkspaces.com/
Métricas do cliente (para mais de 3.0 aplicativos de WorkSpaces clientes)	Domínio: skylight-client-dshttps://.ap-northeast-1.amazonaws.com
Serviço de mensagens dinâmicas (para mais de 3.0 aplicativos WorkSpaces clientes)	Domínio: ws-client-servicehttps://.ap-northeast-1.amazonaws.com
Configurações de diretório	Autenticação do cliente no diretório de clientes antes de fazer login no WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<região>/<ID do diretório> Conexões de clientes macOS: • https://d32i4gd7pg4909.cloudfront.net/ Configurações de diretório do cliente: • https://d21ui22avrxoh6.cloudfront.net/prod/<região>/<ID do diretório> Gráficos da página de login para marcas conjuntas no nível de diretório do cliente:

Categoria	Detalhes
	• https://d1cbg795sa4g1u.cloudfront.net/prod/<região>/<ID do diretório> Arquivo CSS para estilizar as páginas de login: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript arquivo para as páginas de login: • Ásia-Pacífico (Tóquio): https://d2c2t8mxjhq5z1.cloudfront.net/
Serviço de registro Forrester	https://fls-na.amazon.com/
Servidores de Verificação de Integridade (DRP)	Servidores de verificação de integridade
Endpoints de autenticação de cartão inteligente pré-sessão	https://smartcard.ap-northeast-1.signin.aws
Dependência de registro (para Web Access e Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Páginas de login do usuário	https://<directory id>.awsapps.com/ (em que <directory id> é o domínio do cliente)
WS Broker	Domínio: • ws-broker-servicehttps://.ap-northeast-1.amazonaws.com
WorkSpaces Endpoints da API	Domínio: • https://workspaces.ap-northeast-1.amazonaws.com

Categoria	Detalhes
Agente de sessão (PCM)	Domínio: • https://skylight-cm.ap-northeast-1.amazonaws.com
Servidores TURN do Acesso via Web para PCoIP	Servidor: • turn:*.ap-northeast-1.rdn.amazonaws.com
Nome do host de verificação de integridade	drp-nrt.amazonworkspaces.com
Endereços IP para verificação de integridade	• 18.178.102.247 • 54.64.174.128
Intervalos de endereços IP públicos dos servidores de gateway PCoIP	• 18.180.178.0 - 18.180.178.255 • 18.180.180.0 - 18.180.181.255 • 54.250.251.0 - 54.250.251.255
Intervalo de endereços IP dos servidores de gateway do WSP	3.14.164.0/22
Nome de domínio do gateway WSP	*.prod.ap-northeast-1.highlander.aws.a2z.com
Intervalos de endereço IP de interface de gerenciamento	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

Canadá (Central)

Domínios e Endereços IP para adicionar à sua lista de permissões

Categoria	Detalhes
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Atualização automática do cliente	https://d2td7dqidlhjx7.cloudfront.net/
Verificação de conectividade	https://connectivity.amazonworkspaces.com/

Categoria	Detalhes
Métricas do cliente (para mais de 3.0 aplicativos de WorkSpaces clientes)	Domínio: skylight-client-dshttps://.ca-central-1.amazonaws.com
Serviço de mensagens dinâmicas (para mais de 3.0 aplicativos WorkSpaces clientes)	Domínio: ws-client-servicehttps://.ca-central-1.amazonaws.com

Categoria	Detalhes
Configurações de diretório	Autenticação do cliente no diretório de clientes antes de fazer login no WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<região>/<ID do diretório> Conexões de clientes macOS: • https://d32i4gd7pg4909.cloudfront.net/ Configurações de diretório do cliente: • https://d21ui22avrxoh6.cloudfront.net/prod/<região>/<ID do diretório> Gráficos da página de login para marcas conjuntas no nível de diretório do cliente: • https://d1cbg795sa4g1u.cloudfront.net/prod/<região>/<ID do diretório> Arquivo CSS para estilizar as páginas de login: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript arquivo para as páginas de login: • Canadá (Central): https://d2wfbsypmqjmog.cloudfront.net/
Serviço de registro Forrester	https://fls-na.amazon.com/
Servidores de Verificação de Integridade (DRP)	Servidores de verificação de integridade

Categoria	Detalhes
Dependência de registro (para Web Access e Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Páginas de login do usuário	https://<directory id>.awsapps.com/ (em que <directory id> é o domínio do cliente)
WS Broker	Domínio: • ws-broker-servicehttps://.ca-central-1.amazonaws.com
WorkSpaces Endpoints da API	Domínio: • https://workspaces.ca-central-1.amazonaws.com
Agente de sessão (PCM)	Domínio: • https://skylight-cm.ca-central-1.amazonaws.com
Servidores TURN do Acesso via Web para PCoIP	Servidor: • turn:*.ca-central-1.rdn.amazonaws.com
Nome do host de verificação de integridade	drp-yul.amazonworkspaces.com
Endereços IP para verificação de integridade	• 52.60.69.16 • 52.60.80.237 • 52.60.173.117 • 52.60.201.0
Intervalos de endereços IP públicos dos servidores de gateway PCoIP	• 15.223.100.0 - 15.223.100.255 • 15.223.102.0 - 15.223.103.255 • 35.183.255.0 - 35.183.255.255

Categoria	Detalhes
Intervalo de endereços IP dos servidores de gateway do WSP	3.97.20.0/22
Nome de domínio do gateway WSP	*.prod.ca-central-1.highlander.aws.a2z.com
Intervalos de endereço IP de interface de gerenciamento	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

Europa (Frankfurt)

Domínios e Endereços IP para adicionar à sua lista de permissões

Categoria	Detalhes
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Atualização automática do cliente	https://d2td7dqidlhjx7.cloudfront.net/
Verificação de conectividade	https://connectivity.amazonworkspaces.com/
Métricas do cliente (para mais de 3.0 aplicativos de WorkSpaces clientes)	Domínio: skylight-client-dshttps://.eu-central-1.amazonaws.com
Serviço de mensagens dinâmicas (para mais de 3.0 aplicativos WorkSpaces clientes)	Domínio: ws-client-servicehttps://.eu-central-1.amazonaws.com
Configurações de diretório	Autenticação do cliente no diretório de clientes antes de fazer login no WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<região>/<ID do diretório> Conexões de clientes macOS:

Categoria	Detalhes
	• https://d32i4gd7pg4909.cloudfront.net/ Configurações de diretório do cliente: • https://d21ui22avrxoh6.cloudfront.net/prod/<região>/<ID do diretório> Gráficos da página de login para marcas conjuntas no nível de diretório do cliente: • https://d1cbg795sa4g1u.cloudfront.net/prod/<região>/<ID do diretório> Arquivo CSS para estilizar as páginas de login: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript arquivo para as páginas de login: • Europa (Frankfurt): https://d1whcm49570jjw.cloudfront.net/
Serviço de registro Forrester	https://fls-na.amazon.com/
Servidores de Verificação de Integridade (DRP)	Servidores de verificação de integridade
Dependência de registro (para Web Access e Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Páginas de login do usuário	https://<directory id>.awsapps.com/ (em que <directory id> é o domínio do cliente)

Categoria	Detalhes
WS Broker	Domínio: • ws-broker-servicehttps://.eu-central-1.amazonaws.com
WorkSpaces Endpoints da API	Domínio: • https://workspaces.eu-central-1.amazonaws.com
Agente de sessão (PCM)	Domínio: • https://skylight-cm.eu-central-1.amazonaws.com
Servidores TURN do Acesso via Web para PCoIP	Servidor: • turn:*.eu-central-1.rdn.amazonaws.com
Nome do host de verificação de integridade	drp-fra.amazonworkspaces.com
Endereços IP para verificação de integridade	• 52.59.191.224 • 52.59.191.225 • 52.59.191.226 • 52.59.191.227
Intervalos de endereços IP públicos dos servidores de gateway PCoIP	• 18.156.52.0 - 18.156.52.255 • 18.156.54.0 - 18.156.55.255 • 52.59.127.0 - 52.59.127.255
Intervalo de endereços IP dos servidores de gateway do WSP	18.192.216.0/22
Nome de domínio do gateway WSP	*.prod.eu-central-1.highlander.aws.a2z.com
Intervalos de endereço IP de interface de gerenciamento	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

Europa (Irlanda)

Domínios e Endereços IP para adicionar à sua lista de permissões

Categoria	Detalhes
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Atualização automática do cliente	https://d2td7dqidlhjx7.cloudfront.net/
Verificação de conectividade	https://connectivity.amazonworkspaces.com/
Métricas do cliente (para mais de 3.0 aplicativos de WorkSpaces clientes)	Domínio: skylight-client-dshttps://.eu-west-1.amazonaws.com
Serviço de mensagens dinâmicas (para mais de 3.0 aplicativos WorkSpaces clientes)	Domínio: ws-client-servicehttps://.eu-west-1.amazonaws.com
Configurações de diretório	Autenticação do cliente no diretório de clientes antes de fazer login no WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<região>/<ID do diretório> Conexões de clientes macOS: • https://d32i4gd7pg4909.cloudfront.net/ Configurações de diretório do cliente: • https://d21ui22avrxoh6.cloudfront.net/prod/<região>/<ID do diretório> Gráficos da página de login para marcas conjuntas no nível de diretório do cliente:

Categoria	Detalhes
	• https://d1cbg795sa4g1u.cloudfront.net/prod/<região>/<ID do diretório> Arquivo CSS para estilizar as páginas de login: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript arquivo para as páginas de login: • Europa (Irlanda): https://d3pgffbf39h4k4.cloudfront.net/
Serviço de registro Forrester	https://fls-na.amazon.com/
Servidores de Verificação de Integridade (DRP)	Servidores de verificação de integridade
Endpoints de autenticação de cartão inteligente pré-sessão	https://smartcard.eu-west-1.signin.aws
Dependência de registro (para Web Access e Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Páginas de login do usuário	https://<directory id>.awsapps.com/ (em que <directory id> é o domínio do cliente)
WS Broker	Domínio: • ws-broker-servicehttps://.eu-west-1.amazonaws.com
WorkSpaces Endpoints da API	Domínio: • https://workspaces.eu-west-1.amazonaws.com

Categoria	Detalhes
Agente de sessão (PCM)	Domínio: • https://skylight-cm.eu-west-1.amazonaws.com
Servidores TURN do Acesso via Web para PCoIP	Servidor: • turn:*.eu-west-1.rdn.amazonaws.com
Nome do host de verificação de integridade	drp-dub.amazonworkspaces.com
Endereços IP para verificação de integridade	• 18.200.177.86 • 52.48.86.38 • 54.76.137.224
Intervalos de endereços IP públicos dos servidores de gateway PCoIP	• 3.249.28.0 - 3.249.29.255 • 52.19.124.0 - 52.19.125.255
Intervalo de endereços IP dos servidores de gateway do WSP	3.248.176.0/22
Nome de domínio do gateway WSP	*.prod.eu-west-1.highlander.aws.a2z.com
Intervalos de endereço IP de interface de gerenciamento	• PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16 e 198.19.0.0/16 • WSP: 10.0.0.0/8

Europa (Londres)

Domínios e Endereços IP para adicionar à sua lista de permissões

Categoria	Detalhes
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Atualização automática do cliente	https://d2td7dqidlhjx7.cloudfront.net/

Categoria	Detalhes
Verificação de conectividade	https://connectivity.amazonworkspaces.com/
Métricas do cliente (para mais de 3.0 aplicativos de WorkSpaces clientes)	Domínio: skylight-client-dshttps://.eu-west-2.amazonaws.com
Serviço de mensagens dinâmicas (para mais de 3.0 aplicativos WorkSpaces clientes)	Domínio: ws-client-servicehttps://.eu-west-2.amazonaws.com

Categoria	Detalhes
Configurações de diretório	Autenticação do cliente no diretório de clientes antes de fazer login no WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<região>/<ID do diretório> Conexões de clientes macOS: • https://d32i4gd7pg4909.cloudfront.net/ Configurações de diretório do cliente: • https://d21ui22avrxoh6.cloudfront.net/prod/<região>/<ID do diretório> Gráficos da página de login para marcas conjuntas no nível de diretório do cliente: • https://d1cbg795sa4g1u.cloudfront.net/prod/<região>/<ID do diretório> Arquivo CSS para estilizar as páginas de login: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript arquivo para as páginas de login: • Europa (Londres): https://d16q6638mh01s7.cloudfront.net/
Serviço de registro Forrester	https://fls-na.amazon.com/
Servidores de Verificação de Integridade (DRP)	Servidores de verificação de integridade

Categoria	Detalhes
Dependência de registro (para Web Access e Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Páginas de login do usuário	https://<directory id>.awsapps.com/ (em que <directory id> é o domínio do cliente)
WS Broker	Domínio: • ws-broker-servicehttps://.eu-west-2.amazonaws.com
WorkSpaces Endpoints da API	Domínio: • https://workspaces.eu-west-2.amazonaws.com
Agente de sessão (PCM)	Domínio: • https://skylight-cm.eu-west-2.amazonaws.com
Servidores TURN do Acesso via Web para PCoIP	Servidor: • turn:*.eu-west-2.rdn.amazonaws.com
Nome do host de verificação de integridade	drp-lhr.amazonworkspaces.com
Endereços IP para verificação de integridade	• 35.176.62.54 • 35.177.255.44 • 52.56.46.102 • 52.56.111.36
Intervalos de endereços IP públicos dos servidores de gateway PCoIP	• 18.132.21.0 - 18.132.21.255 • 18.132.22.0 - 18.132.23.255 • 35.176.32.0 - 35.176.32.255

Categoria	Detalhes
Intervalo de endereços IP dos servidores de gateway do WSP	18.134.68.0/22
Nome de domínio do gateway WSP	*.prod.eu-west-2.highlander.aws.a2z.com
Intervalos de endereço IP de interface de gerenciamento	• 198.19.0.0/16 • WSP: 10.0.0.0/8

América do Sul (São Paulo)

Domínios e Endereços IP para adicionar à sua lista de permissões

Categoria	Detalhes
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Atualização automática do cliente	https://d2td7dqidlhjx7.cloudfront.net/
Verificação de conectividade	https://connectivity.amazonworkspaces.com/
Métricas do cliente (para mais de 3.0 aplicativos de WorkSpaces clientes)	Domínio: skylight-client-dshttps://.sa-east-1.amazonaws.com
Serviço de mensagens dinâmicas (para mais de 3.0 aplicativos WorkSpaces clientes)	Domínio: ws-client-servicehttps://.sa-east-1.amazonaws.com
Configurações de diretório	Autenticação do cliente no diretório de clientes antes de fazer login no WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<região>/<ID do diretório> Conexões de clientes macOS:

Categoria	Detalhes
	• https://d32i4gd7pg4909.cloudfront.net/ Configurações de diretório do cliente: • https://d21ui22avrxoh6.cloudfront.net/prod/<região>/<ID do diretório> Gráficos da página de login para marcas conjuntas no nível de diretório do cliente: • https://d1cbg795sa4g1u.cloudfront.net/prod/<região>/<ID do diretório> Arquivo CSS para estilizar as páginas de login: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript arquivo para as páginas de login: • América do Sul (São Paulo): https://d2lh2qc5bdoq4b.cloudfront.net/
Serviço de registro Forrester	https://fls-na.amazon.com/
Servidores de Verificação de Integridade (DRP)	Servidores de verificação de integridade
Dependência de registro (para Web Access e Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Páginas de login do usuário	https://<directory id>.awsapps.com/ (em que <directory id> é o domínio do cliente)

Categoria	Detalhes
WS Broker	Domínio: • ws-broker-servicehttps://.sa-east-1.amazonaws.com
WorkSpaces Endpoints da API	Domínio: • https://workspaces.sa-east-1.amazonaws.com
Agente de sessão (PCM)	Domínio: • https://skylight-cm.sa-east-1.amazonaws.com
Servidores TURN do Acesso via Web para PCoIP	Servidor: • turn:*.sa-east-1.rdn.amazonaws.com
Nome do host de verificação de integridade	drp-gru.amazonworkspaces.com
Endereços IP para verificação de integridade	• 18.231.0.105 • 52.67.55.29 • 54.233.156.245 • 54.233.216.234
Intervalos de endereços IP públicos dos servidores de gateway PCoIP	• 18.230.103.0 - 18.230.103.255 • 18.230.104.0 - 18.230.105.255 • 54.233.204.0 - 54.233.204.255
Intervalo de endereços IP dos servidores de gateway do WSP	15.228.64.0/22
Nome de domínio do gateway WSP	*.prod.sa-east-1.highlander.aws.a2z.com
Intervalos de endereço IP de interface de gerenciamento	• 198.19.0.0/16 • WSP: 10.0.0.0/8

África (Cidade do Cabo)

Domínios e Endereços IP para adicionar à sua lista de permissões

Categoria	Detalhes
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Atualização automática do cliente	https://d2td7dqidlhjx7.cloudfront.net/
Verificação de conectividade	https://connectivity.amazonworkspaces.com/
Métricas do cliente (para mais de 3.0 aplicativos de WorkSpaces clientes)	Domínio: skylight-client-dshttps://.af-south-1.amazonaws.com
Serviço de mensagens dinâmicas (para mais de 3.0 aplicativos WorkSpaces clientes)	Domínio: ws-client-servicehttps://.af-south-1.amazonaws.com
Configurações de diretório	Autenticação do cliente no diretório de clientes antes de fazer login no WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<região>/<ID do diretório> Conexões de clientes macOS: • https://d32i4gd7pg4909.cloudfront.net/ Configurações de diretório do cliente: • https://d21ui22avrxoh6.cloudfront.net/prod/<região>/<ID do diretório> Gráficos da página de login para marcas conjuntas no nível de diretório do cliente:

Categoria	Detalhes
	• https://d1cbg795sa4g1u.cloudfront.net/prod/<região>/<ID do diretório> Arquivo CSS para estilizar as páginas de login: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript arquivo para as páginas de login: • África (Cidade do Cabo): https://di5ygl2cs0mrh.cloudfront.net/
Serviço de registro Forrester	https://fls-na.amazon.com/
Servidores de Verificação de Integridade (DRP)	Servidores de verificação de integridade
Dependência de registro (para Web Access e Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Páginas de login do usuário	https://<directory id>.awsapps.com/ (em que <directory id> é o domínio do cliente)
WS Broker	Domínio: • ws-broker-servicehttps://.af-south-1.amazonaws.com
WorkSpaces Endpoints da API	Domínio: • https://workspaces.af-south-1.amazonaws.com
Agente de sessão (PCM)	Domínio: • https://skylight-cm.af-south-1.amazonaws.com

Categoria	Detalhes
Nome do host de verificação de integridade	drp-cpt.amazonworkspaces.com
Endereços IP para verificação de integridade	• 18.231.0.105 • 52.67.55.29 • 54.233.156.245 • 54.233.216.234
Intervalos de endereços IP públicos dos servidores de gateway PCoIP	• 13.246.120.0 - 13.246.123.255
Intervalo de endereços IP dos servidores de gateway do WSP	15.228.64.0/22
Nome de domínio do gateway WSP	*.prod.af-south-1.highlander.aws.a2z.com
Intervalos de endereço IP de interface de gerenciamento	• 172.31.0.0/16 e 198.19.0.0/16 • WSP: 10.0.0.0/8

Israel (Tel Aviv)

Domínios e Endereços IP para adicionar à sua lista de permissões

Categoria	Detalhes
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Atualização automática do cliente	https://d2td7dqidlhjx7.cloudfront.net/
Verificação de conectividade	https://connectivity.amazonworkspaces.com/
Métricas do cliente (para mais de 3.0 aplicativos de WorkSpaces clientes)	Domínio: skylight-client-dshttps://.il-central-1.amazonaws.com
Serviço de mensagens dinâmicas (para mais de 3.0 aplicativos WorkSpaces clientes)	Domínio:

Categoria	Detalhes
	ws-client-servicehttps://.il-central-1.amazon aws.com
Configurações de diretório	Autenticação do cliente no diretório de clientes antes de fazer login no WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<região>/<ID do diretório> Conexões de clientes macOS: • https://d32i4gd7pg4909.cloudfront.net/ Configurações de diretório do cliente: • https://d21ui22avrxoh6.cloudfront.net/prod/<região>/<ID do diretório> Gráficos da página de login para marcas conjuntas no nível de diretório do cliente: • Arquivo CSS para estilizar as páginas de login: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript arquivo para as páginas de login: • Israel (Tel Aviv); —
Serviço de registro Forrester	https://fls-na.amazon.com/
Servidores de Verificação de Integridade (DRP)	Servidores de verificação de integridade

Categoria	Detalhes
Dependência de registro (para Web Access e Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Páginas de login do usuário	https://<directory id>.awsapps.com/ (em que <directory id> é o domínio do cliente)
WS Broker	Domínio: • ws-broker-servicehttps://.il-central-1.amazonaws.com
WorkSpaces Endpoints da API	Domínio: • https://workspaces.il-central-1.amazonaws.com
Agente de sessão (PCM)	Domínio: • https://skylight-cm.il-central-1.amazonaws.com
Servidores TURN do Acesso via Web para PCoIP	Servidor: • turno: *.il-central-1.rdn.amazonaws.com
Nome do host de verificação de integridade	drp-tlv.amazonworkspaces.com
Endereços IP para verificação de integridade	• 51.17.52.90 • 51.17.109.231 • 51.16.190.43
Intervalos de endereços IP públicos dos servidores do gateway PCoIP	• 51.17.28.0-51.17.31.255
Intervalo de endereços IP dos servidores de gateway do WSP	51.17.72.0/22
Nome de domínio do gateway WSP	*.prod.il-central-1.highlander.aws.a2z.com

Categoria	Detalhes
Intervalos de endereço IP de interface de gerenciamento	• 198.19.0.0/16 • WSP: 10.0.0.0/8

AWS GovCloud Região (Oeste dos EUA)

Domínios e Endereços IP para adicionar à sua lista de permissões

Categoria	Detalhes
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Atualização automática do cliente	https://s3.amazonaws.com/ workspaces-client-updates /prod/pdt/windows/ .xml WorkSpaces AppCast
Verificação de conectividade	https://connectivity.amazonworkspaces.com/
Métricas do cliente (para mais de 3.0 aplicativos de WorkSpaces clientes)	Domínio: https://skylight-client-ds. us-gov-west-1.amazonaws.com
Serviço de mensagens dinâmicas (para mais de 3.0 aplicativos WorkSpaces clientes)	Domínio: https://ws-client-service. us-gov-west-1.amazonaws.com
Configurações de diretório	Autenticação do cliente no diretório de clientes antes de fazer login no WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<região>/<ID do diretório> Conexões de clientes macOS: • https://d32i4gd7pg4909.cloudfront.net/

Categoria	Detalhes
	Configurações de diretório do cliente: • https://s3.amazonaws.com/ workspaces-client-properties /prod/pdt/ <directory ID> Gráficos da página de login para marcas conjuntas no nível de diretório do cliente: • https://s3.amazonaws.com/ workspaces-client-assets /prod/pdt/ <directory ID> Arquivo CSS para estilizar as páginas de login: • https://s3.amazonaws.com/ workspaces-clients-css /workspaces_v2.css JavaScript arquivo para as páginas de login: • Não aplicável
Serviço de registro Forrester	https://fls-na.amazon.com/
Servidores de Verificação de Integridade (DRP)	Servidores de verificação de integridade
Endpoints de autenticação de cartão inteligente pré-sessão	https://smartcard.signin. amazonaws-us-gov.com
Dependência de registro (para Web Access e Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Páginas de login do usuário	https://login. us-gov-home<directory id>.awsapps.com/directory/<directory id>/(onde está o domínio do cliente)

Categoria	Detalhes
WS Broker	Domínio: • https://ws-broker-service. us-gov-west-1.amazonaws.com • https://ws-broker-service-fips. us-gov-west-1.amazonaws.com
WorkSpaces Endpoints da API	Domínio: • https://workspaces. us-gov-west-1.amazonaws.com • https://workspaces-fips. us-gov-west-1.amazonaws.com
Agente de sessão (PCM)	Domínio: • https://skylight-cm. us-gov-west-1.amazonaws.com • https://skylight-cm-fips. us-gov-west-1.amazonaws.com
Nome do host de verificação de integridade	drp-pdt.amazonworkspaces.com
Endereços IP para verificação de integridade	• 52.61.60.65 • 52.61.65.14 • 52.61.88.170 • 52.61.137.87 • 52.61.155.110 • 52.222.20.88
Intervalos de endereços IP públicos dos servidores do gateway PCoIP	• 52.61.193.0 - 52.61.193.255

Categoria	Detalhes
Intervalo de endereços IP dos servidores de gateway do WSP	• 3.32.139.0/24 • 3.30.129.0/24 • 3.30.130.0/23
Nome de domínio do gateway WSP	*.prod. us-gov-west-1.highlander.aws.a2z.com
Intervalos de endereço IP de interface de gerenciamento	• 198.19.0.0/16 • WSP: 10.0.0.0/8 e 192.169.0.0/16

AWS GovCloud Região (Leste dos EUA)

Domínios e Endereços IP para adicionar à sua lista de permissões

Categoria	Detalhes
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Atualização automática do cliente	https://s3.amazonaws.com/ workspaces-client-updates /prod/osu/windows/ .xml WorkSpaces AppCast
Verificação de conectividade	https://connectivity.amazonworkspaces.com/
Métricas do cliente (para mais de 3.0 aplicativos de WorkSpaces clientes)	Domínio: https://skylight-client-ds. us-gov-east-1.amazonaws.com
Serviço de mensagens dinâmicas (para mais de 3.0 aplicativos WorkSpaces clientes)	Domínio: https://ws-client-service. us-gov-east-1.amazonaws.com
Configurações de diretório	Autenticação do cliente no diretório de clientes antes de fazer login no WorkSpace:

Categoria	Detalhes
	• https://d32i4gd7pg4909.cloudfront.net/prod/<região>/<ID do diretório> Conexões de clientes macOS: • https://d32i4gd7pg4909.cloudfront.net/ Configurações de diretório do cliente: • https://s3.amazonaws.com/ workspaces-client-properties /prod/osu/ <directory ID> Gráficos da página de login para marcas conjuntas no nível de diretório do cliente: • https://s3.amazonaws.com/ workspaces-client-assets /prod/osu/ <directory ID> Arquivo CSS para estilizar as páginas de login: • https://s3.amazonaws.com/ workspaces-clients-css /workspaces_v2.css JavaScript arquivo para as páginas de login: • Não aplicável
Serviço de registro Forrester	https://fls-na.amazon.com/
Servidores de Verificação de Integridade (DRP)	Servidores de verificação de integridade
Endpoints de autenticação de cartão inteligente pré-sessão	https://smartcard.signin. amazonaws-us-gov.com
Dependência de registro (para Web Access e Teradici PCoIP Zero Clients)	https://s3.amazonaws.com

Categoria	Detalhes
Páginas de login do usuário	https://login. us-gov-home<directory id>.awsapps.com/directory/<directory id>/(onde está o domínio do cliente)
WS Broker	Domínio: • https://ws-broker-service. us-gov-east-1.amazonaws.com • https://ws-broker-service-fips. us-gov-east-1.amazonaws.com
WorkSpaces Endpoints da API	Domínio: • https://workspaces. us-gov-east-1.amazonaws.com • https://workspaces-fips. us-gov-east-1.amazonaws.com
Agente de sessão (PCM)	Domínio: • https://skylight-cm. us-gov-east-1.amazonaws.com • https://skylight-cm-fips. us-gov-east-1.amazonaws.com
Nome do host de verificação de integridade	drp-osu.amazonworkspaces.com
Endereços IP para verificação de integridade	• 18.253.251.70 • 18.254.0.118
Intervalos de endereços IP públicos dos servidores do gateway PCoIP	• 18.254.140.0 - 18.254.143.255
Intervalo de endereços IP dos servidores de gateway do WSP	18.254.148.0/22
Nome de domínio do gateway WSP	*.prod. us-gov-east-1.highlander.aws.a2z.com

Categoria	Detalhes
Intervalos de endereço IP de interface de gerenciamento	• 198.19.0.0/16 • WSP: 10.0.0.0/8

Requisitos de rede de clientes do Amazon WorkSpaces

Os usuários do WorkSpaces podem se conectar aos WorkSpaces usando a aplicação cliente para um dispositivo compatível. Como alternativa, eles podem usar um navegador da Web para se conectar a WorkSpaces que oferecem suporte a esse tipo de acesso. Para obter uma lista de WorkSpaces que oferecem suporte ao acesso por navegador da web, consulte “Quais pacotes do Amazon WorkSpaces dão suporte a acesso pela web?” em Acesso de clientes, acesso à Web e experiência do usuário.

> **Note**
>
> Um navegador da web não pode ser usado para se conectar ao WorkSpaces do Amazon Linux.

> **Important**
>
> A partir de 1.º de outubro de 2020, os clientes não poderão mais usar o cliente do Acesso via Web do Amazon WorkSpaces para se conectarem a WorkSpaces personalizados do Windows 7 ou a WorkSpaces do tipo traga a sua própria licença (BYOL) do Windows 7.

Para proporcionar aos usuários uma boa experiência com seus WorkSpaces, verifique se seus dispositivos clientes cumprem os seguintes requisitos de rede:

- O dispositivo cliente deve ter uma conexão de Internet banda larga. Recomendamos planejar um mínimo de 1 Mbps por usuário simultâneo assistindo a uma janela de vídeo de 480p. Dependendo dos requisitos de qualidade do usuário para a resolução de vídeo, pode ser necessária mais largura de banda.

- A rede à qual o dispositivo cliente está conectado e qualquer firewall no dispositivo cliente devem ter determinadas portas abertas para os intervalos de endereços IP dos vários serviços da AWS. Para obter mais informações, consulte Requisitos de endereço IP e porta para WorkSpaces.
- Para obter a melhor performance para PCoIP, o tempo de ida e volta (RTT) da rede do cliente até a região onde estão os WorkSpaces deve ser menor que 100 ms. Se o RTT estiver entre 100 ms e 200 ms, o usuário poderá acessar o WorkSpace, mas a performance será afetada. Se o RTT estiver entre 200 ms e 375 ms, a performance será reduzida. Se o RTT exceder 375 ms, a conexão do cliente do WorkSpaces será encerrada.

  Para obter a melhor performance para o WorkSpaces Streaming Protocol (WSP), o RTT da rede do cliente até a região onde estão os WorkSpaces deve ser menor que 250 ms. Se o RTT estiver entre 250 ms e 400 ms, o usuário poderá acessar o WorkSpace, mas a performance será reduzida.

  Para verificar o RTT para as várias regiões da AWS a partir de sua localização, use a Verificação de integridade da conexão do Amazon WorkSpaces.
- Para usar webcams com o WSP, recomendamos uma largura de banda de upload mínima de 1,7 megabits por segundo.
- Se os usuários acessarem seus WorkSpaces através de uma rede privada virtual (VPN), a conexão deverá oferecer suporte a uma unidade de transmissão máxima (MTU) de, pelo menos, 1.200 bytes.

  > **Note**
  >
  > Não é possível acessar o WorkSpaces por meio de uma VPN conectada à sua Virtual Private Cloud (VPC). Para acessar o WorkSpaces usando uma VPN, a conectividade da Internet (por meio de endereços IP públicos da VPN) é necessária, conforme descrito em Requisitos de endereço IP e porta para WorkSpaces.
- Os clientes exigem acesso HTTPS a recursos do WorkSpaces hospedados pelo serviço e pelo Amazon Simple Storage Service (Amazon S3). Os clientes não são compatíveis com o redirecionamento de proxy no nível de aplicativo. O acesso HTTPS é necessário para que os usuários possam concluir com êxito o registro e acessar seus WorkSpaces.
- Para permitir o acesso a partir de dispositivos PCoIP cliente zero, é necessário usar um pacote de protocolos PCoIP para o WorkSpaces. Também é necessário habilitar o Network Time Protocol (NTP) no Teradici. Para obter mais informações, consulte Configurar clientes zero PCoIP para WorkSpaces.

- Para clientes 3.0+, se você estiver usando autenticação única (SSO) no Amazon WorkDocs, será necessário seguir as instruções em Autenticação única no Guia de administração da AWS Directory Service.

É possível verificar se um dispositivo cliente cumpre os requisitos de rede da seguinte forma.

Como verificar os requisitos de rede para clientes 3.0+

1. Abra o cliente do WorkSpaces. Se esta for a primeira vez que você abre o cliente, será solicitado que você insira o código de registro que recebeu no e-mail de convite.
2. Dependendo do cliente que você estiver usando, siga um dos procedimentos a seguir.

Se você estiver usando...	Faça o seguinte
Clientes Windows ou Linux	No canto superior direito do aplicativo cliente, selecione o ícone Network (Rede) .
Cliente para macOS	Selecione Connections (Conexões), Network (Rede).

   A aplicação cliente testa a conexão de rede, as portas e o tempo de ida e volta e relata os resultados desses testes.
3. Feche a caixa de diálogo Network (Rede) para retornar à página de login.

Como verificar os requisitos de rede para clientes 1.0+ e 2.0+

1. Abra o cliente do WorkSpaces. Se esta for a primeira vez que você abre o cliente, será solicitado que você insira o código de registro que recebeu no e-mail de convite.
2. Selecione Network (Rede) no canto inferior direito do aplicativo cliente. A aplicação cliente testa a conexão de rede, as portas e o tempo de ida e volta e relata os resultados desses testes.
3. Escolha Dismiss (Descartar) para voltar para a página de login.

Restrinja o WorkSpaces acesso a dispositivos confiáveis

Por padrão, os usuários podem acessá-los WorkSpaces de qualquer dispositivo compatível conectado à Internet. Se sua empresa limita o acesso aos dados corporativos a dispositivos confiáveis (também conhecidos como dispositivos gerenciados), você pode restringir o WorkSpaces acesso a dispositivos confiáveis com certificados válidos.

Quando você ativa esse recurso, WorkSpaces usa a autenticação baseada em certificado para determinar se um dispositivo é confiável. Se o aplicativo WorkSpaces cliente não puder verificar se um dispositivo é confiável, ele bloqueia as tentativas de login ou reconexão a partir do dispositivo.

Para cada diretório, você pode importar até dois certificados raiz. Se você importar dois certificados raiz, WorkSpaces apresente-os ao cliente e o cliente encontrará o primeiro certificado correspondente válido que se encadeia a qualquer um dos certificados raiz.

Clientes compatíveis

- Android, em execução em sistemas Android ou em sistemas Android compatíveis com Chrome OS
- macOS
- Windows

Important

Este recurso não é compatível com os seguintes clientes:

- WorkSpaces aplicativos cliente para Linux ou iPad
- Clientes de terceiros, incluindo, mas não se limitando a, Teradici PCoIP, clientes RDP e aplicações de área de trabalho remota.

Note

Ao habilitar o acesso para clientes específicos, certifique-se de bloquear o acesso para outros tipos de dispositivos que você não precisa. Para obter mais informações sobre como fazer isso, consulte a Etapa 3.7 abaixo.

Etapa 1: Criar os certificados

Este recurso exige dois tipos de certificados: certificados raiz gerados por uma autoridade de certificação (CA) interna e certificados de cliente que se associam a um certificado raiz.

Requisitos

- Os certificados raiz devem ser arquivos codificados por Base64 no formato CRT, CERT ou PEM.
- Os certificados raiz devem atender ao seguinte padrão de expressão regular, o que significa que cada linha codificada, exceto a última, deve ter exatamente 64 caracteres: `-{5}BEGIN CERTIFICATE-{5}\u000D?\u000A([A-Za-z0-9/+]{64} \u000D?\u000A)*[A-Za-z0-9/+]{1,64}={0,2}\u000D?\u000A-{5}END CERTIFICATE-{5}(\u000D?\u000A)`.
- Os certificados de dispositivo devem incluir um nome comum.
- Os certificados de dispositivo devem incluir as seguintes extensões: `Key Usage: Digital Signature` e `Enhanced Key Usage: Client Authentication`.
- Todos os certificados na cadeia, desde o certificado de dispositivo até a Autoridade certificadora raiz confiável, devem ser instalados no dispositivo cliente.
- O tamanho máximo da cadeia de certificados compatível é 4.
- WorkSpaces atualmente não oferece suporte a mecanismos de revogação de dispositivos, como listas de revogação de certificados (CRL) ou Protocolo de Status de Certificado Online (OCSP), para certificados de clientes.
- Use um algoritmo de criptografia forte. Recomendamos SHA256 com RSA, SHA256 com ECDSA, SHA384 com ECDSA ou SHA512 com ECDSA.
- Para macOS, se o certificado do dispositivo estiver no conjunto de chaves do sistema, recomendamos que você autorize o aplicativo WorkSpaces cliente a acessar esses certificados. Caso contrário, os usuários devem inserir credenciais de cadeia de chaves quando fazem login ou se reconectam.

Etapa 2: Implantar certificados de cliente nos dispositivos confiáveis

Nos dispositivos confiáveis para usuários, você deve instalar um pacote de certificados que inclua todos os certificados na cadeia, desde o certificado do dispositivo até a Autoridade de Certificação raiz confiável. Você pode usar a melhor solução para instalar os certificados na sua frota de dispositivos clientes; por exemplo, o System Center Configuration Manager (SCCM) ou o gerenciamento de dispositivos móveis (MDM). Observe que o SCCM e o MDM podem,

opcionalmente, realizar uma avaliação da postura de segurança para determinar se os dispositivos atendem às políticas corporativas de acesso. WorkSpaces

Os aplicativos WorkSpaces cliente pesquisam certificados da seguinte forma:

- Android: vá para Configurações, selecione Segurança e localização, Credenciais e selecione Instalar do cartão SD.
- Sistemas Chrome OS compatíveis com Android: abra as configurações do Android e selecione Segurança e localização, Credenciais e escolha Instalar do cartão SD.
- macOS: pesquisa certificados de cliente no conjunto de chaves.
- Windows: pesquisa nos repositórios de certificados raiz e de usuário em busca de certificados de cliente.

Etapa 3: Configurar a restrição

Depois que você tiver implementado os certificados do cliente nos dispositivos confiáveis, poderá ativar o acesso restrito no nível de diretório. Isso exige que o aplicativo WorkSpaces cliente valide o certificado em um dispositivo antes de permitir que um usuário faça login em um WorkSpace.

Para configurar a restrição

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecionar Diretórios.
3. Selecione o diretório e escolha Ações, Atualizar detalhes.
4. Expanda Opções de controle de acesso.
5. Em Para cada tipo de dispositivo, especifique quais dispositivos podem acessar WorkSpaces, escolha Dispositivos confiáveis.
6. Importe até dois certificados raiz. Para cada certificado raiz, faça o seguinte:
    a. Escolha Importar.
    b. Copie o corpo do certificado no formulário.
    c. Escolha Importar.
7. Especifique se outros tipos de dispositivos têm acesso WorkSpaces a.
    a. Role para baixo até a seção Other Platforms (Outras plataformas). Por padrão, os clientes WorkSpaces Linux estão desativados e os usuários podem acessá-los a WorkSpaces partir

de seus dispositivos iOS, dispositivos Android, Web Access, Chromebooks e dispositivos zero client PCoIP.

b. Selecione os tipos de dispositivos a serem ativados e limpe os tipos de dispositivo a serem desativados.

c. Para bloquear o acesso de todos os tipos de dispositivo selecionados, escolha Bloquear.

8. Escolha Atualizar e sair.

Integração do WorkSpaces com o SAML 2.0

A integração do SAML 2.0 com WorkSpaces para a autenticação de sessão de área de trabalho permite que os usuários usem suas credenciais e métodos de autenticação existentes do provedor de identidades (IdP) SAML 2.0 por meio do navegador da web padrão. Ao usar seu IdP para autenticar usuários nos WorkSpaces, é possível proteger os WorkSpaces empregando recursos do IdP, como autenticação multifator e políticas de acesso contextual.

Fluxo de trabalho de autenticação

As seguintes seções descrevem o fluxo de trabalho de autenticação iniciado pela aplicação cliente do WorkSpaces, pelo Acesso via Web do WorkSpaces e por um provedor de identidades (IdP) SAML 2.0:

- Quando o fluxo é iniciado pelo IdP. Por exemplo, quando os usuários escolhem uma aplicação no portal do usuário do IdP em um navegador da web.
- Quando o fluxo é iniciado pelo cliente do WorkSpaces. Por exemplo, quando os usuários abrem a aplicação cliente e fazem login.
- Quando o fluxo é iniciado pelo Acesso via Web do WorkSpaces. Por exemplo, quando os usuários abrem o Acesso via Web em um navegador e fazem login.

Nesses exemplos, os usuários inserem `user@example.com` para entrar no IdP. O IdP possui uma aplicação de provedor de serviços SAML 2.0 configurada para um diretório do WorkSpaces e os usuários estão autorizados na aplicação WorkSpaces SAML 2.0. Os usuários criam um WorkSpace para seus nomes de usuário, `user`, em um diretório habilitado para autenticação SAML 2.0. Além disso, os usuários instalam a aplicação cliente do WorkSpaces em seus dispositivos ou usam o Acesso via Web em um navegador da web.

Fluxo iniciado pelo provedor de identidades (IdP) com a aplicação cliente

O fluxo iniciado pelo IdP permite que os usuários registrem automaticamente a aplicação cliente do WorkSpaces em seus dispositivos sem precisar inserir um código de registro do WorkSpaces. Os usuários não fazem login em seus WorkSpaces usando o fluxo iniciado pelo IdP. A autenticação do WorkSpaces deve ter origem na aplicação cliente.

1. Os usuários fazem login no IdP usando um navegador da web.
2. Depois de entrar no IdP, eles escolhem a aplicação WorkSpaces no portal do usuário do IdP.
3. Os usuários são redirecionados para essa página no navegador e a aplicação cliente do WorkSpaces é aberta automaticamente.

4. A aplicação cliente do WorkSpaces agora está registrada e os usuários podem prosseguir com o login clicando em Continuar a fazer login no WorkSpaces.

Fluxo iniciado pelo provedor de identidades (IdP) com o Acesso via Web

O fluxo do Acesso via Web iniciado por IdP permite que os usuários registrem automaticamente os WorkSpaces por meio de um navegador da web sem precisar inserir um código de registro do WorkSpaces. Os usuários não fazem login em seus WorkSpaces usando o fluxo iniciado pelo IdP. A autenticação do WorkSpaces deve ter origem no Acesso via Web.

1. Os usuários fazem login no IdP usando um navegador da web.
2. Depois de entrar no IdP, os usuários clicam na aplicação WorkSpaces no portal do usuário do IdP.

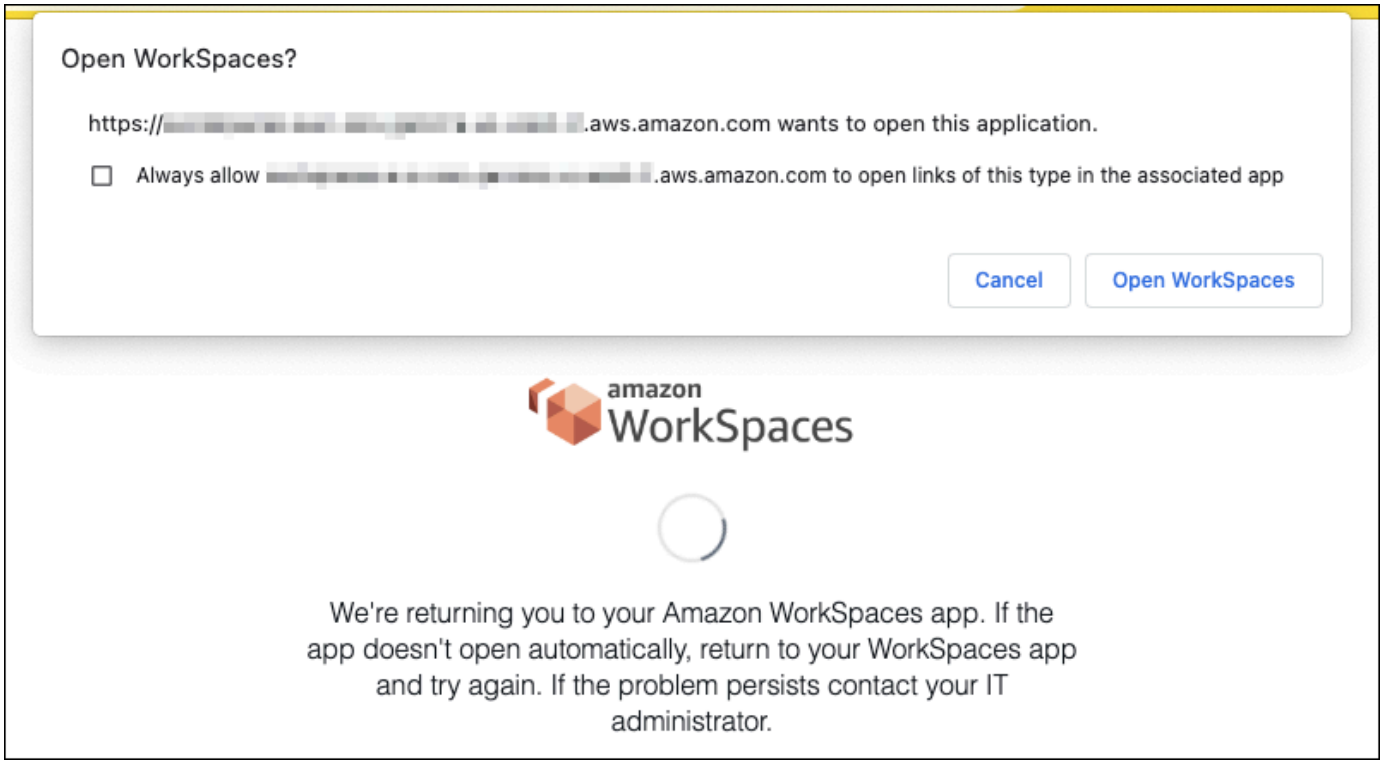
3. Os usuários são redirecionados para essa página no navegador. Para abrir WorkSpaces, escolha Amazon WorkSpaces no navegador.

4. A aplicação cliente do WorkSpaces agora está registrada e os usuários podem prosseguir com o login por meio do Acesso via Web do WorkSpaces.

Fluxo iniciado pelo cliente do WorkSpaces

O fluxo iniciado pelo cliente permite que os usuários façam login em seus WorkSpaces após entrarem em um IdP.

1. Os usuários inicializam a aplicação cliente do WorkSpaces (se ela ainda não estiver em execução) e clicam em Continuar a fazer login no WorkSpaces.
2. Os usuários são redirecionados para o navegador padrão para que façam login no IdP. Se os usuários já estiverem conectados ao IdP no navegador, eles não precisarão fazer login novamente e pularão essa etapa.
3. Depois de fazer login no IdP, os usuários são redirecionados para um pop-up. Siga as instruções para permitir que o navegador abra a aplicação cliente.



4. Os usuários são redirecionados para a aplicação cliente do WorkSpaces para que concluam o login no WorkSpace. Os nomes de usuário do WorkSpaces são preenchidos automaticamente com base na declaração SAML 2.0 do IdP. Ao usar a autenticação baseada em certificado (CBA), os usuários são automaticamente conectados.
5. Os usuários estão conectados ao WorkSpace.

Fluxo iniciado pelo Acesso via Web do WorkSpaces

O fluxo iniciado pelo Acesso via Web permite que os usuários façam login nos WorkSpaces após se conectarem a um IdP.

1. Os usuários inicializam o Acesso via Web do WorkSpaces e escolhem Fazer login.
2. Na mesma guia do navegador, os usuários são redirecionados para o portal do IdP. Se os usuários já estiverem conectados ao IdP no navegador, eles não precisarão fazer login novamente e podem pular essa etapa.
3. Depois de fazer login no IdP, os usuários são redirecionados para essa página no navegador e clicam em Fazer login no WorkSpaces.
4. Os usuários são redirecionados para a aplicação cliente do WorkSpaces para que concluam o login no WorkSpace. Os nomes de usuário do WorkSpaces são preenchidos automaticamente

com base na declaração SAML 2.0 do IdP. Ao usar a autenticação baseada em certificado (CBA), os usuários são automaticamente conectados.

5. Os usuários estão conectados ao WorkSpace.

Configurar o SAML 2.0

Ative o registro e o login WorkSpaces do aplicativo cliente WorkSpaces para seus usuários usando as credenciais do provedor de identidade (IdP) e os métodos de autenticação do SAML 2.0 configurando a federação de identidades usando o SAML 2.0. Para definir a federação de identidades usando o SAML 2.0, use o perfil do IAM e o URL de estado de retransmissão para configurar o IdP e habilitar a AWS. Isso concede aos usuários federados acesso a um WorkSpaces diretório. O estado de retransmissão é o endpoint do WorkSpaces diretório para o qual os usuários são encaminhados após o login bem-sucedido. AWS

Conteúdo

Requisitos

- A autenticação SAML 2.0 está disponível nas seguintes regiões:
  - Região Leste dos EUA (N. da Virgínia)
  - Região Oeste dos EUA (Oregon)
  - Região África (Cidade do Cabo)
  - Região Ásia-Pacífico (Mumbai)
  - Região Ásia-Pacífico (Seul)

  - Região Ásia-Pacífico (Singapura)
  - Região Ásia-Pacífico (Sydney)
  - Região Ásia-Pacífico (Tóquio)
  - Região do Canadá (Central)
  - Região Europa (Frankfurt)
  - Região Europa (Irlanda)
  - Região Europa (Londres)
  - Região América do Sul (São Paulo)
  - Região de Israel (Tel Aviv)
  - AWS GovCloud (Oeste dos EUA)
  - AWS GovCloud (Leste dos EUA)
- Para usar a autenticação SAML 2.0 com WorkSpaces, o IdP deve oferecer suporte a SSO não solicitado iniciado pelo IdP com um recurso de destino de link direto ou URL de endpoint de estado de retransmissão. Exemplos IdPs incluem ADFS, Azure AD, Duo Single Sign-On, Okta e. PingFederate PingOne Para obter mais informações, consulte a documentação do IdP.
- A autenticação do SAML 2.0 funcionará com o WorkSpaces Launch usando o Simple AD, mas isso não é recomendado, pois o Simple AD não se integra ao SAML 2.0. IdPs
- A autenticação SAML 2.0 é compatível com os seguintes WorkSpaces clientes. Outras versões do cliente não são compatíveis com a autenticação SAML 2.0. Abra o Amazon WorkSpaces Client Downloads para encontrar as versões mais recentes:
  - Aplicação cliente para Windows versão 5.1.0.3029 ou posterior
  - Cliente para macOS versão 5.x ou posterior
  - Cliente Linux para Ubuntu 22.04 versão 2024.1 ou posterior, Ubuntu 20.04 versão 24.1 ou posterior
  - Web Access

  Outras versões do cliente não poderão se conectar à autenticação WorkSpaces habilitada para SAML 2.0, a menos que o fallback esteja ativado. Para obter mais informações, consulte Habilitar a autenticação SAML 2.0 no WorkSpaces diretório.

Para step-by-step obter instruções sobre como integrar o SAML 2.0 com WorkSpaces o uso do ADFS, do Azure AD, do Duo Single Sign-On, do Okta PingFederate e do Enterprise OneLogin, consulte o PingOne Guia de implementação da autenticação Amazon WorkSpaces SAML.

Pré-requisitos

Preencha os pré-requisitos a seguir antes de configurar sua conexão do provedor de identidade (IdP) SAML 2.0 com um diretório. WorkSpaces

1. Configure seu IdP para integrar identidades de usuário do Microsoft Active Directory que é usado com o diretório. WorkSpaces Para um usuário com um WorkSpace, os atributos de SaM AccountName e e-mail para o usuário do Active Directory e os valores da declaração SAML devem corresponder para que o usuário faça login WorkSpaces usando o IdP. Para obter mais informações sobre a integração do Active Directory com seu IdP, consulte a documentação do seu IdP.
2. Configurar o IdP para estabelecer uma relação de confiança AWS.

   - Consulte Integração de provedores de soluções SAML de terceiros com AWS para obter mais informações sobre como configurar AWS a federação. Exemplos relevantes incluem a integração do IdP com o AWS IAM para acessar o console AWS de gerenciamento.
   - Usar o IdP para gerar e fazer download de um documento de metadados de federação que descreva a empresa como um IdP. Este documento XML assinado é usado para estabelecer a confiança da parte dependente. Salvar este arquivo em um local para acessar posteriormente no console do IAM.
3. Crie ou registre um diretório WorkSpaces usando o console WorkSpaces de gerenciamento. Para obter mais informações, consulte Gerenciar diretórios para WorkSpaces. A autenticação SAML 2.0 para WorkSpaces é compatível com os seguintes tipos de diretório:

   - AD Connector
   - AWS Microsoft AD gerenciado
4. Crie um WorkSpace para um usuário que possa entrar no IdP usando um tipo de diretório compatível. Você pode criar um WorkSpace usando o console WorkSpaces de gerenciamento ou a WorkSpaces API. AWS CLI Para obter mais informações, consulte Iniciar uma área de trabalho virtual usando WorkSpaces.

Etapa 1: criar um provedor de identidade SAML no IAM AWS

Primeiro, crie um SAML IdP AWS no IAM. Esse IdP define a relação de AWS confiança entre IdP e IdP de sua organização usando o documento de metadados gerado pelo software IdP em sua organização. Para obter mais informações, consulte Criação e gerenciamento de um provedor de identidade do IAM SAML (console). Para obter informações sobre como trabalhar com SAML IdPs

em AWS GovCloud (Oeste dos EUA) e AWS GovCloud (Leste dos EUA), consulte AWS Identity and Access Management.

Etapa 2: Criar um perfil do IAM de federação SAML 2.0

A seguir, crie um perfil do IAM de federação SAML 2.0. Essa etapa estabelece uma relação de confiança entre o IAM e o IdP da sua organização, o que identifica seu IdP como uma entidade confiável para federação.

Como criar um perfil do IAM para o IdP SAML

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Perfis > Criar perfil.
3. Em Tipo de perfil, escolha Federação SAML 2.0.
4. Em Provedor SAML, selecionar o IdP SAML que você criou.

   > **Important**
   >
   > Não escolha nenhum dos dois métodos de acesso SAML 2.0 (Permitir somente acesso programático ou Permitir acesso programático e pelo Console de Gerenciamento da Amazon Web Services).

5. Em Atributo, selecione SAML:sub_type.
6. Em Valor, insira `persistent`. Esse valor restringe o acesso de perfis a solicitações de streaming de usuários do SAML que incluam uma declaração do tipo de assunto de SAML com um valor persistente. Se o SAML:sub_type for persistente, o IdP envia o mesmo valor exclusivo para o elemento NameID em todas as solicitações de SAML de um usuário específico. Para obter mais informações sobre a declaração SAML:sub_type, consulte a seção Identificação exclusiva de usuários na federação baseada em SAML em Como usar a federação baseada em SAML para acesso à API a. AWS
7. Verificar as informações de confiança do SAML 2.0 confirmando a entidade confiável e a condição corretas e, em seguida, selecionar Próximo: Permissões.
8. Na página Anexar políticas de permissões, selecione Próximo: Etiquetas.
9. (Opcional) Insira uma chave e um valor para cada etiqueta que deseja adicionar. Para obter mais informações, consulte Recursos de etiquetas do IAM.
10. Ao concluir, selecione Próximo: revisão. Você pode criar e incorporar uma política em linha para esse perfil posteriormente.

11. Em Nome do perfil, insira um nome que identifique a finalidade desse perfil. Como várias entidades podem fazer referência ao perfil, não é possível editar o nome do perfil depois que ele é criado.
12. (Opcional) Em Descrição da função, insira uma descrição para o novo perfil.
13. Revisar os detalhes do perfil e selecionar Criar perfil.
14. Adicione a TagSession permissão sts: à política de confiança da sua nova função do IAM. Para obter mais informações, consulte Passar tags de sessão no AWS STS. Nos detalhes do novo perfil do IAM, selecione a guia Relações de confiança e escolha Editar relação de confiança*. Quando o editor Editar política de relacionamento de confiança for aberto, adicione a permissão sts: TagSession *, da seguinte forma:

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Principal": {
            "Federated": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:saml-provider/
IDENTITY-PROVIDER"
        },
        "Action": [
            "sts:AssumeRoleWithSAML",
            "sts:TagSession"
        ],
        "Condition": {
            "StringEquals": {
                "SAML:aud": "https://signin.aws.amazon.com/saml"
            }
        }
    }]
}
```

Substitua `IDENTITY-PROVIDER` pelo nome do IdP SAML criado na etapa 1. Depois, escolha Atualizar política de confiança.

Etapa 3: Incorporar uma política em linha para o perfil do IAM

A seguir, incorpore uma política do IAM em linha para o perfil que você criou. Quando você incorpora uma política em linha, as permissões nela não podem ser anexadas acidentalmente à entidade principal errada. A política em linha fornece aos usuários federados acesso ao WorkSpaces diretório.

> **Important**
>
> As políticas do IAM para gerenciar o acesso AWS com base no IP de origem não são compatíveis com a `workspaces:Stream` ação. Para gerenciar controles de acesso IP para WorkSpaces, use grupos de controle de acesso IP. Além disso, ao usar a autenticação SAML 2.0, você pode usar políticas de controle de acesso IP se elas estiverem disponíveis no seu IdP do SAML 2.0.

1. Nos detalhes do perfil do IAM que você criou, escolha a guia Permissões e adicione as permissões necessárias à política de permissões do perfil. O assistente Criar política será iniciado.
2. Em Criar política, selecione a guia JSON.
3. Copie e cole a política JSON a seguir na janela JSON. Em seguida, modifique o recurso inserindo seu Código AWS da Região, ID da conta e ID do diretório. Na política a seguir, `"Action": "workspaces:Stream"` está a ação que fornece aos WorkSpaces usuários permissões para se conectarem às sessões de desktop no WorkSpaces diretório.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "workspaces:Stream",
            "Resource": "arn:aws:workspaces:REGION-CODE:ACCOUNT-ID-WITHOUT-
HYPHENS:directory/DIRECTORY-ID",
            "Condition": {
                "StringEquals": {
                    "workspaces:userId": "${saml:sub}"
                }
            }
        }
```

```
    ]
}
```

`REGION-CODE`Substitua pela AWS região em que seu WorkSpaces diretório existe. `DIRECTORY-ID`Substitua pelo ID do WorkSpaces diretório, que pode ser encontrado no console WorkSpaces de gerenciamento. Para recursos em AWS GovCloud (Oeste dos EUA) ou AWS GovCloud (Leste dos EUA), use o seguinte formato para o ARN:. `arn:aws-us-gov:workspaces:REGION-CODE:ACCOUNT-ID-WITHOUT-HYPHENS:directory/DIRECTORY-ID`

4. Ao concluir, selecionar Revisar política. O Validador de política indica se há erros de sintaxe.

Etapa 4: Configurar um provedor de identidades SAML 2.0

Em seguida, dependendo do seu IdP do SAML 2.0, talvez seja necessário atualizar manualmente seu IdP para AWS confiar como provedor de serviços fazendo o upload do arquivo em https://signin.aws.amazon.com/static/saml-metadata.xml para `saml-metadata.xml` o seu IdP. Esta etapa atualiza os metadados do seu IdP. Para alguns IdPs, a atualização pode já estar configurada. Se for esse o caso, prosseguir para a próxima etapa.

Se esta atualização ainda não estiver configurada no seu IdP, revise a documentação fornecida pelo IdP para obter informações sobre como atualizar os metadados. Alguns provedores dão a opção de digitar o URL, e o IdP obtém e instala o arquivo para você. Outros exigem que você baixe o arquivo pelo URL e forneça como arquivo local.

> **Important**
>
> No momento, você também pode autorizar usuários em seu IdP a acessar WorkSpaces o aplicativo que você configurou em seu IdP. Os usuários autorizados a acessar o WorkSpaces aplicativo do seu diretório não têm automaticamente um WorkSpace criado para eles. Da mesma forma, os usuários que WorkSpace criaram um para eles não estão automaticamente autorizados a acessar o WorkSpaces aplicativo. Para se conectar com êxito a uma autenticação WorkSpace usando SAML 2.0, o usuário deve ser autorizado pelo IdP e ter WorkSpace criado uma.

Etapa 5: Criar declarações para a resposta de autenticação SAML

Em seguida, configure as informações que seu IdP envia AWS como atributos SAML em sua resposta de autenticação. Dependendo do IdP, isso já está configurado. Nesse caso, pule esta etapa e prossiga para Step 6: Configure the relay state of your federation.

Se essas informações ainda não estiverem configuradas no seu IdP, forneça o seguinte:

- NameID de assunto de SAML: o identificador exclusivo do usuário que está fazendo login. O valor deve corresponder ao nome WorkSpaces do usuário e normalmente é o AccountName atributo SaM para o usuário do Active Directory.
- Tipo de assunto de SAML (com um valor definido como `persistent`): definir o valor como `persistent` garante que o IdP envia o mesmo valor exclusivo para o elemento `NameID` em todas as solicitações SAML de determinado usuário. Garanta que a política do IAM inclua uma condição para permitir apenas solicitações SAML com sub_type de SAML definido como `persistent`, conforme descrito em Step 2: Create a SAML 2.0 federation IAM role.
- Elemento **`Attribute`** com o atributo **`Name`** definido como **`https://aws.amazon.com/SAML/Attributes/Role`**: este elemento contém um ou mais elementos `AttributeValue` que listam o perfil do IAM e o IdP SAML para o qual o usuário é mapeado pelo IdP.
  O perfil e o IdP são especificados como um par de ARNs delimitados por vírgulas.
  Um exemplo do valor esperado é`arn:aws:iam::ACCOUNTNUMBER:role/ROLENAME,arn:aws:iam::ACCOUNTNUMBER:saml-provider/PROVIDERNAME`.
- **`Attribute`**elemento com o **`Name`** atributo definido como **`https://aws.amazon.com/SAML/Attributes/RoleSessionName`** — Esse elemento contém um `AttributeValue` elemento que fornece um identificador para as credenciais AWS temporárias emitidas para o SSO. O valor no `AttributeValue` elemento deve ter entre 2 e 64 caracteres, pode conter apenas caracteres alfanuméricos, sublinhados e os seguintes caracteres: _ . : / = + - @. Não pode conter espaços. O valor geralmente é um endereço de e-mail ou um nome de entidade principal de usuário (UPN). Não deve ser um valor que inclua um espaço, como o nome de exibição de um usuário.
- Elemento **`Attribute`** com o atributo **`Name`** definido como **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`**: este elemento contém um elemento `AttributeValue` que fornece o endereço de e-mail do usuário. O valor deve corresponder ao endereço de e-mail WorkSpaces do usuário, conforme definido no WorkSpaces diretório. Os valores da etiqueta podem incluir combinações de letras, números, espaços e caracteres _ . : / = + - @. Para obter mais informações, consulte Regras para etiquetar no IAM e no AWS STS no Guia do usuário do IAM.

- Elemento **`Attribute`** com o atributo **`Name`** definido como **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:UserPrincipalName`** (opcional): este elemento contém um elemento `AttributeValue` que fornece o `userPrincipalName` do Active Directory para o usuário que está fazendo login. O valor deve ser fornecido no formato `username@domain.com`. Este parâmetro é usado com autenticação baseada em certificado como Nome Alternativo do Assunto no certificado do usuário final. Para obter mais informações, consulte Certificate-Based Authentication.
- Elemento **`Attribute`** com o atributo **`Name`** definido como **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:ObjectSid`** (opcional): este elemento contém um elemento que fornece o identificador de segurança (SID) do Active Directory para o usuário que está fazendo login. Esse parâmetro é usado com a autenticação baseada em certificado para permitir um mapeamento forte para o usuário do Active Directory. Para obter mais informações, consulte Certificate-Based Authentication.
- Elemento **`Attribute`** com o atributo **`Name`** definido como **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:ClientUserName`** (opcional): este elemento contém um elemento `AttributeValue` que fornece um formato de nome de usuário alternativo. Use esse atributo se você tiver casos de uso que exijam formatos de nome de usuário`corp\username`, como`corp.example.com\username`, ou `username@corp.example.com` para fazer login usando o WorkSpaces cliente. As chaves e os valores da etiqueta podem incluir qualquer combinação de letras, números, espaços e caracteres _ : / . + = @ -. Para obter mais informações, consulte Regras para etiquetar no IAM e no AWS STS no Guia do usuário do IAM. Para reivindicar os formatos `corp\username` ou `corp.example.com\username`, substitua \ por / na declaração SAML.
- **`Attribute`**elemento com o **`Name`** atributo definido como https://aws.amazon.com/SAML/Attributes/:Domain PrincipalTag (opcional) — Esse elemento contém um elemento `AttributeValue` que fornece o nome de domínio totalmente qualificado (FQDN) do Active Directory DNS para usuários que fazem login. Esse parâmetro é usado com autenticação baseada em certificado quando o Active Directory `userPrincipalName` do usuário contém um sufixo alternativo. O valor deve ser fornecido no`domain.com`, incluindo quaisquer subdomínios.
- **`Attribute`**elemento com o **`Name`** atributo definido como https://aws.amazon.com/SAML/Attributes/ SessionDuration (opcional) — Esse elemento contém um `AttributeValue` elemento que especifica o tempo máximo em que uma sessão de streaming federada para um usuário pode permanecer ativa antes que a reautenticação seja necessária. O valor padrão é de 3.600 segundos (60 minutos). Para obter mais informações, consulte Atributo SAML SessionDuration.

> **Note**
>
> Embora `SessionDuration` seja um atributo opcional, recomendamos incluí-lo na resposta SAML. Se você não especificar esse atributo, a duração da sessão será definida como um valor padrão de 3600 segundos (60 minutos). WorkSpaces as sessões de desktop são desconectadas após a expiração da duração da sessão.

Para obter mais informações sobre como configurar esses elementos, consulte Configuração de declarações SAML para a resposta de autenticação no Guia de usuário do IAM. Para obter informações sobre requisitos de configuração específicos do seu IdP, consulte a documentação do seu IdP.

Etapa 6: Configurar o estado de retransmissão da federação

Em seguida, use seu IdP para configurar o estado de retransmissão da sua federação para apontar para a URL do estado de retransmissão do WorkSpaces diretório. Após a autenticação bem-sucedida AWS, o usuário é direcionado ao endpoint do WorkSpaces diretório, definido como o estado de retransmissão na resposta de autenticação SAML.

O URL do estado de retransmissão tem o seguinte formato:

```
https://relay-state-region-endpoint/sso-idp?registrationCode=registration-code
```

Crie sua URL de estado de retransmissão a partir do código de registro do WorkSpaces diretório e do endpoint de estado de retransmissão associado à região na qual seu diretório está localizado. O código de registro pode ser encontrado no console WorkSpaces de gerenciamento.

Opcionalmente, se você estiver usando o redirecionamento entre regiões WorkSpaces, poderá substituir o código de registro pelo nome de domínio totalmente qualificado (FQDN) associado aos diretórios em suas regiões primária e de failover. Para obter mais informações, consulte Redirecionamento entre regiões para a Amazon. WorkSpaces Ao usar o redirecionamento entre regiões e a autenticação SAML 2.0, os diretórios primário e de failover precisam ser habilitados para a autenticação SAML 2.0 e configurados de forma independente com o IdP, usando o endpoint de estado de retransmissão associado a cada região. Isso permitirá que o FQDN seja configurado

corretamente quando os usuários registrarem seus aplicativos WorkSpaces clientes antes de fazer login e permitirá que os usuários se autentiquem durante um evento de failover.

A tabela a seguir lista os endpoints do estado de retransmissão para as regiões em que a autenticação WorkSpaces SAML 2.0 está disponível.

Regiões em que a autenticação WorkSpaces SAML 2.0 está disponível

Região	Endpoint de estado de retransmissão
Região Leste dos EUA (N. da Virgínia)	• workspaces.euc-sso.us-east-1.aws.amazon.com • (FIPS) workspaces.euc-sso-fips.us-east-1.aws.amazon.com
Região Oeste dos EUA (Oregon)	• workspaces.euc-sso.us-west-2.aws.amazon.com • (FIPS) workspaces.euc-sso-fips.us-west-2.aws.amazon.com
Região África (Cidade do Cabo)	workspaces.euc-sso.af-south-1.aws.amazon.com
Região Ásia-Pacífico (Mumbai)	workspaces.euc-sso.ap-south-1.aws.amazon.com
Região Ásia-Pacífico (Seul)	https://workspaces.ap-northeast-2.amazonaws.com
Região Ásia-Pacífico (Singapura)	https://workspaces.ap-southeast-1.amazonaws.com
Região Ásia-Pacífico (Sydney)	https://workspaces.ap-southeast-2.amazonaws.com
Região Ásia-Pacífico (Tóquio)	https://workspaces.ap-northeast-1.amazonaws.com
Região Canadá (Central)	workspaces.euc-sso.ca-central-1.aws.amazon.com

Região	Endpoint de estado de retransmissão
Região Europa (Frankfurt)	workspaces.euc-sso.eu-central-1.aws.amazon.com
Região Europa (Irlanda)	workspaces.euc-sso.eu-west-1.aws.amazon.com
Região Europa (Londres)	workspaces.euc-sso.eu-west-2.aws.amazon.com
Região América do Sul (São Paulo)	workspaces.euc-sso.sa-east-1.aws.amazon.com
Região de Israel (Tel Aviv)	workspaces.euc-sso.il-central-1.aws.amazon.com
AWS GovCloud (Oeste dos EUA)	• workspaces.euc-sso.us-gov-west-1.amazonaws-us-gov.com • (FIPS) workspaces.euc-sso-fips.us-gov-west-1.amazonaws-us-gov.com **Note** Para obter mais informações sobre, consulte o Guia do usuário da Amazon WorkSpacesAWS GovCloud (EUA).

Região	Endpoint de estado de retransmissão
AWS GovCloud (Leste dos EUA)	• workspaces.euc-sso.us-gov-east-1.amazonaws-us-gov.com • (FIPS) workspaces.euc-sso-fips.us-gov-east-1.amazonaws-us-gov.com **Note** Para obter mais informações sobre, consulte o Guia do usuário da Amazon WorkSpacesAWS GovCloud (EUA).

Etapa 7: habilitar a integração com o SAML 2.0 em seu diretório WorkSpaces

Você pode usar o WorkSpaces console para habilitar a autenticação SAML 2.0 no WorkSpaces diretório.

Habilitar integração com SAML 2.0

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecionar Diretórios.
3. Escolha o ID do diretório para o seu WorkSpaces.
4. Em Autenticação, selecione Editar.
5. Selecione Editar provedor de identidades SAML 2.0.
6. Desmarcar Habilitar autenticação SAML 2.0.
7. Em URL de acesso de usuários e Nome do parâmetro de link profundo do IdP, insira valores que sejam aplicáveis ao IdP e à aplicação configurados na etapa 1. O valor padrão para o nome do parâmetro de link direto do IdP é “RelayState“se você omitir esse parâmetro. A tabela a seguir lista URLs de acesso de usuários e nomes de parâmetros exclusivos de vários provedores de identidades para aplicações.

Domínios e endereços IP para adicionar à sua lista de permissões

Provedor de identidades	Parâmetro	URL de acesso de usuário
ADFS	`RelayState`	`https://<host>/adfs/ls/idpinitiatedsignon.aspx?RelayState=RPID=<relaying-party-uri>`
Azure AD	`RelayState`	`https://myapps.microsoft.com/signin/<app_id>?tenantId=<tenant_id>`
Duo Single Sign-On	`RelayState`	`https://<sub-domain>.sso.duosecurity.com/saml2/sp/<app_id>/sso`
Okta	`RelayState`	`https://<sub_domain>.okta.com/app/<app_name>/<app_id>/sso/saml`
OneLogin	`RelayState`	`https://<sub-domain>.onelogin.com/trust/saml2/http-post/sso/<app-id>`
JumpCloud	`RelayState`	`https://sso.jumpcloud.com/saml2/<app-id>`
Auth0	`RelayState`	`https://<DefaultTenatName>.us.auth0.com/samlp/<Client_Id>`

Provedor de identidades	Parâmetro	URL de acesso de usuário
PingFederate	`TargetResource`	`https://<host>/idp/startSSO.ping?PartnerSpId=<sp_id>`
PingOne para Enterprise	`TargetResource`	`https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=<app_id>&idpid=<idp_id>`

O URL de acesso do usuário geralmente é definido pelo provedor para SSO não solicitado iniciado pelo IdP. Um usuário pode inserir esse URL em um navegador da web para se federar diretamente à aplicação SAML. Para testar o URL de acesso do usuário e os valores dos parâmetros do seu IdP, selecionar Testar. Copie e cole o URL de teste em uma janela privada no seu navegador atual ou em outro navegador para testar o logon do SAML 2.0 sem interromper a sessão atual do console AWS de gerenciamento. Quando o fluxo iniciado pelo IdP é aberto, você pode registrar seu WorkSpaces cliente. Para obter mais informações, consulte Identity provider (IdP)-initiated flow.

8. Gerenciar as configurações de fallback marcando ou desmarcando Permitir login de clientes que não suportam SAML 2.0. Ative essa configuração para continuar fornecendo aos usuários acesso ao WorkSpaces uso de tipos ou versões de clientes que não oferecem suporte ao SAML 2.0 ou se os usuários precisarem de tempo para atualizar para a versão mais recente do cliente.

> **Note**
>
> Essa configuração permite que os usuários ignorem o SAML 2.0 e façam login usando autenticação de diretório usando versões de cliente mais antigas.

9. Para usar SAML com o cliente web, habilite o Acesso via Web. Para obter mais informações, consulte Habilitar e configurar o Amazon WorkSpaces Web Access.

> **Note**
>
> PCoIP com SAML não é compatível com o Acesso via Web.

10. Selecionar Salvar. Seu WorkSpaces diretório agora está habilitado com a integração com o SAML 2.0. Você pode usar os fluxos iniciados pelo IdP e iniciados pelo aplicativo cliente para registrar os aplicativos WorkSpaces do cliente e fazer login. WorkSpaces

Autenticação baseada em certificado

Você pode usar a autenticação baseada em certificado com WorkSpaces para remover a solicitação do usuário para a senha do domínio do Active Directory. Ao usar a autenticação baseada em certificado com um domínio do Active Directory, você pode:

- Basear-se no seu provedor de identidades SAML 2.0 para autenticar o usuário e fornecer declarações SAML que correspondam ao usuário no Active Directory.
- Habilitar uma experiência de autenticação única com menos prompts do usuário.
- Habilitar fluxos de autenticação sem senha usando seu provedor de identidades SAML 2.0.

A autenticação baseada em certificado usa AWS Private CA recursos em sua conta. AWS AWS Private CA permite a criação de hierarquias de autoridade de certificação (CA) privada, incluindo CAs raiz e subordinadas. Com AWS Private CA, você pode criar sua própria hierarquia de CA e emitir certificados com ela para autenticar usuários internos. Para mais informações, consulte o Guia do usuário do AWS Private Certificate Authority.

Ao usar AWS Private CA para autenticação baseada em certificado, WorkSpaces solicitará certificados para seus usuários automaticamente durante a autenticação da sessão. Os usuários são autenticados no Active Directory usando um cartão inteligente virtual provisionado com os certificados.

A autenticação baseada em certificado é compatível com pacotes do Windows WorkSpaces on WorkSpaces Streaming Protocol (WSP) usando os aplicativos clientes mais recentes do WorkSpaces Web Access, Windows e macOS. Abra os downloads WorkSpaces do Amazon Client para encontrar as versões mais recentes:

- Cliente Windows versão 5.5.0 ou posterior
- Cliente para macOS versão 5.6.0 ou posterior

Para obter mais informações sobre como configurar a autenticação baseada em certificados com a Amazon WorkSpaces, consulte Como configurar a autenticação baseada em certificados para a

WorkSpaces Amazon e Considerações de design em ambientes altamente regulamentados para autenticação baseada em certificados com 2.0 e. AppStream WorkSpaces

Pré-requisitos

Conclua as etapas a seguir antes de habilitar a autenticação baseada em certificado.

1. Configure seu WorkSpaces diretório com a integração do SAML 2.0 para usar a autenticação baseada em certificado. Para obter mais informações, consulte WorkSpacesIntegração com o SAML 2.0.
2. Configure o atributo `userPrincipalName` na declaração SAML. Para obter mais informações, consulte Como criar declarações para a resposta de autenticação SAML.
3. Configure o atributo `ObjectSid` na declaração SAML. Essa etapa é opcional para realizar um mapeamento robusto para o usuário do Active Directory. A autenticação baseada em certificado falhará se o atributo não corresponder ao Identificador de segurança (SID) do Active Directory do usuário especificado no `NameID` de SAML_Subject. Para obter mais informações, consulte Como criar declarações para a resposta de autenticação SAML.
4. Adicione a TagSession permissão sts: à sua política de confiança de função do IAM usada com sua configuração do SAML 2.0, caso ela ainda não esteja presente. Essa permissão é necessária para usar a autenticação baseada em certificado. Para obter mais informações, consulte Como criar um perfil do IAM para a federação do SAML 2.0.
5. Crie uma autoridade de certificação (CA) privada usando AWS Private CA se você não tiver uma configurada com seu Active Directory. AWS Private CA é necessário usar a autenticação baseada em certificado. Para obter mais informações, consulte Planejando sua AWS Private CA implantação e siga as orientações para configurar uma CA para autenticação baseada em certificado. As AWS Private CA configurações a seguir são as mais comuns para casos de uso de autenticação baseada em certificado:
   a. Opções de tipos de CA:
      i. Modo de uso de CA de certificados de curta duração (recomendado se você estiver usando a CA apenas para emitir certificados de usuário final para autenticação baseada em certificado)
      ii. Hierarquia de nível único com uma CA raiz (como alternativa, escolha uma CA subordinada se desejar integração com uma hierarquia de CAs existente)
   b. Opções de algoritmos de chave: RSA 2048
   c. Opções de nome distinto de assunto: use uma combinação de opções para identificar a CA em seu repositório de Autoridades de Certificação Raiz Confiáveis do Active Directory.

d. Opções de revogação de certificado: distribuição de CRL

> **Note**
>
> A autenticação baseada em certificado requer um ponto de distribuição de CRL on-line acessível pela área de trabalho e pelo controlador do domínio. Isso requer acesso não autenticado ao bucket do Amazon S3 configurado para entradas privadas do CA CRL ou CloudFront uma distribuição que terá acesso ao bucket do S3 se estiver bloqueando o acesso público. Para obter mais informações sobre essas opções, consulte Como planejar uma lista de revogação de certificados (CRL).

6. Marque sua CA privada com uma chave denominada `euc-private-ca` a fim de designar a CA para uso com a autenticação baseada em certificado do EUC. A chave não exige um valor. Para obter mais informações, consulte Gerenciamento de etiquetas para sua CA privada.
7. A autenticação baseada em certificado usa cartões inteligentes virtuais para o login. Seguindo as Diretrizes para habilitar o login por cartão inteligente com autoridades de certificação de terceiros no Active Directory, execute as seguintes etapas:
   - Configure controladores de domínio com um certificado de controlador de domínio para autenticar usuários de cartões inteligentes. Se você tiver uma CA corporativa dos Serviços de Certificados do Active Directory configurada em seu Active Directory, os controladores de domínio serão automaticamente registrados com certificados que permitem o login por cartão inteligente. Se você não tiver os Serviços de Certificados do Active Directory, consulte Requisitos para certificados de controlador de domínio de uma AC de terceiros. Você pode criar um certificado de controlador de domínio com o AWS Private CA. Se fizer isso, não use uma CA privada configurada para certificados de curta duração.

     > **Note**
     >
     > Se você estiver usando AWS Managed Microsoft AD, poderá configurar os Serviços de Certificados em uma instância do EC2 para atender aos requisitos de certificados de controlador de domínio. Veja, AWS Launch Wizardpor exemplo, implantações AWS Managed Microsoft AD configuradas com os Serviços de Certificados do Active Directory. AWS A CA privada pode ser configurada como subordinada à CA dos Serviços de Certificados do Active Directory ou pode ser configurada como sua própria raiz durante o uso AWS Managed Microsoft AD.
     > Uma tarefa adicional de configuração com os Serviços de AWS Managed Microsoft AD Certificados do Active Directory é criar regras de saída do grupo de segurança

VPC dos controladores para a instância EC2 que executa os Serviços de Certificados, permitindo que as portas TCP 135 e 49152-65535 habilitem o registro automático de certificados. Além disso, a instância do EC2 em execução também deve permitir acesso de entrada nessas mesmas portas das instâncias do domínio, incluindo controladores de domínio. Para obter mais informações sobre como localizar o grupo de segurança, AWS Managed Microsoft AD consulte Configurar suas sub-redes e grupos de segurança da VPC.

- No AWS Private CA console ou usando o SDK ou a CLI, selecione sua CA e, no certificado CA, exporte o certificado privado da CA. Para obter mais informações, consulte Como exportar um certificado privado.
- Publique a CA no Active Directory. Faça login em um controlador de domínio ou em uma máquina associada a um domínio. Copie o certificado privado da CA para qualquer `<path>\<file>` e execute os comandos a seguir como administrador de domínio. Você também pode usar uma política de grupo e a Microsoft PKI Health Tool (PKIView) para publicar a CA. Para obter mais informações, consulte Instruções de configuração.

```
certutil -dspublish -f <path>\<file> RootCA
certutil -dspublish -f  <path>\<file> NTAuthCA
```

Verifique se os comandos foram concluídos com êxito e, em seguida, remova o arquivo do certificado privado. Dependendo das configurações de replicação do Active Directory, pode levar vários minutos para que a CA seja publicada nos controladores de domínio e nas instâncias de área de trabalho.

Note

- É necessário que o Active Directory distribua a CA às Autoridades de Certificação Raiz Confiáveis e aos repositórios Enterprise NTAuth automaticamente para WorkSpaces desktops quando eles se juntam ao domínio.
- Os controladores de domínio do Active Directory devem estar no modo de compatibilidade para que a imposição do certificado ofereça suporte à autenticação baseada em certificados. Para obter mais informações, consulte KB5014754 — Alterações na autenticação baseada em certificado em controladores de domínio do Windows na documentação do Microsoft Support. Se você estiver usando o Microsoft

AD AWS gerenciado, consulte Definir as configurações de segurança do diretório para obter mais informações.

Habilitar a autenticação baseada em certificado

Conclua as etapas a seguir para habilitar a autenticação baseada em certificado.

1. Abra o WorkSpaces console emhttps://console.aws.amazon.com/workspaces.
2. No painel de navegação, selecionar Diretórios.
3. Escolha o ID do diretório para o seu WorkSpaces.
4. Em Autenticação, clique em Editar.
5. Clique em Editar autenticação baseada em certificado.
6. Marque Habilitar a autenticação baseada em certificado.
7. Confirme se o ARN da CA privada está associado na lista. A CA privada deve estar na mesma AWS conta e Região da AWS ser marcada com uma chave autorizada euc-private-ca a aparecer na lista.
8. Clique em Salvar alterações A autenticação baseada em certificado está habilitada.
9. Reinicie seus pacotes do Windows WorkSpaces on WorkSpaces Streaming Protocol (WSP) para que as alterações entrem em vigor. Para obter mais informações, consulte Reinicializar um WorkSpace.
10. Após a reinicialização, quando os usuários se autenticarem via SAML 2.0 usando um cliente compatível, eles não receberão mais uma solicitação para inserir a senha do domínio.

> **Note**
>
> Quando a autenticação baseada em certificado está habilitada para entrar WorkSpaces, os usuários não são solicitados a fazer a autenticação multifator (MFA), mesmo se ativada no Diretório. Ao usar a autenticação baseada em certificado, a MFA pode ser habilitada por meio do provedor de identidades SAML 2.0. Para obter mais informações sobre AWS Directory Service MFA, consulte Autenticação multifator (AD Connector) ou Habilitar autenticação multifator para. AWS Managed Microsoft AD

Gerenciar a autenticação baseada em certificado

Certificado CA

Em uma configuração comum, o certificado CA privado tem validade de 10 anos. Para obter mais informações sobre como substituir uma CA com certificado expirado ou reemitir a CA com um novo período de validade, consulte Como gerenciar o ciclo de vida da CA privada.

Certificados de usuário final

Os certificados de usuário final emitidos pela AWS Private CA para autenticação WorkSpaces baseada em certificados não exigem renovação ou revogação. Esses certificados são de curta duração. WorkSpacesemite automaticamente um novo certificado a cada 24 horas. Esses certificados de usuário final têm um período de validade mais curto do que uma distribuição típica de AWS Private CA CRL. Como resultado, os certificados de usuário final não precisam ser revogados e não aparecerão em uma CRL.

Relatórios de auditoria

Você pode criar um relatório de auditoria para listar todos os certificados que sua CA privada emitiu ou revogou. Para obter mais informações, consulte Como usar relatórios de auditoria com sua CA privada.

Registro e Monitoramento

Você pode usar AWS CloudTrailpara gravar chamadas de API para AWS Private CA by WorkSpaces. Para obter mais informações, consulte Usando CloudTrail. No Histórico de CloudTrail eventos, você pode visualizar `GetCertificate` os `IssueCertificate` nomes dos `acm-pca.amazonaws.com` eventos da fonte do evento criados pelo nome WorkSpaces `EcmAssumeRoleSession` do usuário. Esses eventos serão registrados para cada solicitação de autenticação baseada em certificado do EUC.

Habilitar o compartilhamento de PCA entre contas

Ao usar o compartilhamento entre contas de CA privada, você pode conceder permissões a outras contas para usar uma CA centralizada, o que elimina a necessidade de uma CA privada em todas as contas. A CA pode gerar e emitir certificados usando o AWS Resource Access Manager para gerenciar permissões. O compartilhamento entre contas de CA privada pode ser usado com a WorkSpaces Autenticação Baseada em Certificado (CBA) na mesma região. AWS

Para usar um recurso de CA privada compartilhado com o WorkSpaces CBA

1. Configure a CA privada para CBA em uma conta centralizada AWS . Para ter mais informações, consulte Autenticação baseada em certificado.
2. Compartilhe a CA privada com as AWS contas de recursos em que WorkSpaces os recursos utilizam o CBA seguindo as etapas em Como usar a AWS RAM para compartilhar sua CA privada do ACM entre contas. Você não precisa concluir a etapa 3 para criar um certificado. Você pode compartilhar a CA privada com AWS contas individuais ou compartilhar por meio de AWS Organizations. Para compartilhar com contas individuais, você precisa aceitar a CA privada compartilhada em sua conta de recursos usando o console do Resource Access Manager (RAM) ou as APIs. Ao configurar o compartilhamento, confirme se o compartilhamento de recursos de RAM da CA privada na conta do recurso está usando o modelo de permissão `AWSRAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority` gerenciada. Esse modelo se alinha ao modelo de PCA usado pela função de WorkSpaces serviço ao emitir certificados CBA.
3. Depois que o compartilhamento for bem-sucedido, você poderá visualizar a CA privada compartilhada usando o console da CA privada na conta do recurso.
4. Use a API ou a CLI para associar o ARN privado da CA ao CBA nas propriedades do seu diretório. WorkSpaces No momento, o WorkSpaces console não oferece suporte à seleção de ARNs de CA privados compartilhados. Exemplos de comandos da CLI:

```
aws workspaces modify-certificate-based-auth-properties –resource-id <value> –
certificate-based-auth-properties Status=<value>,CertificateAuthorityArn=<value>
```

Usar cartões inteligentes para autenticação

Os pacotes Windows e Linux WorkSpaces on WorkSpaces Streaming Protocol (WSP) permitem o uso de cartões inteligentes Common Access Card (CAC) e Personal Identity Verification (PIV) para autenticação.

A Amazon WorkSpaces oferece suporte ao uso de cartões inteligentes para autenticação pré-sessão e autenticação durante a sessão. A autenticação pré-sessão se refere à autenticação por cartão inteligente que é executada enquanto os usuários estão fazendo login em seus WorkSpaces. A autenticação em sessão se refere à autenticação executada após o login.

Por exemplo, os usuários podem usar cartões inteligentes para autenticação em sessão enquanto trabalham com navegadores e aplicações da web. Eles também podem usar cartões inteligentes para ações que exigem permissões administrativas. Por exemplo, se o usuário tiver permissões administrativas no Linux WorkSpace, ele poderá usar cartões inteligentes para se autenticar ao executar `sudo sudo -i` comandos.

Conteúdo

Requisitos

- É necessário um diretório do Active Directory Connector (AD Connector) para a autenticação pré-sessão. O AD Connector usa autenticação mútua de Transport Layer Security (TLS mútuo) baseada em certificado para autenticar usuários no Active Directory usando um certificado de cartão inteligente baseado em hardware ou software. Para obter mais informações sobre como configurar o AD Connector e o diretório on-premises, consulte Configuração do diretório.
- Para usar um cartão inteligente com Windows ou Linux WorkSpace, o usuário deve usar o cliente Amazon WorkSpaces Windows versão 3.1.1 ou posterior ou o cliente WorkSpaces macOS versão 3.1.5 ou posterior. Para obter mais informações sobre o uso de cartões inteligentes com os clientes Windows e macOS, consulte Smart Card Support no Amazon WorkSpaces User Guide.
- Os certificados de CA raiz e cartão inteligente devem atender a determinados requisitos. Para obter mais informações, consulte Habilitar a autenticação mTLS no AD Connector para usar com cartões inteligentes no Guia de administração do AWS Directory Service e Requisitos de certificado na documentação da Microsoft.

  Além desses requisitos, os certificados de usuário empregados para autenticação por cartão inteligente na Amazon WorkSpaces devem incluir os seguintes atributos:

  - O usuário do AD userPrincipalName (UPN) no campo subjectAltName (SAN) do certificado. Recomendamos emitir certificados de cartão inteligente para o UPN padrão do usuário.
  - O atributo de uso estendido de chave (EKU) para autenticação de cliente (1.3.6.1.5.5.7.3.2).
  - O atributo EKU para login com cartão inteligente (1.3.6.1.4.1.311.20.2.2).

- Para autenticação pré-sessão, o protocolo OCSP (Protocolo de status de certificado on-line) é necessário para verificação de revogação do certificado. Para autenticação em sessão, o OCSP é recomendado, mas não obrigatório.

Limitações

- Somente o aplicativo cliente WorkSpaces Windows versão 3.1.1 ou posterior e o aplicativo cliente macOS versão 3.1.5 ou posterior são atualmente suportados para autenticação por cartão inteligente.
- O aplicativo cliente WorkSpaces Windows 3.1.1 ou posterior oferece suporte a cartões inteligentes somente quando o cliente está sendo executado em uma versão de 64 bits do Windows.
- Atualmente, WorkSpaces o Ubuntu não oferece suporte à autenticação por cartão inteligente.
- Somente os diretórios do AD Connector são atualmente compatíveis com a autenticação por cartão inteligente.
- A autenticação em sessão está disponível em todas as regiões em que o WSP é compatível. A autenticação pré-sessão está disponível nas seguintes regiões:
  - Região Ásia-Pacífico (Sydney)
  - Região Ásia-Pacífico (Tóquio)
  - Região Europa (Irlanda)
  - AWS GovCloud Região (Leste dos EUA)
  - AWS GovCloud Região (Oeste dos EUA)
  - Região Leste dos EUA (N. da Virgínia)
  - Região Oeste dos EUA (Oregon)
- Para autenticação em sessão e autenticação pré-sessão no Linux ou no Windows WorkSpaces, atualmente, somente um cartão inteligente é permitido por vez.
- Para a autenticação pré-sessão, não há suporte para habilitar a autenticação por cartão inteligente e a autenticação de login no mesmo diretório.
- Somente placas CAC e PIV são compatíveis no momento. Outros tipos de cartões inteligentes baseados em hardware ou software também podem funcionar, mas não foram totalmente testados para uso com o WSP.

Configuração do diretório

Para habilitar a autenticação por cartão inteligente, você deve configurar o diretório do AD Connector e o diretório on-premises da maneira a seguir.

Configuração do diretório do AD Connector

Antes de começar, verifique se o diretório do AD Connector foi configurado conforme descrito nos Pré-requisitos do AD Connector no Guia de administração do AWS Directory Service . Especificamente, verifique se você abriu as portas necessárias no firewall.

Para concluir a configuração do diretório do AD Connector, siga as instruções em Habilitar a autenticação mTLS no AD Connector para usar com cartões inteligentes no Guia de administração do AWS Directory Service .

> **Note**
>
> A autenticação por cartão inteligente exige que a Delegação Restrita Kerberos (KCD) funcione corretamente. O KCD exige que a parte do nome de usuário da conta de serviço do AD Connector corresponda ao SaM AccountName do mesmo usuário. Um SaM não AccountName pode exceder 20 caracteres.

Configuração de diretórios on-premises

Além de configurar o diretório do AD Connector, você também deve garantir que os certificados emitidos para os controladores de domínio do diretório on-premises tenham o conjunto de uso estendido de chave (EKU) “Autenticação KDC”. Para fazer isso, use o modelo de certificado de autenticação Kerberos padrão dos Serviços de Domínio do Active Directory (AD DS). Não use um modelo de certificado de Controlador de domínio ou um modelo de certificado de Autenticação do controlador de domínio, pois esses modelos não contêm as configurações necessárias para a autenticação por cartão inteligente.

Ativar cartões inteligentes para Windows WorkSpaces

Para obter orientações gerais sobre como habilitar a autenticação por cartão inteligente no Windows, consulte Diretrizes para habilitar o logon de cartão inteligente com autoridades de certificação de terceiros na documentação da Microsoft.

Como detectar a tela de bloqueio do Windows e desconectar a sessão

Para permitir que os usuários desbloqueiem o Windows WorkSpaces habilitado para autenticação pré-sessão com cartão inteligente quando a tela está bloqueada, você pode ativar a detecção da tela de bloqueio do Windows nas sessões dos usuários. Quando a tela de bloqueio do Windows é detectada, a WorkSpace sessão é desconectada e o usuário pode se reconectar do WorkSpaces cliente usando seu cartão inteligente.

Você pode habilitar a desconexão da sessão quando a tela de bloqueio do Windows for detectada usando as configurações de Política de grupo. Para ter mais informações, consulte Habilitar ou desabilitar a desconexão da sessão ao bloquear a tela para WSP.

Como habilitar a autenticação em sessão ou pré-sessão

Por padrão, o Windows não WorkSpaces está habilitado para oferecer suporte ao uso de cartões inteligentes para autenticação pré-sessão ou durante a sessão. Se necessário, você pode habilitar a autenticação em sessão e pré-sessão para Windows WorkSpaces usando as configurações da Política de Grupo. Para ter mais informações, consulte Habilitar ou desabilitar o redirecionamento de cartão inteligente para WSP.

Para usar a autenticação pré-sessão, além de atualizar as configurações de Política de grupo, você também deve habilitar a autenticação pré-sessão por meio das configurações de diretório do AD Connector. Para obter mais informações, siga as instruções em Habilitar a autenticação mTLS no AD Connector para usar em cartões inteligentes no Guia de administração do AWS Directory Service .

Como permitir que os usuários usem cartões inteligentes em um navegador

Se os usuários estiverem usando o Chrome como navegador, nenhuma configuração especial será necessária para usar cartões inteligentes.

Se os usuários estiverem usando o Firefox como navegador, você pode permitir que eles usem cartões inteligentes no Firefox por meio da Política de grupo. Você pode usar esses modelos de Política de Grupo do Firefox no GitHub.

Por exemplo, você pode instalar a versão de 64 bits do OpenSC para Windows, para oferecer suporte ao PKCS #11 e, em seguida, usar a configuração de Política de grupo a seguir, onde *NAME_OF_DEVICE* é o valor que você deseja usar para identificar o PKCS #11, como `OpenSC`, e onde *PATH_TO_LIBRARY_FOR_DEVICE* é o caminho para o módulo PKCS #11. Esse caminho deve apontar para uma biblioteca com uma extensão .DLL, como `C:\Program Files\OpenSC Project\OpenSC\pkcs11\onepin-opensc-pkcs11.dll`.

```
Software\Policies\Mozilla\Firefox\SecurityDevices\NAME_OF_DEVICE
 = PATH_TO_LIBRARY_FOR_DEVICE
```

Tip

Se estiver usando o OpenSC, você também pode carregar o módulo OpenSC `pkcs11` no Firefox executando o programa `pkcs11-register.exe`. Para executar esse programa, clique duas vezes no arquivo em `C:\Program Files\OpenSC Project\OpenSC\tools\pkcs11-register.exe` ou abra uma janela do prompt de comando e execute o seguinte comando:

```
"C:\Program Files\OpenSC Project\OpenSC\tools\pkcs11-register.exe"
```

Para verificar se o módulo OpenSC `pkcs11` foi carregado no Firefox, faça o seguinte:

1. Se o Firefox já estiver em execução, feche-o.
2. Abra o Firefox. Selecione o botão de menu

   no canto superior direito e, em seguida, selecione Opções.
3. Na página about:preferences, no painel de navegação esquerdo, selecione Privacidade e segurança.
4. Em Certificados, selecione Dispositivos de segurança.
5. Na caixa de diálogo Gerenciador de dispositivos, você deve ver o Framework de cartão inteligente OpenSC (0.21) na navegação à esquerda, e ela deve ter os seguintes valores ao selecioná-la:

   Módulo: `OpenSC smartcard framework (0.21)`

   Caminho: `C:\Program Files\OpenSC Project\OpenSC\pkcs11\onepin-opensc-pkcs11.dll`

Solução de problemas

Para obter informações sobre como solucionar problemas de cartões inteligentes, consulte Problemas de certificado e configuração na documentação da Microsoft.

Algumas questões comuns que podem causar problemas:

- Mapeamento incorreto dos slots para os certificados.
- Ter vários certificados no cartão inteligente que possam corresponder ao usuário. Os certificados são correspondidos de acordo com os seguintes critérios:
  - A CA raiz para o certificado.
  - Os campos <KU> e <EKU> do certificado.
  - O UPN no assunto do certificado.
- Ter vários certificados que tenham <EKU>msScLogin no uso de chave.

Em geral, é melhor ter apenas um certificado para autenticação por cartão inteligente que esteja mapeado no primeiro slot do cartão inteligente.

As ferramentas para gerenciar os certificados e as chaves no cartão inteligente (como remover ou remapear os certificados e as chaves) podem ser específicas do fabricante. Para obter mais informações, consulte a documentação fornecida pelo fabricante dos seus cartões inteligentes.

Ativar cartões inteligentes para Linux WorkSpaces

> **Note**
>
> Atualmente, o Linux WorkSpaces no WSP tem as seguintes limitações:
>
> - Área de transferência, entrada de áudio, entrada de vídeo e redirecionamento de fuso horário não são compatíveis.
> - Não há compatibilidade para vários monitores.
> - Você deve usar o aplicativo cliente WorkSpaces do Windows para se conectar ao Linux WorkSpaces no WSP.

Para habilitar o uso de cartões inteligentes no Linux WorkSpaces, você precisa incluir um arquivo de certificado CA raiz no formato PEM na WorkSpace imagem.

Como obter o certificado CA raiz

Você pode obter o certificado CA raiz de várias formas:

- Você pode usar um certificado CA raiz operado por uma autoridade de certificação de terceiros.

- Você pode exportar seu próprio certificado CA raiz usando o site de inscrição web, que é `http://ip_address/certsrv` ou`http://fqdn/certsrv`, onde *`ip_address`* e *`fqdn`* são o endereço IP e o nome de domínio totalmente qualificado (FQDN) do servidor de certificação CA raiz. Para obter mais informações sobre como usar o site de inscrição web, consulte Como exportar o certificado de autoridade de certificação raiz na documentação da Microsoft.
- Você pode usar o procedimento a seguir para exportar o certificado de CA raiz de um servidor de certificação de CA raiz que esteja executando os Serviços de Certificados do Active Directory (AD CS). Para obter informações sobre a instalação do AD CS, consulte Instalar a autoridade de certificação na documentação da Microsoft.

  1. Faça login no servidor CA raiz usando uma conta de administrador.
  2. No menu Iniciar do Windows, abra uma janela do prompt de comando (Iniciar > Sistema Windows > Prompt de comando).
  3. Use o seguinte comando para exportar o certificado de CA raiz para um novo arquivo, onde *`rootca`*`.cer` é o nome do arquivo:

     ```
     certutil -ca.cert rootca.cer
     ```

     Para obter mais informações sobre como executar o certutil, consulte certutil na documentação da Microsoft.
  4. Use o comando OpenSSL a seguir para converter o certificado de CA raiz exportado do formato DER para o formato PEM, em que *`rootca`* é o nome do certificado. Para obter mais informações sobre OpenSSL, consulte www.openssl.org.

     ```
     openssl x509 -inform der -in rootca.cer -out /tmp/rootca.pem
     ```

Para adicionar seu certificado CA raiz ao seu Linux WorkSpaces

Para ajudá-lo a habilitar cartões inteligentes, adicionamos o script `enable_smartcard` aos nossos pacotes Amazon Linux WSP. Esse script executa as seguintes ações:

- Importe o certificado de CA raiz para o banco de dados Network Security Services (NSS).
- Instala o módulo `pam_pkcs11` para autenticação do módulo de autenticação conectável (PAM).
- Executa uma configuração padrão, que inclui a ativação `pkinit` durante o WorkSpace provisionamento.

O procedimento a seguir explica como usar o `enable_smartcard` script para adicionar seu certificado CA raiz ao Linux WorkSpaces e habilitar cartões inteligentes para o Linux WorkSpaces.

1. Crie um novo Linux WorkSpace com o protocolo WSP ativado. Ao iniciar o WorkSpace no WorkSpaces console da Amazon, na página Selecionar pacotes, certifique-se de selecionar WSP para o protocolo e, em seguida, selecione um dos pacotes públicos do Amazon Linux 2.
2. No novo WorkSpace, execute o comando a seguir como root, onde *`pem-path`* está o caminho para o arquivo de certificado CA raiz no formato PEM.

   ```
   /usr/lib/skylight/enable_smartcard --ca-cert pem-path
   ```

   > **Note**
   >
   > O Linux WorkSpaces pressupõe que os certificados nos cartões inteligentes sejam emitidos para o nome principal de usuário (UPN) padrão do usuário, como, por exemplo*`sAMAccountName`*@*`domain`*, onde *`domain`* está um nome de domínio totalmente qualificado (FQDN).
   > Para usar sufixos UPN alternativos, `run /usr/lib/skylight/enable_smartcard --help` para obter mais informações. O mapeamento para sufixos UPN alternativos é exclusivo para cada usuário. Portanto, esse mapeamento deve ser realizado individualmente no de cada usuário WorkSpace.

3. (Opcional) Por padrão, todos os serviços estão habilitados para usar a autenticação por cartão inteligente no Linux WorkSpaces. Para limitar a autenticação por cartão inteligente para serviços específicos, você deve editar `/etc/pam.d/system-auth`. Remova o comentário da linha `auth` para `pam_succeed_if.so` e edite a lista de serviços conforme necessário.

   Depois o comentário da linha `auth` for removido, para permitir que um serviço use a autenticação por cartão inteligente, você deve adicioná-lo à lista. Para fazer com que um serviço use somente autenticação por senha, é necessário removê-lo da lista.
4. Execute quaisquer personalizações adicionais no. WorkSpace Por exemplo, talvez você queira adicionar uma política em todo o sistema para permitir que os usuários usem cartões inteligentes no Firefox. (Os usuários do Chrome devem habilitar cartões inteligentes em seus próprios clientes. Para obter mais informações, consulte Smart Card Support no Amazon WorkSpaces User Guide.)
5. Crie uma WorkSpace imagem e um pacote personalizados a partir do WorkSpace.

6. Use o novo pacote personalizado para lançá-lo WorkSpaces para seus usuários.

Como permitir que os usuários usem cartões inteligentes no Firefox

Você pode permitir que seus usuários usem cartões inteligentes no Firefox adicionando uma SecurityDevices política à sua WorkSpace imagem do Linux. Para obter mais informações sobre como adicionar políticas de todo o sistema ao Firefox, consulte os modelos de políticas da Mozilla em. GitHub

1. No WorkSpace que você está usando para criar sua WorkSpace imagem, crie um novo arquivo chamado `policies.json` in`/usr/lib64/firefox/distribution/`.
2. No arquivo JSON, adicione a SecurityDevices política a seguir, onde *`NAME_OF_DEVICE`* está o valor que você deseja usar para identificar o `pkcs` módulo. Por exemplo, é possível usar um valor como `"OpenSC"`:

```
{
    "policies": {
        "SecurityDevices": {
            "NAME_OF_DEVICE": "/usr/lib64/opensc-pkcs11.so"
        }
    }
}
```

Solução de problemas

Para solucionar problemas, recomendamos adicionar o utilitário `pkcs11-tools`. Esse utilitário permite que você execute as seguintes ações:

- Liste cada cartão inteligente.
- Liste os slots em cada cartão inteligente.
- Liste os certificados em cada cartão inteligente.

Algumas questões comuns que podem causar problemas:

- Mapeamento incorreto dos slots para os certificados.
- Ter vários certificados no cartão inteligente que possam corresponder ao usuário. Os certificados são correspondidos de acordo com os seguintes critérios:

  - A CA raiz para o certificado.
  - Os campos <KU> e <EKU> do certificado.
  - O UPN no assunto do certificado.
- Ter vários certificados que tenham <EKU>msScLogin no uso de chave.

Em geral, é melhor ter apenas um certificado para autenticação por cartão inteligente que esteja mapeado no primeiro slot do cartão inteligente.

As ferramentas para gerenciar os certificados e as chaves no cartão inteligente (como remover ou remapear os certificados e as chaves) podem ser específicas do fabricante. Ferramentas adicionais que você pode usar para trabalhar com cartões inteligentes são:

- `opensc-explorer`
- `opensc-tool`
- `pkcs11_inspect`
- `pkcs11_listcerts`
- `pkcs15-tool`

Como habilitar log de depuração

Para solucionar os problemas de configuração `pam_pkcs11` e `pam-krb5`, você pode ativar o log de depuração.

1. No arquivo `/etc/pam.d/system-auth-ac`, edite a ação `auth` e altere o parâmetro `nodebug` de `pam_pksc11.so` para `debug`.
2. No arquivo `/etc/pam_pkcs11/pam_pkcs11.conf`, altere `debug = false;` para `debug = true;`. A opção `debug` se aplica separadamente a cada módulo mapeador, portanto, talvez seja necessário alterá-la diretamente na seção `pam_pkcs11` e também na seção apropriada do mapeador (por padrão, é `mapper generic`).
3. No arquivo `/etc/pam.d/system-auth-ac`, edite a ação `auth` e adicione o parâmetro `debug` ou `debug_sensitive` para `pam_krb5.so`.

Depois de habilitar o log de depuração, o sistema imprime mensagens de depuração `pam_pkcs11` diretamente no terminal ativo. As mensagens de `pam_krb5` estão registradas em `/var/log/secure`.

Para verificar a qual nome de usuário um certificado de cartão inteligente está mapeado, use o seguinte comando `pklogin_finder`:

```
sudo pklogin_finder debug config_file=/etc/pam_pkcs11/pam_pkcs11.conf
```

Quando solicitado, digite o PIN do cartão inteligente. `pklogin_finder` gera como saída em `stdout` o nome de usuário no certificado do cartão inteligente no formato *`NETBIOS`*`\`*`username`*. Esse nome de usuário deve corresponder ao WorkSpace nome de usuário.

Nos Serviços de Domínio do Active Directory (AD DS), o nome de domínio NetBIOS é o nome de domínio anterior ao Windows 2000. Normalmente (mas nem sempre), o nome de domínio NetBIOS é o subdomínio do nome de domínio do Sistema de Nomes de Domínio (DNS). Por exemplo, se o nome do domínio DNS for `example.com`, o nome de domínio NetBIOS geralmente é `EXAMPLE`. Se o nome do domínio DNS for `corp.example.com`, o nome de domínio NetBIOS geralmente é `CORP`.

Por exemplo, para o usuário `mmajor` no domínio `corp.example.com`, a saída de `pklogin_finder` é `CORP\mmajor`.

> **Note**
>
> Se você receber a mensagem `"ERROR:pam_pkcs11.c:504: verify_certificate() failed"`, essa mensagem indica que `pam_pkcs11` encontrou um certificado no cartão inteligente que corresponde aos critérios do nome de usuário, mas que não está vinculado a um certificado de CA raiz reconhecido pela máquina. Quando isso acontece, `pam_pkcs11` gera a mensagem acima e, em seguida, tenta o próximo certificado. Isso permite a autenticação somente se encontrar um certificado que corresponda ao nome de usuário e esteja encadeado a um certificado de CA raiz reconhecido.

Para solucionar problemas de configuração `pam_krb5`, você pode invocar manualmente `kinit` no modo de depuração com o seguinte comando:

```
KRB5_TRACE=/dev/stdout kinit -V
```

Esse comando deve obter com sucesso um tíquete de concessão de tíquetes (TGT) Kerberos. Se isso falhar, tente adicionar explicitamente o nome de entidade principal correto do Kerberos ao comando. Por exemplo, para o usuário `mmajor` no domínio `corp.example.com`, use este comando:

```
KRB5_TRACE=/dev/stdout kinit -V mmajor
```

Se esse comando for bem-sucedido, o problema provavelmente está no mapeamento do nome de WorkSpace usuário para o nome principal do Kerberos. Verifique a seção `[appdefaults]/pam/mappings` no arquivo `/etc/krb5.conf`.

Se esse comando não for bem-sucedido, mas um comando `kinit` baseado em senha tiver sucesso, verifique as configurações relacionadas a `pkinit_` no arquivo `/etc/krb5.conf`. Por exemplo, se o cartão inteligente possuir mais de um certificado, talvez seja necessário fazer alterações no `pkinit_cert_match`.

Forneça acesso à Internet a partir do seu WorkSpace

Você WorkSpaces deve ter acesso à Internet para poder instalar atualizações no sistema operacional e implantar aplicativos. Você pode usar uma das opções a seguir para permitir que você, WorkSpaces em uma nuvem privada virtual (VPC), acesse a Internet.

Opções

- Inicie suas WorkSpaces sub-redes privadas e configure um gateway NAT em uma sub-rede pública em sua VPC.
- Inicie seu WorkSpaces em sub-redes públicas e atribua automaticamente ou manualmente endereços IP públicos ao seu. WorkSpaces

Para obter mais informações sobre essas opções, consulte as seções correspondentes em Configurar uma VPC para WorkSpaces.

Com qualquer uma dessas opções, você deve garantir que o grupo de segurança do seu WorkSpaces permita tráfego de saída nas portas 80 (HTTP) e 443 (HTTPS) para todos os destinos (`0.0.0.0/0`).

Biblioteca de extras do Amazon Linux

Se você estiver usando o repositório Amazon Linux, seu Amazon Linux WorkSpaces deve ter acesso à Internet ou você deve configurar VPC endpoints para esse repositório e para o repositório principal do Amazon Linux. Para obter mais informações, consulte a seção Exemplo: como ativar o acesso aos repositórios da AMI do Amazon Linux em Endpoints do Amazon S3. Os repositórios da Amazon

Linux AMI são buckets do Amazon S3 em cada região. Se desejar que as instâncias em sua VPC acessem os repositórios por meio de um endpoint, crie uma política de endpoint que permita acesso a esses buckets. A política a seguir permite acesso aos repositórios do Amazon Linux.

```
{
  "Statement": [
    {
        "Sid": "AmazonLinux2AMIRepositoryAccess",
        "Principal": "*",
        "Action": [
            "s3:GetObject"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::amazonlinux.*.amazonaws.com/*"
        ]
    }
  ]
}
```

Grupos de segurança para seu WorkSpaces

Quando você registra um diretório com WorkSpaces, ele cria dois grupos de segurança, um para controladores de diretório e outro para WorkSpaces o diretório. O grupo de segurança para controladores de diretório tem um nome que consiste no identificador de diretório seguido por _controllers (por exemplo, d-12345678e1_controllers). O grupo de segurança de WorkSpaces tem um nome que consiste no identificador de diretório seguido por _WorkspacesMembers (por exemplo, D-123456FC11_WorkspacesMembers).

> **Warning**
>
> Evite modificar, excluir ou desanexar os grupos de segurança _controllers e _workspacesMembers. Tenha cuidado ao modificar ou excluir esses grupos de segurança, visto que não é possível recriá-los e adicioná-los novamente depois de terem sido modificados ou excluídos. Para obter mais informações, consulte Grupos de segurança do Amazon EC2 para instâncias do Linux ou Grupos de segurança do Amazon EC2 para instâncias do Windows.

Você pode adicionar um grupo WorkSpaces de segurança padrão a um diretório. Depois de associar um novo grupo de segurança a um WorkSpaces diretório, os novos WorkSpaces que você iniciar ou os existentes WorkSpaces que você reconstruir terão o novo grupo de segurança. Você também pode adicionar esse novo grupo de segurança padrão aos existentes WorkSpaces sem reconstruí-los, conforme explicado posteriormente neste tópico.

Quando você associa vários grupos de segurança a um WorkSpaces diretório, as regras de cada grupo de segurança são efetivamente agregadas para criar um conjunto de regras. Recomendamos que você condense as regras do grupo de segurança o máximo possível.

Para obter mais informações sobre grupos de segurança, consulte Security Groups for Your VPC no Guia do usuário do Amazon VPC.

Para adicionar um grupo de segurança a um WorkSpaces diretório

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecionar Diretórios.
3. Selecione o diretório e escolha Ações, Atualizar detalhes.
4. Expanda Security Group e selecione um security group.
5. Escolha Atualizar e sair.

Para adicionar um grupo de segurança a um existente WorkSpace sem reconstruí-lo, você atribui o novo grupo de segurança à interface de rede elástica (ENI) do. WorkSpace

Para adicionar um grupo de segurança a um existente WorkSpace

1. Encontre o endereço IP de cada um WorkSpace que precisa ser atualizado.
   a. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
   b. Expanda cada um WorkSpace e registre seu endereço WorkSpace IP.
2. Encontre o ENI para cada um WorkSpace e atualize sua atribuição de grupo de segurança.
   a. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
   b. Em Rede e segurança, escolha Interfaces de rede.
   c. Procure o primeiro endereço IP que registrou na etapa 1.
   d. Selecione a ENI associada ao endereço IP, escolha Ações e selecione Alterar grupos de segurança.

e. Selecione o novo grupo de segurança e escolha Salvar.

f. Repita esse processo conforme necessário para qualquer outro WorkSpaces.

Grupos de controle de acesso de IP dos WorkSpaces

O Amazon WorkSpaces permite que você controle de quais endereços IP seus WorkSpaces podem ser acessados. Ao usar grupos de controle baseados em endereço IP, é possível definir e gerenciar os endereços IP confiáveis e só permitir que os usuários acessem seus WorkSpaces quando estiverem conectados a uma rede confiável.

Um grupo de controle de acesso IP atua como um firewall virtual que controla os endereços IP de onde os usuários têm permissão para acessar seus WorkSpaces. Para especificar os intervalos de endereços CIDR, adicione regras ao grupo de controle de acesso de IP, depois associe o grupo ao diretório. Você pode associar cada grupo de controle de acesso IP com um ou mais diretórios. Você pode criar até 100 grupos de controle de acesso de IP por região por conta da AWS. No entanto, é possível associar somente até 25 grupos de controle de acesso IP com um único diretório.

Um grupo de controle de acesso de IP padrão é associado a cada diretório. Esse grupo padrão inclui uma regra padrão que permite que os usuários acessem seus WorkSpaces de qualquer lugar. Não é possível modificar o grupo de controle de acesso de IP padrão para o diretório. Se você não associar um grupo de controle de acesso de IP a um diretório, o grupo padrão será usado. Se você associar um grupo de controle de acesso IP com um diretório, o grupo de controle de acesso IP padrão é desassociado.

Para especificar os endereços IP públicos e intervalos de endereços IP para suas redes confiáveis, adicione regras para seus grupos de controle de acesso IP. Se os usuários acessam seus WorkSpaces por meio de um gateway NAT ou VPN, você deve criar regras que permitam o tráfego de endereços IP públicos para o gateway NAT ou VPN.

> **Note**
>
> - Os grupos de controle de acesso IP não permitem o uso de endereços IP dinâmicos para NATs. Se você estiver usando um NAT, configure-o para usar um endereço IP estático em vez de um endereço IP dinâmico. Verifique se o NAT roteia todo o tráfego UDP por meio do mesmo endereço IP estático durante toda a sessão do WorkSpaces.
> - Os grupos de controle de acesso de IP controlam os endereços IP dos quais os usuários podem conectar suas sessões de streaming aos WorkSpaces. Os usuários ainda podem

executar algumas funcionalidades, como reiniciar, recompilar e desligar, de qualquer endereço IP usando as APIs públicas do Amazon WorkSpaces.

É possível usar esse recurso com o Acesso via Web, clientes zero PCoIP e aplicações cliente para macOS, iPad, Windows, Chromebook e Android.

Criar um grupo de controle de acesso de IP

Você pode criar um grupo de controle de acesso IP conforme indicado a seguir. Cada grupo de controle de acesso IP pode conter até 10 regras.

Para criar um grupo de controle de acesso IP

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione IP Access Controls (Controles de acesso IP).
3. Escolha Create IP Group (Criar grupo de IP).
4. Na caixa de diálogo Create IP Group (Criar grupo de IP), insira um nome e uma descrição para o grupo e escolha Create (Criar).
5. Selecione o grupo e escolha Edit (Editar).
6. Para cada endereço IP, escolha Add Rule (Adicionar regra). Para Source (Origem), insira o endereço IP ou intervalo de endereços IP. Em Description (Descrição), insira uma descrição. Quando terminar de adicionar regras, escolha Save (Salvar).

Associar um grupo de controle de acesso de IP a um diretório

Você pode associar um grupo de controle de acesso IP a um diretório para garantir que os WorkSpaces sejam acessados apenas de redes confiáveis.

Se você associar um grupo de controle de acesso IP, que não tem regras, a um diretório, ele bloqueia todo o acesso a todos os WorkSpaces.

Para associar um grupo de controle de acesso IP a um diretório

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione Directories (Diretórios).

3. Selecione o diretório e escolha Ações, Atualizar detalhes.
4. Expanda IP Access Control Groups (Grupos de controle de acesso IP) e selecione um ou mais grupos de controle de acesso IP.
5. Escolha Atualizar e sair.

Copiar um grupo de controle de acesso de IP

Você pode usar um grupo de controle de acesso IP existente como base para a criação de um novo.

Para criar um grupo de controle de acesso IP a partir de um existente

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione IP Access Controls (Controles de acesso IP).
3. Selecione o grupo e escolha Actions (Ações), Copy to New (Copiar para novo).
4. Na caixa de diálogo Copy IP Group (Copiar grupo de IP), insira um nome e uma descrição para o novo grupo e escolha Copy Group (Copiar grupo).
5. (Opcional) Para modificar as regras copiadas do grupo original, selecione o novo grupo e escolha Edit (Editar). Adicione, atualize ou remova regras conforme necessário. Escolha Save (Salvar).

Excluir um grupo de controle de acesso de IP

Você pode excluir uma regra de um grupo de controle de acesso IP a qualquer momento. Se você remover uma regra que foi usada para permitir uma conexão com um WorkSpace, o usuário é desconectado do WorkSpace.

Antes de excluir um grupo de controle de acesso IP, você deve desassociá-lo a partir de qualquer diretório.

Para excluir um grupo de controle de acesso IP

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione Directories (Diretórios).
3. Para cada diretório associado ao grupo de controle de acesso IP, selecione o diretório e escolha Actions (Ações), Update Details (Atualizar detalhes). Expanda IP Access Control Groups

(Grupos de controle de acesso IP), desmarque a caixa de seleção do grupo de controle de acesso IP e escolha Update and Exit (Atualizar e sair).

4. No painel de navegação, selecione IP Access Controls (Controles de acesso IP).
5. Selecione o grupo e escolha Actions (Ações), Delete IP Group (Excluir grupo de IP).

Configurar clientes zero PCoIP para WorkSpaces

Os clientes zero PCoIP são compatíveis somente com pacotes de WorkSpaces que estão usando o protocolo PCoIP.

Se o dispositivo Zero Client tiver firmware versão 6.0.0 ou posterior, seus usuários poderão se conectar aos seus WorkSpaces diretamente. Quando os usuários estão se conectando diretamente aos WorkSpaces usando um dispositivo cliente zero, recomendamos usar a autenticação multifator (MFA) com seu diretório de WorkSpaces. Para obter mais informações sobre como usar a MFA com seu diretório, consulte a seguinte documentação:

- AWS Managed Microsoft AD: Enable multi-factor authentication for AWS Managed Microsoft AD no Guia de administração do AWS Directory Service
- AD Connector: Enable multi-factor authentication for AD Connector no Guia de administração do AWS Directory Service e Autenticação multifator (AD Connector)
- Domínios confiáveis: Enable multi-factor authentication for AWS Managed Microsoft AD no Guia de administração do AWS Directory Service
- Simple AD: a autenticação multifator não está disponível para o Simple AD.

Desde 13 de abril de 2021, o PCoIP Connection Manager não é mais compatível para uso com versões de firmware de dispositivo cliente zero entre 4.6.0 e 6.0.0. Se o firmware do cliente zero não for a versão 6.0.0 ou posterior, você poderá obter o firmware mais recente por meio de uma assinatura do Desktop Access em https://www.teradici.com/desktop-access.

Important

- No Teradici PCoIP Administrative Web Interface (AWI) ou no Teradici PCoIP Management Console (MC), habilite o Network Time Protocol (NTP). Para o nome DNS do host NTP **`pool.ntp.org`**, use e defina a porta do host NTP como 123. Se o NTP não estiver habilitado, seus usuários de cliente zero PCoIP poderão receber erros de falha de

certificado, como "The supplied certificate is invalid due to timestamp" (O certificado fornecido é inválido devido ao time stamp).

- A partir da versão 20.10.4 do agente PCoIP, o Amazon WorkSpaces desabilita o redirecionamento USB por padrão por meio do registro do Windows. Essa configuração do registro afeta o comportamento dos periféricos USB quando os usuários utilizam dispositivos cliente zero PCoIP para se conectar aos WorkSpaces. Para obter mais informações, consulte Impressoras USB e outros periféricos compatíveis com USB não estão funcionando para clientes zero PCoIP.

Para obter informações sobre a configuração e a conexão com um dispositivo cliente zero PCoIP, consulte PCoIP Zero Client no Guia do usuário do Amazon WorkSpaces. Para obter uma lista de dispositivos cliente zero PCoIP aprovados, consulte PCoIP Zero Clients no site do Teradici.

Configurar o Android para Chromebooks

A versão 2.4.13 é a versão final do aplicativo cliente Amazon WorkSpaces Chromebook. Como o Google está eliminando gradualmente o suporte aos aplicativos Chrome, não haverá mais atualizações no aplicativo cliente do WorkSpaces Chromebook e seu uso não é suportado.

Para Chromebooks compatíveis com a instalação de aplicativos Android, recomendamos usar o aplicativo cliente WorkSpaces Android em vez disso.

Alguns Chromebooks lançados antes de 2019 devem estar habilitados para instalar aplicativos Android antes que os usuários possam instalar o aplicativo cliente Amazon WorkSpaces Android. Para obter mais informações, consulte Sistemas Chrome OS compatíveis com aplicativos Android.

Para gerenciar remotamente a ativação dos Chromebooks de seus usuários para instalar aplicativos Android, consulte Configurar Android em dispositivos Chrome.

Ativar e configurar o Amazon WorkSpaces Web Access

A maioria dos WorkSpaces pacotes oferece suporte ao Amazon WorkSpaces Web Access. Para obter uma lista dos WorkSpaces que oferecem suporte ao acesso por navegador da web, consulte “Quais WorkSpaces pacotes da Amazon oferecem suporte ao Web Access?” em Acesso de clientes, acesso à Web e experiência do usuário.

Note

- O Web Access com WSP para Windows e Ubuntu WorkSpaces é suportado em todas as regiões onde o WSP WorkSpaces está disponível. O WSP para Amazon Linux WorkSpaces está disponível somente em AWS GovCloud (Oeste dos EUA).
- É altamente recomendável usar o Web Access com o WSP WorkSpaces para obter a melhor qualidade de streaming e experiência do usuário. A seguir estão as limitações ao usar o Web Access com PCoIP WorkSpaces:
  - O acesso à Web com PCoIP não é suportado na AWS GovCloud (US) RegionsÁsia-Pacífico (Mumbai), na África (Cidade do Cabo) e em Israel (Tel Aviv)
  - O Web Access com PCoIP só é compatível com Windows WorkSpaces, não com Amazon Linux. WorkSpaces
  - O Web Access não está disponível para alguns Windows 10 WorkSpaces que estão usando o protocolo PCoIP. Se o seu PCoIP WorkSpaces estiver equipado com o Windows Server 2019 ou 2022, o Web Access não estará disponível.
- Você não pode usar um navegador da Web para se conectar a uma GPU habilitada WorkSpaces.
- Se você estiver usando o macOS na VPN e usando o navegador Firefox, o navegador não suportará streaming de PCoIP WorkSpaces usando o Web Access. WorkSpaces Isso se deve a uma limitação na implementação do protocolo WebRTC pelo Firefox.

Important

A partir de 1º de outubro de 2020, os clientes não poderão mais usar o cliente Amazon WorkSpaces Web Access para se conectar ao Windows 7 Custom WorkSpaces ou ao Windows 7 Bring Your Own License (BYOL) WorkSpaces.

Etapa 1: habilitar o acesso via Web ao seu WorkSpaces

Você controla o acesso pela Web ao seu WorkSpaces no nível do diretório. Para cada diretório contendo o qual você deseja permitir WorkSpaces que os usuários acessem por meio do cliente do Web Access, siga as etapas a seguir.

Para habilitar o acesso via Web ao seu WorkSpaces

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecionar Diretórios.
3. Na coluna ID do diretório, escolha o ID do diretório para o qual você deseja habilitar o Acesso via Web.
4. Na página Detalhes do diretório, desça até a seção Outras plataformas e escolha Editar.
5. Selecione Web Access.
6. Escolha Salvar.

> **Note**
>
> Depois de habilitar o Web Access, reinicie o seu WorkSpace para que a alteração seja aplicada.

Etapa 2: Configurar o acesso de entrada e saída às portas para Acesso via Web

O Amazon WorkSpaces Web Access exige acesso de entrada e saída para determinadas portas. Para ter mais informações, consulte Portas para o Web Access.

Etapa 3: Definir as configurações da Política de Grupo e da política de segurança a fim de permitir que os usuários façam login

A Amazon WorkSpaces depende de uma configuração específica da tela de login para permitir que os usuários façam login com sucesso a partir do seu cliente Web Access.

Para permitir que os usuários do Web Access façam login em seus WorkSpaces, você deve definir uma configuração de Política de Grupo e três configurações de Política de Segurança. Se essas configurações não estiverem definidas corretamente, os usuários poderão enfrentar longos tempos de login ou telas pretas ao tentarem fazer login no seu WorkSpaces. Para definir essas configurações, use os procedimentos a seguir.

Você pode usar Objetos de Política de Grupo (GPOs) para aplicar configurações para gerenciar o Windows WorkSpaces ou os usuários que fazem parte do seu WorkSpaces diretório do Windows.

Recomendamos que você crie uma unidade organizacional para seus objetos de WorkSpaces computador e uma unidade organizacional para seus objetos de WorkSpaces usuário.

Para obter informações sobre como usar as ferramentas de administração do Active Directory para trabalhar com GPOs, consulte Installing the Active Directory Administration Tools no Guia de administração da AWS Directory Service .

Para permitir que o agente de WorkSpaces logon troque de usuário

Na maioria dos casos, quando um usuário tenta fazer login em um WorkSpace, o campo do nome do usuário é preenchido previamente com o nome desse usuário. No entanto, se um administrador tiver estabelecido uma conexão RDP com o WorkSpace para realizar tarefas de manutenção, o campo do nome do usuário será preenchido com o nome do administrador.

Para evitar esse problema, desative a configuração da política de grupo Hide entry points for Fast User Switching (Ocultar pontos de entrada para troca rápida de usuários). Quando você desativa essa configuração, o agente de WorkSpaces logon pode usar o botão Alternar usuário para preencher o campo do nome do usuário com o nome correto.

1. Abra a ferramenta Gerenciamento de Política de Grupo (gpmc.msc), navegue até e selecione um GPO no nível do domínio ou do controlador de domínio do diretório que você usa para o seu WorkSpaces. (Se você tiver o modelo administrativo da Política de WorkSpaces Grupo instalado em seu domínio, poderá usar o WorkSpaces GPO para suas contas WorkSpaces de máquina.)
2. Escolha Action (Ação), Edit (Editar) no menu principal.
3. No Editor de gerenciamento de política de grupo, selecione Computer Configuration (Configuração da política), Policies (Políticas), Administrative Templates (Modelos administrativos), System (Sistema) e Logon.
4. Abra a configuração Hide entry points for Fast User Switching (Ocultar pontos de entrada para a troca rápida de usuários).
5. Na caixa de diálogo Hide entry points for Fast User Switching (Ocultar pontos de entrada para a troca rápida de usuários) selecioneDisabled (Desabilitado) e clique em OK.

Como ocultar o último nome de usuário com o qual foi feito logon

Por padrão, a lista de últimos usuários com os quais foi feito logon é exibida em vez do botão Switch User (Trocar de usuário). Dependendo da configuração do WorkSpace, a lista pode não exibir o quadro Outro usuário. Quando essa situação ocorre, se o nome de usuário pré-preenchido não estiver correto, o agente de WorkSpaces logon não poderá preencher o campo com o nome correto.

Para evitar esse problema, ative a configuração da política de segurança Interactive logon: Don't display last signed-in (Logon interativo: não exibir o último usuário que fez login) ou Interactive logon: Do not display last user name (Logon interativo: não exibir o último nome de usuário).

1. Abra a ferramenta Gerenciamento de Política de Grupo (gpmc.msc), navegue até e selecione um GPO no nível do domínio ou do controlador de domínio do diretório que você usa para o seu WorkSpaces. (Se você tiver o modelo administrativo da Política de WorkSpaces Grupo instalado em seu domínio, poderá usar o WorkSpaces GPO para suas contas WorkSpaces de máquina.)
2. Escolha Action (Ação), Edit (Editar) no menu principal.
3. No Editor de gerenciamento de política de grupo, selecione Computer Configuration (Configuração do computador), Windows Settings (Configurações do Windows), Security Settings (Configurações de segurança), Local Policies (Políticas locais) e Security Options (Opções de segurança).
4. Abra uma das seguintes configurações:
   - Para o Windows 7: Logon interativo: não exibir o último usuário que fez login
   - Para o Windows 10: Logon interativo: não exibir o último nome de usuário
5. Na caixa de diálogo Properties (Propriedades) da configuração, selecione Enabled (Habilitado) e clique em OK.

Como exigir que os usuários pressionem CTRL+ALT+DEL antes de fazer logon

Para o WorkSpaces Web Access, você precisa exigir que os usuários pressionem CTRL+ALT+DEL antes de poderem fazer login. Exigir que os usuários pressionem CTRL+ALT+DEL antes de fazer logon garante que os eles estejam usando um caminho confiável ao inserir as senhas.

1. Abra a ferramenta Gerenciamento de Política de Grupo (gpmc.msc), navegue até e selecione um GPO no nível do domínio ou do controlador de domínio do diretório que você usa para o seu WorkSpaces. (Se você tiver o modelo administrativo da Política de WorkSpaces Grupo instalado em seu domínio, poderá usar o WorkSpaces GPO para suas contas WorkSpaces de máquina.)
2. Escolha Action (Ação), Edit (Editar) no menu principal.
3. No Editor de gerenciamento de política de grupo, selecione Computer Configuration (Configuração do computador), Windows Settings (Configurações do Windows), Security Settings (Configurações de segurança), Local Policies (Políticas locais) e Security Options (Opções de segurança).

4. Abra a configuração e logon: Do not require CTRL+ALT+DEL (Logon interativo: não exigir CTRL +ALT+DEL).
5. Na guia Local Security Setting (Configuração de segurança local), selecione Disabled (Desativado) e OK.

Como exibir as informações de usuário e de domínio quando a sessão está bloqueada

O agente de WorkSpaces logon procura o nome e o domínio do usuário. Depois que essa configuração for definida, a tela de bloqueio exibirá o nome completo do usuário (se ele estiver especificado no Active Directory), o nome de domínio e o nome de usuário dele.

1. Abra a ferramenta Gerenciamento de Política de Grupo (gpmc.msc), navegue até e selecione um GPO no nível do domínio ou do controlador de domínio do diretório que você usa para o seu WorkSpaces. (Se você tiver o modelo administrativo da Política de WorkSpaces Grupo instalado em seu domínio, poderá usar o WorkSpaces GPO para suas contas WorkSpaces de máquina.)
2. Escolha Action (Ação), Edit (Editar) no menu principal.
3. No Editor de gerenciamento de política de grupo, selecione Computer Configuration (Configuração do computador), Windows Settings (Configurações do Windows), Security Settings (Configurações de segurança), Local Policies (Políticas locais) e Security Options (Opções de segurança).
4. Abra a configuração Interactive logon: Display user information when the session is locked (Logon interativo: exibir informações do usuário quando a sessão for bloqueada).
5. Na guia Local Security Setting (Configuração de segurança local), selecione User display name, domain and user names (Nome de exibição, domínio e nomes de usuário) e selecione OK.

Como aplicar as alterações de configuração da política de grupo e da política de segurança

As alterações nas configurações da Política de Grupo e da Política de Segurança entram em vigor após a próxima atualização da Política de Grupo WorkSpace e após a reinicialização da WorkSpace sessão. Para aplicar as alterações na política de grupo e na política de segurança nos procedimentos anteriores, siga um destes procedimentos:

- Reinicie o WorkSpace (no WorkSpaces console da Amazon, selecione o e, em seguida WorkSpace, escolha Ações, Reinicialização WorkSpaces).
- Em um prompt de comando administrativo, insira gpupdate /force.

Configurar o Amazon WorkSpaces para a autorização do FedRAMP ou a conformidade com o SRG do DoD

Para estar em conformidade com o Programa Federal de Gerenciamento de Riscos e Autorizações (FedRAMP) ou com o Guia de Requisitos de Segurança (SRG) de computação em nuvem do Department of Defense (DoD), você deve configurar o Amazon WorkSpaces para usar a criptografia de endpoint dos Padrões Federais de Processamento de Informações (FIPS) no nível do diretório. Você também deve usar uma região da AWS nos EUA que tenha autorização do FedRAMP ou esteja em conformidade com o SRG do DoD.

O nível de autorização do FedRAMP (moderado ou alto) ou o nível de impacto do SRG do DoD (2, 4 ou 5) depende da região da AWS nos EUA na qual o Amazon WorkSpaces está sendo usado. Para obter os níveis de autorização do FedRAMP e a conformidade com o SRG do DoD aplicáveis a cada região, consulte Serviços da AWS no escopo por programa de conformidade.

> **Note**
>
> Além de usar a criptografia de endpoints FIPS, você também pode criptografar os WorkSpaces. Para obter mais informações, consulte Encriptado WorkSpaces.

Requisitos

- Você deve criar seus WorkSpaces em uma região da AWS nos EUA que tenha a autorização do FedRAMP ou esteja em conformidade com o SRG do DoD.
- O diretório dos WorkSpaces deve ser configurado para usar o FIPS 140-2 Validated Mode (Modo validado FIPS 140-2) para criptografia de endpoint.

  > **Note**
  >
  > Para usar a configuração FIPS 140-2 Validated Mode (Modo validado FIPS 140-2) o diretório dos WorkSpaces deve ser novo ou todos os WorkSpaces existentes no diretório devem usar o FIPS 140-2 Validated Mode para criptografia de endpoint. Caso contrário, você não poderá usar essa configuração e, portanto, os WorkSpaces criados não estarão em conformidade com os requisitos de segurança do FedRAMP ou do DoD.

- Os usuários devem acessar seus WorkSpaces de um dos seguintes aplicativos cliente do WorkSpaces:

- Windows: 2.4.3 ou posterior
- macOS: 2.4.3 ou posterior
- Linux: 3.0.0 ou posterior
- iOS: 2.4.1 ou posterior
- Android: 2.4.1 ou posterior
- Tablet Fire: 2.4.1 ou posterior
- ChromeOS: 2.4.1 ou posterior
- Web Access

Como usar a criptografia de endpoint do FIPS

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione Directories (Diretórios).
3. Verifique se o diretório onde você deseja criar WorkSpaces autorizados pelo FedRAMP e em conformidade com o SRG do DoD não tem WorkSpaces existentes associados a ele. Se houver WorkSpaces associados ao diretório e o diretório ainda não estiver habilitado para usar o modo validado FIPS 140-2, encerre os WorkSpaces ou crie um novo diretório.
4. Escolha o diretório que atende aos critérios acima e escolha Actions (Ações), Update Details (Atualizar detalhes).
5. Na página Update Directory Details (Atualizar detalhes do diretório) escolha a seta para expandir a seção Access Control Options (Opções de controle de acesso).
6. Em Endpoint Encryption (Criptografia de endpoint), escolha FIPS 140-2 Validated Mode (Modo validado FIPS 140-2) em vez de TLS Encryption Mode (Standard) [Modo de criptografia TLS (Padrão)].
7. Escolha Atualizar e sair.
8. Agora, nesse diretório, você poderá criar WorkSpaces autorizados pelo FedRAMP e em conformidade com o SRG do DoD. Para acessar esses WorkSpaces, os usuários devem usar um dos aplicativos cliente de WorkSpaces listados anteriormente na seção Requisitos.

Habilite conexões SSH para seu Linux WorkSpaces

Se você ou seus usuários quiserem se conectar ao seu Amazon Linux WorkSpaces usando a linha de comando, você pode habilitar conexões SSH. Você pode habilitar conexões SSH para todos WorkSpaces em um diretório ou para indivíduos WorkSpaces em um diretório.

Para habilitar conexões SSH, crie um novo grupo de segurança ou atualize um existente e adicione uma regra para permitir o tráfego de entrada para essa finalidade. Os grupos de segurança atuam como firewall para instâncias associadas, controlando o tráfego de entrada e de saída no nível da instância. Depois de criar ou atualizar seu grupo de segurança, seus usuários e outras pessoas podem usar o PuTTY ou outros terminais para se conectar de seus dispositivos ao Amazon Linux. WorkSpaces Para ter mais informações, consulte the section called “Grupos de segurança”.

Para ver um tutorial em vídeo, consulte Como posso me conectar ao meu Linux Amazon WorkSpaces usando SSH? no Centro de AWS Conhecimento.

Conteúdo

Pré-requisitos para conexões SSH com o Amazon Linux WorkSpaces

- Habilitando o tráfego SSH de entrada para um WorkSpace — Para adicionar uma regra para permitir o tráfego SSH de entrada para um ou mais Amazon Linux WorkSpaces, certifique-se de ter os endereços IP públicos ou privados dos dispositivos que exigem conexões SSH com o seu. WorkSpaces Por exemplo, você pode especificar os endereços IP públicos de dispositivos fora da sua nuvem privada virtual (VPC) ou o endereço IP privado de outra instância do EC2 na mesma VPC que a sua. WorkSpace

  Se você planeja se conectar a um WorkSpace de seu dispositivo local, você pode usar a frase de pesquisa “qual é o meu endereço IP” em um navegador da Internet ou usar o seguinte serviço: Verifique o IP.
- Conectando-se a um WorkSpace — As informações a seguir são necessárias para iniciar uma conexão SSH de um dispositivo para um Amazon Linux. WorkSpace

- O nome de NetBIOS do domínio do Active Directory ao qual você está conectado.
- Seu nome WorkSpace de usuário.
- O endereço IP público ou privado do ao WorkSpace qual você deseja se conectar.

  Privado: se sua VPC estiver conectada a uma rede corporativa e você tiver acesso a essa rede, poderá especificar o endereço IP privado do. WorkSpace

  Público: se você WorkSpace tiver um endereço IP público, poderá usar o WorkSpaces console para encontrar o endereço IP público, conforme descrito no procedimento a seguir.

Para encontrar os endereços IP do Amazon Linux ao qual WorkSpace você deseja se conectar e seu nome de usuário

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione WorkSpaces.
3. Na lista de WorkSpaces, escolha WorkSpace aquela para a qual você deseja habilitar as conexões SSH.
4. Na coluna Modo de execução, confirme se o WorkSpace status é Disponível.
5. Clique na seta à esquerda do WorkSpace nome para exibir o resumo em linha e observe as seguintes informações:

   - O WorkSpace IP. Esse é o endereço IP privado do WorkSpace.

     O endereço IP privado é necessário para obter a interface de rede elástica associada ao WorkSpace. A interface de rede é necessária para recuperar informações como o grupo de segurança ou o endereço IP público associado ao WorkSpace.
   - O WorkSpace nome de usuário. Esse é o nome de usuário que você especifica para se conectar ao WorkSpace.
6. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
7. No painel de navegação, selecione Network Interfaces.
8. Na caixa de pesquisa, digite o WorkSpace IP que você anotou na Etapa 5.
9. Selecione a interface de rede associada ao WorkSpaceIP.
10. Se você WorkSpace tiver um endereço IP público, ele será exibido na coluna IP público IPv4. Anote esse endereço, se necessário.

Para encontrar o nome de NetBIOS do domínio do Active Directory ao qual você está conectado

1. Abra o AWS Directory Service console em https://console.aws.amazon.com/directoryservicev2/.
2. Na lista de diretórios, clique no link ID do diretório do WorkSpace.
3. Na seção Directory details (Detalhes do diretório), anote o Directory NetBIOS name (Nome do diretório NetBIOS).

Habilite conexões SSH para todo o Amazon Linux WorkSpaces em um diretório

Para habilitar conexões SSH para todo o Amazon Linux WorkSpaces em um diretório, faça o seguinte.

Para criar um grupo de segurança com uma regra para permitir tráfego SSH de entrada para todo o Amazon Linux WorkSpaces em um diretório

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Grupos de segurança.
3. Escolha Create Security Group.
4. Digite um nome e, se quiser, uma descrição para seu grupo de segurança.
5. Para VPC, escolha a VPC que contém as conexões SSH para as WorkSpaces quais você deseja habilitar.
6. Na guia Inbound (Entrada), selecione Add Rule (Adicionar regra) e siga estas etapas:
   - Para Tipo, escolha SSH.
   - Para Protocol (Protocolo), o TCP é especificado automaticamente quando você seleciona SSH.
   - Para Port Range (Intervalo de portas), 22 é especificada automaticamente quando você seleciona SSH.
   - Em Source, especifique o intervalo CIDR dos endereços IP públicos dos computadores que os usuários usarão para se conectar aos seus WorkSpaces. Por exemplo, uma rede corporativa ou uma rede doméstica.
   - Em Description (Descrição), digite uma descrição para a regra. Essa etapa é opcional.
7. Escolha Criar.

Autenticação baseada em senha no Amazon Linux 2 WorkSpaces

O Amazon Linux 2 WorkSpaces lançado antes de 10 de novembro de 2023 tem a autenticação de senha SSH habilitada por padrão. Para Amazon Linux 2 WorkSpaces lançado após 10 de novembro. de 2023, a autenticação por senha SSH é desabilitada por padrão.

Para desativar a autenticação por senha em WorkSpaces instâncias existentes do Amazon Linux 2

1. Inicie o WorkSpaces cliente e faça login no seu WorkSpace.
2. Abra a janela do Terminal (Aplicação > Ferramentas do sistema > Terminal MATE).
3. Na janela do Terminal, execute o comando a seguir.

```
sudo sed -E -i 's|^#?(PasswordAuthentication)\s.*|\1 no|' /etc/ssh/sshd_config
```

Para habilitar a autenticação por senha em WorkSpaces instâncias recém-criadas do Amazon Linux 2

1. Inicie o WorkSpaces cliente e faça login no seu WorkSpace.
2. Abra a janela do Terminal (Aplicação > Ferramentas do sistema > Terminal MATE).
3. Na janela do Terminal, execute o comando a seguir.

```
sudo sed -E -i 's|^#?(PasswordAuthentication)\s.*|\1 yes|' /etc/ssh/sshd_config
```

Ao contrário do Ubuntu WorkSpaces, o Amazon Linux 2, WorkSpaces por padrão, não preserva as configurações de autenticação por senha SSH em imagens personalizadas. Se você quiser habilitar a autenticação por senha SSH por padrão no Amazon Linux 2 WorkSpaces provisionada a partir de uma imagem personalizada, além de habilitar a autenticação por senha, você também deve alterar o `/etc/cloud/cloud.cfg` arquivo para remover a linha contida `ssh_pwauth` ao criar uma imagem personalizada. Para alterar o arquivo `/etc/cloud/cloud.cfg`, execute o seguinte comando:

```
sudo sed -i '/^\s*ssh_pwauth:.*$/d' /etc/cloud/cloud.cfg
```

Habilite conexões SSH com um Amazon Linux específico WorkSpace

Para habilitar conexões SSH com um Amazon Linux específico WorkSpace, faça o seguinte.

Para adicionar uma regra a um grupo de segurança existente para permitir tráfego SSH de entrada para um Amazon Linux específico WorkSpace

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Network & Security (Rede e segurança), selecione Network Interfaces (Interfaces de rede).
3. Na barra de pesquisa, digite o endereço IP privado para o WorkSpace qual você deseja habilitar as conexões SSH.
4. Na coluna Security groups (Grupos de segurança), clique em um link para o grupo de segurança.
5. Na guia Entrada, escolha Editar.
6. Selecione Add Rule (Adicionar regra) e faça o seguinte:
   - Para Tipo, escolha SSH.
   - Para Protocol (Protocolo), o TCP é especificado automaticamente quando você seleciona SSH.
   - Para Port Range (Intervalo de portas), 22 é especificada automaticamente quando você seleciona SSH.
   - Em Source (Origem), selecione My IP (Meu IP) ou Custom (Personalizado) e especifique um único endereço de IP ou um intervalo na notação CIDR. Por exemplo, se o endereço IPv4 for `203.0.113.25`, especifique `203.0.113.25/32` para listar esse único endereço IPv4 em notação CIDR. Se sua empresa alocar endereços de um intervalo, especifique o intervalo inteiro, como `203.0.113.0/24`.
   - Em Description (Descrição), digite uma descrição para a regra. Essa etapa é opcional.
7. Escolha Salvar.

Conecte-se a um Amazon Linux WorkSpace usando Linux ou PuTTY

Depois de criar ou atualizar seu grupo de segurança e adicionar a regra necessária, seus usuários e outras pessoas podem usar o Linux ou o PuTTY para se conectar de seus dispositivos ao seu. WorkSpaces

> **Note**
>
> Antes de concluir qualquer um dos procedimentos a seguir, verifique se você tem o seguinte:

- O nome de NetBIOS do domínio do Active Directory ao qual você está conectado.
- O nome de usuário que você usa para se conectar ao WorkSpace.
- O endereço IP público ou privado do ao WorkSpace qual você deseja se conectar.

Para obter instruções sobre como obter essas informações, consulte “Pré-requisitos para conexões SSH com o Amazon Linux WorkSpaces”, anteriormente neste tópico.

Para se conectar a um Amazon Linux WorkSpace usando Linux

1. Abra o prompt de comando como administrador e insira o seguinte comando. Em *Nome do NetBIOS, Nome de usuário* e *WorkSpace IP*, insira os valores aplicáveis.

   ```
   ssh "NetBIOS_NAME\Username"@WorkSpaceIP
   ```

   Veja a seguir um exemplo do comando SSH onde:

   - O *NetBIOS_NAME* é "anycompany"
   - The *Username* (Nome de usuário) é "janedoe"
   - O *WorkSpace IP* é 203.0.113.25

   ```
   ssh "anycompany\janedoe"@203.0.113.25
   ```

2. Quando solicitado, digite a mesma senha que você usa ao se autenticar com o WorkSpaces cliente (sua senha do Active Directory).

Para se conectar a um Amazon Linux WorkSpace usando PuTTY

1. Abra o PuTTY.
2. Na caixa de diálogo PuTTY Configuration (Configuração PuTTy), siga estas etapas:

   - Para Host Name (or IP address) [Nome de host (ou endereço IP)], insira o seguinte comando. Substitua os valores pelo nome NetBIOS do domínio do Active Directory ao qual você está conectado, pelo nome de usuário que você usa para se conectar ao WorkSpace e pelo endereço IP do domínio ao qual você deseja se conectar. WorkSpace

```
NetBIOS_NAME\Username@WorkSpaceIP
```

- Em Porta, insira **22**.
- Para Connection type (Tipo de conexão), escolha SSH.

Para um exemplo do comando SSH, consulte a etapa 1 no procedimento anterior.

3. Escolha Open (Abrir).
4. Quando solicitado, digite a mesma senha que você usa ao se autenticar com o WorkSpaces cliente (sua senha do Active Directory).

Componentes de configuração e serviço necessários para WorkSpaces

Como WorkSpace administrador, você deve entender o seguinte sobre a configuração necessária e os componentes de serviço.

- the section called “Configuração da tabela de roteamento”
- the section called “Componentes para Windows”
- the section called “Componentes para Linux”
- the section called “Componentes para Ubuntu”

Configuração necessária da tabela de roteamento

Recomendamos que você não modifique a tabela de roteamento em nível de sistema operacional para a. WorkSpace O WorkSpaces serviço requer as rotas pré-configuradas nesta tabela para monitorar o estado do sistema e atualizar os componentes do sistema. Se forem necessárias alterações na tabela de roteamento para sua organização, entre em contato com o AWS Support ou com a equipe da sua AWS conta antes de aplicar qualquer alteração.

Componentes de serviço necessários para Windows

No Windows WorkSpaces, os componentes do serviço são instalados nos seguintes locais. Não exclua, altere, bloqueie ou coloque esses objetos quarentena. Se você fizer isso, não WorkSpace funcionará corretamente.

Se o software antivírus estiver instalado no WorkSpace, certifique-se de que ele não interfira nos componentes do serviço instalados nos seguintes locais.

- `C:\Program Files\Amazon`
- `C:\Program Files\NICE`
- `C:\Program Files\Teradici`
- `C:\Program Files (x86)\Teradici`
- `C:\ProgramData\Amazon`
- `C:\ProgramData\NICE`
- `C:\ProgramData\Teradici`

Agente PCoIP de 32 bits

Em 29 de março de 2021, atualizamos o agente PCoIP de 32 bits para 64 bits. Para Windows WorkSpaces que está usando o protocolo PCoIP, isso significa que a localização dos arquivos Teradici mudou de para. `C:\Program Files (x86)\Teradici` `C:\Program Files\Teradici` Como atualizamos os agentes PCoIP durante janelas de manutenção regulares, alguns de vocês WorkSpaces podem ter usado o agente de 32 bits por mais tempo do que outros durante a transição.

Se você configurou regras de firewall, exclusões de software antivírus (no lado do cliente e do host), configurações de Objeto de Política de Grupo (GPO) ou configurações para o Microsoft System Center Configuration Manager (SCCM), Microsoft Endpoint Configuration Manager ou ferramentas de gerenciamento de configuração semelhantes com base no caminho completo para o agente de 32 bits, também deve adicionar o caminho completo para o agente de 64 bits a essas configurações.

Se você estiver filtrando os caminhos para qualquer componente PCoIP de 32 bits, não se esqueça de adicionar os caminhos às versões de 64 bits dos componentes. Como WorkSpaces talvez nem todos sejam atualizados ao mesmo tempo, não substitua o caminho de 32 bits pelo caminho de 64 bits, ou alguns dos seus WorkSpaces podem não funcionar. Por exemplo, se você estiver baseando as exclusões ou os filtros de comunicação em `C:\Program Files (x86)\Teradici \PCoIP Agent\bin\pcoip_server_win32.exe`, também deverá adicionar `C:\Program Files\Teradici\PCoIP Agent\bin\pcoip_server.exe`. Da mesma forma, se você estiver baseando as exclusões ou os filtros de comunicação em `C:\Program Files (x86)\Teradici \PCoIP Agent\bin\pcoip_agent.exe`, também deverá adicionar `C:\Program Files \Teradici\PCoIP Agent\bin\pcoip_agent.exe`.

Alteração do serviço de árbitro PCoIP — Esteja ciente de que o serviço de árbitro PCoIP (`C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_arbiter_win32.exe`) é removido quando você é atualizado para usar o agente de WorkSpaces 64 bits.

Clientes zero PCoIP e dispositivos USB — A partir da versão 20.10.4 do agente PCoIP, a WorkSpaces Amazon desativa o redirecionamento de USB por padrão por meio do registro do Windows. Essa configuração do registro afeta o comportamento dos periféricos USB quando seus usuários estão usando dispositivos PCoIP zero client para se conectar aos seus. WorkSpaces Para ter mais informações, consulte Impressoras USB e outros periféricos compatíveis com USB não estão funcionando para clientes zero PCoIP.

Componentes de serviço necessários para Linux

No Amazon Linux WorkSpaces, os componentes do serviço são instalados nos seguintes locais. Não exclua, altere, bloqueie ou coloque esses objetos quarentena. Se você fizer isso, não WorkSpace funcionará corretamente.

> **Note**
>
> Fazer alterações em arquivos diferentes `/etc/pcoip-agent/pcoip-agent.conf` pode fazer com que você pare WorkSpaces de funcionar e pode exigir que você os reconstrua. Para obter informações sobre como modificar `/etc/pcoip-agent/pcoip-agent.conf`, consulte Gerencie seu Amazon Linux WorkSpaces.

- `/etc/dhcp/dhclient.conf`
- `/etc/logrotate.d/pcoip-agent`
- `/etc/logrotate.d/pcoip-server`
- `/etc/os-release`
- `/etc/pam.d/pcoip`
- `/etc/pam.d/pcoip-session`
- `/etc/pcoip-agent`
- `/etc/profile.d/system-restart-check.sh`
- `/etc/X11/default-display-manager`
- `/etc/yum/pluginconf.d/halt_os_update_check.conf`
- `/etc/systemd/system/euc-analytic-agent.service`

- /lib/systemd/system/pcoip.service
- /lib/systemd/system/pcoip-agent.service
- /lib64/security/pam_self.so
- /usr/bin/pcoip-fne-view-license
- /usr/bin/pcoip-list-licenses
- /usr/bin/pcoip-validate-license
- /usr/bin/euc-analytics-agent
- /usr/lib/firewalld/services/pcoip-agent.xml
- /usr/lib/modules-load.d/usb-vhci.conf
- /usr/lib/pcoip-agent
- /usr/lib/skylight
- /usr/lib/systemd/system/pcoip.service
- /usr/lib/systemd/system/pcoip.service.d/
- /usr/lib/systemd/system/skylight-agent.service
- /usr/lib/tmpfiles.d/pcoip-agent.conf
- /usr/lib/yum-plugins/halt_os_update_check.py
- /usr/sbin/pcoip-agent
- /usr/sbin/pcoip-register-host
- /usr/sbin/pcoip-support-bundler
- /usr/share/doc/pcoip-agent
- /usr/share/pcoip-agent
- /usr/share/selinux/packages/pcoip-agent.pp
- /usr/share/X11
- /var/crash/pcoip-agent
- /var/lib/pcoip-agent
- /var/lib/skylight
- /var/log/pcoip-agent
- /var/log/skylight
- /var/logs/wsp
- /var/log/eucanalytics

Componentes de serviço necessários para Ubuntu

No Ubuntu WorkSpaces, os componentes do serviço são instalados nos seguintes locais. Não exclua, altere, bloqueie ou coloque esses objetos quarentena. Se você fizer isso, não WorkSpace funcionará corretamente.

- `/etc/X11/default-display-manager`
- `/etc/X11/xorg.conf`
- `/etc/dcv`
- `/etc/default/grub.d/zz-hibernation.cfg`
- `/etc/netplan`
- `/etc/os-release`
- `/etc/pam.d/dcv`
- `/etc/pam.d/dcv-graphical-sso`
- `/etc/sssd/sssd.conf`
- `/etc/wsp`
- `/etc/systemd/system/euc-analytic-agent.service`
- `/lib64/security/pam_self.so`
- `/usr/lib/skylight`
- `/usr/lib/systemd/system/dcvserver.service`
- `/usr/lib/systemd/system/dcvsessionlauncher.service`
- `/usr/lib/systemd/system/skylight-agent.service`
- `/usr/lib/systemd/system/wspdcvhostadapter.service`
- `/usr/lib/systemd/system/xdcv-console-update.service`
- `/usr/lib/systemd/system/xdcv-console.path`
- `/usr/lib/systemd/system/xdcv-console.service`
- `/usr/share/X11`
- `/usr/bin/euc-analytics-agent`
- `/var/lib/skylight`
- `/var/log/skylight`
- `/var/log/eucanalytics`

Gerenciar diretórios para WorkSpaces

O WorkSpaces usa um diretório para armazenar e gerenciar informações para seus WorkSpaces e usuários. Você pode usar uma das opções a seguir:

- AD Connector: use seu Microsoft Active Directory existente on-premises. Os usuários podem entrar em seus WorkSpaces usando suas credenciais no local e acessar os recursos no local dos seus WorkSpaces.
- AWS Managed Microsoft AD: crie um Microsoft Active Directory hospedado na AWS.
- Simple AD: crie um diretório compatível com o Microsoft Active Directory, com tecnologia Samba 4 e hospedado na AWS.
- Confiança cruzada: crie uma relação de confiança entre o diretório do AWS Managed Microsoft AD e o domínio on-premises.

Para assistir a tutoriais que demonstram como configurar esses diretórios e ativar os WorkSpaces, consulte Inicializar uma área de trabalho virtual usando WorkSpaces.

> **Tip**
>
> Para obter uma exploração detalhada das considerações de design de diretórios e de nuvem privada virtual (VPC) para vários cenários de implantação, consulte Best Practices for Deploying Amazon WorkSpaces.

Depois de criar um diretório, você executará a maioria das tarefas de administração de diretório com ferramentas como as ferramentas de administração do Active Directory. Você pode executar algumas tarefas de administração de diretório usando o console do WorkSpaces e outras tarefas usando a política de grupo. Para obter mais informações sobre como gerenciar usuários e grupos, consulte Gerenciar usuários de WorkSpaces e Configurar as ferramentas de administração do Active Directory para WorkSpaces.

> **Note**
>
> - Diretórios compartilhados não são compatíveis para uso no Amazon WorkSpaces no momento.

- Se você configurar o diretório do AWS Managed Microsoft AD para replicação multirregional, somente o diretório na região primária poderá ser registrado para uso no Amazon WorkSpaces. As tentativas de registrar o diretório em uma região replicada para uso com o Amazon WorkSpaces vão falhar. A replicação multirregional com o AWS Managed Microsoft AD não é compatível para uso com o Amazon WorkSpaces em regiões replicadas.
- O Simple AD e o AD Connector são disponibilizados gratuitamente para uso com os WorkSpaces. Se não houver WorkSpaces sendo usados com o diretório do Simple AD ou do AD Connector por 30 dias consecutivos, o registro desse diretório será automaticamente cancelado para uso com o Amazon WorkSpaces, e você será cobrado por esse diretório de acordo com os Preços do AWS Directory Service.

  Para excluir diretórios vazios, consulte Excluir o diretório dos WorkSpaces. Se você excluir o diretório do Simple AD ou do AD Connector, sempre poderá criar um novo quando quiser começar a usar o WorkSpaces novamente.

Índice

Registrar um diretório com o WorkSpaces

Para permitir que o WorkSpaces use um diretório existente do AWS Directory Service, você deve registrá-lo com o WorkSpaces. Depois de registrar um diretório, você pode ativar os WorkSpaces no diretório.

Requisitos

Para registrar um diretório para uso com o WorkSpaces, ele deve atender aos seguintes requisitos:

- Se você estiver usando o AWS Managed Microsoft AD ou o Simple AD, seu diretório poderá estar em uma sub-rede privada dedicada, desde que o diretório tenha acesso à VPC em que os WorkSpaces estão localizados.

Para obter mais informações sobre o design de diretórios e VPC, consulte o whitepaper Best Practices for Deploying Amazon WorkSpaces.

> **Note**
>
> O Simple AD e o AD Connector são disponibilizados gratuitamente para uso com os WorkSpaces. Se não houver WorkSpaces sendo usados com o diretório do Simple AD ou do AD Connector por 30 dias consecutivos, o registro desse diretório será automaticamente cancelado para uso com o Amazon WorkSpaces, e você será cobrado por esse diretório de acordo com os Preços do AWS Directory Service.
> Para excluir diretórios vazios, consulte Excluir o diretório dos WorkSpaces. Se você excluir o diretório do Simple AD ou do AD Connector, sempre poderá criar um novo quando quiser começar a usar o WorkSpaces novamente.

Para registrar um diretório

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione Directories (Diretórios).
3. Selecione o diretório.
4. Escolha Ações, Registrar.

> **Note**
>
> - Diretórios compartilhados não são compatíveis para uso no Amazon WorkSpaces no momento.
> - Se o diretório do AWS Managed Microsoft AD tiver sido configurado para replicação multirregional, somente o diretório na região primária poderá ser registrado para uso no Amazon WorkSpaces. As tentativas de registrar o diretório em uma região replicada para uso com o Amazon WorkSpaces vão falhar. A replicação multirregional

com o AWS Managed Microsoft AD não é compatível para uso no Amazon WorkSpaces em regiões replicadas.

5. Selecione duas sub-redes da sua VPC que não estejam na mesma zona de disponibilidade. Essas sub-redes serão usadas para iniciar os WorkSpaces. Para obter mais informações, consulte Zonas de disponibilidade para a Amazon WorkSpaces.

> **Note**
>
> Se você não souber quais sub-redes escolher, selecione Sem preferência.

6. Para Enable Self Service Permissions (Habilitar permissões de autoatendimento), selecione Yes (Sim) para habilitar os usuários a recriar seus WorkSpaces, alterar o tamanho do volume, o tipo de computação e o modo de execução. A habilitação pode afetar o quanto você paga pelo Amazon WorkSpaces. Caso contrário, selecione No (Não).
7. Em Habilitar Amazon WorkDocs, selecione Sim para registrar o diretório para uso no Amazon WorkDocs ou Não para não usá-lo.

> **Note**
>
> Essa opção será exibida somente se o Amazon WorkDocs estiver disponível na região e se você não estiver usando o AWS Managed Microsoft AD. Se você estiver usando o AWS Managed Microsoft AD, conclua o registro do diretório e consulte Habilitar o Amazon WorkDocs para o AWS Managed Microsoft AD.

8. Escolha Register. Inicialmente, o valor de Registrado é `REGISTERING`. Depois de concluir o registro, o valor é `Yes`.

Ao terminar de usar o diretório com o WorkSpaces, você pode cancelar o registro. Você deve cancelar o registro de um diretório para poder excluí-lo. Se você quiser cancelar o registro e excluir um diretório, é necessário primeiro localizar e remover todos os aplicativos e serviços que estão registrados no diretório. Para obter mais informações, consulte Delete Your Directory no Guia de Administração do AWS Directory Service.

Para cancelar o registro de um diretório

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.

2. No painel de navegação, selecione Directories (Diretórios).
3. Selecione o diretório.
4. Escolha Actions e Deregister.
5. Quando a confirmação for solicitada, escolha Cancelar registro. Cancelado o registro, o valor de Registrado é No.

Atualize os detalhes do diretório para o seu WorkSpaces

Você pode concluir as seguintes tarefas de gerenciamento de diretórios usando o WorkSpaces console.

Tarefas

- Selecionar uma unidade organizacional
- Configurar endereços IP públicos automáticos
- Controlar o acesso de dispositivos
- Gerenciar permissões de administrador local
- Atualizar a conta do AD Connector (AD Connector)
- Autenticação multifator (AD Connector)

Selecionar uma unidade organizacional

WorkSpace as contas de máquina são colocadas na unidade organizacional (OU) padrão do WorkSpaces diretório. Inicialmente, as contas da máquina de WorkSpaces serão colocados na UO dos computadores de seu diretório ou do diretório ao qual o AD Connector está conectado. Você pode selecionar outra UO em seu diretório ou no diretório conectado ou especificar um UO em outro domínio de destino. Observe que você só pode selecionar uma UO por diretório.

Depois de selecionar uma nova OU, as contas da máquina para tudo o WorkSpaces que é criado ou reconstruído são colocadas na OU recém-selecionada.

Como selecionar uma unidade organizacional

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecionar Diretórios.

3. Escolha seu diretório.
4. Em Domínio de destino e unidade organizacional, escolha Editar.
5. Para encontrar uma OU, em Destino e unidade organizacional, você pode começar a digitar todo ou parte do nome da OU e escolher a OU que deseja usar.
6. (Opcional) Escolha um nome distinto de OU para substituir sua OU selecionada por uma OU personalizada.
7. Escolha Salvar.
8. (Opcional) Reconstrua o existente WorkSpaces para atualizar a OU. Para ter mais informações, consulte Reconstrua um WorkSpace.

Configurar endereços IP públicos automáticos

Depois de ativar a atribuição automática de endereços IP públicos, cada um WorkSpace que você inicia recebe um endereço IP público do pool de endereços públicos fornecido pela Amazon. A WorkSpace em uma sub-rede pública pode acessar a Internet por meio do gateway da Internet se tiver um endereço IP público. WorkSpaces que já existem antes de você ativar a atribuição automática, não recebem endereços públicos até que você os reconstrua.

Observe que você não precisa habilitar a atribuição automática de endereços públicos se WorkSpaces estiver em sub-redes privadas e tiver configurado um gateway NAT para a nuvem privada virtual (VPC) ou se WorkSpaces estiver em sub-redes públicas e tiver atribuído endereços IP elásticos a elas. Para ter mais informações, consulte Configurar uma VPC para WorkSpaces.

> **Warning**
>
> Se você associar um endereço IP elástico de sua propriedade a um WorkSpace e depois desassociar esse endereço IP elástico do WorkSpace, ele WorkSpace perderá seu endereço IP público e não obterá automaticamente um novo do pool fornecido pela Amazon. Para associar um novo endereço IP público do pool fornecido pela Amazon ao WorkSpace, você deve reconstruir o. WorkSpace Se você não quiser reconstruir o WorkSpace, deverá associar outro endereço IP elástico de sua propriedade ao WorkSpace.

Como configurar endereços IP elásticos

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.

2. No painel de navegação, selecionar Diretórios.
3. Selecione o diretório para o seu WorkSpaces.
4. Escolha Ações, Atualizar detalhes.
5. Expanda Acesso à Internet e selecione Ativar ou Desativar.
6. Escolha Atualizar.

Controlar o acesso de dispositivos

Você pode especificar os tipos de dispositivos aos quais você tem acesso WorkSpaces. Além disso, você pode restringir o acesso WorkSpaces a dispositivos confiáveis (também conhecidos como dispositivos gerenciados).

Para controlar o acesso do dispositivo ao WorkSpaces

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecionar Diretórios.
3. Escolha seu diretório.
4. Em Opções de controle de acesso, escolha Editar.
5. Em Dispositivos confiáveis, especifique quais tipos de dispositivos podem ser WorkSpaces acessados selecionando Permitir tudo, Dispositivos confiáveis ou Negar tudo. Para ter mais informações, consulte Restrinja o WorkSpaces acesso a dispositivos confiáveis.
6. Escolha Salvar.

Gerenciar permissões de administrador local

Você pode especificar se os usuários são administradores locais em seus aplicativos WorkSpaces, o que permite que eles instalem o aplicativo e modifiquem as configurações deles WorkSpaces. Os usuários são administradores locais por padrão. Se você modificar essa configuração, a alteração se aplicará a todas as novas WorkSpaces que você criar e a todas as WorkSpaces que você reconstruir.

Para modificar permissões de administrador local

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecionar Diretórios.

3. Escolha seu diretório.
4. Em Configurações do administrador local, escolha Editar.
5. Para garantir que os usuários sejam administradores locais, escolha Habilitar configuração do administrador local.
6. Escolha Salvar.

Atualizar a conta do AD Connector (AD Connector)

Você pode atualizar a conta do AD Connector que é usada para ler usuários e grupos e associar contas WorkSpaces de máquina ao seu diretório do AD Connector.

Para atualizar a conta do AD Connector

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecionar Diretórios.
3. Selecione seu diretório e escolha Exibir detalhes.
4. Em Conta do conector AD, escolha Editar.
5. Insira as credenciais de acesso da nova conta.
6. Escolha Salvar.

Autenticação multifator (AD Connector)

Você pode habilitar a autenticação multifator (MFA) para o diretório do AD Connector. Para obter mais informações sobre como usar a autenticação multifator com o AWS Directory Service, consulte Habilitar a autenticação multifator para o AD Connector e Pré-requisitos do AD Connector.

> **Note**
>
> - O servidor RADIUS pode ser hospedado por AWS ou pode ser on-premises.
> - Os nomes de usuário devem corresponder entre o Active Directory e servidor RADIUS.

Como habilitar a autenticação multifator

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.

2. No painel de navegação, selecionar Diretórios.
3. Selecione seu diretório e escolha Ações, Atualizar detalhes.
4. Expanda Multi-factor Authentication e, em seguida, selecione Ativar Multi-factor Authentication.
5. Em Endereço(s) IP do servidor RADIUS, digite os endereços IP de seus endpoints do servidor RADIUS separados por vírgulas ou digite o endereço IP do seu load balancer do servidor RADIUS.
6. Em Porta, digite a porta que o servidor RADIUS está usando para comunicações. A rede on-premises deve permitir tráfego de entrada pela porta do servidor RADIUS padrão (UDP:1812) a partir do AD Connector.
7. Em Código de segredo compartilhado e Confirmar código de segredo compartilhado, digite o código de segredo compartilhado para o servidor RADIUS.
8. Em Protocolo, escolha o protocolo para o seu servidor RADIUS.
9. Em Tempo-limite do servidor, digite o tempo de espera, em segundos, para o servidor RADIUS responder. Esse valor deve ser entre 1 e 50.
10. Em Máximo de tentativas, digite o número de tentativas de comunicação com o servidor RADIUS. Esse valor deve ser entre 0 e 10.
11. Escolha Atualizar e sair.

A Multi-factor Authentication fica disponível quando o Status RADIUS está Ativado. Enquanto a autenticação multifator está sendo configurada, os usuários não podem fazer login em seus WorkSpaces.

Atualizar servidores DNS do Amazon WorkSpaces

Se precisar atualizar os endereços IP do servidor DNS do Active Directory após iniciar os WorkSpaces, você também deverá atualizar os WorkSpaces com as novas configurações do servidor DNS.

Você pode atualizar os WorkSpaces com as novas configurações de DNS de uma das seguintes maneiras:

- Atualize as configurações de DNS nos WorkSpaces antes de atualizar as configurações de DNS para o Active Directory.
- Recompile os WorkSpaces depois de atualizar as configurações de DNS para o Active Directory.

Recomendamos atualizar as configurações de DNS nos WorkSpaces antes de atualizar as configurações de DNS no Active Directory (conforme explicado na Etapa 1 do procedimento a seguir).

Se preferir recompilar os WorkSpaces, atualize um dos endereços IP do servidor DNS no Active Directory (Etapa 2) e siga o procedimento em Reconstrua um WorkSpace para recompilar os WorkSpaces. Após reconstruir os WorkSpaces, siga o procedimento na Etapa 3 para testar as atualizações do servidor DNS. Após concluir essa etapa, atualize o endereço IP do segundo servidor DNS no Active Directory e recompile os WorkSpaces novamente. Siga o procedimento na Etapa 3 para testar a segunda atualização do servidor DNS. Conforme observado na seção Práticas recomendadas, recomendamos atualizar os endereços IP do servidor DNS um por vez.

Práticas recomendadas

Ao atualizar as configurações do serviço DNS, recomendamos as seguintes práticas:

- Para evitar desconexões e inacessibilidade aos recursos do domínio, é altamente recomendável realizar atualizações nos servidores DNS durante os horários fora de pico ou durante um período de manutenção planejado.
- Não inicie novos WorkSpaces durante os 15 minutos antes e os 15 minutos após a alteração das configurações do servidor DNS.
- Ao atualizar as configurações do servidor DNS, altere um endereço IP de servidor DNS por vez. Verifique se a primeira atualização está correta antes de atualizar o segundo endereço IP. Recomendamos realizar o procedimento a seguir (Etapa 1, Etapa 2 e Etapa 3) duas vezes para atualizar os endereços IP um por vez.

Etapa 1: Atualizar as configurações do servidor DNS nos WorkSpaces

No procedimento a seguir, os valores atuais e novos do endereço IP do servidor DNS são referidos da seguinte forma:

- Endereços IP atuais do DNS: *`OldIP1`*, *`OldIP2`*
- Novos endereços IP do DNS: *`NewIP1`*, *`NewIP2`*

> **Note**
>
> Se esta for a segunda vez que você está realizando esse procedimento, substitua *OldIP1* por *OldIP2* e *NewIP1* por *NewIP2*.

Atualizar as configurações do servidor DNS para WorkSpaces do Windows

Se você tiver vários WorkSpaces, poderá implantar a atualização de registro nos WorkSpaces a seguir aplicando um Objeto de Política de Grupo (GPO) na UO do Active Directory para os WorkSpaces. Para obter mais informações sobre como trabalhar com GPOs, consulte Gerencie seu Windows WorkSpaces.

Você pode fazer essas atualizações usando o Editor do Registro ou o Windows PowerShell. Os dois procedimentos são descritos nesta seção.

Como atualizar as configurações do registro DNS usando o Editor do Registro

1. No Windows WorkSpace, abra a caixa de pesquisa do Windows e digite **`registry editor`** para abrir o Editor de Registro (regedit.exe).
2. Quando perguntado “Deseja permitir que este aplicativo faça alterações no seu dispositivo?”, escolha Sim.
3. No Editor do Registro, navegue para a seguinte entrada do Registro:

   HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\SkyLight
4. Abra a chave de registro DomainJoinDns. Atualize *OldIP1* com *NewIP1* e, em seguida, escolha OK.
5. Feche o Editor de Registro.
6. Reinicie o WorkSpace ou o serviço SkyLightWorkspaceConfigService.

   > **Note**
   >
   > Após reiniciar o serviço SkyLightWorkspaceConfigService, pode levar até 1 minuto para que o adaptador de rede reflita a alteração.
7. Prossiga para a Etapa 2 e atualize as configurações do servidor DNS no Active Directory para substituir *OldIP1* por *NewIP1*.

Como atualizar as configurações do registro DNS usando o PowerShell

O procedimento a seguir usa comandos do PowerShell para atualizar o registro e reiniciar o serviço SkyLightWorkspaceConfigService.

1. No Windows WorkSpace, abra a caixa de pesquisa do Windows e digite **`powershell`**. Escolha Executar como administrador.
2. Quando perguntado “Deseja permitir que este aplicativo faça alterações no seu dispositivo?”, escolha Sim.
3. Na janela do PowerShell, execute o comando a seguir para recuperar os endereços IP atuais do servidor DNS.

   ```
   Get-ItemProperty -Path HKLM:\SOFTWARE\Amazon\SkyLight -Name DomainJoinDNS
   ```

   Você deve receber a saída a seguir.

   ```
   DomainJoinDns : OldIP1,OldIP2
   PSPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE
   \Amazon\SkyLight
   PSParentPath  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE
   \Amazon
   PSChildName   : SkyLight
   PSDrive       : HKLM
   PSProvider    : Microsoft.PowerShell.Core\Registry
   ```

4. Na janela do PowerShell, execute o comando a seguir para alterar *`OldIP1`* para *`NewIP1`*. Garanta deixar *`OldIP2`* como está por enquanto.

   ```
   Set-ItemProperty -Path HKLM:\SOFTWARE\Amazon\SkyLight -Name DomainJoinDNS -Value
    "NewIP1,OldIP2"
   ```

5. Execute o comando a seguir para reiniciar o serviço SkyLightWorkspaceConfigService.

   ```
   restart-service -Name SkyLightWorkspaceConfigService
   ```

   > **Note**
   >
   > Após reiniciar o serviço SkyLightWorkspaceConfigService, pode levar até 1 minuto para que o adaptador de rede reflita a alteração.

6. Prossiga para a Etapa 2 e atualize as configurações do servidor DNS no Active Directory para substituir *OldIP1* por *NewIP1*.

Atualizar as configurações do servidor DNS para WorkSpaces do Linux

Se tiver mais de um Linux WorkSpace, é recomendável usar uma solução de gerenciamento de configuração para distribuir e aplicar políticas. Por exemplo, você pode usar o AWS OpsWorks for Chef Automate, o AWS OpsWorks for Puppet Enterprise ou o Ansible.

Como atualizar as configurações do servidor DNS em um WorkSpace do Linux

1. No Linux WorkSpace, abra uma janela do Terminal (Aplicações > Ferramentas do sistema > Terminal MATE).
2. Use o comando Linux a seguir para editar o arquivo `/etc/dhcp/dhclient.conf`. Você deve ter privilégios de usuário raiz para editar esse arquivo. Torne-se raiz usando o comando `sudo -i` ou execute todos os comandos com o `sudo` conforme mostrado.

   ```
   sudo vi /etc/dhcp/dhclient.conf
   ```

   No arquivo `/etc/dhcp/dhclient.conf`, você verá o comando `prepend` a seguir, onde *OldIP1* e *OldIP2* são os endereços IP dos servidores DNS.

   ```
   prepend domain-name-servers OldIP1, OldIP2; # skylight
   ```
3. Substitua *OldIP1* por *NewIP1* e deixe *OldIP2* como está por enquanto.
4. Salve as alterações para `/etc/dhcp/dhclient.conf`.
5. Reinicie o WorkSpace.
6. Prossiga para a Etapa 2 e atualize as configurações do servidor DNS no Active Directory para substituir *OldIP1* por *NewIP1*.

Etapa 2: Atualizar as configurações do servidor DNS para o Active Directory

Nesta etapa, atualize as configurações do servidor DNS para o Active Directory. Conforme observado na seção Práticas recomendadas, recomendamos atualizar os endereços IP do servidor DNS um por vez.

Para atualizar as configurações do servidor DNS para o Active Directory, consulte a seguinte documentação no Guia de administração da AWS Directory Service:

- AD Connector: Atualizar o endereço de DNS para o AD Connector
- AWS Managed Microsoft AD: configurar encaminhadores condicionais de DNS para o domínio no local
- Simple AD: configurar DNS

Após atualizar as configurações do servidor DNS, vá para a Etapa 3.

Etapa 3: Testar as configurações atualizadas do servidor DNS

Após concluir a Etapa 1 e a Etapa 2, use o procedimento a seguir para verificar se as configurações atualizadas do servidor DNS estão funcionando conforme o esperado.

No procedimento a seguir, os valores atuais e novos do endereço IP do servidor DNS são referidos da seguinte forma:

- Endereços IP atuais do DNS: *`OldIP1`*, *`OldIP2`*
- Novos endereços IP do DNS: *`NewIP1`*, *`NewIP2`*

> **Note**
>
> Se esta for a segunda vez que você está realizando esse procedimento, substitua *`OldIP1`* por *`OldIP2`* e *`NewIP1`* por *`NewIP2`*.

Teste as configurações atualizadas do servidor DNS para Windows WorkSpaces

1. Desligue o servidor DNS *`OldIP1`*.
2. Faça login em um Windows WorkSpace.
3. No menu Start (Iniciar) do Windows, escolha Windows System (Sistema Windows) e selecione Command Prompt (Prompt de comando).
4. Execute o comando a seguir, onde *`AD_Name`* é o nome do Active Directory (por exemplo, `corp.example.com`).

```
nslookup AD_Name
```

O comando `nslookup` deve retornar a saída a seguir. (Se esta for a segunda vez que você executa esse procedimento, deverá ver *NewIP2* no lugar de *OldIP2*.)

```
Server:  Full_AD_Name
Address:  NewIP1

Name:    AD_Name
Addresses:  OldIP2
          NewIP1
```

5. Se a saída não for a esperada ou se você receber algum erro, repita a Etapa 1.
6. Aguarde uma hora e confirme que nenhum problema do usuário foi relatado. Verifique se *NewIP1* está recebendo consultas ao DNS e respondendo com as respostas.
7. Após verificar que o primeiro servidor DNS está funcionando corretamente, repita a Etapa 1 para atualizar o segundo servidor DNS, desta vez substituindo *OldIP2* por *NewIP2*. Depois, repita as etapas 2 e 3.

Testar as configurações atualizadas do servidor DNS para WorkSpaces do Linux

1. Desligue o servidor DNS *OldIP1*.
2. Faça login em um Linux WorkSpace.
3. No Linux WorkSpace, abra uma janela do Terminal (Aplicações > Ferramentas do sistema > Terminal MATE).
4. Os endereços IP do servidor DNS retornados na resposta DHCP são gravados no arquivo local `/etc/resolv.conf` no WorkSpace. Execute o comando a seguir para ver o conteúdo do arquivo `/etc/resolv.conf` .

```
cat /etc/resolv.conf
```

Você deve ver a saída a seguir. (Se esta for a segunda vez que você executa esse procedimento, deverá ver *NewIP2* no lugar de *OldIP2*.)

```
; This file is generated by Amazon WorkSpaces
; Modifying it can make your WorkSpace inaccessible until reboot
```

```
options timeout:2 attempts:5
; generated by /usr/sbin/dhclient-script
search region.compute.internal
nameserver NewIP1
nameserver OldIP2
nameserver WorkSpaceIP
```

> **Note**
>
> Se fizer modificações manuais no arquivo `/etc/resolv.conf`, essas alterações serão perdidas quando o WorkSpace for reiniciado.

5. Se a saída não for a esperada ou se você receber algum erro, repita a Etapa 1.
6. Os endereços IP reais do servidor DNS são armazenados no arquivo `/etc/dhcp/dhclient.conf`. Para ver o conteúdo desse arquivo, execute o comando a seguir.

```
sudo cat /etc/dhcp/dhclient.conf
```

Você deve ver a saída a seguir. (Se esta for a segunda vez que você executa esse procedimento, deverá ver *NewIP2* no lugar de *OldIP2*.)

```
# This file is generated by Amazon WorkSpaces
# Modifying it can make your WorkSpace inaccessible until rebuild
prepend domain-name-servers NewIP1, OldIP2; # skylight
```

7. Aguarde uma hora e confirme que nenhum problema do usuário foi relatado. Verifique se *NewIP1* está recebendo consultas ao DNS e respondendo com as respostas.
8. Após verificar que o primeiro servidor DNS está funcionando corretamente, repita a Etapa 1 para atualizar o segundo servidor DNS, desta vez substituindo *OldIP2* por *NewIP2*. Depois, repita as etapas 2 e 3.

Excluir o diretório dos WorkSpaces

Você pode excluir o diretório dos WorkSpaces se ele não estiver mais sendo usado por outros WorkSpaces ou aplicações, como Amazon WorkDocs, Amazon WorkMail ou Amazon Chime. Você deve cancelar o registro de um diretório para poder excluí-lo.

> **Note**
>
> O Simple AD e o AD Connector são disponibilizados gratuitamente para uso com os WorkSpaces. Se não houver WorkSpaces sendo usados com o diretório do Simple AD ou do AD Connector por 30 dias consecutivos, o registro desse diretório será automaticamente cancelado para uso com o Amazon WorkSpaces, e você será cobrado por esse diretório de acordo com os Preços do AWS Directory Service.
> Se você excluir o diretório do Simple AD ou do AD Connector, sempre poderá criar um novo quando quiser começar a usar o WorkSpaces novamente.

O que acontece quando um diretório é excluído

Quando um diretório do Simple AD ou do AWS Directory Service for Microsoft Active Directory é excluído, todos os dados e snapshots do diretório são excluídos e não podem ser recuperados. Após a exclusão do diretório, todas as instâncias do Amazon EC2 agregadas ao diretório permanecem intactas. No entanto, você não pode usar as credenciais do diretório para fazer login nessas instâncias. Em tais instâncias, você deve fazer login com uma Conta da AWS local para a instância.

Quando um diretório do AD Connector é excluído, seu diretório on-premises permanece intacto. Todas as instâncias do Amazon EC2 agregadas ao diretório também permanecem intactas e agregadas ao diretório on-premises. Você ainda pode usar as credenciais do diretório para fazer login nessas instâncias.

Como excluir um diretório

1. Exclua todos os WorkSpaces no diretório. Para obter mais informações, consulte Excluir um WorkSpace.
2. Localize e remova todos os aplicativos e serviços registrados no diretório. Para obter mais informações, consulte Delete Your Directory no Guia de Administração do AWS Directory Service.
3. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
4. No painel de navegação, selecione Directories (Diretórios).
5. Selecione o diretório e escolha Ações, Cancelar o registro.
6. Quando a confirmação for solicitada, escolha Cancelar registro.
7. Selecione o diretório novamente e escolha Ações, Excluir.

8. Quando a confirmação for solicitada, escolha Delete (Excluir).

> **Note**
>
> A remoção de atribuições de aplicativo às vezes pode levar mais tempo do que o esperado. Se você receber a seguinte mensagem de erro, verifique se removeu todas as atribuições de aplicativo e aguarde de 30 a 60 minutos antes de tentar excluir o diretório novamente:
>
> ```
> An Error Has Occurred
> Cannot delete the directory because it still has authorized applications.
> Additional directory details can be viewed at the Directory Service console.
> ```

9. (Opcional) Depois de excluir todos os recursos na rede virtual privada (VPC) para seu diretório, você pode excluir a VPC e liberar o endereço IP elástico usado para o gateway NAT. Para obter mais informações, consulte Deleting your VPC e Trabalhar com endereços IP elásticos no Guia do usuário do Amazon VPC.
10. (Opcional) Para excluir todos os pacotes personalizados e imagens que não serão mais usados, consulte Excluir um WorkSpaces pacote ou imagem personalizada.

Habilitar o Amazon WorkDocs para o AWS Managed Microsoft AD

Se você estiver usando o AWS Managed Microsoft AD com o Amazon WorkSpaces, você pode habilitar o Amazon WorkDocs para seu diretório por meio do console do Amazon WorkDocs ou do console da AWS Directory Service.

> **Note**
>
> O Amazon WorkDocs não está disponível em todas as regiões da AWS em que o Amazon WorkSpaces está disponível. Para obter mais informações, consulte Preços do Amazon WorkDocs.

Como habilitar o WorkDocs por meio do console do Amazon WorkDocs

1. Abra o console do Amazon WorkDocs em https://console.aws.amazon.com/zocalo/.
2. Escolha Create a new WorkDocs Site (Criar novo site do WorkDocs).

3. Em Standard Setup (Configuração padrão), escolha Launch (Iniciar).
4. Selecione o diretório e crie o nome do site.
5. Especifique o usuário que administrará o site do WorkDocs. Você pode usar o administrador ou qualquer usuário criado no diretório.

Para obter mais informações, consulte Getting Started with AWS Managed Microsoft AD no Guia de administração do Amazon WorkDocs.

Para habilitar o WorkDocs por meio do console do AWS Directory Service

1. Abra o console do AWS Directory Service em https://console.aws.amazon.com/directoryservicev2/.
2. No painel de navegação, selecione Directories (Diretórios).
3. Na página Directories (Diretórios), escolha o diretório.
4. Na página Directory details (Detalhes do diretório), selecione a guia Application management (Gerenciamento de aplicativos).
5. Na seção Application access URL (URL de acesso ao aplicativo), se um URL de acesso não tiver sido atribuído ao diretório, o botão Create (Criar) será exibido. Digite um alias do diretório e escolha Create (Criar). Para obter mais informações, consulte Creating an Access URL no Guia de administração do AWS Directory Service.
6. Na seção Application access URL (URL de acesso ao aplicativo), selecione Enable (Habilitar) para habilitar o logon único do Amazon WorkDocs. Para obter mais informações, consulte Single Sign-On no Guia de administração do AWS Directory Service.

Configurar as ferramentas de administração do Active Directory para WorkSpaces

Você executará a maioria das tarefas administrativas para o seu diretório de WorkSpaces com ferramentas de gerenciamento de diretório, como as ferramentas de administração do Active Directory. No entanto, você usará o console do WorkSpaces para executar algumas tarefas relacionadas a diretórios. Para obter mais informações, consulte Gerenciar diretórios para WorkSpaces.

Se você criar um diretório com o AWS Managed Microsoft AD ou o Simple AD que inclui cinco ou mais WorkSpaces, recomendamos centralizar a administração em uma instância do Amazon EC2

Embora seja possível instalar as ferramentas de gerenciamento de diretório em um WorkSpace, usar uma instância do Amazon EC2 é uma solução mais robusta.

Para configurar as ferramentas de administração do Active Directory

1. Inicie uma instância do Amazon EC2 para Windows e junte-a ao diretório de WorkSpaces usando uma das seguintes opções:

   - Se você ainda não tem uma instância do Amazon EC2 para Windows existente, você pode unir a instância ao domínio de diretório ao iniciar a instância. Para obter mais informações, consulte Seamlessly join a Windows EC2 instance no Guia de administração do AWS Directory Service.
   - Se você já tem uma instância do Amazon EC2 para Windows existente, você pode associá-la ao diretório manualmente. Para obter mais informações, consulte Manually Add a Windows Instance no Guia de administração do AWS Directory Service.

2. Instale as ferramentas de administração do Active Directory na instância do Amazon EC2 para Windows. Para obter mais informações, consulte Installing the Active Directory Administration Tools no Guia do administrador do AWS Directory Service.

   > **Note**
   >
   > Ao instalar as ferramentas de administração do Active Directory, selecione também Gerenciamento de políticas de grupo para instalar a ferramenta Editor de gerenciamento de política de grupo (gpmc.msc).

   Quando a instalação do recurso estiver concluída, as ferramentas do Active Directory estarão disponíveis no menu Iniciar do Windows, em Ferramentas Administrativas do Windows.

3. Execute as ferramentas como um administrador do diretório da seguinte forma:

   a. No menu Iniciar do Windows, abra Ferramentas Administrativas do Windows.

   b. Mantenha a tecla Shift pressionada, clique com o botão direito no atalho da ferramenta que deseja usar e selecione Executar como outro usuário.

   c. Insira as credenciais de login do administrador. Com o Simple AD, o nome do usuário é **`Administrator`**, e com o AWS Managed Microsoft AD, o administrador é **`Admin`**.

Agora você pode executar tarefas de administração de diretório usando as ferramentas do Active Directory que você já conhece. Por exemplo, você pode usar a ferramenta Usuários e Computadores do Active Directory para adicionar e remover usuários, promover a administrador do diretório ou redefinir a senha de um usuário. Observe que você deve estar conectado à sua instância do Windows como um usuário que tem permissões para gerenciar usuários no diretório.

Como promover um usuário a administrador de diretório

> **Note**
>
> Este procedimento se aplica somente a diretórios criados com o Simple AD, não com o AWS Managed AD. Para diretórios criados com o AWS Managed AD, consulte Manage Users and Groups in AWS Managed Microsoft AD no Guia de administração do AWS Directory Service.

1. Abra a ferramenta Usuários e Computadores do Active Directory.
2. Navegue até a pasta Usuários em seu domínio e selecione o usuário a ser promovido.
3. Selecione Ação, Propriedades.
4. Na caixa de diálogo Propriedades do ***nome de usuário***, selecione Membro de.
5. Adicione o usuário aos seguintes grupos e selecione OK.
   - Administrators
   - Domain Admins
   - Enterprise Admins
   - Group Policy Creator Owners
   - Schema Admins

Para adicionar ou remover usuários

É possível criar usuários usando o console do Amazon WorkSpaces somente durante o processo de execução de um WorkSpace e não é possível excluir usuários usando o console do Amazon WorkSpaces. A maioria das tarefas de gerenciamento de usuários, incluindo o gerenciamento de grupos de usuários, devem ser realizadas por meio do diretório.

> **Important**
>
> Antes de remover um usuário, é necessário excluir o WorkSpace atribuído a ele. Para obter mais informações, consulte Excluir um WorkSpace.

O processo usado para gerenciar usuários e grupos depende de qual tipo de diretório você está usando.

- Se você estiver usando o AWS Managed Microsoft AD, consulte Manage Users and Groups in AWS Managed Microsoft AD no Guia de administração do AWS Directory Service.
- Se você estiver usando o Simple AD, consulte Manage Users and Groups in Simple AD no Guia de administração do AWS Directory Service.
- Se você usar o Microsoft Active Directory por meio do AD Connector ou uma relação de confiança, poderá gerenciar usuários e grupos usando o módulo do Active Directory.

Para redefinir uma senha do usuário

Quando você redefinir a senha de um usuário existente, não defina Usuário deve alterar a senha no próximo login. Caso contrário, os usuários não poderão se conectar aos seus WorkSpaces. Em vez disso, atribua uma senha temporária segura a cada usuário e instrua-os a alterá-la manualmente de dentro do WorkSpace na próxima vez que fizerem login.

> **Note**
>
> Se você estiver usando o AD Connector ou se os usuários estiverem na região AWS GovCloud (Oeste dos EUA), eles não poderão redefinir as próprias senhas. (A opção Esqueceu sua senha? na tela de login da aplicação cliente do WorkSpaces não estará disponível.)

Inicializar uma área de trabalho virtual usando WorkSpaces

Com o WorkSpaces, você pode provisionar áreas de trabalho virtuais do Microsoft Windows, Amazon Linux ou Ubuntu Linux baseados na nuvem para os usuários, conhecidas como WorkSpaces.

Note

O valor Nome do computador mostrado para um WorkSpace no console do Amazon WorkSpaces varia, dependendo do tipo de WorkSpace que você iniciou (Amazon Linux, Ubuntu ou Windows). O nome do computador de um WorkSpace pode ter um de seguintes formatos:

- Amazon Linux: A-*xxxxxxxxxxxxx*
- Ubuntu: U-*xxxxxxxxxxxxx*
- Windows: IP-C*xxxxxx* ou WSAMZN-*xxxxxxx* ou EC2AMAZ-*xxxxxxx*

Para WorkSpaces do Windows, o formato do nome do computador é determinado pelo tipo de pacote e, no caso de WorkSpaces criados a partir de pacotes públicos ou de pacotes personalizados baseados em imagens públicas, pelo momento em que as imagens públicas foram criadas.
A partir de 22 de junho de 2020, os WorkSpaces do Windows inicializados de pacotes públicos têm o formato WSAMZN-*xxxxxxx* para nomes de computador, em vez do formato IP-C*xxxxxx*.
Para pacotes personalizados baseados em uma imagem pública, se a imagem pública tiver sido criada antes de 22 de junho de 2020, os nomes dos computadores estarão no formato EC2AMAZ-*xxxxxxx*. Se a imagem pública foi criada em 22 de junho de 2020 ou posteriormente, os nomes dos computadores estão no formato WSAMZN-*xxxxxxx*.
Para pacotes do tipo traga a sua própria licença (BYOL), o formato DESKTOP-*xxxxxxx* ou EC2AMAZ-*xxxxxxx* é usado para os nomes dos computadores por padrão.
Se você especificou um formato personalizado para os nomes dos computadores em seus pacotes personalizados ou BYOL, seu formato personalizado substituirá esses padrões. Para especificar um formato personalizado, consulte Crie uma WorkSpaces imagem e um pacote personalizados.
Importante: se você alterar o nome do computador de um WorkSpace por meio das configurações do sistema do Windows, não poderá mais acessar o WorkSpace.

O WorkSpaces usa um diretório para armazenar e gerenciar informações para seus WorkSpaces e usuários. Você pode realizar uma das seguintes ações:

- Crie um diretório do Simple AD.
- Crie um AWS Directory Service para Microsoft Active Directory, também conhecido como Microsoft AD gerenciado pela AWS.
- Conecte-se a um Microsoft Active Directory existente usando o Active Directory Connector.
- Crie uma relação de confiança entre o diretório do Microsoft AD gerenciado pela AWS e o domínio no local.

> **Note**
>
> - Diretórios compartilhados não são compatíveis para uso no Amazon WorkSpaces no momento.
> - Se você configurar o diretório do AWS Managed Microsoft AD para replicação multirregional, somente o diretório na região primária poderá ser registrado para uso no Amazon WorkSpaces. As tentativas de registrar o diretório em uma região replicada para uso com o Amazon WorkSpaces vão falhar. A replicação multirregional com o AWS Managed Microsoft AD não é compatível para uso com o Amazon WorkSpaces em regiões replicadas.
> - O Simple AD e o AD Connector são disponibilizados gratuitamente para uso com os WorkSpaces. Se não houver WorkSpaces sendo usados com o diretório do Simple AD ou do AD Connector por 30 dias consecutivos, o registro desse diretório será automaticamente cancelado para uso com o Amazon WorkSpaces, e você será cobrado por esse diretório de acordo com os Preços do AWS Directory Service.
>
>   Para excluir diretórios vazios, consulte Excluir o diretório dos WorkSpaces. Se você excluir o diretório do Simple AD ou do AD Connector, sempre poderá criar um novo quando quiser começar a usar o WorkSpaces novamente.

Os tutoriais a seguir mostram como iniciar um WorkSpace usando as opções de serviço de diretório com suporte.

Tutoriais

- Inicializar um WorkSpace usando o AWS Managed Microsoft AD

- Inicializar um WorkSpace usando o Simple AD
- Inicializar um WorkSpace usando o AD Connector
- Inicializar um WorkSpace usando um domínio confiável

Inicializar um WorkSpace usando o AWS Managed Microsoft AD

O WorkSpaces permite provisionar áreas de trabalho virtuais e baseadas na nuvem do Windows e do Linux, que são conhecidas como WorkSpaces.

O WorkSpaces usa diretórios para armazenar e gerenciar informações para seus WorkSpaces e usuários. Para seu diretório, você pode escolher entre o Simple AD, o AD Connector ou o AWS Directory Service para o Microsoft Active Directory, também conhecido como Microsoft AD gerenciado pela AWS. Além disso, você pode estabelecer um relacionamento de confiança entre o diretório do Microsoft AD gerenciado pela AWS e o domínio no local.

Neste tutorial, iniciamos um WorkSpace que usa o Microsoft AD gerenciado pela AWS. Para tutoriais que usam as outras opções, consulte Inicializar uma área de trabalho virtual usando WorkSpaces.

Tarefas

- Antes de começar
- Etapa 1: criar um diretório do Microsoft AD gerenciado pela AWS
- Etapa 2: criar um WorkSpace
- Etapa 3: Conecte-se ao WorkSpace
- Próximas etapas

Antes de começar

- O WorkSpaces não está disponível em todas as regiões. Verifique as regiões compatíveis e selecione uma região para seus WorkSpaces. Para obter mais informações sobre as regiões compatíveis, consulte os preços do WorkSpaces por região da AWS.
- Ao ativar um WorkSpace, você deve selecionar um pacote do WorkSpace. O pacote é uma combinação de sistema operacional e recursos de armazenamento, computação e software. Para obter mais informações, consulte Pacotes do Amazon WorkSpaces.

- Ao criar um diretório usando o AWS Directory Service ou ativar um WorkSpace, você deve criar ou selecionar uma Virtual Private Cloud configurada com uma sub-rede pública e duas sub-redes privadas. Para obter mais informações, consulte Configurar uma VPC para WorkSpaces.

Etapa 1: criar um diretório do Microsoft AD gerenciado pela AWS

Primeiro, crie um diretório do Microsoft AD gerenciado pela AWS. O AWS Directory Service cria dois servidores de diretório, um em cada uma das sub-redes privadas de sua VPC. Observe que inicialmente não há usuários no diretório. Você adicionará um usuário na próxima etapa ao ativar o WorkSpace.

> **Note**
>
> - Diretórios compartilhados não são compatíveis para uso no Amazon WorkSpaces no momento.
> - Se o diretório do AWS Managed Microsoft AD tiver sido configurado para replicação multirregional, somente o diretório na região primária poderá ser registrado para uso no Amazon WorkSpaces. As tentativas de registrar o diretório em uma região replicada para uso com o Amazon WorkSpaces vão falhar. A replicação multirregional com o AWS Managed Microsoft AD não é compatível para uso com o Amazon WorkSpaces em regiões replicadas.

Para criar um diretório do Microsoft AD gerenciado pela AWS

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione Directories (Diretórios).
3. Escolha Configurar diretório, Criar Microsoft AD.
4. Configure o diretório da seguinte forma:

    a. Em Organization name (Nome da organização), insira um nome de organização exclusivo para o seu diretório (por exemplo, my-demo-directory). Esse nome deve ter pelo menos quatro caracteres, conter apenas caracteres alfanuméricos e hífens (-) e começar ou terminar com um caractere diferente de um hífen.

    b. Em Directory DNS (DNS do diretório), insira o nome do diretório totalmente qualificado (por exemplo, workspaces.demo.com).

> **Important**
>
> Se você precisar atualizar o servidor DNS após iniciar seus WorkSpaces, siga o procedimento em Atualizar servidores DNS do Amazon WorkSpaces para garantir que os WorkSpaces sejam atualizados adequadamente.

c. Em NetBIOS name (Nome NetBIOS), insira um nome curto para o diretório (por exemplo, workspaces).

d. Em Admin password (Senha do administrador) e Confirm password (Confirmar senha), insira uma senha para a conta do administrador do diretório. Para obter mais informações sobre os requisitos de senha, consulte Create Your AWS Managed Microsoft AD Directory no Guia de administração do AWS Directory Service.

e. (Opcional) Em Description (Descrição), insira uma descrição para a política.

f. Em VPC, selecione a VPC que você criou.

g. Em Sub-redes, selecione as duas sub-redes privadas (com os blocos CIDR `10.0.1.0/24` e `10.0.2.0/24`).

h. Escolha Next Step.

5. Escolha Criar Microsoft AD.
6. Escolha Done (Concluído). O status inicial do diretório é `Creating`. Quando a criação de diretórios estiver completa, o status será `Active`.

Etapa 2: criar um WorkSpace

Agora que você criou um diretório do Microsoft AD gerenciado pela AWS, já pode criar um WorkSpace.

Para criar um WorkSpace

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione WorkSpaces.
3. Escolha Ativar WorkSpaces.
4. Na página Selecionar um diretório, escolha o diretório criado e, em seguida, selecione Próxima etapa. O WorkSpaces registra seu diretório.
5. Na página Identificar usuários, adicione um novo usuário ao seu diretório da seguinte forma:

a. Preencha o Nome do usuário, Nome, Sobrenome e E-mail. Use um endereço de e-mail ao qual você tenha acesso.

b. Escolha Criar usuários.

c. Escolha Next Step.

6. Na página Selecionar pacote, selecione um pacote e, em seguida, escolha Próxima etapa.

> **Note**
>
> Analise os usos e as especificações recomendados de cada pacote para ajudar a garantir a escolha do pacote mais adequado para os usuários. Para obter mais informações sobre cada caso de uso, consulte Pacotes do Amazon WorkSpaces. Para obter mais informações sobre especificações de pacotes, usos recomendados e preços, consulte Preço do Amazon WorkSpaces.

7. Na página Configuração de WorkSpaces, escolha um modo de execução e selecione Próxima etapa.

8. Na página Revisar e ativar WorkSpaces, escolha Ativar WorkSpaces. O status inicial do WorkSpace é `PENDING`. Ao terminar de ativar os WorkSpaces, o status é `AVAILABLE` e um convite é enviado ao endereço de e-mail que você especificou para o usuário.

> **Note**
>
> Os convites por e-mail não são enviados se o usuário já existir no Active Directory. Em vez disso, envie manualmente um convite por e-mail ao usuário. Para obter mais informações, consulte Enviar um convite por e-mail.

9. (Opcional) Se o Amazon WorkDocs for compatível com a região, será possível habilitar o Amazon WorkDocs para todos os usuários no diretório. Para obter mais informações, consulte Habilitar o Amazon WorkDocs para o AWS Managed Microsoft AD. Para obter mais informações sobre o Amazon WorkDocs, consulte Amazon WorkDocs Drive no Guia de administração do Amazon WorkDocs.

Etapa 3: Conecte-se ao WorkSpace

Depois de receber o e-mail de convite, você pode se conectar ao seu WorkSpace usando o cliente de sua escolha. Depois de fazer login, o cliente exibe o desktop WorkSpace.

Para se conectar ao WorkSpace

1. Abra o link no e-mail de convite. Quando solicitado, especifique uma senha e ative o usuário. Lembre-se dessa senha, pois você precisará dela para fazer login em seu WorkSpace.

   > **Note**
   >
   > As senhas diferenciam maiúsculas de minúsculas e devem ter entre 8 e 64 caracteres. As senhas devem conter pelo menos um caractere de cada uma das seguintes categorias: letras minúsculas (a-z), letras maiúsculas (A-Z), números (0-9) e ~!@#$ %^&*_-+=`|\(){}[]:;'"<>,.?/.

2. Consulte WorkSpaces Clients no Guia do usuário do Amazon WorkSpaces para obter mais informações sobre os requisitos de cada cliente e, em seguida, execute uma das seguintes opções:

   - Quando solicitado, faça download de um dos aplicativos clientes ou ative o Web Access.
   - Se você não receber o prompt e ainda não tiver instalado uma aplicação cliente, abra https://clients.amazonworkspaces.com/ e faça download de uma das aplicações cliente ou inicialize o Acesso via Web.

   > **Note**
   >
   > Não é possível usar um navegador da web (Acesso via Web) para se conectar aos WorkSpaces do Amazon Linux.

3. Inicie o cliente, digite o código de registro do e-mail de convite e selecione Registrar.
4. Quando for necessário fazer login, insira as credenciais de login do usuário e clique em Fazer login.
5. (Opcional) Quando solicitado a salvar suas credenciais, escolha Sim.

Próximas etapas

Você pode continuar a personalizar o WorkSpace que acabou de criar. Por exemplo, é possível instalar o software e, em seguida, criar um pacote personalizado do seu WorkSpace. Você também pode realizar várias tarefas administrativas nos WorkSpaces e em seu diretório de WorkSpaces. Se

você terminar o trabalho com o WorkSpace, poderá excluí-lo. Para obter mais informações, consulte a documentação a seguir.

- Crie uma WorkSpaces imagem e um pacote personalizados
- Administre seu WorkSpaces
- Gerenciar diretórios para WorkSpaces
- Excluir um WorkSpace

Para obter mais informações sobre o uso das aplicações cliente do WorkSpaces, como configurar vários monitores ou usar dispositivos periféricos, consulte WorkSpaces Clients e Peripheral Device Support no Guia do usuário do Amazon WorkSpaces.

Inicializar um WorkSpace usando o Simple AD

O WorkSpaces permite provisionar áreas de trabalho virtuais e baseadas na nuvem do Microsoft Windows e do Linux, que são conhecidas como WorkSpaces.

O WorkSpaces usa diretórios para armazenar e gerenciar informações para seus WorkSpaces e usuários. Para seu diretório, você pode escolher entre o Simple AD, o AD Connector ou o AWS Directory Service para o Microsoft Active Directory, também conhecido como Microsoft AD gerenciado pela AWS. Além disso, você pode estabelecer um relacionamento de confiança entre o diretório do Microsoft AD gerenciado pela AWS e o domínio no local.

Neste tutorial, ativamos um WorkSpace que usa o Simple AD. Para tutoriais que usam as outras opções, consulte Inicializar uma área de trabalho virtual usando WorkSpaces.

Tarefas

- Antes de começar
- Etapa 1: Criar um diretório do Simple AD
- Etapa 2: criar um WorkSpace
- Etapa 3: Conecte-se ao WorkSpace
- Próximas etapas

Antes de começar

- O Simple AD não está disponível em todas as regiões. Verifique as regiões compatíveis e selecione uma região para seu diretório do Simple AD. Para obter mais informações sobre as regiões compatíveis com o Simple AD, consulte Region Availability for AWS Directory Service.
- O WorkSpaces não está disponível em todas as regiões. Verifique as regiões compatíveis e selecione uma região para seus WorkSpaces. Para obter mais informações sobre as regiões compatíveis, consulte os preços do WorkSpaces por região da AWS.
- Ao ativar um WorkSpace, você deve selecionar um pacote do WorkSpace. O pacote é uma combinação de sistema operacional e recursos de armazenamento, computação e software. Para obter mais informações, consulte Pacotes do Amazon WorkSpaces.
- Ao criar um diretório usando o AWS Directory Service ou ativar um WorkSpace, você deve criar ou selecionar uma Virtual Private Cloud configurada com uma sub-rede pública e duas sub-redes privadas. Para obter mais informações, consulte Configurar uma VPC para WorkSpaces.

Etapa 1: Criar um diretório do Simple AD

Crie um diretório do Simple AD. O AWS Directory Service cria dois servidores de diretório, um em cada uma das sub-redes privadas de sua VPC. Observe que inicialmente não há usuários no diretório. Você adicionará um usuário na próxima etapa ao criar o WorkSpace.

> **Note**
>
> O Simple AD é disponibilizado gratuitamente para uso com os WorkSpaces. Se não houver WorkSpaces sendo usados com o diretório do Simple AD por 30 dias consecutivos, o registro desse diretório será automaticamente cancelado para uso com o Amazon WorkSpaces, e você será cobrado por esse diretório de acordo com os Preços do AWS Directory Service. Para excluir diretórios vazios, consulte Excluir o diretório dos WorkSpaces. Se você excluir o diretório do Simple AD, sempre poderá criar um novo quando quiser começar a usar o WorkSpaces novamente.

Para criar um diretório do Simple AD

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione Directories (Diretórios).

3. Selecione Configurar diretório, Simple AD e Próximo.
4. Configure o diretório da seguinte forma:

   a. Em Organization name (Nome da organização), insira um nome de organização exclusivo para seu diretório (por exemplo, my-example-directory). Esse nome deve ter pelo menos quatro caracteres, conter apenas caracteres alfanuméricos e hífens (-) e começar ou terminar com um caractere diferente de um hífen.

   b. Em Nome do DNS do diretório, insira o nome do diretório totalmente qualificado (por exemplo, example.com).

   > **Important**
   >
   > Se você precisar atualizar o servidor DNS após iniciar seus WorkSpaces, siga o procedimento em Atualizar servidores DNS do Amazon WorkSpaces para garantir que os WorkSpaces sejam atualizados adequadamente.

   c. Em NetBIOS name (Nome NetBIOS), insira um nome curto para o diretório (por exemplo, example).

   d. Em Admin password (Senha do administrador) e Confirm password (Confirmar senha), insira uma senha para a conta do administrador do diretório. Para obter mais informações sobre os requisitos de senha, consulte How to Create a Microsoft AD Directory no Guia de administração do AWS Directory Service.

   e. (Opcional) Em Description (Descrição), insira uma descrição para a política.

   f. Em Tamanho do diretório, selecione Pequeno.

   g. Em VPC, selecione a VPC que você criou.

   h. Em Sub-redes, selecione as duas sub-redes privadas (com os blocos CIDR `10.0.1.0/24` e `10.0.2.0/24`).

   i. Escolha Next (Próximo).

5. Selecione Criar diretório.
6. O status inicial do diretório é `Requested` e, em seguida, `Creating`. Quando a criação do diretório estiver concluída (isso pode levar alguns minutos), o status será `Active`.

O que acontece durante a criação do diretório

O WorkSpaces executa as seguintes tarefas em seu nome:

- Cria um perfil do IAM para permitir que o serviço WorkSpaces crie interfaces de rede elásticas e liste os diretórios de seus WorkSpaces. Essa função tem o nome `workspaces_DefaultRole`.
- Configura um diretório do Simple AD na VPC que é usado para armazenar informações do usuário e do WorkSpace. O diretório tem uma conta de administrador com o nome de usuário Administrador e a senha especificada.
- Cria dois security groups, um para controladores do diretório e outro para os WorkSpaces no diretório.

Etapa 2: criar um WorkSpace

Agora você está pronto para ativar o WorkSpace.

Para criar um WorkSpace para um usuário

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione WorkSpaces.
3. Escolha Ativar WorkSpaces.
4. Na página Selecionar um diretório, faça o seguinte:
   a. Em Diretório, escolha o diretório que você criou.
   b. Em Habilitar permissões de autoatendimento, selecione Sim ou Não e insira uma descrição.
   c. Em Ativar o Amazon WorkDocs, selecione Sim.

      > **Note**
      >
      > Essa opção só estará disponível se o Amazon WorkDocs estiver disponível na região selecionada.

   d. Escolha Next Step. O WorkSpaces registra seu diretório do Simple AD.
5. Na página Identificar usuários, adicione um novo usuário ao seu diretório da seguinte forma:
   a. Preencha o Nome do usuário, Nome, Sobrenome e E-mail. Use um endereço de e-mail ao qual você tenha acesso.
   b. Escolha Criar usuários.
   c. Escolha Next Step.
6. Na página Selecionar pacote, selecione um pacote e, em seguida, escolha Próxima etapa.

> **Note**
>
> Analise os usos e as especificações recomendados de cada pacote para ajudar a garantir a escolha do pacote mais adequado para os usuários. Para obter mais informações sobre cada caso de uso, consulte Pacotes do Amazon WorkSpaces. Para obter mais informações sobre especificações de pacotes, usos recomendados e preços, consulte Preço do Amazon WorkSpaces.

7. Na página Configuração de WorkSpaces, escolha um modo de execução e selecione Próxima etapa.
8. Na página Revisar e ativar WorkSpaces, escolha Ativar WorkSpaces. O status inicial do WorkSpace é `PENDING`. Ao terminar de iniciar os WorkSpaces (isso pode levar até 20 minutos), o status é `AVAILABLE` e um convite é enviado ao endereço de e-mail especificado para o usuário.

> **Note**
>
> Os convites por e-mail não são enviados se o usuário já existir no Active Directory. Em vez disso, envie manualmente um convite por e-mail ao usuário. Para obter mais informações, consulte Enviar um convite por e-mail.

Etapa 3: Conecte-se ao WorkSpace

Depois de receber o e-mail de convite, você pode se conectar ao seu WorkSpace usando o cliente de sua escolha. Depois de fazer login, o cliente exibe o desktop WorkSpace.

Para se conectar ao WorkSpace

1. Abra o link no e-mail de convite. Quando solicitado, insira uma senha e ative o usuário. Lembre-se dessa senha, pois você precisará dela para fazer login em seu WorkSpace.

> **Note**
>
> As senhas diferenciam maiúsculas de minúsculas e devem ter entre 8 e 64 caracteres. As senhas devem conter pelo menos um caractere de cada uma das seguintes

categorias: letras minúsculas (a-z), letras maiúsculas (A-Z), números (0-9) e ~!@#$ %^&*_-+=`|\(){}[]:;'"<>,.?/.

2. Consulte WorkSpaces Clients no Guia do usuário do Amazon WorkSpaces para obter mais informações sobre os requisitos de cada cliente e, em seguida, execute uma das seguintes opções:

   - Quando receber o prompt, faça download de uma das aplicações cliente ou inicie o Acesso via Web.
   - Se você não receber o prompt e ainda não tiver instalado uma aplicação cliente, abra https://clients.amazonworkspaces.com/ e faça download de uma das aplicações cliente ou inicialize o Acesso via Web.

   > **Note**
   >
   > Não é possível usar um navegador da web (Acesso via Web) para se conectar aos WorkSpaces do Amazon Linux.

3. Inicie o cliente, digite o código de registro do e-mail de convite e selecione Registrar.
4. Quando for necessário fazer login, insira as credenciais de login do usuário e clique em Fazer login.
5. (Opcional) Quando solicitado a salvar suas credenciais, escolha Sim.

Próximas etapas

Você pode continuar a personalizar o WorkSpace que acabou de criar. Por exemplo, é possível instalar o software e, em seguida, criar um pacote personalizado do seu WorkSpace. Você também pode realizar várias tarefas administrativas nos WorkSpaces e em seu diretório de WorkSpaces. Se você terminar o trabalho com o WorkSpace, poderá excluí-lo. Para obter mais informações, consulte a documentação a seguir.

- Crie uma WorkSpaces imagem e um pacote personalizados
- Administre seu WorkSpaces
- Gerenciar diretórios para WorkSpaces
- Excluir um WorkSpace

Para obter mais informações sobre o uso das aplicações cliente do WorkSpaces, como configurar vários monitores ou usar dispositivos periféricos, consulte WorkSpaces Clients e Peripheral Device Support no Guia do usuário do Amazon WorkSpaces.

Inicializar um WorkSpace usando o AD Connector

O WorkSpaces permite provisionar áreas de trabalho virtuais e baseadas na nuvem do Microsoft Windows e do Linux, que são conhecidas como WorkSpaces.

O WorkSpaces usa diretórios para armazenar e gerenciar informações para seus WorkSpaces e usuários. Para seu diretório, você pode escolher entre o Simple AD, o AD Connector ou o AWS Directory Service para o Microsoft Active Directory, também conhecido como Microsoft AD gerenciado pela AWS. Além disso, você pode estabelecer um relacionamento de confiança entre o diretório do Microsoft AD gerenciado pela AWS e o domínio no local.

Neste tutorial, ativamos um WorkSpace que usa o AD Connector. Para tutoriais que usam as outras opções, consulte Inicializar uma área de trabalho virtual usando WorkSpaces.

Tarefas

Antes de começar

- O WorkSpaces não está disponível em todas as regiões. Verifique as regiões compatíveis e selecione uma região para seus WorkSpaces. Para obter mais informações sobre as regiões compatíveis, consulte os preços do WorkSpaces por região da AWS.
- Ao ativar um WorkSpace, você deve selecionar um pacote do WorkSpace. O pacote é uma combinação de sistema operacional e recursos de armazenamento, computação e software. Para obter mais informações, consulte Pacotes do Amazon WorkSpaces.
- Crie uma Virtual Private Cloud com pelo menos duas sub-redes privadas. Para obter mais informações, consulte Configurar uma VPC para WorkSpaces. A VPC deve estar conectada à sua rede no local por meio de uma conexão de rede privada virtual (VPN) ou AWS Direct Connect.

Para obter mais informações, consulte AD Connector Prerequisites no Guia de administração do AWS Directory Service.

- Conceda acesso à Internet no WorkSpace. Para obter mais informações, consulte Forneça acesso à Internet a partir do seu WorkSpace.

Etapa 1: Criar um AD Connector

> **Note**
>
> O AD Connector é disponibilizado gratuitamente para uso com os WorkSpaces. Se não houver WorkSpaces sendo usados com o diretório do AD Connector por 30 dias consecutivos, o registro desse diretório será automaticamente cancelado para uso com o Amazon WorkSpaces, e você será cobrado por esse diretório de acordo com os Preços do AWS Directory Service.
> Para excluir diretórios vazios, consulte Excluir o diretório dos WorkSpaces. Se você excluir o diretório do AD Connector, sempre poderá criar um novo quando quiser começar a usar o WorkSpaces novamente.

Como criar um AD Connector

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione Directories (Diretórios).
3. Escolha Configurar diretório, Criar AD Connector.
4. Em Organization name (Nome da organização), insira um nome de organização exclusivo para seu diretório (por exemplo, my-example-directory). Esse nome deve ter pelo menos quatro caracteres, conter apenas caracteres alfanuméricos e hífens (-) e começar ou terminar com um caractere diferente de um hífen.
5. Em Connected directory DNS (DNS do diretório conectado), insira o nome de seu diretório local totalmente qualificado (por exemplo, example.com).
6. Em Connected directory NetBIOS name (Nome NetBIOS do diretório conectado), insira o nome curto de seu diretório local (por exemplo, example).
7. Em Connector account username (Nome do usuário da conta do Connector), insira o nome de usuário de um usuário em seu diretório local. O usuário deve ter permissões para ler usuários e grupos, criar objetos de computador e inserir computadores no domínio.

8. Em Senha da conta do Connector e Confirmar senha, insira a senha para o usuário on-premises.
9. Em DNS address (Endereço DNS), insira o endereço IP de pelo menos um servidor DNS em seu diretório local.

> **Important**
>
> Se você precisar atualizar o endereço IP do servidor DNS após iniciar seus WorkSpaces, siga o procedimento em Atualizar servidores DNS do Amazon WorkSpaces para garantir que os WorkSpaces sejam atualizados adequadamente.

10. (Opcional) Em Description (Descrição), insira uma descrição para a política.
11. Mantenha Tamanho como Pequeno.
12. Em VPC, selecione sua VPC.
13. Em Sub-redes, selecione as sub-redes. Os servidores DNS que você especificou devem ser acessíveis em cada sub-rede.
14. Escolha Next Step.
15. Escolha Criar AD Connector. A conexão do diretório leva vários minutos. O status inicial do diretório é `Requested` e, em seguida, `Creating`. Quando a criação de diretórios estiver completa, o status será `Active`.

Etapa 2: criar um WorkSpace

Agora você está pronto para ativar os WorkSpaces para um ou mais usuários em seu diretório no local.

Como iniciar um WorkSpace para um usuário existente

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione WorkSpaces.
3. Escolha Ativar WorkSpaces.
4. Em Diretório, escolha o diretório que você criou.
5. (Opcional) Se esta for a primeira vez que você inicia um WorkSpace nesse diretório, e o Amazon WorkDocs for compatível na região, você poderá habilitar ou desabilitar o Amazon WorkDocs

para todos os usuários no diretório. Para obter mais informações sobre o Amazon WorkDocs, consulte Amazon WorkDocs Drive no Guia de administração do Amazon WorkDocs.

6. Escolha Next (Próximo). O WorkSpaces registra seu AD Connector.
7. Selecione um ou mais usuários existentes do seu diretório no local. Não adicione novos usuários a um diretório on-premises por meio do console do WorkSpaces.

   Para encontrar os usuários a serem selecionados, insira todo o nome ou parte do nome do usuário e escolha Search (Pesquisar) ou Show All Users (Mostrar todos os usuários). Observe que não é possível selecionar um usuário que não tenha um endereço de e-mail.

   Depois de selecionar os usuários, escolha Adicionar selecionado e, em seguida, escolha Próxima etapa.
8. Em Selecionar pacote, escolha o pacote padrão do WorkSpace para ser usado nos WorkSpaces. Em Atribuir pacotes de WorkSpaces, você pode escolher outro pacote para um WorkSpace individual, se necessário. Quando terminar, escolha Próxima etapa.

   > **Note**
   >
   > Analise os usos e as especificações recomendados de cada pacote para ajudar a garantir a escolha do pacote mais adequado para os usuários. Para obter mais informações sobre cada caso de uso, consulte Pacotes do Amazon WorkSpaces. Para obter mais informações sobre especificações de pacotes, usos recomendados e preços, consulte Preço do Amazon WorkSpaces.
9. Escolha um modo de execução para os seus WorkSpaces e selecione Próxima etapa. Para obter mais informações, consulte Gerenciar o modo de execução do WorkSpace.
10. Escolha Ativar WorkSpaces. O status inicial do WorkSpace é `PENDING`. Quando a ativação estiver concluída, o status será `AVAILABLE`.
11. Envie convites para o endereço de e-mail de cada usuário. (Esses convites não serão enviados automaticamente se você estiver usando o AD Connector.) Para obter mais informações, consulte Enviar um convite por e-mail.

Etapa 3: Conecte-se ao WorkSpace

Você pode se conectar ao seu WorkSpace usando o cliente de sua escolha. Depois de fazer login, o cliente exibe o desktop WorkSpace.

Para se conectar ao WorkSpace

1. Abra o link no e-mail de convite.
2. Consulte WorkSpaces Clients no Guia do usuário do Amazon WorkSpaces para obter mais informações sobre os requisitos de cada cliente e, em seguida, execute uma das seguintes opções:
   - Quando solicitado, faça download de um dos aplicativos clientes ou ative o Web Access.
   - Se você não receber o prompt e ainda não tiver instalado uma aplicação cliente, abra https://clients.amazonworkspaces.com/ e faça download de uma das aplicações cliente ou inicialize o Acesso via Web.

   > **Note**
   >
   > Não é possível usar um navegador da web (Acesso via Web) para se conectar aos WorkSpaces do Amazon Linux.

3. Inicie o cliente, digite o código de registro do e-mail de convite e selecione Registrar.
4. Quando for necessário fazer login, insira as credenciais de login do usuário e clique em Fazer login.
5. (Opcional) Quando solicitado a salvar suas credenciais, escolha Sim.

> **Note**
>
> Como você está usando o AD Connector, seus usuários não poderão redefinir suas próprias senhas. (A opção Esqueceu sua senha? na tela de login do aplicativo cliente do WorkSpaces não estará disponível.) Para obter informações sobre como redefinir senhas de usuários, consulte Configurar as ferramentas de administração do Active Directory para WorkSpaces.

Próximas etapas

Você pode continuar a personalizar o WorkSpace que acabou de criar. Por exemplo, é possível instalar o software e, em seguida, criar um pacote personalizado do seu WorkSpace. Você também pode realizar várias tarefas administrativas nos WorkSpaces e em seu diretório de WorkSpaces. Se

você terminar o trabalho com o WorkSpace, poderá excluí-lo. Para obter mais informações, consulte a documentação a seguir.

- Crie uma WorkSpaces imagem e um pacote personalizados
- Administre seu WorkSpaces
- Gerenciar diretórios para WorkSpaces
- Excluir um WorkSpace

Para obter mais informações sobre o uso das aplicações cliente do WorkSpaces, como configurar vários monitores ou usar dispositivos periféricos, consulte WorkSpaces Clients e Peripheral Device Support no Guia do usuário do Amazon WorkSpaces.

Inicializar um WorkSpace usando um domínio confiável

O WorkSpaces permite provisionar áreas de trabalho virtuais e baseadas na nuvem do Microsoft Windows, do Amazon Linux ou do Ubuntu Linux, que são conhecidas como WorkSpaces.

O WorkSpaces usa diretórios para armazenar e gerenciar informações para seus WorkSpaces e usuários. Para seu diretório, você pode escolher entre o Simple AD, o AD Connector ou o AWS Directory Service para o Microsoft Active Directory, também conhecido como Microsoft AD gerenciado pela AWS. Além disso, você pode estabelecer um relacionamento de confiança entre o diretório do Microsoft AD gerenciado pela AWS e o domínio no local.

Neste tutorial, ativamos um WorkSpace que usa um relacionamento de confiança. Para tutoriais que usam as outras opções, consulte Inicializar uma área de trabalho virtual usando WorkSpaces.

Tarefas

- Antes de começar
- Etapa 1: Estabelecer uma relação de confiança
- Etapa 2: criar um WorkSpace
- Etapa 3: Conecte-se ao WorkSpace
- Próximas etapas

Antes de começar

- A inicialização do WorkSpaces com Contas da AWS em um domínio confiável separado funciona com o AWS Managed Microsoft AD quando ele é configurado com uma relação de confiança com o diretório on-premises. No entanto, WorkSpaces usando o Simple AD ou o AD Connector não podem iniciar WorkSpaces para usuários de um domínio confiável.
- O WorkSpaces não está disponível em todas as regiões. Verifique as regiões compatíveis e selecione uma região para seus WorkSpaces. Para obter mais informações sobre as regiões compatíveis, consulte os preços do WorkSpaces por região da AWS.
- Ao ativar um WorkSpace, você deve selecionar um pacote do WorkSpace. Pacote é uma combinação de recursos de armazenamento, computação e software. Para obter mais informações, consulte Pacotes do Amazon WorkSpaces.
- Ao criar um diretório usando o AWS Directory Service ou ativar um WorkSpace, você deve criar ou selecionar uma Virtual Private Cloud configurada com uma sub-rede pública e duas sub-redes privadas. Para obter mais informações, consulte Configurar uma VPC para WorkSpaces.

Etapa 1: Estabelecer uma relação de confiança

Para configurar o relacionamento de confiança

1. Configure o Microsoft AD gerenciado pela AWS na sua virtual private cloud (VPC). Para obter mais informações, consulte Criar seu diretório do AWS Managed Microsoft AD no Guia de administração do AWS Directory Service.

> **Note**
>
> - Diretórios compartilhados não são compatíveis para uso no Amazon WorkSpaces no momento.
> - Se o diretório do AWS Managed Microsoft AD tiver sido configurado para replicação multirregional, somente o diretório na região primária poderá ser registrado para uso no Amazon WorkSpaces. As tentativas de registrar o diretório em uma região replicada para uso com o Amazon WorkSpaces vão falhar. A replicação multirregional com o AWS Managed Microsoft AD não é compatível para uso com o Amazon WorkSpaces em regiões replicadas.

2. Crie uma relação de confiança entre o Microsoft AD gerenciado pela AWS e o domínio no local. Verifique se a confiança está configurada bidirecionalmente. Para obter mais informações, consulte Tutorial: Create a Trust Relationship Between Your AWS Managed Microsoft AD and Your On-Premises Domain no Guia de administração do AWS Directory Service.

Uma confiança unidirecional ou bidirecional pode ser usada para fazer o gerenciamento e a autenticação com o WorkSpaces, e para que ele possa ser provisionado para usuários e grupos on-premises. Para obter mais informações, consulte Deploy Amazon WorkSpaces using a One-Way Trust Resource Domain with AWS Directory Service.

> **Note**
>
> Os WorkSpaces do Ubuntu usam o System Security Services Daemon (SSSD) para integração com o Active Directory, e o SSSD não é compatível com a confiança de floresta. Em vez disso, configure a confiança externa. A confiança bidirecional é recomendada para WorkSpaces do Amazon Linux e Ubuntu.

Etapa 2: criar um WorkSpace

Depois de estabelecer uma relação de confiança entre o Microsoft AD gerenciado pela AWS e o domínio no local do Microsoft Active Directory, você pode provisionar o WorkSpaces para usuários no domínio local.

Observe que você deve garantir que as configurações do GPO sejam replicadas entre domínios antes de aplicá-las ao WorkSpaces.

Como iniciar o WorkSpaces para usuários em um domínio local confiável

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione WorkSpaces.
3. Escolha Ativar WorkSpaces.
4. Na página Selecionar um diretório, escolha o diretório recém-registrado e, em seguida, selecione Próxima etapa.
5. Na página Identificar usuários, faça o seguinte:

    a. Em Selecionar confiança da floresta, selecione o relacionamento de confiança que você criou.

b. Selecione os usuários no domínio no local e, em seguida, escolha Adicionar selecionado.

c. Escolha Next Step.

6. Selecione o pacote a ser usado nos WorkSpaces e, em seguida, escolha Próxima etapa.

> **Note**
>
> Analise os usos e as especificações recomendados de cada pacote para ajudar a garantir a escolha do pacote mais adequado para os usuários. Para obter mais informações sobre cada caso de uso, consulte Pacotes do Amazon WorkSpaces. Para obter mais informações sobre especificações de pacotes, usos recomendados e preços, consulte Preço do Amazon WorkSpaces.

7. Escolha o modo de execução, escolha as configurações de criptografia e configure as tags. Quando terminar, escolha Próxima etapa.

8. Escolha Ativar WorkSpaces. Observe que pode levar até 20 minutos para os WorkSpaces se tornarem disponíveis e até 40 minutos se a criptografia estiver habilitada. O status inicial do WorkSpace é `PENDING`. Quando a ativação estiver concluída, o status será `AVAILABLE`.

9. Envie convites para o endereço de e-mail de cada usuário. (Esses convites não serão enviados automaticamente se você estiver usando uma relação de confiança.) Para obter mais informações, consulte Enviar um convite por e-mail.

Etapa 3: Conecte-se ao WorkSpace

Depois de receber o e-mail de convite, você pode se conectar ao seu WorkSpace.
Os usuários poderão inserir os nomes de usuário como username, corp\username ou corp.example.com\username).

Para se conectar ao WorkSpace

1. Abra o link no e-mail de convite. Quando solicitado, insira uma senha e ative o usuário. Lembre-se dessa senha, pois você precisará dela para fazer login em seu WorkSpace.

> **Note**
>
> As senhas diferenciam maiúsculas de minúsculas e devem ter entre 8 e 64 caracteres. As senhas devem conter pelo menos um caractere de cada uma das seguintes

categorias: letras minúsculas (a-z), letras maiúsculas (A-Z), números (0-9) e ~!@#$ %^&*_-+=`|\(){}[]:;"'<>,.?/.

2. Consulte WorkSpaces Clients no Guia do usuário do Amazon WorkSpaces para obter mais informações sobre os requisitos de cada cliente e, em seguida, execute uma das seguintes opções:

   - Quando solicitado, faça download de um dos aplicativos clientes ou ative o Web Access.
   - Se você não receber o prompt e ainda não tiver instalado uma aplicação cliente, abra https://clients.amazonworkspaces.com/ e faça download de uma das aplicações cliente ou inicialize o Acesso via Web.

   > **Note**
   >
   > Não é possível usar um navegador da web (Acesso via Web) para se conectar aos WorkSpaces do Amazon Linux.

3. Inicie o cliente, digite o código de registro do e-mail de convite e selecione Registrar.
4. Quando for necessário fazer login, insira as credenciais de login do usuário e clique em Fazer login.
5. (Opcional) Quando solicitado a salvar suas credenciais, escolha Sim.

Próximas etapas

Você pode continuar a personalizar o WorkSpace que acabou de criar. Por exemplo, é possível instalar o software e, em seguida, criar um pacote personalizado do seu WorkSpace. Você também pode realizar várias tarefas administrativas nos WorkSpaces e em seu diretório de WorkSpaces. Se você terminar o trabalho com o WorkSpace, poderá excluí-lo. Para obter mais informações, consulte a documentação a seguir.

- Crie uma WorkSpaces imagem e um pacote personalizados
- Administre seu WorkSpaces
- Gerenciar diretórios para WorkSpaces
- Excluir um WorkSpace

Para obter mais informações sobre o uso das aplicações cliente do WorkSpaces, como configurar vários monitores ou usar dispositivos periféricos, consulte WorkSpaces Clients e Peripheral Device Support no Guia do usuário do Amazon WorkSpaces.

Administrar usuários do WorkSpace

A cada WorkSpace é atribuído um único usuário e não pode ser compartilhado por vários usuários. Por padrão, somente um WorkSpace por usuário por diretório é permitido.

Índice

Gerenciar usuários de WorkSpaces

Como administrador do WorkSpaces, é possível executar as tarefas a seguir para gerenciar usuários de WorkSpaces.

Editar informações de usuário

Você pode usar o console do WorkSpaces para editar as informações de usuário de um WorkSpace.

> **Note**
>
> Esse recurso estará disponível somente se você usar o AWS Managed Microsoft AD ou o Simple AD. Se você usar o Microsoft Active Directory por meio do AD Connector ou uma relação de confiança, poderá gerenciar usuários e grupos usando o módulo do Active Directory.

Como editar as informações do usuário

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione WorkSpaces.
3. Selecione um usuário e clique em Ações, Editar usuários.

4. Atualize os campos Nome, Sobrenome e E-mail, conforme necessário.
5. Escolha Atualizar.

Adicionar ou excluir usuários

É possível criar usuários usando o console do Amazon WorkSpaces somente durante o processo de inicialização de um WorkSpace e não é possível excluir usuários usando o console do Amazon WorkSpaces. A maioria das tarefas de gerenciamento de usuários, incluindo o gerenciamento de grupos de usuários, devem ser realizadas por meio do diretório.

Como adicionar ou excluir usuários e grupos

Para adicionar, excluir ou gerenciar usuários e grupos, é necessário fazer isso em todo o diretório. Você executará a maioria das tarefas administrativas para o seu diretório de WorkSpaces com ferramentas de gerenciamento de diretório, como as ferramentas de administração do Active Directory. Para obter mais informações, consulte Configurar as ferramentas de administração do Active Directory para WorkSpaces.

> **Important**
>
> Antes de remover um usuário, é necessário excluir o WorkSpace atribuído a ele. Para obter mais informações, consulte Excluir um WorkSpace.

O processo usado para gerenciar usuários e grupos depende de qual tipo de diretório você está usando.

- Se você estiver usando o AWS Managed Microsoft AD, consulte Manage Users and Groups in AWS Managed Microsoft AD no Guia de administração do AWS Directory Service.
- Se você estiver usando o Simple AD, consulte Manage Users and Groups in Simple AD no Guia de administração do AWS Directory Service.
- Se você usar o Microsoft Active Directory por meio do AD Connector ou uma relação de confiança, poderá gerenciar usuários e grupos usando o módulo do Active Directory.

Enviar um convite por e-mail

Você pode enviar um convite por e-mail a um usuário manualmente, se necessário.

> **Note**
>
> Se você estiver usando o AD Connector ou um domínio confiável, os convites de boas-vindas não serão enviados automaticamente por e-mail para os usuários, portanto, será necessário enviá-los manualmente. Os e-mails de convite também não são enviados automaticamente se o usuário já existir no Active Directory.

Como reenviar um convite por e-mail

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione WorkSpaces.
3. Na página WorkSpaces, use a caixa de pesquisa para pesquisar o usuário ao qual você deseja enviar um convite e selecione o WorkSpace correspondente nos resultados da pesquisa. É possível selecionar apenas um WorkSpace por vez.
4. Selecione Ações, Convidar usuários.
5. Na página Convidar usuários para o WorkSpace, selecione Enviar convite.

Criar vários WorkSpaces para um usuário

Por padrão, você pode criar apenas um WorkSpace por usuário por diretório. No entanto, se necessário, você poderá criar mais de um WorkSpace para um usuário, dependendo da configuração do diretório.

- Se você tiver apenas um diretório para seus WorkSpaces, crie vários nomes de usuário para o usuário. Por exemplo, uma usuária chamada Mary Major pode ter mmajor1, mmajor2 e assim por diante como nomes de usuário. Cada nome de usuário está associado a um WorkSpace diferente no mesmo diretório. No entanto, os WorkSpaces têm o mesmo código de registro, desde que todos sejam criados no mesmo diretório na mesma região da AWS.
- Se você tiver vários diretórios para seus WorkSpaces, crie os WorkSpaces para o usuário em diretórios separados. Você pode usar o mesmo nome de usuário ou nomes de usuário diferentes nos diretórios. Os WorkSpaces terão códigos de registro diferentes.

> **Tip**
>
> Use o mesmo nome de usuário base para cada WorkSpace para localizar todos os WorkSpaces criados para um usuário com facilidade.
> Por exemplo, se você tiver uma usuária chamada Mary Major com o nome de usuário mmajor do Active Directory, crie WorkSpaces para ela com nomes de usuário como mmajor, mmajor1, mmajor2, mmajor3 ou outras variantes, como mmajor_windows ou mmajor_linux. Desde que todos os WorkSpaces tenham o mesmo nome de usuário base inicial (mmajor), é possível classificar o nome de usuário no console do WorkSpaces para agrupar todos os WorkSpaces desse usuário.

> **Important**
>
> - Um usuário pode ter um WorkSpace com PCoIP e outro WorkSpace com WSP, desde que ambos estejam localizados em diretórios separados. O mesmo usuário não pode ter um WorkSpace com PCoIP e outro WorkSpace com WSP no mesmo diretório.
> - Se você estiver configurando vários WorkSpaces para uso com o redirecionamento entre regiões, deverá configurar os WorkSpaces em diretórios diferentes em regiões da AWS e usar os mesmos nomes de usuário em cada diretório. Para obter mais informações sobre o redirecionamento entre regiões, consulte Redirecionamento entre regiões para a Amazon WorkSpaces.

Para alternar entre os WorkSpaces, o usuário faz login com o nome de usuário e o código de registro associados a um determinado Workspace. Se o usuário estiver usando uma versão 3.0+ dos aplicativos cliente de WorkSpaces para Windows, macOS ou Linux, o usuário poderá atribuir nomes diferentes aos WorkSpaces acessando Configurações, Gerenciar informações de login no aplicativo cliente.

Personalize a forma como os usuários fazem login em seus WorkSpaces

Personalize o acesso de seus usuários WorkSpaces usando identificadores uniformes de recursos (URIs) para fornecer uma experiência de login simplificada que se integra aos fluxos de trabalho

existentes em sua organização. Por exemplo, você pode gerar automaticamente URIs de login que registram seus usuários usando o código de WorkSpaces registro deles. Como resultado:

- Os usuários podem ignorar o processo de registro manual.
- Seus nomes de usuário são inseridos automaticamente na página de login WorkSpaces do cliente.
- Se a autenticação multifator (MFA) for usada na organização, os nomes de usuário e os códigos de MFA serão inseridos automaticamente na página de login do cliente.

O acesso ao URI funciona com códigos de registro baseados em região (por exemplo, `WSpdx +ABC12D`) e códigos de registro baseados em nome de domínio totalmente qualificado (FQDN) (por exemplo, `desktop.example.com`). Para obter mais informações sobre como criar e usar códigos de registro baseados em FQDN, consulte Redirecionamento entre regiões para a Amazon WorkSpaces.

Você pode configurar o acesso ao URI WorkSpaces para aplicativos cliente nos seguintes dispositivos compatíveis:

- Computadores Windows
- Computadores macOS
- Computadores Ubuntu Linux 18.04, 20.04 e 22.04
- iPads
- Dispositivos Android

Para usar URIs para acessar seus WorkSpaces, os usuários devem primeiro instalar o aplicativo cliente em seu dispositivo abrindo https://clients.amazonworkspaces.com/ us-iso-eastus-isob-east

O acesso à URI é suportado nos navegadores Firefox e Chrome em computadores Windows e macOS, no navegador Firefox em computadores Ubuntu Linux 18.04, 20.04 e 22.04 e nos navegadores Internet Explorer e Microsoft Edge em computadores Windows. Para obter mais informações sobre WorkSpaces clientes, consulte WorkSpaces Clientes no Guia WorkSpaces do usuário da Amazon.

> **Note**
>
> Em dispositivos Android, o acesso ao URI funciona apenas com o navegador Firefox e não com o navegador Google Chrome.

Para configurar o acesso ao URI ao WorkSpaces, use qualquer um dos formatos de URI descritos na tabela a seguir.

> **Note**
>
> Se o componente de dados de seu URI incluir qualquer um dos seguintes caracteres reservados, recomendamos usar a codificação em percentual no componente de dados para evitar ambiguidade:
> `@ : / ? & =`
> Por exemplo, se tiver nomes de usuário que incluam qualquer um desses caracteres, você deverá codificar em percentual esses nomes de usuário no URI. Para obter mais informações, consulte Uniform Resource Identifier (URI): Generic Syntax.

Sintaxe compatível	Descrição
workspaces://	Abre o aplicativo WorkSpaces cliente. (Observação: não há suporte para o uso de workspaces:// por si só no aplicativo cliente Linux.)
workspaces://@registrationcode	Registra um usuário usando seu código WorkSpaces de registro. Também exibe a página de login do cliente.
workspaces://username@registrationcode	Registra um usuário usando seu código WorkSpaces de registro. Também insere automaticamente o nome de usuário no campo username na página de login do cliente.
workspaces://username@registrationcode?MFACode=mfa	Registra um usuário usando seu código WorkSpaces de registro. Também insere automaticamente o nome de usuário no campo username e o código de autenticação multifator (MFA) no campo MFA code na página de login do cliente.
workspaces://@registrationcode?MFACode=mfa	Registra um usuário usando seu código WorkSpaces de registro. Também insere automaticamente o código de autenticação multifator (MFA) no campo MFA code (Código MFA) na página de login do cliente.

> **Note**
>
> Se os usuários abrirem um link de URI quando já estiverem conectados a um WorkSpace cliente Windows, uma nova WorkSpaces sessão será aberta e a WorkSpaces sessão original permanecerá aberta. Se os usuários abrirem um link WorkSpace de URI quando estiverem conectados a um cliente macOS, iPad ou Android, nenhuma nova sessão será aberta; somente a WorkSpaces sessão original permanecerá aberta.

Habilite recursos de WorkSpace gerenciamento de autoatendimento para seus usuários

Em WorkSpaces, você pode habilitar recursos WorkSpace de gerenciamento de autoatendimento para que seus usuários tenham mais controle sobre sua experiência. Também pode reduzir a carga de trabalho da equipe de suporte de TI para WorkSpaces. Quando você ativa os recursos de autoatendimento, os usuários podem realizar uma ou mais das seguintes tarefas diretamente do WorkSpaces cliente:

- Armazene em cache as credenciais dos usuários no seu cliente. Isso permite que eles se reconectem WorkSpace sem reinserir suas credenciais.
- Reinicie (reinicie) seu. WorkSpace
- Aumente o tamanho dos volumes raiz e do usuário em seus WorkSpace.
- Altere o tipo de computação (pacote) para seus. WorkSpace
- Mude o modo de execução de seus WorkSpace.
- Reconstrua seus. WorkSpace

Clientes compatíveis

- Android, em execução em sistemas Android ou em sistemas Android compatíveis com Chrome OS
- Linux
- macOS
- Windows

Para habilitar recursos de gerenciamento de autoatendimento para seus usuários

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecionar Diretórios.
3. Escolha o diretório em que você deseja ativar os recursos de gerenciamento de autoatendimento.
4. Role para baixo até Permissões de autoatendimento e escolha Editar. Ative ou desative as seguintes opções conforme necessário para determinar as tarefas WorkSpace de gerenciamento que os usuários podem realizar a partir do cliente:

   - Lembrar de mim: os usuários podem escolher se devem armazenar em cache suas credenciais no cliente marcando a caixa de seleção Lembrar de mim ou Mantenha-me conectado na tela de login. As credenciais são armazenadas em cache na RAM apenas. Quando os usuários optam por armazenar suas credenciais em cache, eles podem se reconectar às suas WorkSpaces sem precisar inseri-las novamente. Para controlar por quanto tempo os usuários podem armazenar em cache suas credenciais, consulte Definir o tempo de vida máximo para um tíquete Kerberos.
   - Reiniciar WorkSpace a partir do cliente — Os usuários podem reiniciar (reinicializar) seus. WorkSpace A reinicialização desconecta o usuário do seu WorkSpace, o desliga e o reinicializa. Os dados de usuário, o sistema operacional e as configurações do sistema não são afetados.
   - Aumentar o tamanho do volume — Os usuários podem expandir os volumes raiz e de usuário WorkSpace para um tamanho especificado sem entrar em contato com o suporte de TI. Os usuários podem aumentar o tamanho do volume raiz (para Windows, a unidade C:; para Linux,/) até 175 GB e o tamanho do volume do usuário (para Windows, a unidade D:; para Linux, /home) até 100 GB. WorkSpace os volumes raiz e de usuário vêm em grupos definidos que não podem ser alterados. Os grupos disponíveis são [Raiz(GB), Usuário(GB)]: [80, 10], [80, 50], [80, 100], [175 a 2.000, 100 a 2.000]. Para ter mais informações, consulte Modificar um WorkSpace.

     Para um recém-criado WorkSpace, os usuários devem esperar 6 horas antes de poderem aumentar o tamanho dessas unidades. Depois disso, eles podem solicitar aumento uma vez em um período de 6 horas. Enquanto um aumento no tamanho do volume está em andamento, os usuários podem realizar a maioria das tarefas em seus WorkSpace. As tarefas que eles não podem realizar são: alterar o tipo de WorkSpace computação, alternar o modo de WorkSpace execução, reiniciá-lo ou WorkSpace reconstruí-lo. WorkSpace Quando o

processo estiver concluído, ele WorkSpace deverá ser reinicializado para que as alterações entrem em vigor. Esse processo pode levar até uma hora.

> **Note**
>
> Se os usuários aumentarem o tamanho do volume WorkSpace, isso aumentará a taxa de cobrança deles WorkSpace.

- Alterar o tipo de computação — Os usuários podem alternar WorkSpace entre os tipos de computação (pacotes). Para um pacote recém-criado WorkSpace, os usuários devem esperar 6 horas antes de poderem mudar para um pacote diferente. Depois disso, eles podem mudar para um pacote maior somente uma vez em um período de 6 horas, ou para um pacote menor uma vez em um período de 30 dias. Quando uma alteração do tipo de WorkSpace computação está em andamento, os usuários são desconectados deles WorkSpace e não podem usar ou alterar o. WorkSpace O WorkSpace é reinicializado automaticamente durante o processo de alteração do tipo de computação. Esse processo pode levar até uma hora.

  > **Note**
  >
  > Se os usuários alterarem o tipo de WorkSpace computação, isso alterará a taxa de cobrança deles. WorkSpace

- Alternar modo de execução — Os usuários podem alternar WorkSpace entre os modos de AutoStopexecução AlwaysOne de execução. Para ter mais informações, consulte Gerenciar o modo de execução do WorkSpace.

  > **Note**
  >
  > Se os usuários mudarem o modo de execução deles WorkSpace, isso alterará a taxa de cobrança deles WorkSpace.

- Reconstruir WorkSpace a partir do cliente — Os usuários podem reconstruir o sistema operacional de a WorkSpace até seu estado original. Quando a WorkSpace é reconstruído, o volume do usuário (unidade D:) é recriado a partir do backup mais recente. Como os backups são concluídos a cada 12 horas, os dados dos usuários podem ter até 12 horas. Para um recém-criado WorkSpace, os usuários devem esperar 12 horas antes de poderem reconstruir seu WorkSpace. Quando uma WorkSpace reconstrução está em andamento, os usuários são

desconectados dela WorkSpace e não podem usá-la nem fazer alterações nela. WorkSpace Esse processo pode levar até uma hora.

- Uploads de registros de diagnóstico — Os usuários podem carregar arquivos de log do WorkSpaces cliente diretamente WorkSpaces para solucionar problemas sem interromper o uso do cliente. WorkSpaces Se você habilitar o upload de registros de diagnóstico para seus usuários ou permitir que eles mesmos façam isso, os arquivos de log serão enviados WorkSpaces automaticamente. Você pode ativar o upload do registro de diagnóstico antes ou durante uma sessão WorkSpaces de streaming.

5. Escolha Salvar.

Habilitar a otimização de áudio do Amazon Connect para os usuários

No console de gerenciamento do WorkSpaces, você pode habilitar a otimização de áudio do Painel de Controle de Contatos (CCP) do Amazon Connect para as frotas do WorkSpaces a fim de aumentar a segurança e habilitar áudio de qualidade nativa. Depois de habilitar a otimização de áudio do CCP, o áudio do CCP será processado pelos endpoints de cliente, enquanto os usuários de WorkSpaces podem interagir com o CCP nos próprios WorkSpaces.

A otimização de áudio do Painel de Controle de Contatos (CCP) do Amazon Connect funciona com:

- O cliente do WorkSpaces para Windows.
- WorkSpaces do Amazon Linux e do Windows.
- WorkSpaces usando PCoIP ou WSP.

Requisitos

- É necessário estar configurado com o Amazon Connect.
- Você deve criar um CCP personalizado com a API Stream do Amazon Connect criando um CCP sem mídia para sinalização de chamada. Dessa forma, a mídia é processada no desktop local usando o CCP padrão, e os controles de sinalização e chamada são processados na conexão remota com o CCP sem mídia. Para obter mais informações sobre a API Streams do Amazon Connect, consulte o repositório do GitHub em https://github.com/aws/amazon-connect-streams. O CCP personalizado que você cria é o CCP que seus agentes do Amazon Connect usarão em seus WorkSpaces.

- Você deve ter um navegador da web instalado nos endpoints do cliente do WorkSpaces que seja compatível com o Amazon Connect. Para ver a lista de navegadores compatíveis, consulte Browsers supported by Amazon Connect.

> **Note**
>
> Se os usuários usarem navegadores que não são compatíveis, eles serão solicitados a baixar um navegador compatível quando tentarem fazer login no CCP.

Habilitar a otimização de áudio do Amazon Connect

Para habilitar a otimização de áudio do Amazon Connect para usuários:

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione Directories (Diretórios).
3. Selecione o diretório e escolha Actions (Ações), Update Details (Atualizar detalhes).
4. Expanda Otimização de áudio do Amazon Connect.

> **Note**
>
> Antes de configurar com o Amazon Connect, clique em Atualizar para salvar quaisquer alterações não salvas feitas anteriormente no console de gerenciamento.

5. Selecione Configurar Amazon Connect.
6. Insira um nome para o Painel de Controle de Contatos (CCP) do Amazon Connect.

> **Note**
>
> O nome que você der ao seu CCP será usado no menu de complemento do usuário. Escolha um nome que seja significativo para os usuários.

7. Insira o URL do Painel de Controle de Contatos do Amazon Connect gerado pelo Amazon Connect. Para obter mais informações sobre como encontrar o URL, consulte Provide access to the Contact Control Panel.
8. Selecione Criar Amazon Connect.

Atualizar os detalhes de otimização de áudio do Amazon Connect do diretório

Para atualizar os detalhes de otimização de áudio do Amazon Connect do diretório:

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione Directories (Diretórios).
3. Selecione o diretório e escolha Actions (Ações), Update Details (Atualizar detalhes).
4. Expanda Otimização de áudio do Amazon Connect.

> **Note**
>
> Antes de configurar com o Amazon Connect, clique em Atualizar para salvar quaisquer alterações não salvas feitas anteriormente no console de gerenciamento.

5. Selecione Configurar Amazon Connect.
6. Escolha Editar.
7. Selecione o diretório e escolha Actions (Ações), Update Details (Atualizar detalhes).
8. Atualize o nome e o URL do Painel de Controle de Contatos do Amazon Connect.
9. Escolha Save (Salvar).

Excluir a otimização de áudio do Amazon Connect do diretório

Para excluir uma otimização de áudio do Amazon Connect do diretório:

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione Directories (Diretórios).
3. Selecione o diretório e escolha Actions (Ações), Update Details (Atualizar detalhes).
4. Expanda Otimização de áudio do Amazon Connect.

> **Note**
>
> Antes de configurar com o Amazon Connect, clique em Atualizar para salvar quaisquer alterações não salvas feitas anteriormente no console de gerenciamento.

5. Selecione Configurar Amazon Connect.
6. Selecione Excluir Amazon Connect.

Para obter mais informações, consulte Agent training guide.

Habilitar uploads de log de diagnóstico

Para solucionar problemas WorkSpaces do cliente, ative os carregamentos automáticos de registros de diagnóstico. Atualmente, isso é compatível com clientes Windows, macOS, Linux e Web Access.

> **Note**
>
> No momento, o recurso de upload de registros de diagnóstico do WorkSpaces cliente não está disponível na região AWS GovCloud (Oeste dos EUA).

Uploads de log de diagnóstico

Com os carregamentos de registros de diagnóstico, você pode carregar arquivos de log WorkSpaces do cliente diretamente WorkSpaces para solucionar problemas sem interromper o uso do cliente. WorkSpaces Se você habilitar o upload de registros de diagnóstico para seus usuários ou permitir que eles mesmos façam isso, os arquivos de log serão enviados WorkSpaces automaticamente para. Você pode ativar o upload do registro de diagnóstico antes ou durante uma sessão WorkSpaces de streaming.

Para carregar automaticamente os registros de diagnóstico de dispositivos gerenciados, instale um WorkSpaces cliente que ofereça suporte a carregamentos de diagnóstico. O upload do log é habilitado por padrão. Você pode modificar as configurações de uma das seguintes maneiras:

Opção 1: usar o AWS console

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecionar Diretórios.
3. Escolha o nome do diretório para o qual você deseja habilitar o log de diagnóstico.
4. Role para baixo até Permissão de autoatendimento.
5. Escolha Exibir detalhes
6. Selecione Editar.

7. Selecione Uploads de log de diagnóstico.
8. Selecione Salvar.

Opção 2: Usar uma chamada de API

Você pode editar as configurações do diretório para ativar ou desativar o cliente WorkSpaces Windows, macOS e Linux para carregar registros de diagnóstico automaticamente usando uma chamada de API. Se ativado, quando ocorre um problema com o cliente, os registros são enviados WorkSpaces sem a interação do usuário. Para obter mais informações, consulte a referência WorkSpaces da API.

Você também pode permitir que os usuários decidam se querem habilitar os uploads automáticos de log de diagnóstico após a instalação do cliente. Para obter mais informações, consulte Aplicativo cliente WorkSpaces Windows, aplicativo cliente WorkSpaces macOS e aplicativo cliente WorkSpaces Linux.

> **Note**
>
> - Os logs de diagnóstico não contêm informações confidenciais. Você pode desabilitar os uploads automáticos de log de diagnóstico para os usuários no nível do diretório ou permitir que os usuários desabilitem esses recursos por conta própria.
> - Para acessar o recurso de upload de registros de diagnóstico, você precisa instalar as seguintes versões dos WorkSpaces clientes:
>   - 5.4.0 ou posterior do cliente Windows
>   - 5.8.0 ou posterior do cliente macOS
>   - 2023.1 do cliente Ubuntu 22.04
>   - 2023.1 do cliente Ubuntu 20.04
>   - Você também pode acessar o recurso de carregamento do log de diagnóstico com o cliente Web Access.

Administre seu WorkSpaces

Você pode administrar seu WorkSpaces usando o WorkSpaces console.

Para realizar tarefas de administração de diretórios, consulte the section called “Configurar a administração de diretório”.

> **Note**
>
> - Certifique-se de atualizar os drivers de dependência de rede, como ENA, NVMe e drivers PV, no seu. WorkSpaces Você deve fazer isso pelo menos uma vez a cada 6 meses. Para obter mais informações, consulte Instalar ou atualizar o driver do Elastic Network Adapter (ENA) Drivers do AWS NVMe para instâncias do Windows e Atualizar os drivers fotovoltaicos nas instâncias do Windows.
> - Certifique-se de atualizar periodicamente os agentes EC2Config, EC2Launch e EC2Launch V2 para as versões mais recentes. Você deve fazer isso pelo menos uma vez a cada 6 meses. Para obter mais informações, consulte Atualizar EC2Config e EC2Launch.

Conteúdo

- Reconstrua um WorkSpace
- Restaurar um WorkSpace
- Traga sua própria licença (BYOL) do Microsoft 365
- Atualize o Windows BYOL WorkSpaces
- Migre um WorkSpace
- Excluir um WorkSpace

Gerencie seu Windows WorkSpaces

Você pode usar Objetos de Política de Grupo (GPOs) para aplicar configurações para gerenciar o Windows WorkSpaces ou os usuários que fazem parte do seu WorkSpaces diretório do Windows.

> **Note**
>
> As instâncias do Linux não seguem a política de grupo. Para obter informações sobre o gerenciamento do Amazon Linux WorkSpaces, consulteGerencie seu Amazon Linux WorkSpaces.

Recomendamos que você crie uma unidade organizacional para seus objetos de WorkSpaces computador e uma unidade organizacional para seus objetos de WorkSpaces usuário.

Para usar as configurações de Política de Grupo específicas da Amazon WorkSpaces, você deve instalar o modelo administrativo da Política de Grupo para o protocolo ou protocolos que você está usando, seja PCoIP ou WorkSpaces Streaming Protocol (WSP).

> **Warning**
>
> As configurações da Política de Grupo podem afetar a experiência de seus WorkSpace usuários da seguinte forma:
>
> - A implementação de uma mensagem de login interativa para exibir um banner de login impede que os usuários possam acessar seus. WorkSpaces A configuração da Política de Grupo da mensagem de logon interativa não é atualmente suportada pelo WorkSpaces PCoIP. A mensagem de login é suportada no WSP WorkSpaces, e os usuários precisam fazer login novamente após aceitarem o banner de login.

- Desabilitar o armazenamento removível por meio das configurações de Política de Grupo causa uma falha de login que faz com que os usuários sejam conectados a um perfil temporário sem acesso à unidade D.
- A remoção de usuários do grupo local de Usuários da Área de Trabalho Remota por meio das configurações da Política de Grupo impede que esses usuários possam se autenticar por meio dos aplicativos WorkSpaces cliente. Para obter mais informações sobre essa configuração de Política de Grupo, consulte Permitir logon por meio dos Serviços de Área de Trabalho Remota na documentação da Microsoft.
- Se você remover o grupo de usuários incorporado da política de segurança Permitir login localmente, seus WorkSpaces usuários do PCoIP não conseguirão se conectar a eles WorkSpaces por meio dos aplicativos WorkSpaces cliente. Seu PCoIP WorkSpaces também não receberá atualizações para o software do agente PCoIP. As atualizações do agente PCoIP podem conter correções de segurança e outras correções, ou podem habilitar novos recursos para você. WorkSpaces Para obter mais informações sobre como trabalhar com essa política de segurança, consulte Permitir logon localmente na documentação da Microsoft.
- As configurações de política de grupo podem ser usadas para restringir o acesso à unidade. Se você definir as configurações da Política de Grupo para restringir o acesso à unidade C ou à unidade D, os usuários não poderão acessar suas WorkSpaces. Para evitar que esse problema ocorra, verifique se os usuários podem acessar as unidades C e D.
- O recurso de WorkSpaces entrada de áudio requer acesso de login local dentro do. WorkSpace O recurso de entrada de áudio está habilitado por padrão para Windows. WorkSpaces No entanto, se você tiver uma configuração de Política de Grupo que restrinja o login local dos usuários WorkSpaces, a entrada de áudio não funcionará no seu. WorkSpaces Se você remover essa configuração de Política de Grupo, o recurso de entrada de áudio será ativado após a próxima reinicialização do. WorkSpace Para obter mais informações sobre essa configuração de política de grupo, consulte Permitir logon localmente na documentação da Microsoft.

  Para obter mais informações sobre como habilitar ou desabilitar o redirecionamento de entrada de áudio, consulte Habilitar ou desabilitar o redirecionamento da entrada de áudio para PCoIP ou Habilitar ou desabilitar o redirecionamento da entrada de áudio para WSP.
- Usar a Política de Grupo para definir o plano de energia do Windows como Balanceado ou Economizador de Energia pode fazer WorkSpaces com que você durma quando eles ficam inativos. É altamente recomendável usar a Política de Grupo para definir o plano de

energia do Windows como Alto desempenho. Para ter mais informações, consulte Meu Windows WorkSpace adormece quando fica ocioso.

- Algumas configurações de Política de Grupo forçam os usuários a fazer logoff quando eles são desconectados de uma sessão. Todos os aplicativos que os usuários abriram WorkSpaces estão fechados.
- "Definir limite de tempo para sessões ativas, mas ociosas dos Serviços de Área de Trabalho Remota" atualmente não é suportado no WorkSpaces WSP. Evite usá-lo durante as sessões do WSP, pois isso causa uma desconexão mesmo quando há atividade e a sessão não está ociosa.

Para obter informações sobre como usar as ferramentas de administração do Active Directory para trabalhar com GPOs, consulte Configurar as ferramentas de administração do Active Directory para WorkSpaces.

Conteúdo

- Solução de problemas

Instale os arquivos de modelo administrativo da Política de Grupo para o WorkSpaces Streaming Protocol (WSP)

Para usar as configurações de Política de Grupo específicas para WorkSpaces o uso do Protocolo de WorkSpaces Streaming (WSP), você deve adicionar o modelo administrativo `wsp.admx` e os `wsp.adml` arquivos da Política de Grupo do WSP ao Armazenamento Central do controlador de domínio do seu WorkSpaces diretório. Para obter mais informações sobre os arquivos `.admx` e `.adml`, consulte Como criar e gerenciar o Repositório Central para Modelos Administrativos da Política de Grupo no Windows.

O procedimento a seguir descreve como criar o repositório central e adicionar os arquivos de modelo administrativo a ele. Execute o procedimento a seguir em uma administração de diretório WorkSpace ou instância do Amazon EC2 que esteja associada ao seu WorkSpaces diretório.

Como instalar os arquivos de modelo administrativo de política de grupo para WSP

1. Em um Windows em execução WorkSpace, faça uma cópia dos `wsp.adml` arquivos `wsp.admx` e no `C:\Program Files\Amazon\WSP` diretório.
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra o Windows File Explorer e, na barra de endereço, insira o nome de domínio totalmente qualificado (FQDN) da sua organização, como. `\\example.com`
3. Abra a pasta `sysvol`.
4. Abra a pasta com o nome *`FQDN`*.
5. Abra a pasta `Policies`. O endereço agora deve ser `\\`*`FQDN`*`\sysvol\`*`FQDN`*`\Policies`.
6. Se ele ainda não existir, crie uma pasta chamada `PolicyDefinitions`.
7. Abra a pasta `PolicyDefinitions`.
8. Copie o arquivo `wsp.admx` na pasta `\\`*`FQDN`*`\sysvol\`*`FQDN`*`\Policies\PolicyDefinitions`.
9. Crie uma pasta chamada `en-US` na pasta `PolicyDefinitions`.
10. Abra a pasta `en-US`.
11. Copie o arquivo `wsp.adml` na pasta `\\`*`FQDN`*`\sysvol\`*`FQDN`*`\Policies\PolicyDefinitions\en-US`.

Como verificar se os arquivos de modelo administrativo estão instalados corretamente

1. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management ()gpmc.msc.
2. Expanda a floresta (Floresta: ***FQDN***).
3. Expanda os Domínios.
4. Expanda o FQDN (por exemplo, `example.com`).
5. Expanda Objetos de Política de Grupo.
6. Selecione Política de domínio padrão, abra o menu de contexto (clique com o botão direito do mouse) e selecione Editar.

> **Note**
>
> Se o domínio que dá suporte ao WorkSpaces for um AWS Managed Microsoft AD diretório, você não poderá usar a Política de Domínio Padrão para criar seu GPO. Em vez disso, você deve criar e vincular o GPO no contêiner de domínio que tem privilégios delegados.
>
> Quando você cria um diretório com AWS Managed Microsoft AD, AWS Directory Service cria uma unidade organizacional (OU) *`yourdomainname`* sob a raiz do domínio. O nome dessa UO é baseado no nome NetBIOS digitado quando você criou o diretório. Se você não especificar um nome NetBIOS, será usado como padrão a primeira parte do nome DNS do diretório (por exemplo, no caso de `corp.example.com`, o nome NetBIOS seria `corp`).
>
> Para criar o GPO, em vez de selecionar Política de domínio padrão, selecione a UO *`yourdomainname`* (ou qualquer UO sob ela), abra o menu de contexto (clique com o botão direito do mouse) e selecione Criar um GPO neste domínio e vinculá-lo aqui.
>
> Para obter mais informações sobre a UO *`yourdomainname`*, consulte What Gets Created no Guia de administração do AWS Directory Service .

7. No Editor de gerenciamento de política de grupo, selecione Configuração do computador, Políticas, Modelos administrativos, Amazon e WSP.
8. Agora você pode usar esse objeto de Política de Grupo do WSP para modificar as configurações da Política de Grupo que são específicas para WorkSpaces o uso do WSP.

Gerenciar configurações de política de grupo para o WorkSpaces Streaming Protocol (WSP)

Use as configurações da Política de Grupo para gerenciar seus Windows WorkSpaces que usam o WSP.

Configurar o suporte à impressora para WSP

Por padrão, WorkSpaces ativa a impressão remota básica, que oferece recursos de impressão limitados porque usa um driver de impressora genérico no lado do host para garantir uma impressão compatível.

A impressão remota avançada para clientes Windows (indisponível para o WSP) permite que você use recursos específicos da impressora, como impressão de dois lados, mas exige a instalação do driver de impressora correspondente no lado do host.

A impressão remota é implementada como um canal virtual. Se os canais virtuais estiverem desabilitados, a impressão remota não funcionará.

Para Windows WorkSpaces, você pode usar as configurações da Política de Grupo para configurar o suporte à impressora conforme necessário.

Como configurar o suporte à impressora

1. Certifique-se de que o modelo administrativo de Política de WorkSpaces Grupo mais recente para o WSP esteja instalado no Armazenamento Central do controlador de domínio do seu WorkSpaces diretório.
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management ()gpmc.msc.
3. Expanda a floresta (Floresta: ***FQDN***).
4. Expanda os Domínios.
5. Expanda o FQDN (por exemplo, `example.com`).
6. Expanda Objetos de Política de Grupo.
7. Selecione Política de domínio padrão, abra o menu de contexto (clique com o botão direito do mouse) e selecione Editar.

> **Note**
>
> Se o domínio que dá suporte ao WorkSpaces for um AWS Managed Microsoft AD diretório, você não poderá usar a Política de Domínio Padrão para criar seu GPO. Em vez disso, selecione a UO *yourdomainname* (ou qualquer UO sob ela), abra o menu de contexto (clique com o botão direito do mouse) e selecione Criar um GPO neste domínio e vinculá-lo aqui. Para obter mais informações sobre a UO *yourdomainname*, consulte What Gets Created no Guia de administração do AWS Directory Service .

8. No Editor de gerenciamento de política de grupo, selecione Configuração do computador, Políticas, Modelos administrativos, Amazon e WSP.
9. Abra a configuração Configure remote printing (Configurar impressão remota).
10. Na caixa de diálogo Configure remote printing (Configurar impressão remota), execute um dos seguintes procedimentos:
    - Para habilitar o redirecionamento da impressora local, selecione Habilitado e, em Opções de impressão, selecione Básico. Para usar automaticamente a impressora padrão do computador cliente, selecione Mapear impressora padrão local para o host remoto.
    - Para desabilitar a impressão, selecione Desabilitado.
11. Escolha OK.
12. A alteração da configuração da Política de Grupo entra em vigor após a próxima atualização da Política de Grupo WorkSpace e após a reinicialização da WorkSpace sessão. Para aplicar as alterações de política de grupo, execute um destes procedimentos:
    - Reinicie o WorkSpace (no WorkSpaces console da Amazon, selecione o e, em seguida WorkSpace, escolha Ações, Reinicialização WorkSpaces).
    - Em um prompt de comando administrativo, insira **`gpupdate /force`**.

Configurar o redirecionamento da área de transferência (copiar/colar) para o WSP

Por padrão, WorkSpaces oferece suporte ao redirecionamento bidirecional da área de transferência (copiar/colar). No Windows WorkSpaces, você pode usar as configurações da Política de Grupo para desativar esse recurso ou definir a direção em que o redirecionamento da área de transferência é permitido.

Para configurar o redirecionamento da área de transferência para Windows WorkSpaces

1. Certifique-se de que o modelo administrativo de Política de WorkSpaces Grupo mais recente para o WSP esteja instalado no Armazenamento Central do controlador de domínio do seu WorkSpaces diretório.
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management ()gpmc.msc.
3. Expanda a floresta (Floresta: ***FQDN***).
4. Expanda os Domínios.
5. Expanda o FQDN (por exemplo, `example.com`).
6. Expanda Objetos de Política de Grupo.
7. Selecione Política de domínio padrão, abra o menu de contexto (clique com o botão direito do mouse) e selecione Editar.

   > **Note**
   >
   > Se o domínio que dá suporte ao WorkSpaces for um AWS Managed Microsoft AD diretório, você não poderá usar a Política de Domínio Padrão para criar seu GPO. Em vez disso, selecione a UO *`yourdomainname`* (ou qualquer UO sob ela), abra o menu de contexto (clique com o botão direito do mouse) e selecione Criar um GPO neste domínio e vinculá-lo aqui. Para obter mais informações sobre a UO *`yourdomainname`*, consulte What Gets Created no Guia de administração do AWS Directory Service .

8. No Editor de gerenciamento de política de grupo, selecione Configuração do computador, Políticas, Modelos administrativos, Amazon e WSP.
9. Abra a configuração Configurar redirecionamento da área de transferência.
10. Na caixa de diálogo Configurar redirecionamento da área de transferência, selecione Habilitado ou Desabilitado.

    Quando a opção Configurar redirecionamento da área de transferência estiver habilitada, as seguintes opções de redirecionamento da área de transferência ficarão disponíveis:

    - Selecione Copiar e colar para permitir o redirecionamento bidirecional de copiar e colar da área de transferência.
    - Selecione Copiar somente para permitir a cópia de dados da área de transferência do servidor somente para a área de transferência do cliente.

- Selecione Colar somente para permitir colar dados da área de transferência do cliente somente na área de transferência do servidor.

11. Escolha OK.
12. A alteração da configuração da Política de Grupo entra em vigor após a próxima atualização da Política de Grupo WorkSpace e após a reinicialização da WorkSpace sessão. Para aplicar as alterações de política de grupo, execute um destes procedimentos:

    - Reinicie o WorkSpace (no WorkSpaces console da Amazon, selecione o e, em seguida WorkSpace, escolha Ações, Reinicialização WorkSpaces).
    - Em um prompt de comando administrativo, insira **`gpupdate /force`**.

Limitação conhecida

Com o redirecionamento da área de transferência habilitado no WorkSpace, se você copiar conteúdo maior que 890 KB de um aplicativo do Microsoft Office, o aplicativo poderá ficar lento ou não responder por até 5 segundos.

Definir o tempo limite para retomar uma sessão para WSP

Quando você perde a conectividade de rede, a sessão ativa WorkSpaces do cliente é desconectada. WorkSpaces os aplicativos cliente para Windows e macOS tentarão reconectar a sessão automaticamente se a conectividade de rede for restaurada em um determinado período de tempo. O tempo limite padrão de retomada da sessão é de 20 minutos (1200 segundos), mas você pode modificar esse valor para WorkSpaces que seja controlado pelas configurações de Política de Grupo do seu domínio.

Com definir o valor de tempo limite de retomada de sessão automático

1. Certifique-se de que o modelo administrativo de Política de WorkSpaces Grupo mais recente para o WSP esteja instalado no Armazenamento Central do controlador de domínio do seu WorkSpaces diretório.
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management ()gpmc.msc.
3. Expanda a floresta (Floresta: ***FQDN***).
4. Expanda os Domínios.
5. Expanda o FQDN (por exemplo, `example.com`).
6. Expanda Objetos de Política de Grupo.

7. Selecione Política de domínio padrão, abra o menu de contexto (clique com o botão direito do mouse) e selecione Editar.

   > **Note**
   >
   > Se o domínio que dá suporte ao WorkSpaces for um AWS Managed Microsoft AD diretório, você não poderá usar a Política de Domínio Padrão para criar seu GPO. Em vez disso, selecione a UO *`yourdomainname`* (ou qualquer UO sob ela), abra o menu de contexto (clique com o botão direito do mouse) e selecione Criar um GPO neste domínio e vinculá-lo aqui. Para obter mais informações sobre a UO *`yourdomainname`*, consulte What Gets Created no Guia de administração do AWS Directory Service .

8. No Editor de gerenciamento de política de grupo, selecione Configuração do computador, Políticas, Modelos administrativos, Amazon e WSP.
9. Abra a configuração Habilitar/desabilitar reconexão automática.
10. Na caixa de diálogo Habilitar/desabilitar a reconexão automática, selecione Habilitado e defina Tempo limite de reconexão (segundos) para o tempo limite desejado em segundos.
11. Escolha OK.
12. A alteração da configuração da Política de Grupo entra em vigor após a próxima atualização da Política de Grupo WorkSpace e após a reinicialização da WorkSpace sessão. Para aplicar as alterações de política de grupo, execute um destes procedimentos:

    - Reinicie o WorkSpace (no WorkSpaces console da Amazon, selecione o e, em seguida WorkSpace, escolha Ações, Reinicialização WorkSpaces).
    - Em um prompt de comando administrativo, insira **`gpupdate /force`**.

Habilitar ou desabilitar o redirecionamento da entrada de vídeo para WSP

Por padrão, WorkSpaces suporta o redirecionamento de dados de uma câmera local. Se necessário para o Windows WorkSpaces, você pode usar as configurações da Política de Grupo para desativar esse recurso.

Para habilitar ou desabilitar o redirecionamento de entrada de vídeo para Windows WorkSpaces

1. Certifique-se de que o modelo administrativo de Política de WorkSpaces Grupo mais recente para o WSP esteja instalado no Armazenamento Central do controlador de domínio do seu WorkSpaces diretório.

2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management ()gpmc.msc.
3. Expanda a floresta (Floresta: ***FQDN***).
4. Expanda os Domínios.
5. Expanda o FQDN (por exemplo, `example.com`).
6. Expanda Objetos de Política de Grupo.
7. Selecione Política de domínio padrão, abra o menu de contexto (clique com o botão direito do mouse) e selecione Editar.

> **Note**
>
> Se o domínio que dá suporte ao WorkSpaces for um AWS Managed Microsoft AD diretório, você não poderá usar a Política de Domínio Padrão para criar seu GPO. Em vez disso, selecione a UO *`yourdomainname`* (ou qualquer UO sob ela), abra o menu de contexto (clique com o botão direito do mouse) e selecione Criar um GPO neste domínio e vinculá-lo aqui. Para obter mais informações sobre a UO *`yourdomainname`*, consulte What Gets Created no Guia de administração do AWS Directory Service .

8. No Editor de gerenciamento de política de grupo, selecione Configuração do computador, Políticas, Modelos administrativos, Amazon e WSP.
9. Abra a configuração Habilitar/desabilitar o redirecionamento de entrada de vídeo.
10. Na caixa de diálogo Habilitar/desabilitar o redirecionamento de entrada de vídeo, selecione Habilitado ou Desabilitado.
11. Escolha OK.
12. A alteração da configuração da Política de Grupo entra em vigor após a próxima atualização da Política de Grupo WorkSpace e após a reinicialização da WorkSpace sessão. Para aplicar as alterações de política de grupo, execute um destes procedimentos:

    - Reinicie o WorkSpace (no WorkSpaces console da Amazon, selecione o e, em seguida WorkSpace, escolha Ações, Reinicialização WorkSpaces).
    - Em um prompt de comando administrativo, insira **`gpupdate /force`**.

Habilitar ou desabilitar o redirecionamento da entrada de áudio para WSP

Por padrão, WorkSpaces suporta o redirecionamento de dados de um microfone local. Se necessário para o Windows WorkSpaces, você pode usar as configurações da Política de Grupo para desativar esse recurso.

Para habilitar ou desabilitar o redirecionamento de entrada de áudio para Windows WorkSpaces

1. Certifique-se de que o modelo administrativo de Política de WorkSpaces Grupo mais recente para o WSP esteja instalado no Armazenamento Central do controlador de domínio do seu WorkSpaces diretório.
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management ()gpmc.msc.
3. Expanda a floresta (Floresta: ***FQDN***).
4. Expanda os Domínios.
5. Expanda o FQDN (por exemplo, `example.com`).
6. Expanda Objetos de Política de Grupo.
7. Selecione Política de domínio padrão, abra o menu de contexto (clique com o botão direito do mouse) e selecione Editar.

   > **Note**
   >
   > Se o domínio que dá suporte ao WorkSpaces for um AWS Managed Microsoft AD diretório, você não poderá usar a Política de Domínio Padrão para criar seu GPO. Em vez disso, selecione a UO *`yourdomainname`* (ou qualquer UO sob ela), abra o menu de contexto (clique com o botão direito do mouse) e selecione Criar um GPO neste domínio e vinculá-lo aqui. Para obter mais informações sobre a UO *`yourdomainname`*, consulte What Gets Created no Guia de administração do AWS Directory Service .

8. No Editor de gerenciamento de política de grupo, selecione Configuração do computador, Políticas, Modelos administrativos, Amazon e WSP.
9. Abra a configuração Habilitar/desabilitar o redirecionamento de entrada de áudio.
10. Na caixa de diálogo Habilitar/desabilitar o redirecionamento de entrada de áudio, selecione Habilitado ou Desabilitado.
11. Escolha OK.

12. A alteração da configuração da Política de Grupo entra em vigor após a próxima atualização da Política de Grupo WorkSpace e após a reinicialização da WorkSpace sessão. Para aplicar as alterações de política de grupo, execute um destes procedimentos:

    - Reinicie o WorkSpace (no WorkSpaces console da Amazon, selecione o e, em seguida WorkSpace, escolha Ações, Reinicialização WorkSpaces).
    - Em um prompt de comando administrativo, insira **`gpupdate /force`**.

Habilitar ou desabilitar o redirecionamento da saída de áudio para WSP

Por padrão, WorkSpaces redireciona os dados para um alto-falante local. Se necessário para o Windows WorkSpaces, você pode usar as configurações da Política de Grupo para desativar esse recurso.

Para habilitar ou desabilitar o redirecionamento de saída de áudio para Windows WorkSpaces

1. Certifique-se de que o modelo administrativo de Política de WorkSpaces Grupo mais recente para o WSP esteja instalado no Armazenamento Central do controlador de domínio do seu WorkSpaces diretório.
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management ()gpmc.msc.
3. Expanda a floresta (Floresta: ***FQDN***).
4. Expanda os Domínios.
5. Expanda seu FQDN. Por exemplo, `example.com`.
6. Expanda Objetos de Política de Grupo.
7. Selecione Política de domínio padrão, abra o menu de contexto (clique com o botão direito do mouse) e selecione Editar.

> **Note**
>
> Se o domínio que dá suporte ao WorkSpaces for um AWS Managed Microsoft AD diretório, você não poderá usar a Política de Domínio Padrão para criar seu GPO. Em vez disso, selecione a UO *`yourdomainname`* (ou qualquer UO sob ela), abra o menu de contexto (clique com o botão direito do mouse) e selecione Criar um GPO neste domínio e vinculá-lo aqui. Para obter mais informações sobre a UO *`yourdomainname`*, consulte What Gets Created no Guia de administração do AWS Directory Service .

8. No Editor de gerenciamento de política de grupo, selecione Configuração do computador, Políticas, Modelos administrativos, Amazon e WSP.
9. Abra a configuração Habilitar/desabilitar o redirecionamento de saída de áudio.
10. Na caixa de diálogo Habilitar/desabilitar o redirecionamento de saída de áudio, selecione Habilitado ou Desabilitado.
11. Escolha OK.
12. A alteração da configuração da Política de Grupo entra em vigor após a próxima atualização da Política de Grupo WorkSpace e após a reinicialização da WorkSpace sessão. Para aplicar as alterações de política de grupo, execute um destes procedimentos:

    - Reinicie o. WorkSpace No WorkSpaces console da Amazon, selecione a e, em seguida WorkSpace, escolha Ações > Reinicializar WorkSpaces.
    - Em um prompt de comando administrativo, insira **`gpupdate /force`**.

Desabilitar o redirecionamento do fuso horário para WSP

Por padrão, o horário em um espaço de trabalho é definido para espelhar o fuso horário do cliente que está sendo usado para se conectar ao WorkSpace. Esse comportamento é controlado por meio do redirecionamento do fuso horário. Talvez você queira desativar a direção do fuso horário por diversos motivos. Por exemplo: .

- A sua empresa quer que todos os funcionários trabalhem em um determinado fuso horário (mesmo que alguns funcionários estejam em outros fusos horários).
- Você agendou tarefas em uma WorkSpace que deve ser executada em um determinado horário em um fuso horário específico.
- Seus usuários que viajam muito querem manter seu fuso horário WorkSpaces em um único fuso horário para fins de consistência e preferência pessoal.

Se necessário para o Windows WorkSpaces, você pode usar as configurações da Política de Grupo para desativar esse recurso.

Para desativar o redirecionamento de fuso horário para Windows WorkSpaces

1. Certifique-se de que o modelo administrativo de Política de WorkSpaces Grupo mais recente para o WSP esteja instalado no Armazenamento Central do controlador de domínio do seu WorkSpaces diretório.

2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management ()gpmc.msc.
3. Expanda a floresta (Floresta: ***FQDN***).
4. Expanda os Domínios.
5. Expanda o FQDN (por exemplo, `example.com`).
6. Expanda Objetos de Política de Grupo.
7. Selecione Política de domínio padrão, abra o menu de contexto (clique com o botão direito do mouse) e selecione Editar.

   > **Note**
   >
   > Se o domínio que dá suporte ao WorkSpaces for um AWS Managed Microsoft AD diretório, você não poderá usar a Política de Domínio Padrão para criar seu GPO. Em vez disso, selecione a UO *`yourdomainname`* (ou qualquer UO sob ela), abra o menu de contexto (clique com o botão direito do mouse) e selecione Criar um GPO neste domínio e vinculá-lo aqui. Para obter mais informações sobre a UO *`yourdomainname`*, consulte What Gets Created no Guia de administração do AWS Directory Service .

8. No Editor de gerenciamento de política de grupo, selecione Configuração do computador, Políticas, Modelos administrativos, Amazon e WSP.
9. Abra a configuração Habilitar/desabilitar o redirecionamento do fuso horário.
10. Na caixa de diálogo Habilitar/desabilitar o redirecionamento do fuso horário, selecione Habilitado.
11. Escolha OK.
12. A alteração da configuração da Política de Grupo entra em vigor após a próxima atualização da Política de Grupo WorkSpace e após a reinicialização da WorkSpace sessão. Para aplicar as alterações de política de grupo, execute um destes procedimentos:

    - Reinicie o WorkSpace (no WorkSpaces console da Amazon, selecione o e, em seguida WorkSpace, escolha Ações, Reinicialização WorkSpaces).
    - Em um prompt de comando administrativo, insira **`gpupdate /force`**.

13. Defina o fuso horário do WorkSpaces para o fuso horário desejado.

O fuso horário do agora WorkSpaces é estático e não reflete mais o fuso horário das máquinas clientes.

Definir configurações de segurança do WSP

Para o WSP, os dados em trânsito são criptografados usando a criptografia TLS 1.2. Por padrão, todas as seguintes cifras são permitidas para criptografia, e o cliente e o servidor negociam qual cifra usar:

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384

Para Windows WorkSpaces, você pode usar as configurações da Política de Grupo para modificar o Modo de Segurança TLS e adicionar novos ou bloquear determinados conjuntos de criptografia. Uma explicação detalhada dessas configurações e dos conjuntos de cifras compatíveis é fornecida na caixa de diálogo de política de grupo Definir configurações de segurança.

Como definir as configurações de segurança do WSP

1. Certifique-se de que o modelo administrativo de Política de WorkSpaces Grupo mais recente para o WSP esteja instalado no Armazenamento Central do controlador de domínio do seu WorkSpaces diretório.
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management ()gpmc.msc.
3. Expanda a floresta (Floresta: ***FQDN***).
4. Expanda os Domínios.
5. Expanda seu FQDN. Por exemplo, `example.com`.
6. Expanda Objetos de Política de Grupo.
7. Selecione Política de domínio padrão, abra o menu de contexto (clique com o botão direito do mouse) e selecione Editar.

> **Note**
>
> Se o domínio que dá suporte ao WorkSpaces for um AWS Managed Microsoft AD diretório, você não poderá usar a Política de Domínio Padrão para criar seu GPO. Em

vez disso, selecione a UO *yourdomainname* (ou qualquer UO sob ela), abra o menu de contexto (clique com o botão direito do mouse) e selecione Criar um GPO neste domínio e vinculá-lo aqui. Para obter mais informações sobre a UO *yourdomainname*, consulte What Gets Created no Guia de administração do AWS Directory Service .

8. No Editor de gerenciamento de política de grupo, selecione Configuração do computador, Políticas, Modelos administrativos, Amazon e WSP.
9. Abra Definir configurações de segurança.
10. Na caixa de diálogo Definir configurações de segurança, selecione Habilitado. Adicione conjuntos de cifras que você deseja permitir e remova os conjuntos de cifras que deseja bloquear. Para obter mais informações sobre essas configurações, consulte as descrições fornecidas na caixa de diálogo Definir configurações de segurança.
11. Escolha OK.
12. A alteração da configuração da Política de Grupo entra em vigor após a próxima atualização da Política de Grupo para o WorkSpace e depois que você reiniciar a WorkSpace sessão. Para aplicar as alterações de política de grupo, execute um destes procedimentos:
    - Para reinicializar o WorkSpace, no WorkSpaces console da Amazon, selecione o e, em seguida WorkSpace, escolha Ações, WorkSpacesReinicialização.
    - Em um prompt de comando administrativo, insira **`gpupdate /force`**.

Configurar extensões para WSP

Por padrão, o suporte para WorkSpaces extensões está desativado. Se necessário, você pode configurar seu WorkSpace para usar extensões das seguintes maneiras:

- Servidor e cliente: habilite extensões para servidor e cliente
- Somente servidor: habilite extensões somente para servidores
- Somente para clientes: habilite extensões somente para clientes

Para Windows WorkSpaces, você pode usar as configurações da Política de Grupo para configurar o uso de extensões.

Como configurar extensões para WSP

1. Certifique-se de que o modelo administrativo de Política de WorkSpaces Grupo mais recente para o WSP esteja instalado no Armazenamento Central do controlador de domínio do seu WorkSpaces diretório.
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management ()gpmc.msc.
3. Expanda a floresta (Floresta: ***FQDN***).
4. Expanda os Domínios.
5. Expanda seu FQDN. Por exemplo, `example.com`.
6. Expanda Objetos de Política de Grupo.
7. Selecione Política de domínio padrão, abra o menu de contexto (clique com o botão direito do mouse) e selecione Editar.

   > **Note**
   >
   > Se o domínio que dá suporte ao WorkSpaces for um AWS Managed Microsoft AD diretório, você não poderá usar a Política de Domínio Padrão para criar seu GPO. Em vez disso, selecione a UO *`yourdomainname`* (ou qualquer UO sob ela), abra o menu de contexto (clique com o botão direito do mouse) e selecione Criar um GPO neste domínio e vinculá-lo aqui. Para obter mais informações sobre a UO *`yourdomainname`*, consulte What Gets Created no Guia de administração do AWS Directory Service .

8. No Editor de gerenciamento de política de grupo, selecione Configuração do computador, Políticas, Modelos administrativos, Amazon e WSP.
9. Abra a configuração Configurar extensões.
10. Na caixa de diálogo Configurar extensões, selecione Habilitado e defina a opção de suporte desejada. Selecione Somente cliente, Servidor e cliente ou Somente servidor.
11. Escolha OK.
12. A alteração da configuração da Política de Grupo entra em vigor após a próxima atualização da Política de Grupo WorkSpace e após a reinicialização da WorkSpace sessão. Para aplicar as alterações de política de grupo, execute um destes procedimentos:

    - Reinicie o. WorkSpace No WorkSpaces console da Amazon, selecione e, em seguida WorkSpace, escolha Ações, Reinicialização WorkSpaces.

- Em um prompt de comando administrativo, insira **`gpupdate /force`**.

Habilitar ou desabilitar o redirecionamento de cartão inteligente para WSP

Por padrão, a Amazon não WorkSpaces está habilitada para oferecer suporte ao uso de cartões inteligentes para autenticação pré-sessão ou durante a sessão. A autenticação pré-sessão se refere à autenticação por cartão inteligente que é executada enquanto os usuários estão fazendo login em seus WorkSpaces. A autenticação em sessão se refere à autenticação executada após o login.

Se necessário, você pode habilitar a autenticação pré-sessão e em sessão para Windows WorkSpaces usando as configurações da Política de Grupo. A autenticação pré-sessão também deve ser habilitada por meio das configurações do diretório do AD Connector usando a ação da EnableClientAuthentication API ou o enable-client-authentication AWS CLI comando. Para obter mais informações, consulte Enable Smart Card Authentication for AD Connector no Guia de administração do AWS Directory Service .

> **Note**
>
> Para permitir o uso de cartões inteligentes com o Windows WorkSpaces, etapas adicionais são necessárias. Para ter mais informações, consulte Usar cartões inteligentes para autenticação.

Para habilitar ou desabilitar o redirecionamento de cartão inteligente para Windows WorkSpaces

1. Certifique-se de que o modelo administrativo de Política de WorkSpaces Grupo mais recente para o WSP esteja instalado no Armazenamento Central do controlador de domínio do seu WorkSpaces diretório.
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management ()gpmc.msc.
3. Expanda a floresta (Floresta: ***FQDN***).
4. Expanda os Domínios.
5. Expanda o FQDN (por exemplo, `example.com`).
6. Expanda Objetos de Política de Grupo.
7. Selecione Política de domínio padrão, abra o menu de contexto (clique com o botão direito do mouse) e selecione Editar.

> **Note**
>
> Se o domínio que dá suporte ao WorkSpaces for um AWS Managed Microsoft AD diretório, você não poderá usar a Política de Domínio Padrão para criar seu GPO. Em vez disso, selecione a UO *yourdomainname* (ou qualquer UO sob ela), abra o menu de contexto (clique com o botão direito do mouse) e selecione Criar um GPO neste domínio e vinculá-lo aqui. Para obter mais informações sobre a UO *yourdomainname*, consulte What Gets Created no Guia de administração do AWS Directory Service .

8. No Editor de gerenciamento de política de grupo, selecione Configuração do computador, Políticas, Modelos administrativos, Amazon e WSP.
9. Abra a configuração Habilitar/desabilitar o redirecionamento de cartão inteligente.
10. Na caixa de diálogo Habilitar/desabilitar o redirecionamento de cartão inteligente, selecione Habilitado ou Desabilitado.
11. Escolha OK.
12. A alteração na configuração da Política de Grupo entra em vigor após a reinicialização da WorkSpace sessão. Para aplicar a alteração da Política de Grupo, reinicie o WorkSpace (no WorkSpaces console da Amazon, selecione a WorkSpace e escolha Ações, Reinicialização WorkSpaces).

Ativar ou desativar o redirecionamento WebAuthn (FIDO2) para WSP

Por padrão, a Amazon WorkSpaces permite o uso de WebAuthn autenticadores para autenticação na sessão. A autenticação na sessão se refere à WebAuthn autenticação que é executada após o login e solicitada pelos aplicativos da web em execução na sessão.

Requisitos

WebAuthn O redirecionamento (FIDO2) para WSP requer o seguinte:

- Agente host WSP versão 2.0.0.1425 ou superior
- WorkSpaces clientes:
  - Linux Ubuntu 22.04 2023.3 ou superior
  - Windows 5.19.0 ou superior
  - Cliente Mac 5.19.0 ou superior

- Navegadores da Web instalados em você que WorkSpaces executa a extensão de WebAuthn redirecionamento Amazon DCV:
  - Google Chrome 116+
  - Microsoft Edge 116+

Ativando ou desativando o WebAuthn redirecionamento (FIDO2) para Windows WorkSpaces

Se necessário, você pode ativar ou desativar o suporte para autenticação em sessão com WebAuthn autenticadores para Windows WorkSpaces usando as configurações da Política de Grupo. Se você habilitar ou não definir essa configuração, o WebAuthn redirecionamento será habilitado e os usuários poderão utilizar autenticadores locais no controle remoto. WorkSpace

Quando o recurso está ativado, todas as WebAuthn solicitações do navegador na sessão são redirecionadas para o cliente local. Os usuários podem usar o Windows Hello ou dispositivos de segurança conectados localmente, como YubiKey outros autenticadores compatíveis com FIDO2, para concluir o processo de autenticação.

Para ativar ou desativar o redirecionamento WebAuthn (FIDO2) para Windows WorkSpaces

1. Certifique-se de que o modelo administrativo de Política de WorkSpaces Grupo mais recente para o WSP esteja instalado no Armazenamento Central do controlador de domínio do seu WorkSpaces diretório.
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management ()gpmc.msc.
3. Expanda a floresta (Floresta: ***FQDN***).
4. Expanda os Domínios.
5. Expanda o FQDN (por exemplo, `example.com`).
6. Expanda Objetos de Política de Grupo.
7. Selecione Política de domínio padrão, abra o menu de contexto (clique com o botão direito do mouse) e selecione Editar.

> **Note**
>
> Se o domínio que dá suporte ao WorkSpaces for um AWS Managed Microsoft AD diretório, você não poderá usar a Política de Domínio Padrão para criar seu GPO. Em vez disso, selecione a UO *`yourdomainname`* (ou qualquer UO sob ela), abra o menu de

contexto (clique com o botão direito do mouse) e selecione Criar um GPO neste domínio e vinculá-lo aqui. Para obter mais informações sobre a UO *yourdomainname*, consulte What Gets Created no Guia de administração do AWS Directory Service .

8. No Editor de gerenciamento de política de grupo, selecione Configuração do computador, Políticas, Modelos administrativos, Amazon e WSP.
9. Abra a configuração Ativar/desativar WebAuthn o redirecionamento.
10. Na caixa de diálogo Ativar/desativar o WebAuthn redirecionamento, escolha Ativado ou Desativado.
11. Escolha OK.
12. A alteração na configuração da Política de Grupo entra em vigor após a reinicialização da WorkSpace sessão. Para aplicar as alterações da Política de Grupo, reinicie o WorkSpace acessando o WorkSpaces console da Amazon e selecionando o. WorkSpace Em seguida, escolha Ações, Reinicializar WorkSpaces).

Instalando a extensão de WebAuthn redirecionamento Amazon DCV

Os usuários precisarão instalar a extensão Amazon DCV WebAuthn Redirection para WebAuthn usá-la após a ativação do recurso, fazendo o seguinte:

- Seus usuários serão solicitados a habilitar a extensão do navegador em seus navegadores.

> **Note**
>
> Esse é um prompt único do navegador. Seus usuários receberão a notificação quando você atualizar a versão do agente WSP para 2.0.0.1425 ou superior. Se seus usuários finais não precisarem do WebAuthn redirecionamento, eles podem simplesmente remover a extensão do navegador. Você também pode bloquear o prompt de instalação da Extensão de WebAuthn Redirecionamento usando a política de GPO abaixo.

- Você pode forçar a instalação da extensão de redirecionamento para seus usuários usando a política de GPO abaixo. Se você ativar a política de GPO, a extensão será instalada automaticamente quando seus usuários iniciarem os navegadores compatíveis com acesso à Internet.
- Seus usuários podem instalar a extensão manualmente com os complementos do Microsoft Edge ou a Chrome Web Store.

Gerencie e instale a extensão do navegador usando a Política de Grupo

Você pode instalar a extensão Amazon DCV WebAuthn Redirection usando a Política de Grupo, centralmente a partir do seu domínio para hosts de sessão associados a um domínio do Active Directory (AD) ou usando o Editor de Política de Grupo Local para cada host de sessão. Esse processo mudará dependendo do navegador que você está usando.

Para Microsoft Edge

1. Baixe e instale o modelo administrativo do Microsoft Edge.
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management ()gpmc.msc.
3. Expanda a floresta (Floresta: ***FQDN***).
4. Expanda os Domínios.
5. Expanda o FQDN (por exemplo, `example.com`).
6. Expanda Objetos de Política de Grupo.
7. Selecione Política de domínio padrão, abra o menu de contexto (clique com o botão direito do mouse) e selecione Editar.
8. Escolha Configuração do computador, modelos administrativos, Microsoft Edge e extensões
9. Abra Definir configurações de gerenciamento de extensões e defina-o como Ativado.
10. Em Definir configurações de gerenciamento de extensões, insira o seguinte:

```
{"ihejeaahjpbegmaaegiikmlphghlfmeh":
{"installation_mode":"force_installed","update_url":"https://edge.microsoft.com/
extensionwebstorebase/v1/crx"}}
```

11. Escolha OK.
12. A alteração na configuração da Política de Grupo entra em vigor após a reinicialização da WorkSpace sessão. Para aplicar as alterações da Política de Grupo, reinicie o WorkSpace acessando o WorkSpaces console da Amazon e selecionando o. WorkSpace Em seguida, escolha Ações, Reinicializar WorkSpaces).

> **Note**
>
> Você pode bloquear a instalação da extensão aplicando a seguinte configuração de gerenciamento de configuração:

```
{"ihejeaahjpbegmaaegiikmlphghlfmeh":
{"installation_mode":"blocked","update_url":"https://edge.microsoft.com/
extensionwebstorebase/v1/crx"}}
```

Para o Google Chrome

1. Baixe e instale o modelo administrativo do Google Chrome. Para obter mais informações, consulte Definir políticas do navegador Chrome em PCs gerenciados.
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management ()gpmc.msc.
3. Expanda a floresta (Floresta: ***FQDN***).
4. Expanda os Domínios.
5. Expanda o FQDN (por exemplo, `example.com`).
6. Expanda Objetos de Política de Grupo.
7. Selecione Política de domínio padrão, abra o menu de contexto (clique com o botão direito do mouse) e selecione Editar.
8. Escolha Configuração do computador, modelos administrativos, Google Chrome e extensões
9. Abra Definir configurações de gerenciamento de extensões e defina-o como Ativado.
10. Em Definir configurações de gerenciamento de extensões, insira o seguinte:

```
{"mmiioagbgnbojdbcjoddlefhmcocfpmn":
{ "installation_mode":"force_installed","update_url":"https://clients2.google.com/
service/update2/crx"}}
```

11. Escolha OK.
12. A alteração na configuração da Política de Grupo entra em vigor após a reinicialização da WorkSpace sessão. Para aplicar as alterações da Política de Grupo, reinicie o WorkSpace acessando o WorkSpaces console da Amazon e selecionando o. WorkSpace Em seguida, escolha Ações, Reinicializar WorkSpaces).

> **Note**
>
> Você pode bloquear a instalação da extensão aplicando a seguinte configuração de gerenciamento de configuração:
>
> ```
> {"mmiioagbgnbojdbcjoddlefhmcocfpmn":
> { "installation_mode":"blocked","update_url":"https://clients2.google.com/
> service/update2/crx"}}
> ```

Habilitar ou desabilitar a desconexão da sessão ao bloquear a tela para WSP

Se necessário, você pode desconectar as WorkSpaces sessões dos usuários quando a tela de bloqueio do Windows for detectada. Para se reconectar a partir do WorkSpaces cliente, os usuários podem usar suas senhas ou seus cartões inteligentes para se autenticar, dependendo do tipo de autenticação habilitado para eles. WorkSpaces

Essa configuração de política de grupo é desabilitada por padrão. Se necessário, você pode habilitar a desconexão da sessão quando a tela de bloqueio do Windows for detectada para o Windows WorkSpaces usando as configurações da Política de Grupo.

> **Note**
>
> - Essa configuração de política de grupo se aplica tanto às sessões autenticadas por senha quanto às autenticadas por cartão inteligente.
> - Para permitir o uso de cartões inteligentes com o Windows WorkSpaces, etapas adicionais são necessárias. Para ter mais informações, consulte Usar cartões inteligentes para autenticação.

Para habilitar ou desabilitar a sessão de desconexão no bloqueio de tela para Windows WorkSpaces

1. Certifique-se de que o modelo administrativo de Política de WorkSpaces Grupo mais recente para o WSP esteja instalado no Armazenamento Central do controlador de domínio do seu WorkSpaces diretório.
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management ()gpmc.msc.

3. Expanda a floresta (Floresta: ***FQDN***).
4. Expanda os Domínios.
5. Expanda o FQDN (por exemplo, `example.com`).
6. Expanda Objetos de Política de Grupo.
7. Selecione Política de domínio padrão, abra o menu de contexto (clique com o botão direito do mouse) e selecione Editar.

> **Note**
>
> Se o domínio que dá suporte ao WorkSpaces for um AWS Managed Microsoft AD diretório, você não poderá usar a Política de Domínio Padrão para criar seu GPO. Em vez disso, selecione a UO *`yourdomainname`* (ou qualquer UO sob ela), abra o menu de contexto (clique com o botão direito do mouse) e selecione Criar um GPO neste domínio e vinculá-lo aqui. Para obter mais informações sobre a UO *`yourdomainname`*, consulte What Gets Created no Guia de administração do AWS Directory Service .

8. No Editor de gerenciamento de política de grupo, selecione Configuração do computador, Políticas, Modelos administrativos, Amazon e WSP.
9. Abra a configuração Habilitar/desabilitar a desconexão da sessão ao bloquear a tela.
10. Na caixa de diálogo Habilitar/desabilitar a desconexão da sessão ao bloquear a tela, selecione Habilitado ou Desabilitado.
11. Escolha OK.
12. A alteração da configuração da Política de Grupo entra em vigor após a próxima atualização da Política de Grupo WorkSpace e após a reinicialização da WorkSpace sessão. Para aplicar as alterações de política de grupo, execute um destes procedimentos:
    - Reinicie o WorkSpace (no WorkSpaces console da Amazon, selecione o e, em seguida WorkSpace, escolha Ações, Reinicialização WorkSpaces).
    - Em um prompt de comando administrativo, insira **`gpupdate /force`**.

Ativar ou desativar o driver de exibição indireta (IDD) para WSP

Por padrão, WorkSpaces suporta o uso do Indirect Display Driver (IDD). Se necessário para o Windows WorkSpaces, você pode usar as configurações da Política de Grupo para desativar esse recurso.

Para ativar ou desativar o driver de exibição indireta (IDD) para Windows WorkSpaces

1. Certifique-se de que o modelo administrativo de Política de WorkSpaces Grupo mais recente para o WSP esteja instalado no Armazenamento Central do controlador de domínio do seu WorkSpaces diretório.
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon Elastic Compute Cloud associada ao seu WorkSpaces diretório, abra a ferramenta de gerenciamento de políticas de grupo (gpmc.msc).
3. Expanda a floresta (Forest:FQDN).
4. Expanda os Domínios.
5. Expanda o FQDN (por exemplo, `example.com`).
6. Expanda Objetos de Política de Grupo.
7. Selecione Política de domínio padrão, abra o contexto clicando com o botão direito do mouse no menu e escolha Editar.

   > **Note**
   >
   > Se o domínio que dá suporte ao WorkSpaces for um diretório AWS gerenciado do Microsoft AD, você não poderá usar a Política de Domínio Padrão para criar seu GPO. Em vez disso, selecione a Unidade `yourdomainname` Organizacional (OU) ou qualquer OU sob esse nome de domínio, abra o contexto clicando com o botão direito do mouse no menu e escolha Criar um GPO neste domínio e Vincule-o aqui. Para obter mais informações sobre a `yourdomainname` OU, consulte What Gets Created no AWS Directory Service Administration Guide.

8. No Editor de gerenciamento de política de grupo, selecione Configuração do computador, Políticas, Modelos administrativos, Amazon e WSP.
9. Abra a configuração Ativar o driver de exibição AWS indireto.
10. Na caixa de diálogo Ativar o driver de exibição AWS indireto, escolha Ativado ou Desativado.
11. Escolha OK.
12. A alteração da configuração da Política de Grupo entra em vigor após a próxima atualização da Política de Grupo WorkSpace e após a reinicialização da WorkSpace sessão. Para aplicar as alterações de política de grupo, execute um destes procedimentos:

    a. Reinicie o WorkSpace (no WorkSpaces console, selecione o e, em seguida WorkSpace, escolha Ações, Reinicializar WorkSpaces).

b. Em um prompt de comando administrativo, insira `gpupdate /force`.

Definir as configurações de exibição para WSP

WorkSpaces permite que você defina várias configurações de exibição diferentes, incluindo a taxa máxima de quadros, a qualidade mínima da imagem, a qualidade máxima da imagem e a codificação YUV. Ajuste essas configurações com base na qualidade da imagem, na capacidade de resposta e na precisão de cores de que você precisa.

Por padrão, o valor máximo da taxa de quadros é 25. O valor máximo da taxa de quadros especifica o máximo permitido de quadros por segundo (fps). O valor 0 indica que não há limite.

Por padrão, o valor mínimo da qualidade da imagem é 30. A qualidade mínima da imagem pode ser otimizada para melhor capacidade de resposta ou melhor qualidade de imagem. Para obter a melhor capacidade de resposta, reduza a qualidade mínima. Para obter a melhor qualidade, aumente a qualidade mínima.

- Os valores ideais para obter a melhor capacidade de resposta estão entre 30 e 90.
- Os valores ideais para obter a melhor qualidade estão entre 60 e 90.

Por padrão, o valor máximo da qualidade da imagem é 80. A qualidade máxima da imagem não afeta a capacidade de resposta ou a qualidade da imagem, mas define um máximo para limitar o uso da rede.

Por padrão, a codificação da imagem é definida como YUV420. Selecionar Habilitar codificação YUV444 habilita a codificação YUV444 para alta precisão de cores.

No Windows WorkSpaces, você pode usar as configurações da Política de Grupo para definir a taxa máxima de quadros, a qualidade mínima da imagem e os valores máximos da qualidade da imagem.

Para definir as configurações de exibição para o Windows WorkSpaces

1. Certifique-se de que o modelo administrativo de Política de WorkSpaces Grupo mais recente para o WSP esteja instalado no Armazenamento Central do controlador de domínio do seu WorkSpaces diretório.
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management ()gpmc.msc.
3. Expanda a floresta (Floresta: ***FQDN***).

4. Expanda os Domínios.
5. Expanda o FQDN. Por exemplo, `example.com`.
6. Expanda Objetos de Política de Grupo.
7. Selecione Política de domínio padrão, abra o menu de contexto (clique com o botão direito do mouse) e selecione Editar.

> **Note**
>
> Se o domínio que dá suporte ao WorkSpaces for um AWS Managed Microsoft AD diretório, você não poderá usar a Política de Domínio Padrão para criar seu GPO. Em vez disso, selecione a UO *`yourdomainname`* (ou qualquer UO sob ela), abra o menu de contexto (clique com o botão direito do mouse) e selecione Criar um GPO neste domínio e vinculá-lo aqui. Para obter mais informações sobre a UO *`yourdomainname`*, consulte What Gets Created no Guia de administração do AWS Directory Service .

8. No Editor de gerenciamento de política de grupo, selecione Configuração do computador, Políticas, Modelos administrativos, Amazon e WSP.
9. Abra a configuração Definir configurações de exibição.
10. Na caixa de diálogo Definir configurações de exibição, selecione Habilitado e, em seguida, defina os valores de taxa máxima de quadros (fps), qualidade mínima de imagem e qualidade máxima de imagem para os níveis desejados.
11. Escolha OK.
12. A alteração da configuração da Política de Grupo entra em vigor após a próxima atualização da Política de Grupo WorkSpace e após a reinicialização da WorkSpace sessão. Para aplicar as alterações de política de grupo, execute um destes procedimentos:
    - Reinicie WorkSpace o. o WorkSpaces console da Amazon, selecione o., em seguida WorkSpace, escolha Ações, Reinicialização WorkSpaces
    - Em um prompt de comando administrativo, insira **`gpupdate /force`**.

Ativar ou desativar o VSync para o driver AWS somente de exibição virtual para WSP

Por padrão, WorkSpaces suporta o uso do recurso VSync para o driver somente de tela AWS virtual. Se necessário para o Windows WorkSpaces, você pode usar as configurações da Política de Grupo para desativar esse recurso.

Para ativar ou desativar o VSync para Windows WorkSpaces

1. Certifique-se de que o modelo administrativo de Política de WorkSpaces Grupo mais recente para o WSP esteja instalado no Armazenamento Central do controlador de domínio do seu WorkSpaces diretório.
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon Elastic Compute Cloud associada ao seu WorkSpaces diretório, abra a ferramenta de gerenciamento de políticas de grupo (gpmc.msc).
3. Expanda a floresta (Forest:FQDN).
4. Expanda os Domínios.
5. Expanda o FQDN (por exemplo, `example.com`).
6. Expanda Objetos de Política de Grupo.
7. Selecione Política de domínio padrão, abra o contexto clicando com o botão direito do mouse no menu e escolha Editar.

   > **Note**
   >
   > Se o domínio que dá suporte ao WorkSpaces for um diretório AWS gerenciado do Microsoft AD, você não poderá usar a Política de Domínio Padrão para criar seu GPO. Em vez disso, escolha a Unidade `yourdomainname` Organizacional (OU) ou qualquer OU sob esse nome de domínio, abra o contexto clicando com o botão direito do mouse no menu, escolha Criar um GPO neste domínio e Vincule-o aqui. Para obter mais informações sobre a `yourdomainname` OU, consulte O que é criado no AWS Directory Service Administration Guide.

8. No Editor de gerenciamento de política de grupo, selecione Configuração do computador, Políticas, Modelos administrativos, Amazon e WSP.
9. Abra o recurso Ativar VSync da configuração AWS Virtual Display Only Driver.
10. No recurso Ativar VSync da caixa de diálogo AWS Virtual Display Only Driver, escolha Ativado ou Desativado.
11. Escolha OK.
12. A alteração da configuração da Política de Grupo entra em vigor após a próxima atualização da Política de Grupo WorkSpace e após a reinicialização da WorkSpace sessão. Para aplicar as alterações da Política de Grupo, faça o seguinte:

    a. Reinicie o WorkSpace fazendo o seguinte:

i. Opção 1 — No WorkSpaces console, escolha o WorkSpace que você deseja reinicializar. Em seguida, escolha Ações, Reinicializar WorkSpaces.

ii. Opção 2 — Em um prompt de comando administrativo, digitegpupdate /force.

b. Reconecte-se ao WorkSpace para aplicar a configuração.

c. Reinicie o espaço de trabalho novamente.

Configurar o detalhamento de log para WSP

Por padrão, o nível de detalhamento do log do WSP WorkSpaces é definido como Info. Você pode definir os níveis de log para níveis de detalhamento que variam de detalhamento mínimo a detalhamento máximo, conforme descrito aqui:

- Erro: detalhamento mínimo
- Aviso
- Info: padrão
- Depuração: detalhamento máximo

Para Windows WorkSpaces, você pode usar as configurações da Política de Grupo para definir os níveis de verbosidade do log.

Para configurar os níveis de verbosidade do log para Windows WorkSpaces

1. Certifique-se de que o modelo administrativo de Política de WorkSpaces Grupo mais recente para o WSP esteja instalado no Armazenamento Central do controlador de domínio do seu WorkSpaces diretório.
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management ()gpmc.msc.
3. Expanda a floresta (Floresta: ***FQDN***).
4. Expanda os Domínios.
5. Expanda seu FQDN. Por exemplo, `example.com`.
6. Expanda Objetos de Política de Grupo.
7. Selecione Política de domínio padrão, abra o menu de contexto (clique com o botão direito do mouse) e selecione Editar.

> **Note**
>
> Se o domínio que dá suporte ao WorkSpaces for um AWS Managed Microsoft AD diretório, você não poderá usar a Política de Domínio Padrão para criar seu GPO. Em vez disso, selecione a UO *yourdomainname* (ou qualquer UO sob ela), abra o menu de contexto (clique com o botão direito do mouse) e selecione Criar um GPO neste domínio e vinculá-lo aqui. Para obter mais informações sobre a UO *yourdomainname*, consulte What Gets Created no Guia de administração do AWS Directory Service .

8. No Editor de gerenciamento de política de grupo, selecione Configuração do computador, Políticas, Modelos administrativos, Amazon e WSP.
9. Abra a configuração Configurar verbosidade do log.
10. Na caixa de diálogo Configurar verbosidade do log, selecione Habilitado e defina o nível de verbosidade do log como depuração, erro, info ou aviso.
11. Escolha OK.
12. A alteração da configuração da Política de Grupo entra em vigor após a próxima atualização da Política de Grupo WorkSpace e após a reinicialização da WorkSpace sessão. Para aplicar as alterações de política de grupo, execute um destes procedimentos:

    - Reinicie o. WorkSpace No WorkSpaces console da Amazon, selecione e, em seguida WorkSpace, escolha Ações, Reinicialização WorkSpaces.
    - Em um prompt de comando administrativo, insira **`gpupdate /force`**.

Instalar o modelo administrativo de política de grupo para PCoIP

Para usar as configurações de Política de Grupo específicas da Amazon WorkSpaces ao usar o protocolo PCoIP, você deve adicionar o modelo administrativo da Política de Grupo apropriado à versão do agente PCoIP (32 bits ou 64 bits) que está sendo usada para o seu. WorkSpaces

> **Note**
>
> Se você tiver uma combinação de agentes de WorkSpaces 32 bits e 64 bits, poderá usar os modelos administrativos da Política de Grupo para agentes de 32 bits, e suas configurações de Política de Grupo serão aplicadas aos agentes de 32 e 64 bits. Quando

todos WorkSpaces estiverem usando o agente de 64 bits, você poderá passar a usar o modelo administrativo para agentes de 64 bits.

Para determinar se você WorkSpaces tem o agente de 32 bits ou o agente de 64 bits

1. Faça login em um WorkSpace e abra o Gerenciador de tarefas escolhendo Exibir, Enviar Ctrl + Alt + Excluir ou clicando com o botão direito do mouse na barra de tarefas e escolhendo Gerenciador de tarefas.
2. No Gerenciador de Tarefas, vá até a guia Detalhes, clique com o botão direito do mouse nos cabeçalhos das colunas e selecione Selecionar colunas.
3. Na caixa de diálogo Selecionar colunas, selecione Plataforma e clique em OK.
4. Na guia Detalhes, localize `pcoip_agent.exe` e verifique seu valor na coluna Plataforma para determinar se o agente PCoIP é de 32 bits ou 64 bits. (Você pode ver uma mistura de WorkSpaces componentes de 32 bits e 64 bits; isso é normal.)

Instalar o modelo administrativo de política de grupo para PCoIP (32 bits)

Para usar as configurações de Política de Grupo específicas WorkSpaces ao usar o protocolo PCoIP com o agente PCoIP de 32 bits, você deve instalar o modelo administrativo da Política de Grupo para PCoIP. Execute o procedimento a seguir em uma administração de diretório WorkSpace ou instância do Amazon EC2 que esteja associada ao seu diretório.

Para obter mais informações sobre como trabalhar com arquivos .adm, consulte Recommendations for managing Group Policy administrative template (.adm) files na documentação da Microsoft.

Como instalar o modelo administrativo de política de grupo para PCoIP

1. Em um Windows em execução WorkSpace, faça uma cópia do `pcoip.adm` arquivo no `C:\Program Files (x86)\Teradici\PCoIP Agent\configuration` diretório.
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management (gpmc.msc) e navegue até a unidade organizacional em seu domínio que contém suas contas WorkSpaces de máquina.
3. Abra o menu de contexto (clique com o botão direito do mouse) da unidade organizacional da conta da máquina e escolha Criar um GPO neste domínio e vinculá-lo aqui.

4. Na caixa de diálogo Novo GPO, insira um nome descritivo para o GPO, como Políticas de WorkSpaces máquina, e deixe o GPO de partida de origem definido como (nenhum). Escolha OK.
5. Abra o menu de contexto (clique com o botão direito do mouse) do novo GPO e selecione Editar.
6. No Editor de gerenciamento de Política de grupo, escolha Configuração do computador, Políticas e Modelos administrativos. Escolha Ação, Adicionar/remover modelos no menu principal.
7. Na caixa de diálogo Adicionar/remover modelos, escolha Adicionar, selecione o arquivo `pcoip.adm` copiado anteriormente e, em seguida, escolha Abrir, Fechar.
8. Feche o editor de gerenciamento de políticas de grupo. Agora você pode usar esse GPO para modificar as configurações de Política de Grupo que são específicas do. WorkSpaces

Como verificar se o arquivo de modelo administrativo está instalado corretamente

1. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta de gerenciamento de políticas de grupo (gpmc.msc) e navegue até o WorkSpaces GPO das suas WorkSpaces contas de máquina e selecione-o. Escolha Action (Ação), Edit (Editar) no menu principal.
2. No Editor de gerenciamento de Política de grupo, escolha Configuração do computador, Políticas, Modelos administrativos, Modelos administrativos clássicos e Variáveis de sessão de PCoIP.
3. Agora você pode usar esse objeto de política de grupo de variáveis de sessão PCoIP para modificar as configurações de política de grupo que são específicas da Amazon WorkSpaces ao usar o PCoIP.

> **Note**
>
> Para permitir que o usuário substitua as configurações, selecione Padrões de administrador substituíveis. Caso contrário, selecione Padrões de administrador não substituíveis.

Instalar o modelo administrativo de política de grupo para PCoIP (64 bits)

Para usar as configurações de Política de Grupo específicas WorkSpaces ao usar o protocolo PCoIP, você deve adicionar o modelo administrativo `PCoIP.admx` e os `PCoIP.adml` arquivos da

Política de Grupo para PCoIP ao Armazenamento Central do controlador de domínio do seu diretório. WorkSpaces Para obter mais informações sobre os arquivos `.admx` e `.adml`, consulte Como criar e gerenciar o Repositório Central para Modelos Administrativos da Política de Grupo no Windows.

O procedimento a seguir descreve como criar o repositório central e adicionar os arquivos de modelo administrativo a ele. Execute o procedimento a seguir em uma administração de diretório WorkSpace ou instância do Amazon EC2 que esteja associada ao seu WorkSpaces diretório.

Como instalar os arquivos de modelo administrativo de política de grupo para PCoIP

1. Em um Windows em execução WorkSpace, faça uma cópia dos `PCoIP.adml` arquivos `PCoIP.admx` e no `C:\Program Files\Teradici\PCoIP Agent\configuration\policyDefinitions` diretório. O arquivo `PCoIP.adml` está na subpasta `en-US` desse diretório.
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra o Windows File Explorer e, na barra de endereço, insira o nome de domínio totalmente qualificado (FQDN) da sua organização, como. `\\example.com`
3. Abra a pasta `sysvol`.
4. Abra a pasta com o nome *`FQDN`*.
5. Abra a pasta `Policies`. O endereço agora deve ser `\\`*`FQDN`*`\sysvol\`*`FQDN`*`\Policies`.
6. Se ele ainda não existir, crie uma pasta chamada `PolicyDefinitions`.
7. Abra a pasta `PolicyDefinitions`.
8. Copie o arquivo `PCoIP.admx` na pasta `\\`*`FQDN`*`\sysvol\`*`FQDN`*`\Policies\PolicyDefinitions`.
9. Crie uma pasta chamada `en-US` na pasta `PolicyDefinitions`.
10. Abra a pasta `en-US`.
11. Copie o arquivo `PCoIP.adml` na pasta `\\`*`FQDN`*`\sysvol\`*`FQDN`*`\Policies\PolicyDefinitions\en-US`.

Como verificar se os arquivos de modelo administrativo estão instalados corretamente

1. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management ()gpmc.msc.
2. Expanda a floresta (Floresta: ***`FQDN`***).
3. Expanda os Domínios.

4. Expanda o FQDN (por exemplo, `example.com`).
5. Expanda Objetos de Política de Grupo.
6. Selecione Política de domínio padrão, abra o menu de contexto (clique com o botão direito do mouse) e selecione Editar.

> **Note**
>
> Se o domínio que dá suporte ao WorkSpaces for um AWS Managed Microsoft AD diretório, você não poderá usar a Política de Domínio Padrão para criar seu GPO. Em vez disso, você deve criar e vincular o GPO no contêiner de domínio que tem privilégios delegados.
>
> Quando você cria um diretório com AWS Managed Microsoft AD, AWS Directory Service cria uma unidade organizacional (OU) *`yourdomainname`* sob a raiz do domínio. O nome dessa UO é baseado no nome NetBIOS digitado quando você criou o diretório. Se você não especificar um nome NetBIOS, será usado como padrão a primeira parte do nome DNS do diretório (por exemplo, no caso de `corp.example.com`, o nome NetBIOS seria `corp`).
>
> Para criar o GPO, em vez de selecionar Política de domínio padrão, selecione a UO *`yourdomainname`* (ou qualquer UO sob ela), abra o menu de contexto (clique com o botão direito do mouse) e selecione Criar um GPO neste domínio e vinculá-lo aqui.
>
> Para obter mais informações sobre a UO *`yourdomainname`*, consulte What Gets Created no Guia de administração do AWS Directory Service .

7. No Editor de gerenciamento de política de grupo, selecione Configuração do computador, Políticas, Modelos administrativos e Variáveis de sessão de PCoIP.
8. Agora você pode usar esse objeto de Política de Grupo de Variáveis de Sessão PCoIP para modificar as configurações de Política de Grupo que são específicas WorkSpaces ao usar o PCoIP.

> **Note**
>
> Para permitir que o usuário substitua as configurações, selecione Padrões de administrador substituíveis. Caso contrário, selecione Padrões de administrador não substituíveis.

Gerenciar configurações de política de grupo para PCoIP

Use as configurações da Política de Grupo para gerenciar seus Windows WorkSpaces que usam PCoIP.

Configurar o suporte à impressora para PCoIP

Por padrão, WorkSpaces ativa a impressão remota básica, que oferece recursos de impressão limitados porque usa um driver de impressora genérico no lado do host para garantir uma impressão compatível.

A impressão remota avançada para clientes Windows permite que você use recursos específicos da impressora, como impressão de dois lados, mas exige a instalação do driver de impressora correspondente no lado do host.

A impressão remota é implementada como um canal virtual. Se os canais virtuais estiverem desabilitados, a impressão remota não funcionará.

Para Windows WorkSpaces, você pode usar as configurações da Política de Grupo para configurar o suporte à impressora conforme necessário.

Como configurar o suporte à impressora

1. Verifique se você instalou o modelo administrativo de Política de WorkSpaces Grupo mais recente para PCoIP (32 bits) ou o modelo administrativo de Política de WorkSpaces Grupo para PCoIP (64 bits).
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management (gpmc.msc) e navegue até Variáveis de sessão PCoIP.
3. Abra a configuração Configure remote printing (Configurar impressão remota).
4. Na caixa de diálogo Configure remote printing (Configurar impressão remota), execute um dos seguintes procedimentos:
   - Para permitir a impressão remota avançada, selecione Enabled (Habilitado) e, em Options (Opções), Configure remote printing (Configurar impressão remota), selecione Basic and Advanced printing for Windows clients (Impressão básica e avançada para clientes Windows). Para usar automaticamente a impressora padrão do computador cliente, selecione Automatically set default printer (Definir impressora padrão automaticamente).

- Para desabilitar a impressão, selecione Enabled (Habilitado) e, em Options (Opções), Configure remote printing (Configurar impressão remota), selecione Printing disabled (Impressão desabilitada).

5. Escolha OK.
6. A alteração da configuração da Política de Grupo entra em vigor após a próxima atualização da Política de Grupo WorkSpace e após a reinicialização da WorkSpace sessão. Para aplicar as alterações de política de grupo, execute um destes procedimentos:

   - Reinicie o WorkSpace (no WorkSpaces console da Amazon, selecione o e, em seguida WorkSpace, escolha Ações, Reinicialização WorkSpaces).
   - Em um prompt de comando administrativo, insira **`gpupdate /force`**.

Por padrão, o redirecionamento automático da impressora local é desabilitado. Você pode usar as configurações da Política de Grupo para habilitar esse recurso para que sua impressora local seja definida como a impressora padrão sempre que você se conectar à sua WorkSpace.

> **Note**
>
> O redirecionamento local da impressora não está disponível para o Amazon Linux. WorkSpaces

Como ativar o redirecionamento automático da impressora local

1. Verifique se você instalou o modelo administrativo de Política de WorkSpaces Grupo mais recente para PCoIP (32 bits) ou o modelo administrativo de Política de WorkSpaces Grupo para PCoIP (64 bits).
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management (gpmc.msc) e navegue até Variáveis de sessão PCoIP.
3. Abra a configuração Configure remote printing (Configurar impressão remota).
4. Selecione Habilitado e, em Opções, Configurar impressão remota, escolha uma das seguintes opções:

   - Impressão básica e avançada para clientes Windows
   - Impressão básica

5. Selecione Definir impressora padrão automaticamente e clique em OK.
6. A alteração da configuração da Política de Grupo entra em vigor após a próxima atualização da Política de Grupo WorkSpace e após a reinicialização da WorkSpace sessão. Para aplicar as alterações de política de grupo, execute um destes procedimentos:

   - Reinicie o WorkSpace (no WorkSpaces console da Amazon, selecione o e, em seguida WorkSpace, escolha Ações, Reinicialização WorkSpaces).
   - Em um prompt de comando administrativo, insira **`gpupdate /force`**.

Ativar ou desativar o redirecionamento da área de transferência (copiar/colar) para PCoIP

Por padrão, WorkSpaces oferece suporte ao redirecionamento da área de transferência. Se necessário para o Windows WorkSpaces, você pode usar as configurações da Política de Grupo para desativar esse recurso.

Para habilitar ou desabilitar o redirecionamento da área de transferência

1. Verifique se você instalou o modelo administrativo de Política de WorkSpaces Grupo mais recente para PCoIP (32 bits) ou o modelo administrativo de Política de WorkSpaces Grupo para PCoIP (64 bits).
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management (gpmc.msc) e navegue até Variáveis de sessão PCoIP.
3. Abra a configuração Configurar redirecionamento da área de transferência.
4. Na caixa de diálogo Configure clipboard redirection (Configurar redirecionamento da área de transferência), selecione Enabled (Habilitado) e escolha uma das configurações a seguir para determinar a direção na qual redirecionamento da área de transferência é permitido. Quando tiver concluído, selecione OK.

   - Desabilitado em ambas as direções
   - Agente habilitado somente para o cliente (WorkSpace para o computador local)
   - Habilitado somente de cliente para agente (computador local para WorkSpace)
   - Habilitado em ambas as direções
5. A alteração da configuração da Política de Grupo entra em vigor após a próxima atualização da Política de Grupo WorkSpace e após a reinicialização da WorkSpace sessão. Para aplicar as alterações de política de grupo, execute um destes procedimentos:

- Reinicie o WorkSpace (no WorkSpaces console da Amazon, selecione o e, em seguida WorkSpace, escolha Ações, Reinicialização WorkSpaces).
- Em um prompt de comando administrativo, insira **`gpupdate /force`**.

Limitação conhecida

Com o redirecionamento da área de transferência habilitado no WorkSpace, se você copiar conteúdo maior que 890 KB de um aplicativo do Microsoft Office, o aplicativo poderá ficar lento ou não responder por até 5 segundos.

Definir o tempo limite para retomar uma sessão para PCoIP

Quando você perde a conectividade de rede, a sessão ativa WorkSpaces do cliente é desconectada. WorkSpaces os aplicativos cliente para Windows e macOS tentarão reconectar a sessão automaticamente se a conectividade de rede for restaurada em um determinado período de tempo. O tempo limite padrão de retomada da sessão é de 20 minutos, mas você pode modificar esse valor para WorkSpaces que seja controlado pelas configurações de Política de Grupo do seu domínio.

Com definir o valor de tempo limite de retomada de sessão automático

1. Verifique se você instalou o modelo administrativo de Política de WorkSpaces Grupo mais recente para PCoIP (32 bits) ou o modelo administrativo de Política de WorkSpaces Grupo para PCoIP (64 bits).
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management (gpmc.msc) e navegue até Variáveis de sessão PCoIP.
3. Abra a configuração Configurar política de reconexão automática de sessão.
4. Na caixa de diálogo Configurar política de reconexão automática de sessão, escolha Ativado, defina a opção Configurar política de reconexão automática de sessão como o tempo limite desejado, em minutos, e escolha OK.
5. A alteração da configuração da Política de Grupo entra em vigor após a próxima atualização da Política de Grupo WorkSpace e após a reinicialização da WorkSpace sessão. Para aplicar as alterações de política de grupo, execute um destes procedimentos:

   - Reinicie o WorkSpace (no WorkSpaces console da Amazon, selecione o e, em seguida WorkSpace, escolha Ações, Reinicialização WorkSpaces).
   - Em um prompt de comando administrativo, insira **`gpupdate /force`**.

Habilitar ou desabilitar o redirecionamento da entrada de áudio para PCoIP

Por padrão, a Amazon WorkSpaces oferece suporte ao redirecionamento de dados de um microfone local. Se necessário para o Windows WorkSpaces, você pode usar as configurações da Política de Grupo para desativar esse recurso.

> **Note**
>
> Se você tiver uma configuração de Política de Grupo que restringe o login local dos usuários WorkSpaces, a entrada de áudio não funcionará no seu. WorkSpaces Se você remover essa configuração de Política de Grupo, o recurso de entrada de áudio será ativado após a próxima reinicialização do. WorkSpace Para obter mais informações sobre essa configuração de política de grupo, consulte Permitir logon localmente na documentação da Microsoft.

Como habilitar ou desabilitar o redirecionamento da entrada de áudio

1. Verifique se você instalou o modelo administrativo de Política de WorkSpaces Grupo mais recente para PCoIP (32 bits) ou o modelo administrativo de Política de WorkSpaces Grupo para PCoIP (64 bits).
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management (gpmc.msc) e navegue até Variáveis de sessão PCoIP.
3. Abra a configuração Habilitar/desabilitar áudio na sessão PCoIP.
4. Na caixa de diálogo Habilitar/desabilitar áudio na sessão PCoIP, selecione Habilitado ou Desabilitado.
5. Escolha OK.
6. A alteração da configuração da Política de Grupo entra em vigor após a próxima atualização da Política de Grupo WorkSpace e após a reinicialização da WorkSpace sessão. Para aplicar as alterações de política de grupo, execute um destes procedimentos:
   - Reinicie o WorkSpace (no WorkSpaces console da Amazon, selecione o e, em seguida WorkSpace, escolha Ações, Reinicialização WorkSpaces).
   - Em um prompt de comando administrativo, insira **`gpupdate /force`**.

Desabilitar o redirecionamento do fuso horário para PCoIP

Por padrão, o horário em um espaço de trabalho é definido para espelhar o fuso horário do cliente que está sendo usado para se conectar ao WorkSpace. Esse comportamento é controlado por meio do redirecionamento do fuso horário. Talvez você queira desativar a direção do fuso horário por diversos motivos:

- A sua empresa quer que todos os funcionários trabalhem em um determinado fuso horário (mesmo que alguns funcionários estejam em outros fusos horários).
- Você agendou tarefas em uma WorkSpace que deve ser executada em um determinado horário em um fuso horário específico.
- Seus usuários que viajam muito querem manter seu fuso horário WorkSpaces em um único fuso horário para fins de consistência e preferência pessoal.

Se necessário para o Windows WorkSpaces, você pode usar as configurações da Política de Grupo para desativar esse recurso.

Como desativar a direção do fuso horário

1. Verifique se você instalou o modelo administrativo de Política de WorkSpaces Grupo mais recente para PCoIP (32 bits) ou o modelo administrativo de Política de WorkSpaces Grupo para PCoIP (64 bits).
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management (gpmc.msc) e navegue até Variáveis de sessão PCoIP.
3. Abra a configuração Configurar redirecionamento do fuso horário.
4. Na caixa de diálogo Configurar redirecionamento do fuso horário, selecione Desabilitado.
5. Escolha OK.
6. A alteração da configuração da Política de Grupo entra em vigor após a próxima atualização da Política de Grupo WorkSpace e após a reinicialização da WorkSpace sessão. Para aplicar as alterações de política de grupo, execute um destes procedimentos:
   - Reinicie o WorkSpace (no WorkSpaces console da Amazon, selecione o e, em seguida WorkSpace, escolha Ações, Reinicialização WorkSpaces).
   - Em um prompt de comando administrativo, insira **`gpupdate /force`**.
7. Defina o fuso horário do WorkSpaces para o fuso horário desejado.

O fuso horário do agora WorkSpaces é estático e não reflete mais o fuso horário das máquinas clientes.

Definir configurações de segurança do PCoIP

Para o PCoIP, os dados em trânsito são criptografados usando a criptografia TLS 1.2 e a assinatura de solicitação SigV4. O protocolo PCoIP usa o tráfego UDP criptografado, com criptografia AES, para streaming de pixels. A conexão de streaming, usando a porta 4172 (TCP e UDP), é criptografada usando cifras AES-128 e AES-256, mas o padrão de criptografia é de 128 bits. Você pode alterar esse padrão para 256 bits usando a configuração de política de grupo Definir configurações de segurança do PCoIP.

Você também pode usar essa configuração de política de grupo para modificar o modo de segurança TLS e bloquear determinados conjuntos de cifras. Uma explicação detalhada dessas configurações e dos conjuntos de cifras suportados é fornecida na caixa de diálogo de política de grupo Definir configurações de segurança do PCoIP.

Como definir as configurações de segurança do PCoIP

1. Verifique se você instalou o modelo administrativo de Política de WorkSpaces Grupo mais recente para PCoIP (32 bits) ou o modelo administrativo de Política de WorkSpaces Grupo para PCoIP (64 bits).
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management (gpmc.msc) e navegue até Variáveis de sessão PCoIP.
3. Abra a configuração Definir configurações de segurança do PCoIP.
4. Na caixa de diálogo Definir configurações de segurança do PCoIP, selecione Habilitado. Para definir a criptografia padrão para tráfego de streaming para 256 bits, acesse a opção Cifras de criptografia de dados PCoIP e selecione Somente AES-256-GCM.
5. (Opcional) Ajuste a configuração do Modo de segurança TLS e, em seguida, liste os conjuntos de cifras que deseja bloquear. Para obter mais informações sobre essas configurações, consulte as descrições fornecidas na caixa de diálogo Definir configurações de segurança do PCoIP.
6. Escolha OK.
7. A alteração da configuração da Política de Grupo entra em vigor após a próxima atualização da Política de Grupo WorkSpace e após a reinicialização da WorkSpace sessão. Para aplicar as alterações de política de grupo, execute um destes procedimentos:

- Reinicie o WorkSpace (no WorkSpaces console da Amazon, selecione o e, em seguida WorkSpace, escolha Ações, Reinicialização WorkSpaces).
- Em um prompt de comando administrativo, insira **`gpupdate /force`**.

Ativar redirecionamento USB para YubiKey U2F

> **Note**
>
> WorkSpaces Atualmente, a Amazon oferece suporte ao redirecionamento USB somente para YubiKey U2F. Outros tipos de dispositivos USB podem ser redirecionados, mas não são compatíveis e podem não funcionar corretamente.

Para habilitar o redirecionamento USB para YubiKey U2F

1. Verifique se você instalou o modelo administrativo de Política de WorkSpaces Grupo mais recente para PCoIP (32 bits) ou o modelo administrativo de Política de WorkSpaces Grupo para PCoIP (64 bits).
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management (gpmc.msc) e navegue até Variáveis de sessão PCoIP.
3. Abra a configuração Habilitar/desabilitar USB na sessão PCoIP.
4. Selecione Habilitado e, em seguida, Salvar.
5. Abra a configuração Configurar regras de dispositivos USB permitidos e não permitidos no PCoIP.
6. Selecione Habilitado e, em Inserir a tabela de autorização USB (máximo de dez regras), configure as regras da lista de permissões de dispositivos USB.
    - Regra de autorização: 110500407. Esse valor é uma combinação do ID de um fornecedor (VID) e do ID de um produto (PID). O formato para uma combinação VID/PID é 1xxxxyyyy, em que xxxx é o VID em formato hexadecimal e yyyy é o PID em formato hexadecimal. Nesse exemplo, 1050 é o VID e 0407 é o PID. Para obter mais valores YubiKey USB, consulte Valores de ID YubiKey USB.
7. Em Inserir a tabela de autorização de USB (máximo de dez regras), configure as regras da lista de bloqueio de dispositivos USB.

- Para Regra de não autorização, defina uma string vazia. Isso significa que somente dispositivos USB na lista de autorização são permitidos.

> **Note**
>
> Você pode definir no máximo dez regras de autorização de USB e no máximo dez regras de não autorização de USB. Use o caractere de barra vertical (|) para separar várias regras. Para obter informações detalhadas sobre as regras de autorização/não autorização, consulte Teradici PCoIP Standard Agent for Windows.

8. Escolha OK.
9. A alteração da configuração da Política de Grupo entra em vigor após a próxima atualização da Política de Grupo WorkSpace e após a reinicialização da WorkSpace sessão. Para aplicar as alterações de política de grupo, execute um destes procedimentos:
   - Reinicie o WorkSpace (no WorkSpaces console da Amazon, selecione o e, em seguida WorkSpace, escolha Ações, Reinicialização WorkSpaces).
   - Em um prompt de comando administrativo, insira **`gpupdate /force`**.

Depois que a configuração entrar em vigor, todos os dispositivos USB compatíveis poderão ser redirecionados para, a WorkSpaces menos que as restrições sejam configuradas por meio da configuração de regras do dispositivo USB.

Definir o tempo de vida máximo para um tíquete Kerberos

Se você não desativou o recurso Lembrar-me do seu Windows WorkSpaces, seus WorkSpace usuários podem usar a caixa de seleção Lembrar-me ou Mantenha-me conectado no aplicativo WorkSpaces cliente para salvar suas credenciais. Esse recurso permite que os usuários se conectem facilmente a eles WorkSpaces enquanto o aplicativo cliente permanece em execução. As credenciais são armazenadas em cache com segurança até o tempo de vida máximo dos tíquetes Kerberos.

Se você WorkSpace usa um diretório AD Connector, pode modificar a vida útil máxima dos tíquetes Kerberos para seus WorkSpaces usuários por meio da Política de Grupo, seguindo as etapas em Vida útil máxima de um tíquete de usuário na documentação do Microsoft Windows.

Para habilitar ou desabilitar o recurso Remember Me (Lembrar de mim), consulte Habilite recursos de WorkSpace gerenciamento de autoatendimento para seus usuários.

Definir as configurações do servidor proxy do dispositivo para acesso à internet

Por padrão, os aplicativos WorkSpaces cliente usam o servidor proxy especificado nas configurações do sistema operacional do dispositivo para tráfego HTTPS (porta 443). Os aplicativos WorkSpaces clientes da Amazon usam a porta HTTPS para atualizações, registro e autenticação.

> **Note**
>
> Servidores proxy que exigem autenticação com credenciais de login não são compatíveis.

Você pode definir as configurações do servidor proxy do dispositivo para o Windows WorkSpaces por meio da Política de Grupo seguindo as etapas em Configurar as configurações de proxy do dispositivo e conectividade com a Internet na documentação da Microsoft.

Para obter mais informações sobre como definir as configurações de proxy no aplicativo cliente WorkSpaces Windows, consulte Proxy Server no Amazon WorkSpaces User Guide.

Para obter mais informações sobre como definir as configurações de proxy no aplicativo cliente WorkSpaces macOS, consulte Proxy Server no Guia do usuário da WorkSpaces Amazon.

Para obter mais informações sobre como definir as configurações de proxy no aplicativo cliente do WorkSpaces Web Access, consulte Proxy Server no Amazon WorkSpaces User Guide.

Aplicar proxy em tráfego de área de trabalho

Para PCoIP WorkSpaces, os aplicativos cliente de desktop não suportam o uso de um servidor proxy nem a decodificação e inspeção de TLS para tráfego da porta 4172 em UDP (para tráfego de desktop). Elas exigem uma conexão direta com as portas 4172.

Para o WSP WorkSpaces, o aplicativo cliente WorkSpaces Windows (versão 5.1 e superior) e o aplicativo cliente macOS (versão 5.4 e superior) oferecem suporte ao uso de servidores proxy HTTP para tráfego TCP da porta 4195. A descriptografia e a inspeção de TLS não são compatíveis.

O WSP não é compatível com o uso de proxy para tráfego de área de trabalho via UDP. Somente aplicativos cliente de desktop WorkSpaces Windows e macOS e o acesso à Web do WSP oferecem suporte ao uso de proxy para tráfego TCP.

> **Note**
>
> Se você optar por usar um servidor proxy, as chamadas de API que o aplicativo cliente faz para os WorkSpaces serviços também serão enviadas por proxy. Tanto as chamadas de API quanto o tráfego de área de trabalho devem passar pelo mesmo servidor proxy.

Recomendação sobre o uso de servidores proxy

Não recomendamos o uso de um servidor proxy com o tráfego do seu WorkSpaces desktop.

O tráfego WorkSpaces de desktop da Amazon já está criptografado, então os proxies não melhoram a segurança. Um proxy representa um salto adicional no caminho da rede que pode afetar a qualidade do streaming ao introduzir a latência. Os proxies também podem reduzir potencialmente a taxa de throughput se um proxy não for dimensionado adequadamente para lidar com o tráfego de streaming de área de trabalho. Além disso, a maioria dos proxies não foi projetada para suportar conexões de longa duração WebSocket (TCP) e pode afetar a qualidade e a estabilidade do streaming.

Se você precisar usar um proxy, localize seu servidor proxy o mais próximo possível do WorkSpace cliente, de preferência na mesma rede, para evitar aumentar a latência da rede, o que pode afetar negativamente a qualidade e a capacidade de resposta do streaming.

Habilite o suporte do Amazon WorkSpaces for Zoom Meeting Media Plugin

O Zoom suporta comunicação otimizada em tempo real para WSP e PCoIP baseados em Windows WorkSpaces, com o plug-in Zoom VDI. A comunicação direta com o cliente permite que as videochamadas ignorem o desktop virtual baseado na nuvem e forneçam uma experiência de Zoom semelhante à local quando a reunião é realizada dentro da casa do usuário. WorkSpace

Ativar o plug-in Zoom Meeting Media para WSP

Antes de instalar os componentes do Zoom VDI, atualize sua WorkSpaces configuração para oferecer suporte à otimização do Zoom.

Pré-requisitos

Antes de usar o plug-in, verifique se os seguintes requisitos foram atendidos.

- WorkSpaces Cliente Windows versão 5.10.0+ com Zoom VDI Plugin versão 5.17.10+
- Dentro do seu WorkSpaces — Cliente Zoom VDI Meeting versão 5.17.10+

Antes de começar

1. Ative a configuração da Política de Grupo de Extensões. Para ter mais informações, consulte Configurar extensões para WSP.
2. Desative a configuração da Política de Grupo de reconexão automática. Para ter mais informações, consulte Definir o tempo limite para retomar uma sessão para WSP.

Instalação dos componentes do Zoom

Para ativar a otimização do Zoom, instale dois componentes, fornecidos pelo Zoom, no seu Windows WorkSpaces. Para obter mais informações, consulte Usando o Zoom para Amazon Web Services.

1. Instale a versão 5.12.6+ do cliente Zoom VDI Meeting em seu. WorkSpace
2. Instale o plug-in Zoom VDI (Windows Universal Installer) versão 5.12.6+ no cliente em que o seu está instalado WorkSpace
3. Verifique se o plug-in está otimizando o tráfego do Zoom, confirmando se o status do plug-in VDI aparece como Conectado no cliente Zoom VDI. Para obter mais informações, consulte Como confirmar a WorkSpaces otimização da Amazon.

Ativar o plug-in Zoom Meeting Media para PCoIP

Usuários com permissão administrativa para o Active Directory podem gerar uma chave de registro usando seu Objeto de Política de Grupo (GPO). Isso permite que os usuários enviem a chave do registro para todo o Windows WorkSpaces em seu domínio usando uma atualização forçada. Como alternativa, usuários com direitos administrativos também podem instalar chaves de registro individualmente em seu WorkSpaces host.

Pré-requisitos

Antes de usar o plug-in, verifique se os seguintes requisitos foram atendidos.

- WorkSpaces Cliente Windows versão 5.4.0+ com Zoom VDI Plugin versão 5.12.6+.
- Dentro do seu WorkSpaces — Cliente Zoom VDI Meeting versão 5.12.6+.

Crie a chave do registro em um WorkSpaces host Windows

Conclua o procedimento a seguir para criar uma chave de registro em um WorkSpaces host Windows. A chave do registro é necessária para usar o Zoom no Windows WorkSpaces.

1. Abra o Editor do registro do Windows como administrador.
2. Acesse `\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Amazon`.
3. Se a chave Extensão não existir, clique com o botão direito do mouse e selecione Novo > Chave e nomeie-a como Extensão.
4. Na nova chave Extensão, clique com o botão direito do mouse e selecione Novo > DWORD e nomeie-a como Habilitar. O nome deve estar em letras minúsculas.
5. Escolha o novo DWORD e altere o valor para 1.
6. Reinicie o computador para concluir o processo.
7. Em seu WorkSpaces host, baixe e instale o cliente Zoom VDI mais recente. Em seu WorkSpaces cliente (5.4 ou superior), baixe e instale o plug-in de cliente Zoom VDI mais recente para a Amazon. WorkSpaces Para obter mais informações, consulte VDI releases and downloads no site de suporte do Zoom.

Inicie o Zoom para iniciar sua videochamada.

Solução de problemas

Conclua as ações a seguir para solucionar problemas do Zoom no Windows WorkSpaces.

- Confirme se a chave do registro foi ativada corretamente.
- Acesse `C:\ProgramData\Amazon\Amazon WorkSpaces Extension`. Você deve ver `wse_core_dll`.
- As versões no host e nos clientes devem estar corretas e ser iguais.

Se você continuar enfrentando dificuldades, entre em contato AWS Support usando o AWS Support Centro.

Você pode usar os exemplos a seguir para aplicar um GPO como administrador do diretório.

- WSE.adml

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitionResources xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" revision="1.0"
 schemaVersion="1.0" xmlns="http://www.microsoft.com/GroupPolicy/PolicyDefinitions">
    <!-- 'displayName' and 'description' don't appear anywhere. All Windows native
 GPO template files have them set like this. -->
    <displayName>enter display name here</displayName>
    <description>enter description here</description>

    <resources>
    <stringTable>
        <string id="SUPPORTED_ProductOnly">N/A</string>
        <string id="Amazon">Amazon</string>
        <string id="Amazon_Help">Amazon Group Policies</string>
        <string id="WorkspacesExtension">Workspaces Extension</string>
        <string id="WorkspacesExtension_Help">Workspace Extension Group Policies</
string>

        <!-- Extension Itself -->
        <string id="ToggleExtension">Enable/disable Extension Virtual Channel</
string>
        <string id="ToggleExtension_Help">
Allows two-way Virtual Channel data communication for multiple purposes

By default, Extension is disabled.</string>

    </stringTable>
    </resources>
</policyDefinitionResources>
```

- WSE.admx

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" revision="1.0" schemaVersion="1.0" xmlns="http://
www.microsoft.com/GroupPolicy/PolicyDefinitions">
    <policyNamespaces>
        <target prefix="WorkspacesExtension"
 namespace="Microsoft.Policies.Amazon.WorkspacesExtension" />
    </policyNamespaces>
    <supersededAdm fileName="wse.adm" />
```

```
    <resources minRequiredRevision="1.0" />
    <supportedOn>
        <definitions>
            <definition name="SUPPORTED_ProductOnly"
 displayName="$(string.SUPPORTED_ProductOnly)"/>
        </definitions>
    </supportedOn>
    <categories>
        <category name="Amazon" displayName="$(string.Amazon)"
 explainText="$(string.Amazon_Help)" />
        <category name="WorkspacesExtension"
 displayName="$(string.WorkspacesExtension)"
 explainText="$(string.WorkspacesExtension_Help)">
            <parentCategory ref="Amazon" />
        </category>
    </categories>

    <policies>
        <policy name="ToggleExtension" class="Machine"
 displayName="$(string.ToggleExtension)" explainText="$(string.ToggleExtension_Help)"
 key="Software\Policies\Amazon\Extension" valueName="enable">
            <parentCategory ref="WorkspacesExtension" />
            <supportedOn ref="SUPPORTED_ProductOnly" />
            <enabledValue>
                <decimal value="1" />
            </enabledValue>
            <disabledValue>
                <decimal value="0" />
            </disabledValue>
        </policy>
    </policies>
</policyDefinitions>
```

Gerencie seu Amazon Linux WorkSpaces

Assim como no Windows WorkSpaces, o Amazon Linux WorkSpaces é associado a um domínio, então você pode usar usuários e grupos do Active Directory para:

- Administre seu Amazon Linux WorkSpaces
- Forneça acesso a eles WorkSpaces para os usuários

Como as instâncias do Linux não seguem a política de grupo, recomendamos que você use uma solução de gerenciamento de configuração para distribuir e aplicar a política. Por exemplo, você pode usar o AWS OpsWorks for Chef Automate, o AWS OpsWorks for Puppet Enterprise ou o Ansible.

> **Note**
>
> O redirecionamento local da impressora não está disponível para o Amazon Linux. WorkSpaces

Controle o comportamento do Protocolo de WorkSpaces Streaming (WSP) no Amazon Linux WorkSpaces

O comportamento do WSP é controlado pelas definições de configuração no arquivo `wsp.conf`, que está localizado no diretório `/etc/wsp/`. Para implantar e aplicar as alterações à política, use uma solução de gerenciamento de configuração que seja compatível com o Amazon Linux. Todas as alterações entram em vigor quando o agente é iniciado.

> **Note**
>
> - Se você fizer alterações incorretas ou sem suporte no `wsp.conf` arquivo, as alterações de política podem não ser aplicadas às conexões recém-estabelecidas em seu WorkSpace.
> - Atualmente, os pacotes Amazon Linux WorkSpaces on WSP têm as seguintes limitações:
>   - Atualmente disponível apenas nas regiões AWS GovCloud (Oeste dos EUA) e AWS GovCloud (Leste dos EUA).
>   - A entrada de vídeo não é compatível.
>   - A desconexão da sessão ao bloquear a tela não é compatível.

As seções a seguir descrevem como habilitar ou desabilitar determinados recursos.

Configurar o redirecionamento da área de transferência para o WSP Amazon Linux WorkSpaces

Por padrão, WorkSpaces oferece suporte ao redirecionamento da área de transferência. Use o arquivo de configuração do WSP para configurar esse recurso, se necessário. Essa configuração entra em vigor quando você desconecta e reconecta o. WorkSpace

Para configurar o redirecionamento da área de transferência para o WSP Amazon Linux WorkSpaces

1. Abra o arquivo `wsp.conf` em um editor com direitos elevados usando o seguinte comando.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. ```
   clipboard = X
   ```

   Onde os possíveis valores de *X* são:

   `enabled`: o redirecionamento da área de transferência está habilitado em ambas as direções (padrão)

   `disabled`: o redirecionamento da área de transferência está desabilitado em ambas as direções

   `paste-only`: o redirecionamento da área de transferência está habilitado, mas só permite copiar o conteúdo do dispositivo cliente local e colá-lo na área de trabalho remota do host

   `copy-only`: o redirecionamento da área de transferência está habilitado, mas só permite copiar o conteúdo da área de trabalho remota do host e colá-lo no dispositivo cliente local

Ativar ou desativar o redirecionamento de entrada de áudio para o WSP Amazon Linux WorkSpaces

Por padrão, WorkSpaces oferece suporte ao redirecionamento de entrada de áudio. Use o arquivo de configuração do WSP para desabilitar esse recurso, se necessário. Essa configuração entra em vigor quando você se desconecta e se reconecta ao. WorkSpace
   ```

Para ativar ou desativar o redirecionamento de entrada de áudio para o WSP Amazon Linux WorkSpaces

1. Abra o arquivo `wsp.conf` em um editor com direitos elevados usando o seguinte comando.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. Adicione a linha a seguir ao final do arquivo.

   ```
   audio-in = X
   ```

   Onde os possíveis valores de *X* são:

   `enabled`: o redirecionamento de entrada de áudio está habilitado (padrão)

   `disabled`: o redirecionamento de entrada de áudio está desabilitado

Ativar ou desativar o redirecionamento de fuso horário para o WSP Amazon Linux WorkSpaces

Por padrão, o horário em um espaço de trabalho é definido para espelhar o fuso horário do cliente que está sendo usado para se conectar ao WorkSpace. Esse comportamento é controlado por meio do redirecionamento do fuso horário. Talvez você queira desabilitar a direção do fuso horário por motivos semelhantes aos seguintes:

- A sua empresa quer que todos os funcionários trabalhem em um determinado fuso horário (mesmo que alguns funcionários estejam em outros fusos horários).
- Você agendou tarefas em uma WorkSpace que deve ser executada em um determinado horário em um fuso horário específico.
- Seus usuários que viajam muito querem manter seu fuso horário WorkSpaces em um único fuso horário para fins de consistência e preferência pessoal.

Use o arquivo de configuração do WSP para configurar esse recurso, se necessário. Essa configuração entra em vigor depois que você se desconecta e se reconecta ao. WorkSpace

Para ativar ou desativar o redirecionamento de fuso horário para o WSP Amazon Linux WorkSpaces

1. Abra o arquivo `wsp.conf` em um editor com direitos elevados usando o seguinte comando.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp-agent/wsp.conf
```

2. Adicione a linha a seguir ao final do arquivo.

```
timezone_redirect= X
```

Onde os possíveis valores de *X* são:

enabled: o redirecionamento do fuso horário está habilitado (padrão)

disabled: o redirecionamento do fuso horário está desabilitado

Controle o comportamento do agente PCoIP no Amazon Linux WorkSpaces

O comportamento do agente PCoIP é controlado pelas definições de configuração no arquivo `pcoip-agent.conf`, que está localizado no diretório `/etc/pcoip-agent/`. Para implantar e aplicar as alterações à política, use uma solução de gerenciamento de configuração que seja compatível com o Amazon Linux. Todas as alterações entram em vigor quando o agente é iniciado. Quando você reinicia o agente, todas as conexões abertas são encerradas, e o gerenciador de janelas é reiniciado. Para aplicar quaisquer alterações, recomendamos reinicializar o. WorkSpace

> **Note**
>
> Se você fizer alterações incorretas ou sem suporte no `pcoip-agent.conf` arquivo, poderá fazer com que ele pare WorkSpace de funcionar. Se você WorkSpace parar de funcionar, talvez seja necessário conectar-se ao seu WorkSpace usando SSH para reverter as alterações ou reconstruir o. WorkSpace

As seções a seguir descrevem como habilitar ou desabilitar determinados recursos. Para obter uma lista completa das configurações disponíveis, execute a `man pcoip-agent.conf` partir do terminal em qualquer Amazon Linux WorkSpace.

Configurar o redirecionamento da área de transferência para PCoIP Amazon Linux WorkSpaces

Por padrão, WorkSpaces oferece suporte ao redirecionamento da área de transferência. Use a configuração do agente PCoIP para desativar esse recurso, se necessário. Essa configuração entra em vigor quando você reinicializa o. WorkSpace

Para configurar o redirecionamento da área de transferência para PCoIP Amazon Linux WorkSpaces

1. Abra o arquivo `pcoip-agent.conf` em um editor com direitos elevados usando o seguinte comando.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
   ```

2. Adicione a linha a seguir ao final do arquivo.

   ```
   pcoip.server_clipboard_state = X
   ```

   Onde os possíveis valores de *X* são:

   0: o redirecionamento da área de transferência está desabilitado em ambas as direções

   1: o redirecionamento da área de transferência está habilitado em ambas as direções

   2: o redirecionamento da área de transferência está habilitado apenas do cliente para o agente (permite copiar e colar somente do dispositivo cliente local para a área de trabalho remota do host)

   3: o redirecionamento da área de transferência está habilitado apenas do cliente para o agente (permite copiar e colar somente do dispositivo cliente local para a área de trabalho remota do host)

> **Note**
>
> O redirecionamento da área de transferência é implementado como um canal virtual. Se os canais virtuais estiverem desabilitados, o redirecionamento da área de transferência não funcionará. Para habilitar canais virtuais, consulte PCoIP Virtual Channels na documentação do Teradici.

Ativar ou desativar o redirecionamento de entrada de áudio para PCoIP Amazon Linux WorkSpaces

Por padrão, WorkSpaces oferece suporte ao redirecionamento de entrada de áudio. Use a configuração do agente PCoIP para desativar esse recurso, se necessário. Essa configuração entra em vigor quando você reinicializa o. WorkSpace

Para ativar ou desativar o redirecionamento de entrada de áudio para PCoIP Amazon Linux WorkSpaces

1. Abra o arquivo `pcoip-agent.conf` em um editor com direitos elevados usando o seguinte comando.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
   ```

2. Adicione a linha a seguir ao final do arquivo.

   ```
   pcoip.enable_audio = X
   ```

   Onde os possíveis valores de *X* são:

   0: o redirecionamento de entrada de áudio está desabilitado

   1: o redirecionamento de entrada de áudio está habilitado

Ativar ou desativar o redirecionamento de fuso horário para PCoIP Amazon Linux WorkSpaces

Por padrão, o horário em um espaço de trabalho é definido para espelhar o fuso horário do cliente que está sendo usado para se conectar ao WorkSpace. Esse comportamento é controlado por meio do redirecionamento do fuso horário. Talvez você queira desabilitar a direção do fuso horário por motivos semelhantes aos seguintes:

- A sua empresa quer que todos os funcionários trabalhem em um determinado fuso horário (mesmo que alguns funcionários estejam em outros fusos horários).
- Você agendou tarefas em uma WorkSpace que deve ser executada em um determinado horário em um fuso horário específico.

- Seus usuários que viajam muito querem manter seu fuso horário WorkSpaces em um único fuso horário para fins de consistência e preferência pessoal.

Se necessário para Linux WorkSpaces, você pode usar a configuração do Agente PCoIP para desativar esse recurso. Essa configuração entra em vigor quando você reinicializa o. WorkSpace

Para habilitar ou desabilitar o redirecionamento de fuso horário para PCoIP Amazon Linux WorkSpaces

1. Abra o arquivo `pcoip-agent.conf` em um editor com direitos elevados usando o seguinte comando.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
   ```

2. Adicione a linha a seguir ao final do arquivo.

   ```
   pcoip.enable_timezone_redirect= X
   ```

   Onde os possíveis valores de *X* são:

   0: o redirecionamento do fuso horário está desabilitado

   1: o redirecionamento do fuso horário está habilitado

Conceda acesso SSH aos administradores do Amazon Linux WorkSpaces

Por padrão, somente usuários e contas atribuídos no grupo de administradores de domínio podem se conectar ao Amazon Linux WorkSpaces usando SSH.

Recomendamos que você crie um grupo de administradores dedicado para seus WorkSpaces administradores do Amazon Linux no Active Directory.

Para ativar o acesso sudo para membros do grupo Linux_Workspaces_Admins do Active Directory

1. Edite o arquivo `sudoers` usando `visudo`, conforme mostrado no exemplo a seguir:

   ```
   [example\username@workspace-id ~]$ sudo visudo
   ```

2. Adicione a seguinte linha.

```
%example.com\\Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

Depois de criar o grupo de administradores dedicados, siga estas etapas para ativar o login para os membros do grupo.

Para habilitar o login para membros do grupo Linux_ WorkSpaces _Admins Active Directory

1. Edite `/etc/security/access.conf` com direitos elevados.

```
[example\username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. Adicione a seguinte linha.

```
+:(example\Linux_WorkSpaces_Admins):ALL
```

Para obter mais informações sobre como habilitar conexões SSH, consulte Habilite conexões SSH para seu Linux WorkSpaces.

Substitua o shell padrão para Amazon Linux WorkSpaces

Para substituir o shell padrão para Linux WorkSpaces, recomendamos que você edite o `~/.bashrc` arquivo do usuário. Por exemplo, para usar `Z shell` em vez do shell `Bash`, adicione as seguintes linhas a /home/*username*/`.bashrc`.

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

> **Note**
>
> Depois de fazer essa alteração, você deve reinicializar WorkSpace ou sair do WorkSpace (não apenas desconectar) e, em seguida, fazer login novamente para que a alteração entre em vigor.

Proteger repositórios personalizados contra acesso não autorizado

Para controlar o acesso aos repositórios personalizados, recomendamos usar os recursos de segurança integrados no Amazon Virtual Private Cloud (Amazon VPC) em vez de usar senhas. Por exemplo, use listas de controle de acesso (ACLs) de rede e grupos de segurança. Para obter mais informações sobre esses recursos, consulte Segurança no Guia do usuário do Amazon VPC.

Se você deve usar senhas para proteger seus repositórios, certifique-se de criar arquivos de definição de repositório `yum` conforme mostrado em Arquivos de definição de repositório na documentação do Fedora.

Usar o repositório da Biblioteca de Extras do Amazon Linux

Com o Amazon Linux, é possível usar a Biblioteca de extras para instalar atualizações de aplicação e software em instâncias. Para obter informações sobre como usar a Biblioteca de extras, consulte Biblioteca de extras (Amazon Linux) no Guia do usuário do Amazon EC2 para instâncias do Linux.

> **Note**
>
> Se você estiver usando o repositório Amazon Linux, seu Amazon Linux WorkSpaces deve ter acesso à Internet ou você deve configurar endpoints de nuvem privada virtual (VPC) para esse repositório e para o repositório principal do Amazon Linux. Para ter mais informações, consulte Forneça acesso à Internet a partir do seu WorkSpace.

Use cartões inteligentes para autenticação no Linux WorkSpaces

Os pacotes Linux WorkSpaces on WorkSpaces Streaming Protocol (WSP) permitem o uso de cartões inteligentes Common Access Card (CAC) e Personal Identity Verification (PIV) para autenticação. Para ter mais informações, consulte Usar cartões inteligentes para autenticação.

Definir as configurações do servidor proxy do dispositivo para acesso à internet

Por padrão, os aplicativos WorkSpaces cliente usam o servidor proxy especificado nas configurações do sistema operacional do dispositivo para tráfego HTTPS (porta 443). Os aplicativos WorkSpaces clientes da Amazon usam a porta HTTPS para atualizações, registro e autenticação.

> **Note**
>
> Servidores proxy que exigem autenticação com credenciais de login não são compatíveis.

Você pode definir as configurações do servidor proxy do dispositivo para seu Linux WorkSpaces por meio da Política de Grupo seguindo as etapas em Configurar as configurações de proxy do dispositivo e conectividade com a Internet na documentação da Microsoft.

Para obter mais informações sobre como definir as configurações de proxy no aplicativo cliente WorkSpaces Windows, consulte Proxy Server no Amazon WorkSpaces User Guide.

Para obter mais informações sobre como definir as configurações de proxy no aplicativo cliente WorkSpaces macOS, consulte Proxy Server no Guia do usuário da WorkSpaces Amazon.

Para obter mais informações sobre como definir as configurações de proxy no aplicativo cliente do WorkSpaces Web Access, consulte Proxy Server no Amazon WorkSpaces User Guide.

Aplicar proxy em tráfego de área de trabalho

Para PCoIP WorkSpaces, os aplicativos cliente de desktop não suportam o uso de um servidor proxy nem a decodificação e inspeção de TLS para tráfego da porta 4172 em UDP (para tráfego de desktop). Elas exigem uma conexão direta com as portas 4172.

Para o WSP WorkSpaces, o aplicativo cliente WorkSpaces Windows (versão 5.1 e superior) e o aplicativo cliente macOS (versão 5.4 e superior) oferecem suporte ao uso de servidores proxy HTTP para tráfego TCP da porta 4195. A descriptografia e a inspeção de TLS não são compatíveis.

O WSP não é compatível com o uso de proxy para tráfego de área de trabalho via UDP. Somente aplicativos cliente de desktop WorkSpaces Windows e macOS e o acesso à Web do WSP oferecem suporte ao uso de proxy para tráfego TCP.

> **Note**
>
> Se você optar por usar um servidor proxy, as chamadas de API que o aplicativo cliente faz para os WorkSpaces serviços também serão enviadas por proxy. Tanto as chamadas de API quanto o tráfego de área de trabalho devem passar pelo mesmo servidor proxy.

Recomendação sobre o uso de servidores proxy

Não recomendamos o uso de um servidor proxy com o tráfego do seu WorkSpaces desktop.

O tráfego WorkSpaces de desktop da Amazon já está criptografado, então os proxies não melhoram a segurança. Um proxy representa um salto adicional no caminho da rede que pode afetar a qualidade do streaming ao introduzir a latência. Os proxies também podem reduzir potencialmente a taxa de throughput se um proxy não for dimensionado adequadamente para lidar com o tráfego de streaming de área de trabalho. Além disso, a maioria dos proxies não foi projetada para suportar conexões de longa duração WebSocket (TCP) e pode afetar a qualidade e a estabilidade do streaming.

Se você precisar usar um proxy, localize seu servidor proxy o mais próximo possível do WorkSpace cliente, de preferência na mesma rede, para evitar aumentar a latência da rede, o que pode afetar negativamente a qualidade e a capacidade de resposta do streaming.

Gerencie seu Ubuntu WorkSpaces

Assim como no Windows e no Amazon Linux WorkSpaces, o Ubuntu WorkSpaces é associado a um domínio, então você pode usar usuários e grupos do Active Directory para:

- Administre seu Ubuntu WorkSpaces
- Forneça acesso a eles WorkSpaces para os usuários

Você pode gerenciar o Ubuntu WorkSpaces com a Política de Grupo usando o AdSys. Para obter mais informações, consulte Ubuntu Active Directory integration FAQ. Você também pode usar outras soluções de configuração e gerenciamento, como Landscape e Ansible.

Comportamento do Control WorkSpaces Streaming Protocol (WSP) no Ubuntu WorkSpaces

O comportamento do WSP é controlado pelas definições de configuração no arquivo `wsp.conf`, que está localizado no diretório `/etc/wsp/`. Para implantar e aplicar as alterações à política, use uma solução de gerenciamento de configuração que seja compatível com o Ubuntu. Todas as alterações entram em vigor quando o agente é iniciado.

> **Note**
>
> Se você fizer alterações incorretas ou sem suporte, as `wsp.conf` políticas poderão não ser aplicadas às novas conexões estabelecidas com o seu WorkSpace.

As seções a seguir descrevem como habilitar ou desabilitar determinados recursos.

Ativar ou desativar o redirecionamento da área de transferência para o Ubuntu WorkSpaces

Por padrão, WorkSpaces oferece suporte ao redirecionamento da área de transferência. Use o arquivo de configuração do WSP para desabilitar esse recurso, se necessário.

Para ativar ou desativar o redirecionamento da área de transferência para o Ubuntu WorkSpaces

1. Abra o arquivo `wsp.conf` em um editor com direitos elevados usando o seguinte comando.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. Adicione a linha a seguir ao final do grupo `[policies]`.

   ```
   clipboard = X
   ```

   Onde os possíveis valores de *X* são:

   enabled: o redirecionamento da área de transferência está habilitado em ambas as direções (padrão)

   disabled: o redirecionamento da área de transferência está desabilitado em ambas as direções

   paste-only: o redirecionamento da área de transferência está habilitado e só permite copiar o conteúdo do dispositivo cliente local e colá-lo na área de trabalho remota do host

   copy-only: o redirecionamento da área de transferência está habilitado e só permite copiar o conteúdo da área de trabalho remota do host e colá-lo no dispositivo cliente local

Ativar ou desativar o redirecionamento de entrada de áudio para o Ubuntu WorkSpaces

Por padrão, WorkSpaces oferece suporte ao redirecionamento de entrada de áudio. Use o arquivo de configuração do WSP para desabilitar esse recurso, se necessário.

Para ativar ou desativar o redirecionamento de entrada de áudio para o Ubuntu WorkSpaces

1. Abra o arquivo `wsp.conf` em um editor com direitos elevados usando o seguinte comando.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. Adicione a linha a seguir ao final do grupo `[policies]`.

   ```
   audio-in = X
   ```

   Onde os possíveis valores de *X* são:

   enabled: o redirecionamento de entrada de áudio está habilitado (padrão)

   disabled: o redirecionamento de entrada de áudio está desabilitado

Ativar ou desativar o redirecionamento de entrada de vídeo para o Ubuntu WorkSpaces

Por padrão, WorkSpaces oferece suporte ao redirecionamento de entrada de vídeo. Use o arquivo de configuração do WSP para desabilitar esse recurso, se necessário.

Para ativar ou desativar o redirecionamento de entrada de vídeo para o Ubuntu WorkSpaces

1. Abra o arquivo `wsp.conf` em um editor com direitos elevados usando o seguinte comando.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. Adicione a linha a seguir ao final do grupo `[policies]`.

   ```
   video-in = X
   ```

   Onde os possíveis valores de *X* são:

enabled: o redirecionamento de entrada de vídeo está habilitado (padrão)

disabled: o redirecionamento de entrada de vídeo está desabilitado

Ativar ou desativar o redirecionamento de fuso horário para o Ubuntu WorkSpaces

Por padrão, o horário em um espaço de trabalho é definido para espelhar o fuso horário do cliente que está sendo usado para se conectar ao WorkSpace. Esse comportamento é controlado por meio do redirecionamento do fuso horário. Talvez você queira desabilitar a direção do fuso horário por motivos semelhantes aos seguintes:

- A sua empresa quer que todos os funcionários trabalhem em um determinado fuso horário (mesmo que alguns funcionários estejam em outros fusos horários).
- Você agendou tarefas em uma WorkSpace que deve ser executada em um determinado horário em um fuso horário específico.
- Seus usuários viajam muito e querem mantê-los WorkSpaces em um único fuso horário para fins de consistência e preferência pessoal.

Use o arquivo de configuração do WSP para configurar esse recurso, se necessário.

Para ativar ou desativar o redirecionamento de fuso horário para o Ubuntu WorkSpaces

1. Abra o arquivo `wsp.conf` em um editor com direitos elevados usando o seguinte comando.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Adicione a linha a seguir ao final do grupo `[policies]`.

```
timezone-redirection = X
```

Onde os possíveis valores de *X* são:

enabled: o redirecionamento do fuso horário está habilitado (padrão)

disabled: o redirecionamento do fuso horário está desabilitado

Ativar ou desativar o redirecionamento de impressora para o Ubuntu WorkSpaces

Por padrão, WorkSpaces oferece suporte ao redirecionamento de impressoras. Use o arquivo de configuração do WSP para desabilitar esse recurso, se necessário.

Para ativar ou desativar o redirecionamento de impressora para o Ubuntu WorkSpaces

1. Abra o arquivo `wsp.conf` em um editor com direitos elevados usando o seguinte comando.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. Adicione a linha a seguir ao final do grupo `[policies]`.

   ```
   remote-printing = X
   ```

   Onde os possíveis valores de *X* são:

   enabled: o redirecionamento de impressora está habilitado (padrão)

   disabled: o redirecionamento da impressora está desabilitado

Habilitar ou desabilitar a desconexão da sessão ao bloquear a tela para WSP

Ative a sessão de desconexão no bloqueio de tela para permitir que seus usuários encerrem a WorkSpaces sessão quando a tela de bloqueio for detectada. Para se reconectar a partir do WorkSpaces cliente, os usuários podem usar suas senhas ou seus cartões inteligentes para se autenticar, dependendo do tipo de autenticação habilitado para eles. WorkSpaces

Por padrão, WorkSpaces não suporta a desconexão da sessão no bloqueio de tela. Use o arquivo de configuração do WSP para habilitar esse recurso, se necessário.

Para ativar ou desativar a sessão de desconexão no bloqueio de tela do Ubuntu WorkSpaces

1. Abra o arquivo `wsp.conf` em um editor com direitos elevados usando o seguinte comando.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Adicione a linha a seguir ao final do grupo `[policies]`.

```
disconnect-on-lock = X
```

Onde os possíveis valores de *X* são:

enabled: a desconexão ao bloquear a tela está habilitada

disabled: a desconexão ao bloquear a tela está desabilitada (padrão)

Conceda acesso SSH aos administradores do Ubuntu WorkSpaces

Por padrão, somente usuários e contas atribuídos no grupo Administradores de Domínio podem se conectar ao Ubuntu WorkSpaces usando SSH. Para permitir que outros usuários e contas se conectem ao Ubuntu WorkSpaces usando SSH, recomendamos que você crie um grupo de administradores dedicado para seus WorkSpaces administradores do Ubuntu no Active Directory.

Como habilitar o acesso sudo para membros do grupo **`Linux_WorkSpaces_Admins`** do Active Directory

1. Edite o arquivo `sudoers` usando `visudo`, conforme mostrado no exemplo a seguir:

```
[username@workspace-id ~]$ sudo visudo
```

2. Adicione a seguinte linha.

```
%Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

Depois de criar o grupo de administradores dedicados, siga estas etapas para ativar o login para os membros do grupo.

Como habilitar o login para membros do grupo **`Linux_WorkSpaces_Admins`** do Active Directory

1. Edite /`etc/security/access.conf` com direitos elevados.

```
[username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. Adicione a seguinte linha.

```
+:(Linux_WorkSpaces_Admins):ALL
```

Com o Ubuntu, WorkSpaces você não precisa adicionar um nome de domínio ao especificar o nome de usuário para a conexão SSH e, por padrão, a autenticação por senha está desativada. Para se conectar via SSH, você precisa adicionar sua chave pública SSH ao seu `$HOME/.ssh/authorized_keys` Ubuntu WorkSpace ou editar `/etc/ssh/sshd_config` para PasswordAuthentication configurá-la. `yes` Para obter mais informações sobre como habilitar conexões SSH, consulte Habilitar conexões SSH para seu Linux. WorkSpaces

Substituir o shell padrão para o Ubuntu WorkSpaces

Para substituir o shell padrão do Ubuntu WorkSpaces, recomendamos que você edite o `~/.bashrc` arquivo do usuário. Por exemplo, para usar `Z shell` em vez do shell `Bash`, adicione as seguintes linhas a `/home/username/.bashrc`.

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

> **Note**
>
> Depois de fazer essa alteração, você deve reinicializar WorkSpace ou sair do WorkSpace (não apenas desconectar) e, em seguida, fazer login novamente para que a alteração entre em vigor.

Definir as configurações do servidor proxy do dispositivo para acesso à internet

Por padrão, os aplicativos WorkSpaces cliente usam o servidor proxy especificado nas configurações do sistema operacional do dispositivo para tráfego HTTPS (porta 443). Os aplicativos WorkSpaces clientes da Amazon usam a porta HTTPS para atualizações, registro e autenticação.

> **Note**
>
> Servidores proxy que exigem autenticação com credenciais de login não são compatíveis.

Você pode definir as configurações do servidor proxy do dispositivo para o seu Ubuntu WorkSpaces por meio da Política de Grupo, seguindo as etapas em Configurar as configurações de proxy do dispositivo e conectividade com a Internet na documentação da Microsoft.

Para obter mais informações sobre como definir as configurações de proxy no aplicativo cliente WorkSpaces Windows, consulte Proxy Server no Amazon WorkSpaces User Guide.

Para obter mais informações sobre como definir as configurações de proxy no aplicativo cliente WorkSpaces macOS, consulte Proxy Server no Guia do usuário da WorkSpaces Amazon.

Para obter mais informações sobre como definir as configurações de proxy no aplicativo cliente do WorkSpaces Web Access, consulte Proxy Server no Amazon WorkSpaces User Guide.

Aplicar proxy em tráfego de área de trabalho

Para PCoIP WorkSpaces, os aplicativos cliente de desktop não suportam o uso de um servidor proxy nem a decodificação e inspeção de TLS para tráfego da porta 4172 em UDP (para tráfego de desktop). Elas exigem uma conexão direta com as portas 4172.

Para o WSP WorkSpaces, o aplicativo cliente WorkSpaces Windows (versão 5.1 e superior) e o aplicativo cliente macOS (versão 5.4 e superior) oferecem suporte ao uso de servidores proxy HTTP para tráfego TCP da porta 4195. A descriptografia e a inspeção de TLS não são compatíveis.

O WSP não é compatível com o uso de proxy para tráfego de área de trabalho via UDP. Somente aplicativos cliente de desktop WorkSpaces Windows e macOS e o acesso à Web do WSP oferecem suporte ao uso de proxy para tráfego TCP.

> **Note**
>
> Se você optar por usar um servidor proxy, as chamadas de API que o aplicativo cliente faz para os WorkSpaces serviços também serão enviadas por proxy. Tanto as chamadas de API quanto o tráfego de área de trabalho devem passar pelo mesmo servidor proxy.

Recomendação sobre o uso de servidores proxy

Não recomendamos o uso de um servidor proxy com o tráfego do seu WorkSpaces desktop.

O tráfego WorkSpaces de desktop da Amazon já está criptografado, então os proxies não melhoram a segurança. Um proxy representa um salto adicional no caminho da rede que pode afetar a qualidade do streaming ao introduzir a latência. Os proxies também podem reduzir potencialmente a taxa de throughput se um proxy não for dimensionado adequadamente para lidar com o tráfego de streaming de área de trabalho. Além disso, a maioria dos proxies não foi projetada para suportar conexões de longa duração WebSocket (TCP) e pode afetar a qualidade e a estabilidade do streaming.

Se você precisar usar um proxy, localize seu servidor proxy o mais próximo possível do WorkSpace cliente, de preferência na mesma rede, para evitar aumentar a latência da rede, o que pode afetar negativamente a qualidade e a capacidade de resposta do streaming.

Otimize a Amazon WorkSpaces para comunicação em tempo real

A Amazon WorkSpaces oferece uma ampla variedade de técnicas para facilitar a implantação de aplicativos de Comunicação Unificada (UC), como Microsoft Teams, Zoom, Webex e outros. Nos cenários das aplicações contemporâneas, a maioria das aplicações de UC consiste em uma variedade de recursos, incluindo salas de bate-papo individuais, canais colaborativos de bate-papo em grupo, armazenamento e troca de arquivos sem interrupções, eventos ao vivo, webinars, transmissões, compartilhamento e controle interativos de tela, quadro branco e recursos de

mensagens de áudio/vídeo off-line. A maior parte dessa funcionalidade está perfeitamente disponível WorkSpaces como recursos padrão, sem a necessidade de ajustes ou aprimoramentos adicionais. No entanto, é importante notar que os elementos de comunicação em tempo real, particularmente one-on-one chamadas e reuniões coletivas em grupo, representam uma exceção a essa regra. A incorporação bem-sucedida dessa funcionalidade frequentemente exige foco e planejamento dedicados durante o processo de WorkSpaces implantação.

Ao planejar sua implementação de funcionalidades de comunicação em tempo real de aplicativos de UC na Amazon WorkSpaces, você tem três modos distintos de configuração de Comunicação em Tempo Real (RTC) para escolher. A seleção depende das aplicações específicas disponibilizadas aos usuários e dos dispositivos cliente a serem usados.

Este documento se concentra na otimização da experiência do usuário para os aplicativos de UC mais comuns na Amazon. WorkSpaces Para otimizações específicas do WorkSpaces Core, consulte a documentação específica do parceiro.

Tópicos

Visão geral dos modos de otimização de mídia

A seguir estão as opções de otimização de mídia disponíveis.

Opção 1: Comunicação em tempo real otimizada para mídia (RTC otimizado para mídia)

Nesse modo, aplicativos de UC e VoIP de terceiros são executados WorkSpace remotamente, enquanto sua estrutura de mídia é transferida para o cliente compatível para comunicação direta. Os seguintes aplicativos de UC usam essa abordagem na Amazon WorkSpaces:

- Zoom Meetings
- Cisco Webex Meetings

Para que o modo RTC otimizado para mídia funcione, o fornecedor do aplicativo de UC deve desenvolver a integração WorkSpaces usando um dos kits de desenvolvimento de software (SDK)

disponíveis, como o SDK de extensão DCV. Este modo requer que os componentes de UC sejam instalados no dispositivo cliente.

Para obter mais informações sobre esse modo, consulte Configurar RTC otimizado para mídia.

Opção 2: Comunicação em tempo real otimizada na sessão (RTC otimizado na sessão)

Nesse modo, o aplicativo de UC inalterado é executado no WorkSpace, canalizando o tráfego de áudio e vídeo por meio do Protocolo de WorkSpaces Streaming para o dispositivo cliente. O áudio local do microfone e o fluxo de vídeo de uma webcam são redirecionados para o WorkSpace, onde são consumidos pelo aplicativo de UC. Esse modo fornece ampla compatibilidade de aplicativos e entrega com eficiência o aplicativo de UC do controle remoto WorkSpace para uma variedade de plataformas de clientes. Não é necessário implantar os componentes da aplicação de UC no dispositivo cliente.

Para obter mais informações sobre esse modo, consulte Configurar o RTC otimizado em sessão.

Opção 3: Comunicação direta em tempo real (RTC direto)

Nesse modo, o aplicativo que opera dentro do WorkSpace assume o controle do aparelho telefônico físico ou virtual localizado na mesa do usuário ou no sistema operacional do cliente. Isso faz com que o tráfego de áudio passe do telefone físico na estação de trabalho do usuário ou do telefone virtual operando no dispositivo do cliente até o ponto de chamada remoto. Instâncias notáveis de aplicações que funcionam nesse modo incluem:

- Otimização do Amazon Connect para Amazon WorkSpaces
- Genesys Cloud WebRTC media helper
- Microsoft Teams SIP Gateway
- Microsoft Teams Desk phones and Teams displays
- Participar de uma audioconferência por meio dos recursos de discagem ou “ligar para o meu telefone” da aplicação de UC.

Para obter mais informações sobre esse modo, consulte Configurar o Direct RTC.

Como escolher o modo de otimização de RTC?

Diferentes modos de otimização de RTC podem ser empregados simultaneamente ou configurados para se complementarem como alternativa. Por exemplo, considere habilitar o RTC otimizado

para mídia em reuniões no Cisco Webex. Essa configuração garante que os usuários tenham uma comunicação otimizada ao acessar WorkSpace por meio de um cliente de desktop. No entanto, em cenários em que o Webex é acessado de um quiosque de internet compartilhado sem componentes de otimização de UC, o Webex fará a transição perfeita para o modo RTC otimizado na sessão para manter a funcionalidade. Quando os usuários interagem com várias aplicações de UC, os modos de configuração do RTC podem variar de acordo com requisitos exclusivos.

A tabela a seguir representa os recursos comuns de aplicações de UC e define qual modo de configuração RTC promove o melhor resultado.

Atributo	RTC direto	RTC otimizado para mídia	RTC otimizado em sessão
Chat individual	Não requer configuração RTC		
Salas de bate-papo em grupo	Não requer configuração RTC		
Audioconferência em grupo	O melhor	O melhor	Bom
Videoconferência em grupo	Bom	O melhor	Bom
Chamadas de áudio individuais	O melhor	O melhor	Bom
Chamadas de vídeo individuais	Bom	O melhor	Bom
Quadro branco	Não requer configuração RTC		
Áudio/videoclipes/ mensagens	Não aplicável	Bom	O melhor
Compartilhamento de arquivos	Não aplicável	Depende da aplicação de UC	O melhor

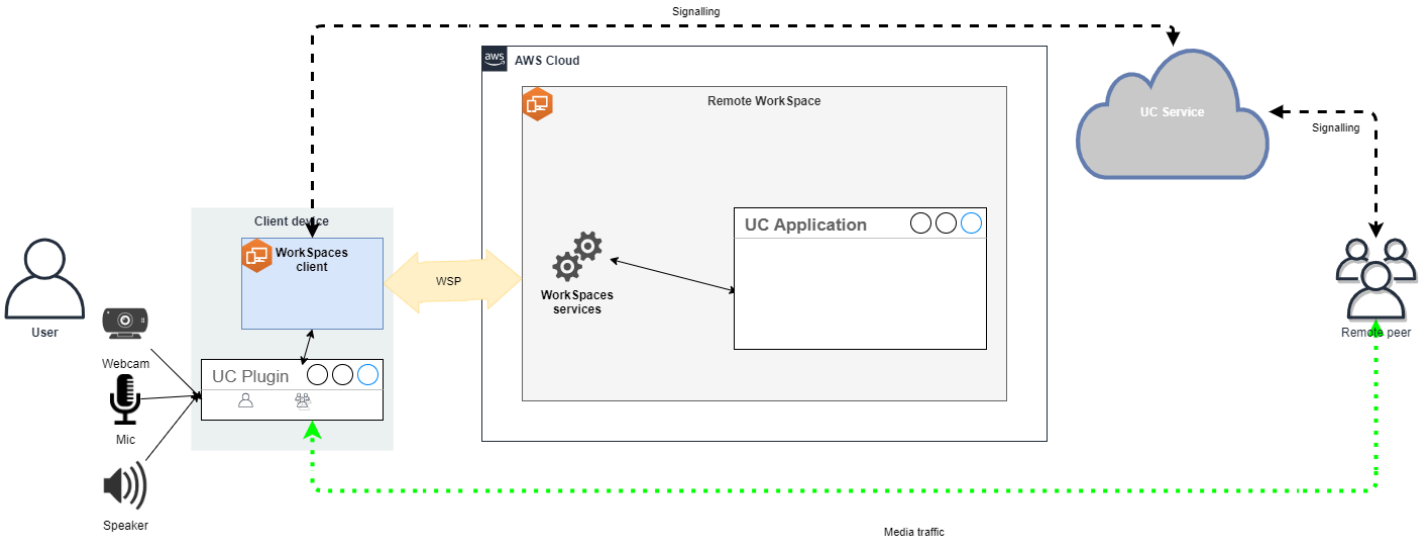
Atributo	RTC direto	RTC otimizado para mídia	RTC otimizado em sessão
Compartilhamento e controle de tela	Não aplicável	Depende da aplicação de UC	O melhor
Webinars/transmissão de eventos	Não aplicável	Bom	O melhor

Orientações para otimização do RTC

Configurar RTC otimizado para mídia

O modo RTC otimizado para mídia é possível graças ao uso dos SDKs da Amazon pelo provedor de aplicações de UC. A arquitetura requer que o fornecedor de UC desenvolva um plug-in ou extensão específico de UC e disponibilize ao cliente.

O SDK, que inclui opções publicamente disponíveis, como o SDK de extensão DCV e versões privadas personalizadas, estabelece um canal de controle entre o módulo de aplicativo UC que opera dentro do WorkSpace e um plug-in no lado do cliente. Normalmente, esse canal de controle instrui a extensão do cliente a iniciar ou participar de uma chamada. Depois que a chamada é estabelecida por meio da extensão do lado do cliente, o plug-in UC captura o áudio do microfone e o vídeo da webcam, que são transmitidos diretamente para a nuvem UC ou para um parceiro de chamada. O áudio recebido é reproduzido localmente e o vídeo é sobreposto na interface do usuário do cliente remoto. O canal de controle é responsável por comunicar o status da chamada.



WorkSpaces Atualmente, a Amazon oferece suporte aos seguintes aplicativos com o modo RTC otimizado para mídia:

- Reuniões Zoom (para PCoIP e WSP) WorkSpaces
- Reuniões Cisco Webex (somente para WorkSpaces WSP)

Se você estiver usando um aplicativo que não esteja na lista, é recomendável entrar em contato com o fornecedor do aplicativo e solicitar suporte para o RTC otimizado para WorkSpaces mídia. Para agilizar esse processo, incentive-os a entrar em contato com aws-av-offloading@amazon .com.

Embora o modo RTC otimizado para mídia melhore o desempenho da chamada e minimize a utilização WorkSpace de recursos, ele possui certas limitações:

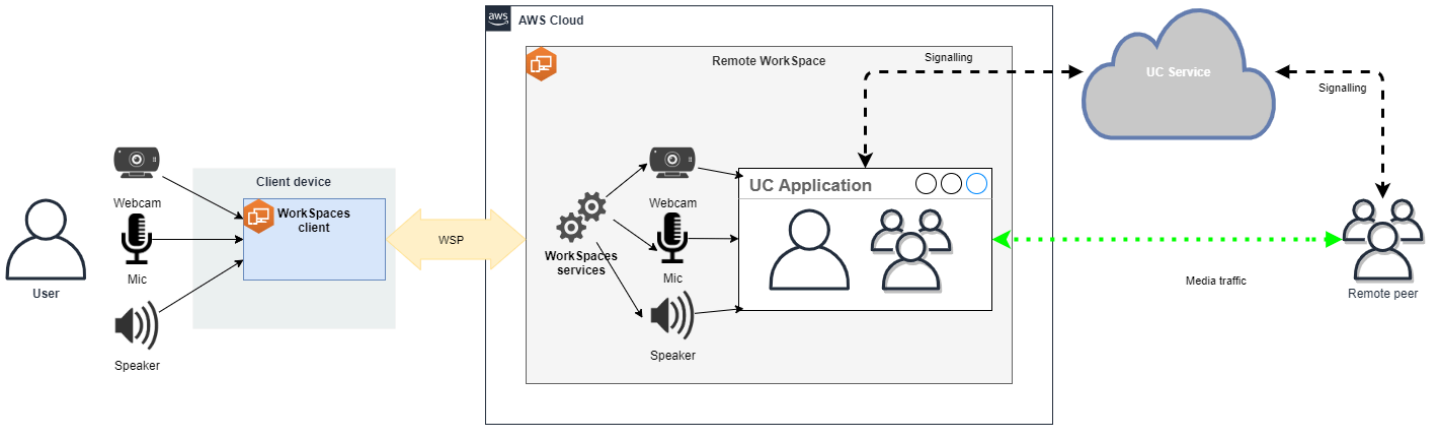
- A extensão do cliente UC deve estar instalada no dispositivo cliente.
- A extensão do cliente UC requer gerenciamento e atualizações independentes.
- As extensões de cliente UC podem não estar disponíveis em determinadas plataformas de clientes, como plataformas móveis ou de web.
- Algumas funcionalidades da aplicação de UC podem ser restritas neste modo; por exemplo, o comportamento de compartilhamento de tela pode ser diferente.
- O uso de extensões do lado do cliente pode não ser adequado para alguns cenários, como traga seu próprio dispositivo (BYOD) ou quiosques compartilhados.

Se o modo RTC otimizado para mídia for inadequado ao ambiente ou se determinados usuários não conseguirem instalar a extensão do cliente, é recomendável configurar o modo RTC otimizado em sessão como uma opção de fallback.

Configurar o RTC otimizado em sessão

No modo RTC otimizado em sessão, o aplicativo de UC opera WorkSpace sem nenhuma modificação, fornecendo uma experiência local semelhante. Os fluxos de áudio e vídeo gerados pelo aplicativo são capturados pelo WorkSpaces Streaming Protocol (WSP) e transmitidos para o lado do cliente. No cliente, os sinais do microfone (no WSP e no PCoIP WorkSpaces) e da webcam (somente no WSP WorkSpaces) são capturados, redirecionados de volta para o aplicativo de UC e transmitidos sem problemas para o WorkSpace aplicativo de UC.

Essa opção garante compatibilidade excepcional, mesmo com aplicações herdadas, oferecendo uma experiência de usuário coesa, independentemente da origem da aplicação. A otimização em sessão também funciona com o cliente de web.



WorkSpaces O Streaming Protocol (WSP) foi meticulosamente otimizado para aprimorar o desempenho do modo RTC remoto. As medidas de otimização incluem:

- Utilização de transporte QUIC adaptável baseado em UDP, garantindo transmissão eficiente de dados.
- Estabelecimento de caminho de áudio de baixa latência, facilitando entrada e saída rápida de áudio.
- Implementação de codecs de áudio otimizados para voz para manter a qualidade do áudio e reduzir a utilização da CPU e da rede.
- Redirecionamento da webcam, permitindo a integração das funcionalidades da webcam.
- Configuração da resolução da webcam para otimizar a performance.
- Integração de codecs de exibição adaptáveis para equilibrar velocidade e qualidade visual.
- Correção de instabilidade de áudio, garantindo transmissão de áudio suave.

Essas otimizações contribuem coletivamente para uma experiência robusta e fluida no modo RTC remoto.

Recomendações de dimensionamento

Para oferecer suporte efetivo ao modo RTC remoto, é crucial garantir o dimensionamento adequado da Amazon. WorkSpaces O controle remoto WorkSpace deve atender ou exceder os requisitos do sistema do respectivo aplicativo de Comunicação Unificada (UC). A tabela a seguir descreve as

WorkSpaces configurações mínimas suportadas e recomendadas para aplicativos de UC populares quando usados para chamadas de vídeo e áudio:

			Chamadas de vídeo		Chamadas de áudio		
Aplicativo	Requisitos de CPU para a aplicação de RTC	Requisitos de RAM para a aplicação de RTC	Suportado minimamente WorkSpace	Recomendado WorkSpace	Suportado minimamente WorkSpace	Recomendado WorkSpace	Referência
Microsoft Teams	2 núcleos necessários, 4 núcleos recomendados	4,0 GB de RAM	Alimentação (4 vCPUs, 16 GB de memória)	PowerPro (8 vCPU, 32 GB de memória)	Performance (2 vCPUs, 8 GB de memória)	Alimentação (4 vCPUs, 16 GB de memória)	Requisitos de hardware para o Microsoft Teams
Zoom	2 núcleos necessários, 4 núcleos recomendados	4,0 GB de RAM	Alimentação (4 vCPUs, 16 GB de memória)	PowerPro (8 vCPU, 32 GB de memória)	Performance (2 vCPUs, 8 GB de memória)	Alimentação (4 vCPUs, 16 GB de memória)	Requisitos do sistema do Zoom: Windows, macOS, Linux
Webex	São necessários os 2 núcleos	4,0 GB de RAM	Alimentação (4 vCPUs, 16 GB de memória)	PowerPro (8 vCPU, 32 GB de memória)	Performance (2 vCPUs, 8 GB de memória)	Alimentação (4 vCPUs, 16 GB de memória)	Requisitos do sistema para serviços Webex

É importante observar que a videoconferência envolve um uso significativo de recursos para codificação e decodificação de vídeo. Em cenários de máquinas físicas, essas tarefas são transferidas para a GPU. Em ambientes sem GPU WorkSpaces, essas tarefas são executadas na

CPU em paralelo com a codificação do protocolo remoto. Portanto, para usuários regularmente envolvidos em streaming de vídeo ou chamadas de vídeo, é altamente recomendável optar pela PowerPro configuração.

O compartilhamento de tela também consome recursos consideráveis, com o consumo de recursos aumentando com resoluções mais altas. Como resultado, em ambientes sem GPU WorkSpaces, o compartilhamento de tela geralmente é limitado a uma taxa de quadros mais baixa.

Aproveite o transporte QUIC baseado em UDP com o WorkSpaces Streaming Protocol (WSP)

O transporte UDP é, em particular, adequado para transmitir aplicações RTC. Para maximizar a eficiência, garanta que a rede esteja configurada para utilizar o transporte QUIC para WSP. Observe que o transporte baseado em UDP está disponível somente para clientes nativos.

Configurar o aplicativo UC para WorkSpaces

Para recursos aprimorados de processamento de vídeo, como desfoque de fundo, planos de fundo virtuais, reações ou hospedagem de eventos ao vivo, optar por uma GPU WorkSpace é essencial para obter um desempenho ideal.

A maioria dos aplicativos de UC fornece orientação para desativar o processamento avançado de vídeo a fim de reduzir a utilização da CPU em ambientes sem GPU. WorkSpaces

Para obter mais informações, consulte os seguintes recursos relacionados:

- Microsoft Teams: Teams for Virtualized Desktop Infrastructure
- Zoom Meetings: Managing the user experience for incompatible VDI plugins
- Webex: Deployment guide for Webex App for Virtual Desktop Infrastructure (VDI) - Manage and troubleshoot Webex App for VDI [Webex App]
- Google Meet: Usando a VDI

Habilitar o redirecionamento de webcam e áudio bidirecional

Por padrão, a Amazon suporta WorkSpaces inerentemente entrada de áudio, saída de áudio e redirecionamento de câmera por meio de entrada de vídeo. No entanto, se esses recursos tiverem sido desabilitados por algum motivo específico, siga as orientações fornecidas para reabilitar o redirecionamento. Para obter mais informações, consulte Ativar ou desativar o redirecionamento de entrada de vídeo para o WSP no Guia de Administração da Amazon. WorkSpaces O usuário precisa selecionar a câmera a ser usada na sessão após a conexão. Para obter mais informações,

os usuários devem consultar Webcams e outros dispositivos de vídeo no Guia WorkSpaces do usuário da Amazon.

Limitar a resolução máxima da webcam

Para usuários que usam Power ou PowerPro WorkSpaces para videoconferência, é altamente recomendável restringir a resolução máxima de webcams redirecionadas. No caso de PowerPro, a resolução máxima recomendada é de 640 pixels de largura por 480 pixels de altura. Para Power, a resolução máxima recomendada é de 320 pixels de largura por 240 pixels de altura.

Concluir as etapas a seguir para configurar a resolução máxima da webcam.

1. Abrir o Editor do Registro do Windows.
2. Navegar até o caminho de registro seguinte:

   ```
   HKEY_USERS/S-1-5-18/Software/GSettings/com/nicesoftware/dcv/webcam
   ```

3. Crie um valor de string chamado `max-resolution` e defina-o para a resolução desejada no formato `(X,Y)`, em que `X` representa a contagem horizontal de pixels (largura) e `Y` representa a contagem vertical de pixels (altura). Por exemplo, especificar `(640,480)`) a representação de uma resolução de 640 pixels de largura e 480 pixels de altura.

Ativar configuração de áudio otimizada por voz

Por padrão, WorkSpaces estão configurados para fornecer áudio 7.1 de alta fidelidade WorkSpaces para o cliente, garantindo uma qualidade superior de reprodução de música. No entanto, se seu caso de uso primário envolver audioconferência ou videoconferência, modificar o perfil do codec de áudio para uma configuração otimizada para voz pode economizar recursos da CPU e da rede.

Concluir as etapas a seguir para configurar o perfil de áudio para otimização de voz.

1. Abrir o Editor do Registro do Windows.
2. Navegar até o caminho de registro seguinte:

   ```
   HKEY_USERS/S-1-5-18/Software/GSettings/com/nicesoftware/dcv/audio
   ```

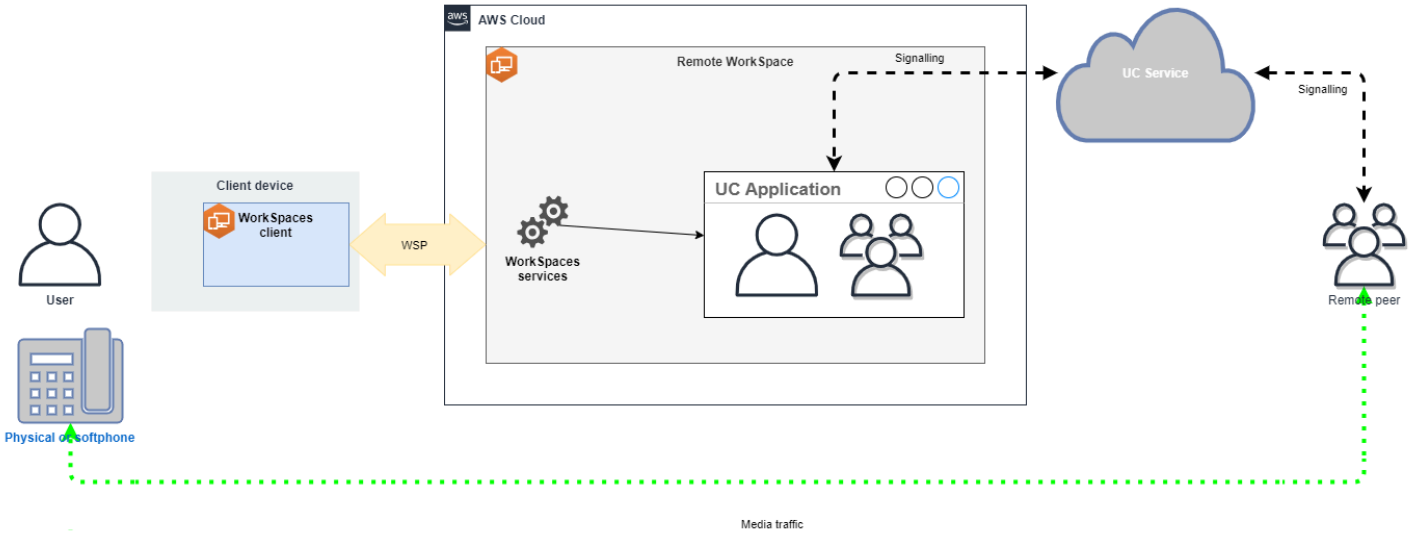
3. Criar um valor de string identificado `default-profile` e definir`voice`.

Usar fones de ouvido de boa qualidade para chamadas de áudio e vídeo

Para aprimorar a experiência de áudio e evitar ecos, é fundamental utilizar fones de ouvido de alta qualidade. A utilização de alto-falantes de mesa pode causar problemas de eco na parte remota da chamada.

Configurar o Direct RTC

A configuração do modo Direct RTC depende do aplicativo específico de Comunicação Unificada (UC) e não requer nenhuma alteração na configuração. WorkSpaces A lista a seguir oferece uma compilação não exaustiva de otimizações para várias aplicações de UC.



- Microsoft Teams:
  - Plan for SIP Gateway
  - Audio Conferencing in Microsoft 365
  - Plan your Teams voice solution
- Zoom Meetings:
  - Enabling or disabling toll call dial-in numbers
  - Using desk phone call control
  - Desk phone companion mode
- Webex:
  - Webex App | Make calls with your desk phone
  - Webex App | Supported calling options
- BlueJeans:

  - Dialing into a Meeting from a Desk Telephone
- Genesys:
  - Genesys Cloud WebRTC media helper
- Amazon Connect:
  - Otimização do Amazon Connect para Amazon WorkSpaces
- Google Meet:
  - Usar um smartphone para ouvir o áudio em uma videochamada

Gerenciar o modo de execução do WorkSpace

O modo de execução de um WorkSpace determina sua disponibilidade imediata e como você paga por ele (mensalmente ou por hora). Você pode escolher entre os seguintes modos de execução ao criar o WorkSpace:

- AlwaysOn: use quando estiver pagando uma taxa fixa mensal para uso ilimitado de WorkSpaces. Esse modo é melhor para usuários que usam o WorkSpace em tempo integral como a principal área de trabalho.
- AutoStop: use quando estiver pagando pelos WorkSpaces por hora. Com esse modo, os WorkSpaces param após um determinado período de desconexão, e o estado das aplicações e dos dados é salvo.

Para obter mais informações, consulte Preços do WorkSpaces.

WorkSpaces no modo AutoStop

Para definir o horário de parada automática, selecione o WorkSpace no console do Amazon WorkSpaces, selecione Ações e Modificar propriedades do modo de execução, depois defina Tempo de AutoStop (horas). Por padrão, a opção Tempo de AutoStop (horas) é definida como 1 hora, o que significa que o WorkSpace é interrompido automaticamente 1 hora após ser desconectado.

Depois que um WorkSpace é desconectado e o período da opção Tempo de AutoStop expira, pode levar mais alguns minutos para que o WorkSpace pare automaticamente. No entanto, a cobrança é interrompida assim que o período da opção Tempo de AutoStop expira, e esse tempo adicional não é cobrado.

Quando possível, o estado da área de trabalho é salvo no volume raiz do WorkSpace. O WorkSpace reinicia quando um usuário faz login e todos os documentos abertos e programas em execução retornam ao estado salvo.

Os WorkSpaces Graphics.g4dn, GraphicsPro.g4dn, Graphics e GraphicsPro no modo AutoStop não preservam o estado dos dados e dos programas quando eles param. Para esses WorkSpaces no modo Autostop, recomendamos salvar o trabalho sempre que terminar de usá-los.

Para WorkSpaces do tipo traga a sua própria licença (BYOL) no modo AutoStop, um grande número de logins simultâneos pode resultar em um aumento significativo no tempo de disponibilidade dos WorkSpaces. Se você espera que muitos usuários façam login nos WorkSpaces BYOL no modo AutoStop ao mesmo tempo, consulte seu gerente de contas para obter orientações.

> **Important**
>
> Os WorkSpaces no modo AutoStop só param automaticamente se os WorkSpaces forem desconectados.

Um WorkSpace é desconectado somente nas seguintes circunstâncias:

- Se o usuário se desconectar manualmente do WorkSpace ou sair da aplicação cliente do Amazon WorkSpaces.
- Se o dispositivo cliente for desligado.
- Se não houver conexão entre o dispositivo cliente e o WorkSpace por mais de 20 minutos.

Como prática recomendada, os usuários de WorkSpaces no modo AutoStop devem se desconectar manualmente dos WorkSpaces quando terminarem de usá-los todos os dias. Para se desconectar manualmente, selecione Desconectar WorkSpace ou Sair do Amazon WorkSpaces no menu do Amazon WorkSpaces nas aplicações cliente do WorkSpaces para Linux, macOS ou Windows. Para Android ou iPad, selecione Desconectar no menu da barra lateral.

Os WorkSpaces no modo AutoStop podem não parar automaticamente nas seguintes situações:

- Se o dispositivo cliente estiver apenas bloqueado, suspenso ou inativo (por exemplo, a tampa do laptop estiver fechada) em vez de desligado, a aplicação WorkSpaces ainda poderá estar em execução em segundo plano. Enquanto a aplicação WorkSpaces ainda estiver em execução, o WorkSpace pode não ser desconectado e, portanto, pode não parar automaticamente.

- O WorkSpaces pode detectar a desconexão somente quando os usuários estão usando clientes WorkSpaces. Se os usuários usam clientes de terceiros, é possível que o WorkSpaces não consiga detectar a desconexão e, portanto, não pare automaticamente e a cobrança não seja suspensa.

Modificar o modo de execução

Você pode alternar entre os modos de execução a qualquer momento.

Para modificar o modo de execução de um WorkSpace

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione WorkSpaces.
3. Selecione o WorkSpace para modificar e selecione Ações, Modificar modo de execução.
4. Selecione o novo modo de execução, AlwaysOn ou AutoStop, e clique em Salvar.

Como modificar o modo de execução de um WorkSpace usando a AWS CLI

Use o comando modify-workspace-properties.

Interromper e iniciar um WorkSpace no modo AutoStop

Quando os WorkSpaces no modo AutoStop são desconectados, eles são interrompidos automaticamente após um período especificado de desconexão, e a cobrança por hora é suspensa. Para otimizar ainda mais os custos, você pode suspender manualmente as cobranças por hora associadas a WorkSpaces no modo AutoStop. O WorkSpace é interrompido e todas as aplicações e dados são salvos para a próxima vez que um usuário fizer login no WorkSpace.

Quando um usuário se conectar novamente a um WorkSpace interrompido, ele será retomado no ponto em que parou, normalmente em menos de 90 segundos.

Você pode reinicializar (reiniciar) WorkSpaces no modo AutoStop que estão disponíveis ou em estado de erro.

Como interromper um WorkSpace de AutoStop

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione WorkSpaces.

3. Selecione o WorkSpace a ser interrompido e clique em Ações, Interromper WorkSpaces.
4. Quando a confirmação for solicitada, clique em Interromper WorkSpaces.

Como iniciar um WorkSpace de AutoStop

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione WorkSpaces.
3. Selecione os WorkSpaces a serem iniciados e clique em Ações, Iniciar WorkSpaces.
4. Quando a confirmação for solicitada, clique em Iniciar WorkSpaces.

Para remover os custos de infraestrutura fixos associados a WorkSpaces AutoStop, remova o WorkSpace da sua conta. Para obter mais informações, consulte Excluir um WorkSpace.

Como interromper e iniciar um WorkSpace no modo AutoStop usando a AWS CLI

Use os comandos stop-WorkSpaces e start-WorkSpaces.

Gerenciar aplicações

Depois de iniciar um WorkSpace, você pode ver a lista de todos os pacotes de aplicativos associados ao seu WorkSpace no WorkSpaces console.

Para ver a lista de todos os pacotes de aplicativos associados ao seu WorkSpace

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação esquerdo, escolha WorkSpaces.
3. Selecione WorkSpace e escolha Exibir detalhes.
4. Em Aplicativos, encontre a lista de aplicativos associados a isso WorkSpace, junto com o status de instalação.

Você pode atualizar os pacotes de aplicativos do seu WorkSpace das seguintes maneiras:

- Instale pacotes de aplicativos em seu WorkSpace
- Desinstale pacotes de aplicativos do seu WorkSpace
- Instale pacotes de aplicativos e desinstale um conjunto diferente de pacotes de aplicativos em seu WorkSpace

> **Note**
>
> - Para atualizar pacotes de aplicativos, eles WorkSpace devem ter um status de `AVAILABLE` ou`STOPPED`.
> - O gerenciamento de aplicativos está disponível somente para Windows WorkSpaces.
> - O gerenciamento de aplicações está disponível somente para pacotes de aplicações assinados por meio da AWS.

Pacotes compatíveis com “Gerenciar aplicações”

Gerenciar aplicativos permite que você instale e desinstale os seguintes aplicativos no seu WorkSpaces. Para o pacote do Microsoft Office 2016 e o Microsoft Office 2019, você pode somente desinstalar.

- Microsoft Office LTSC Professional Plus 2021
- Microsoft Visio LTSC Professional 2021
- Microsoft Project Professional 2021
- Microsoft Office LTSC Standard 2021
- Microsoft Visio LTSC Standard 2021
- Microsoft Project Standard 2021

A seguinte tabela mostra a lista de combinações de aplicações e sistemas operacionais compatíveis e não compatíveis:

	Microsoft Office Professional Plus 2016 (32 bits)	Microsoft Office Professional Plus 2019 (64 bits)	Microsoft LTSC Office Professional Plus/ Standard 2021 (64 bits)	Microsoft Project Professional/Standard 2021 (64 bits)	Microsoft LTSC Visio Professional/Standard 2021 (64 bits)
Windows Server 2016	Desinstalar	Sem compatibilidade	Sem compatibilidade	Sem compatibilidade	Sem compatibilidade
Windows Server 2019	Sem compatibilidade	Desinstalar	Instalar/ desinstalar	Instalar/ desinstalar	Instalar/desinstalar
Windows Server 2022	Sem compatibilidade	Desinstalar	Instalar/ desinstalar	Instalar/ desinstalar	Instalar/desinstalar
Windows 10	Desinstalar	Desinstalar	Instalar/ desinstalar	Instalar/ desinstalar	Instalar/desinstalar
Windows 11	Desinstalar	Desinstalar	Instalar/ desinstalar	Instalar/ desinstalar	Instalar/desinstalar

Important

- Essas aplicações devem seguir as mesmas edições. Por exemplo, você não pode misturar aplicações Standard com aplicações Professional.
- Essas aplicações devem seguir as mesmas versões. Por exemplo, você não pode misturar aplicações de 2019 com aplicações de 2021.
- O Microsoft Office/Visio/Project 2021 Standard/Professional não tem suporte para Value, Graphics e bundles. GraphicsPro WorkSpaces

- Ao desinstalar o pacote de aplicativos Plus para Microsoft Office 2016 do seu WorkSpaces, você perderá o acesso a todas as soluções da Trend Micro que foram incluídas como parte desse WorkSpaces pacote da Amazon. Se você quiser continuar usando as soluções da Trend Micro com sua Amazon WorkSpaces, você pode comprá-las separadamente no AWS mercado.
- Para instalar/desinstalar aplicações do Microsoft 365, é preciso trazer as próprias ferramentas e instaladores. O fluxo de trabalho Gerenciar aplicações não pode instalar/desinstalar aplicações do Microsoft 365.
- Você não pode criar uma imagem personalizada WorkSpaces com aplicativos instalados por meio de Gerenciar aplicativos, mas pode criar uma imagem personalizada WorkSpaces da qual você desinstala pacotes de aplicativos usando Gerenciar aplicativos.
- A resolução de DNS deve estar habilitada para usar a opção “Gerenciar aplicações”.
- Para regiões opcionais, como a África (Cidade do Cabo), a conexão com a WorkSpaces Internet deve estar habilitada no nível do diretório.

Para atualizar pacotes de aplicativos em um WorkSpace

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, escolha WorkSpaces.
3. Selecione WorkSpace e escolha Ações, Gerenciar aplicativos.
4. Em Aplicativos atuais, você verá uma lista de pacotes de aplicativos que já estão instalados nele WorkSpace e, em Escolher aplicativos, você tem uma lista de pacotes de aplicativos que estão disponíveis para instalação nele. WorkSpace
5. Para instalar pacotes de aplicativos nisso WorkSpace:
   a. Selecione um pacote de aplicativos que você deseja instalar nele e escolha Associar. WorkSpace
   b. Repita a etapa anterior para instalar outros pacotes de aplicações.
   c. Enquanto os pacotes de aplicações estiverem sendo instalados, você os verá em Aplicações atuais com o status `Pending install deployment`.
6. Para desinstalar pacotes de aplicativos a partir disso WorkSpace:

a. Em Escolher aplicações, selecione o pacote de aplicações que deseja desinstalar e clique em Desassociar.

b. Repita a etapa anterior para desinstalar outros pacotes de aplicações.

c. Enquanto os pacotes de aplicações estiverem sendo desinstalados, você os verá em Aplicações atuais com o status `Pending uninstall deployment`.

7. Para reverter a instalação ou o estado de instalação dos pacotes, aplique uma das ações a seguir.

   - Se você quiser reverter os pacotes do estado `Pending uninstall deployment`, selecione a aplicação que deseja reverter e clique em Associar.
   - Se você quiser reverter os pacotes do estado `Pending install deployment`, selecione a aplicação que deseja reverter e clique em Desassociar.

8. Depois que os pacotes de aplicações que você escolheu instalar ou desinstalar estiverem em estados pendentes, escolha Implantar aplicações.

   > **Important**
   >
   > Depois de selecionar Implantar aplicativos, a sessão do usuário final será encerrada e não WorkSpaces estará acessível enquanto os aplicativos estiverem sendo instalados ou desinstalados.

9. Para confirmar suas ações, digite confirmar. Selecione forçar para instalar ou desinstalar pacotes de aplicações em um estado de Erro.

10. Para monitorar o andamento dos pacotes de aplicações:

    a. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.

    b. No painel de navegação, escolha WorkSpaces. Você pode ver o status em Status, incluindo as informações a seguir.

       - ATUALIZANDO: a atualização do pacote de aplicações ainda está em andamento.
       - DISPONÍVEL/PARADO - A atualização do pacote de aplicativos foi concluída e WorkSpace está de volta ao seu estado original.

    c. Para monitorar o status de instalação ou desinstalação de seus pacotes de aplicativos, selecione WorkSpace e escolha Exibir detalhes. Em Aplicações, você pode ver o status em Status, incluindo `Pending install`, `Pending uninstall` e `Installed`.

> **Note**
>
> Se seus usuários observarem que seus pacotes de aplicativos recém-instalados por meio de Aplicativos Gerenciados não estão ativados por licença, você poderá realizar uma WorkSpace reinicialização manual. Os usuários podem começar a usar essas aplicações após a reinicialização. Para obter suporte adicional, entre em contato com o AWS Support.

Gerenciando WorkSpaces modificações usando Gerenciar aplicativos

Depois de instalar ou desinstalar pacotes de aplicativos em seu WorkSpaces, as ações a seguir podem afetar as configurações existentes.

- Restaurar um WorkSpace - A restauração de um WorkSpace recria o volume raiz e o volume do usuário, com base nos instantâneos mais recentes desses volumes que foram criados quando o WorkSpace estava íntegro. Os WorkSpace instantâneos completos são tirados a cada 12 horas. Para obter mais informações, consulte Restaurar um WorkSpace. Certifique-se de esperar pelo menos 12 horas antes de restaurar os WorkSpaces que foram modificados usando Gerenciar aplicativos. Restaurar seu instantâneo completo WorkSpaces anterior, que foi modificado usando Gerenciar aplicativos, resultará no seguinte:
  - Os pacotes de aplicativos que foram instalados em você WorkSpaces usando o fluxo de trabalho Gerenciar aplicativos serão removidos do seu WorkSpaces , mas a licença ainda será ativada e você WorkSpaces será cobrado por esses aplicativos. Para recuperar esses pacotes de aplicativos, WorkSpaces você precisa executar o fluxo de trabalho Gerenciar aplicativos novamente, desinstalar o aplicativo para começar do zero e depois instalar novamente.
  - Os pacotes de aplicativos que foram removidos de você WorkSpaces usando o fluxo de trabalho Gerenciar aplicativos voltarão ao seu WorkSpaces. No entanto, esses pacotes de aplicações não funcionarão corretamente porque a ativação da licença estará ausente. Para se livrar desses pacotes de aplicativos, execute uma desinstalação manual desses pacotes de aplicativos do seu. WorkSpaces
- Reconstruir um WorkSpace - Reconstruir um WorkSpace recria o volume raiz. Para obter mais informações, consulte Reconstruir um WorkSpace. A reconstrução dos WorkSpaces que foram modificados usando Gerenciar aplicativos resultará no seguinte:

  - Os pacotes de aplicativos que foram instalados em você WorkSpaces usando o fluxo de trabalho Gerenciar aplicativos serão removidos e desativados do seu. WorkSpaces Para recuperar esses aplicativos, WorkSpaces você precisa executar o fluxo de trabalho Gerenciar aplicativos novamente.
  - Os pacotes de aplicativos que foram removidos do seu fluxo de trabalho WorkSpaces por meio do gerenciamento de aplicativos serão instalados e ativados no seu WorkSpaces. Para remover esses pacotes de aplicativos do seu WorkSpaces, você precisa executar o fluxo de trabalho Gerenciar aplicativos novamente.
- Migrar um WorkSpace - O processo de migração recria o WorkSpace usando um novo volume raiz da imagem do pacote de destino e o volume do usuário do último instantâneo disponível do original. WorkSpace Um novo WorkSpace com um novo WorkSpace ID é criado. Para obter mais informações, consulte Migrar um WorkSpace Migrar seus WorkSpaces que foram modificados usando Gerenciar aplicativos resultará no seguinte:
  - Todo o pacote de aplicativos da fonte WorkSpaces será removido e desativado. O novo destino WorkSpaces herdará os aplicativos do WorkSpaces pacote de destino. Os pacotes de WorkSpaces aplicativos de origem serão cobrados pelo mês inteiro, mas os pacotes de aplicativos no pacote de destino terão uma fatura proporcional.

Modificar um WorkSpace

Depois de iniciar um WorkSpace, você pode modificar sua configuração de três maneiras:

- Você pode alterar o tamanho de seu volume raiz (para Windows, unidade C; para Linux, /) e seu volume de usuário (para Windows, unidade D; para Linux /home).
- Você pode alterar seu tipo de computação para selecionar um novo pacote.
- Você pode modificar o protocolo de streaming usando a AWS CLI ou a WorkSpaces API da Amazon se você tiver WorkSpace sido criado com pacotes PCoIP.

Para ver o estado de modificação atual de um WorkSpace, selecione a seta para mostrar mais detalhes sobre isso WorkSpace. Os possíveis valores para State (Estado) são Modifying Compute (Modificar computação), Modifying Storage (Modificar armazenamento) e None (Nenhum).

Se você quiser modificar um WorkSpace, ele deve ter um status de `AVAILABLE` ou`STOPPED`. Você não pode alterar o tamanho do volume e o tipo de computação ao mesmo tempo.

Alterar o tamanho do volume ou o tipo de computação de a WorkSpace alterará a taxa de cobrança do. WorkSpace

Para permitir que os usuários modifiquem os volumes e os tipos de computação, consulte Habilite recursos de WorkSpace gerenciamento de autoatendimento para seus usuários.

Modificar tamanhos de volumes

Você pode aumentar o tamanho dos volumes raiz e do usuário em até 2.000 GB cada. WorkSpace WorkSpace os volumes raiz e de usuário vêm em grupos definidos que não podem ser alterados. Os grupos disponíveis são:

[Raiz (GB), Usuário (GB)]
[80, 10]
[80, 50]
[80, 100]
[175 a 2000, 100 a 2000]

É possível expandir os volumes raiz e do usuário, sejam eles criptografados ou não, e é possível expandir ambos os volumes uma vez em um período de 6 horas. No entanto, não é possível aumentar o tamanho dos volumes raiz e do usuário ao mesmo tempo. Para obter mais informações, consulte Limitações para aumentar volumes.

> **Note**
>
> Quando você expande um volume para um WorkSpace, estende WorkSpaces automaticamente a partição do volume no Windows ou no Linux. Quando o processo estiver concluído, você deverá reinicializar o WorkSpace para que as alterações entrem em vigor.

Para garantir que seus dados sejam preservados, você não pode diminuir o tamanho dos volumes raiz ou do usuário depois de iniciar um WorkSpace. Em vez disso, certifique-se de especificar os tamanhos mínimos para esses volumes ao lançar um WorkSpace. Você pode iniciar um Value, Standard, Performance, Power ou PowerPro WorkSpace com um mínimo de 80 GB para o volume

raiz e 10 GB para o volume do usuário. Você pode iniciar um Graphics.G4dn, GraphicsPro .g4dn, Graphics ou GraphicsPro WorkSpace com um mínimo de 100 GB para o volume raiz e 100 GB para o volume do usuário.

Enquanto um aumento WorkSpace no tamanho do disco está em andamento, os usuários podem realizar a maioria das tarefas em seus WorkSpace. No entanto, eles não podem alterar o tipo de WorkSpace computação, alternar o modo de WorkSpace execução, reconstruí-los ou reinicializá-los WorkSpace (reiniciá-los). WorkSpace

> **Note**
>
> Se você quiser que seus usuários possam usá-los WorkSpaces enquanto o aumento do tamanho do disco estiver em andamento, certifique-se de que eles WorkSpaces tenham um status de `AVAILABLE` em vez de `STOPPED` antes de redimensionar os volumes do WorkSpaces. Se WorkSpaces estiverem`STOPPED`, eles não poderão ser iniciados enquanto o aumento do tamanho do disco estiver em andamento.

Na maioria dos casos, o processo de aumento do tamanho em disco pode levar até 2 horas. No entanto, se você estiver modificando os tamanhos dos volumes para um grande número de WorkSpaces, o processo pode levar muito mais tempo. Se você tiver um grande número de WorkSpaces modificações, recomendamos entrar em contato AWS Support para obter ajuda.

Limitações para o aumento de volumes

- É possível redimensionar somente volumes SSD.
- Ao iniciar um WorkSpace, você deve esperar 6 horas antes de poder modificar os tamanhos de seus volumes.
- Não é possível aumentar o tamanho dos volumes raiz e do usuário ao mesmo tempo. Para aumentar o volume raiz, é necessário primeiro alterar o volume do usuário para 100 GB. Depois que essa alteração for feita, será possível atualizar o volume raiz para qualquer valor entre 175 e 2.000 GB. Depois que o volume raiz foi alterado para qualquer valor entre 175 e 2.000 GB, é possível atualizar o volume do usuário ainda mais, para qualquer valor entre 100 e 2.000 GB.

  > **Note**
  >
  > Se você quiser aumentar os dois volumes, é necessário esperar 20 a 30 minutos para que a primeira operação seja concluída antes de iniciar a segunda operação.

- A WorkSpace menos que seja Graphics.G4dn, GraphicsPro .g4dn, Graphics ou GraphicsPro WorkSpace, o volume raiz não pode ser inferior a 175 GB quando o volume do usuário é 100 GB. Graphics.g4dn, GraphicsPro .g4dn, Graphics e GraphicsPro WorkSpaces pode ter os volumes raiz e de usuário definidos para no mínimo 100 GB.
- Se o volume do usuário for 50 GB, não será possível atualizar o volume raiz para qualquer valor que não seja 80 GB. Se o volume raiz for 80 GB, o volume do usuário só poderá ser 10, 50 ou 100 GB.

Para modificar o volume raiz de um WorkSpace

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione WorkSpaces.
3. Selecione WorkSpace e escolha Ações, Modificar volume raiz. .
4. Em Tamanhos de volume raiz, escolha um tamanho de volume ou selecione Personalizado para inserir um tamanho de volume personalizado.
5. Escolha Salvar alterações.
6. Quando o aumento do tamanho do disco for concluído, você deverá reinicializar o WorkSpace para que as alterações entrem em vigor. Para evitar perda de dados, certifique-se de que o usuário salve todos os arquivos abertos antes de reinicializar o. WorkSpace

Para modificar o volume do usuário de um WorkSpace

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione WorkSpaces.
3. Selecione WorkSpace e escolha Ações, Modificar volume do usuário. .
4. Em Tamanhos de volume do usuário, escolha um tamanho de volume ou selecione Personalizado para inserir um tamanho de volume personalizado.
5. Escolha Salvar alterações.
6. Quando o aumento do tamanho do disco for concluído, você deverá reinicializar o WorkSpace para que as alterações entrem em vigor. Para evitar perda de dados, certifique-se de que o usuário salve todos os arquivos abertos antes de reinicializar o. WorkSpace

Para alterar os tamanhos de volume de um WorkSpace

Use o modify-workspace-propertiescomando com a `UserVolumeSizeGib` propriedade `RootVolumeSizeGib` or.

Modificar tipo de computação

Você pode alternar WorkSpace entre os tipos Padrão, Potência, Desempenho PowerPro e Computação. Para obter mais informações sobre esses tipos de computação, consulte Amazon WorkSpaces Bundles.

> **Note**
>
> - Você pode alterar o tipo de computação de Graphics.G4dn para .g4dn ou de .g4dn para GraphicsPro Graphics.G4dn. GraphicsPro Você não pode alterar o tipo de computação de Graphics.g4dn e GraphicsPro .g4dn para nenhum outro valor.
> - O pacote Graphics deixará de receber suporte a partir de 30 de novembro de 2023. Recomendamos migrar seu pacote para o WorkSpaces Graphics.g4dn. Para ter mais informações, consulte Migre um WorkSpace.
> - Você não pode alterar o tipo de computação de Graphics e GraphicsPro qualquer outro valor.

Quando você solicita uma alteração computacional, WorkSpaces reinicia o WorkSpace usando o novo tipo de computação. WorkSpaces preserva o sistema operacional, os aplicativos, os dados e as configurações de armazenamento do WorkSpace.

É possível solicitar um tipo de computação maior uma vez em um período de 6 horas ou um tipo de computação menor uma vez a cada 30 dias. Para um recém-lançado WorkSpace, você deve esperar 6 horas antes de solicitar um tipo de computação maior.

Quando uma alteração do tipo de WorkSpace computação está em andamento, os usuários são desconectados deles WorkSpace e não podem usar ou alterar o. WorkSpace O WorkSpace é reinicializado automaticamente durante o processo de alteração do tipo de computação.

> **Important**
>
> Para evitar a perda de dados, certifique-se de que os usuários salvem todos os documentos abertos e outros arquivos do aplicativo antes de alterar o tipo de WorkSpace computação.

O processo de alteração do tipo de computação pode levar até uma hora.

Para alterar o tipo de computação de um WorkSpace

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione WorkSpaces.
3. Selecione WorkSpace e escolha Ações, Modificar tipo de computação.
4. Em Tipo de computação, escolha um tipo de computação.
5. Escolha Salvar alterações.

Para alterar o tipo de computação de um WorkSpace

Use o modify-workspace-propertiescomando com a `ComputeTypeName` propriedade.

Modificar protocolos

Se você WorkSpace foi criado com pacotes PCoIP, você pode modificar o protocolo de streaming usando a AWS CLI ou a API da Amazon. WorkSpaces Isso permite que você migre o protocolo usando o existente WorkSpace sem usar o recurso de WorkSpace migração. Isso também permite que você use o WorkSpaces Streaming Protocol (WSP) e mantenha seu volume raiz sem recriar o PCoIP existente WorkSpaces durante o processo de migração.

- Você só pode modificar seu protocolo se WorkSpace ele foi criado com pacotes PCoIP.
- Antes de modificar o protocolo para WSP, certifique-se de que WorkSpace ele atenda aos seguintes requisitos para um WorkSpace WSP.
  - Seu WorkSpaces cliente oferece suporte ao WSP
  - A região em que o seu WorkSpace está implantado oferece suporte ao WSP
  - Os requisitos de endereço IP e porta para o WSP estão abertos. Para obter mais informações, consulte Requisitos de endereço IP e porta para WorkSpaces.
  - Garanta que seu pacote atual esteja disponível com o WSP.
  - Para obter a melhor experiência com videoconferência, recomendamos usar somente Power ou PowerPro pacotes.

> **Note**
>
> - É altamente recomendável testar com sua empresa não produtiva WorkSpaces antes de começar a alterar o protocolo.
> - Se você modificar o protocolo de PCoIP para WSP e depois modificar o protocolo de volta para PCoIP, não conseguirá se conectar por meio do Web Access. WorkSpaces

Para alterar o protocolo de um WorkSpace

1. [Opcional] WorkSpace Reinicie o seu e espere até que ele esteja no `AVAILABLE` estado antes de modificar o protocolo.
2. [Opcional] Use o `describe-workspaces` comando para listar as WorkSpace propriedades. Verifique se ele está no estado `AVAILABLE` e se o `Protocol` atual está correto.
3. Use o comando `modify-workspace-properties` e modifique a propriedade `Protocols` de `PCOIP` para `WSP` ou vice-versa.

```
aws workspaces modify-workspace-properties
--workspace-id <value>
--workspace-properties "Protocols=[WSP]"
```

> **Important**
>
> A propriedade `Protocols` diferencia maiúsculas de minúsculas. Use `PCOIP` ou`WSP`.

4. Depois de executar o comando, pode levar até 20 minutos para reinicializar e concluir as configurações necessárias. WorkSpace
5. Use o `describe-workspaces` comando novamente para listar as WorkSpace propriedades e verificar se elas estão em um `AVAILABLE` estado e se a `Protocols` propriedade atual foi alterada para o protocolo correto.

> **Note**
>
> - A modificação WorkSpace do protocolo não atualizará a descrição do pacote no console. A descrição do Pacote de inicialização não mudará.

- Se o WorkSpace permanecer em um `UNHEALTHY` estado após 20 minutos, reinicie o WorkSpace no console.

6. Agora você pode se conectar ao seu WorkSpace.

Personalize a WorkSpace marca

A Amazon WorkSpaces permite que você crie uma WorkSpaces experiência familiar para seus usuários usando APIs para personalizar a aparência da sua página de login com seu WorkSpace próprio logotipo de marca, informações de suporte de TI, link de esquecimento da senha e mensagem de login. Sua marca será exibida para seus usuários na página de WorkSpace login, em vez da WorkSpaces marca padrão.

Os seguintes clientes são aceitos:

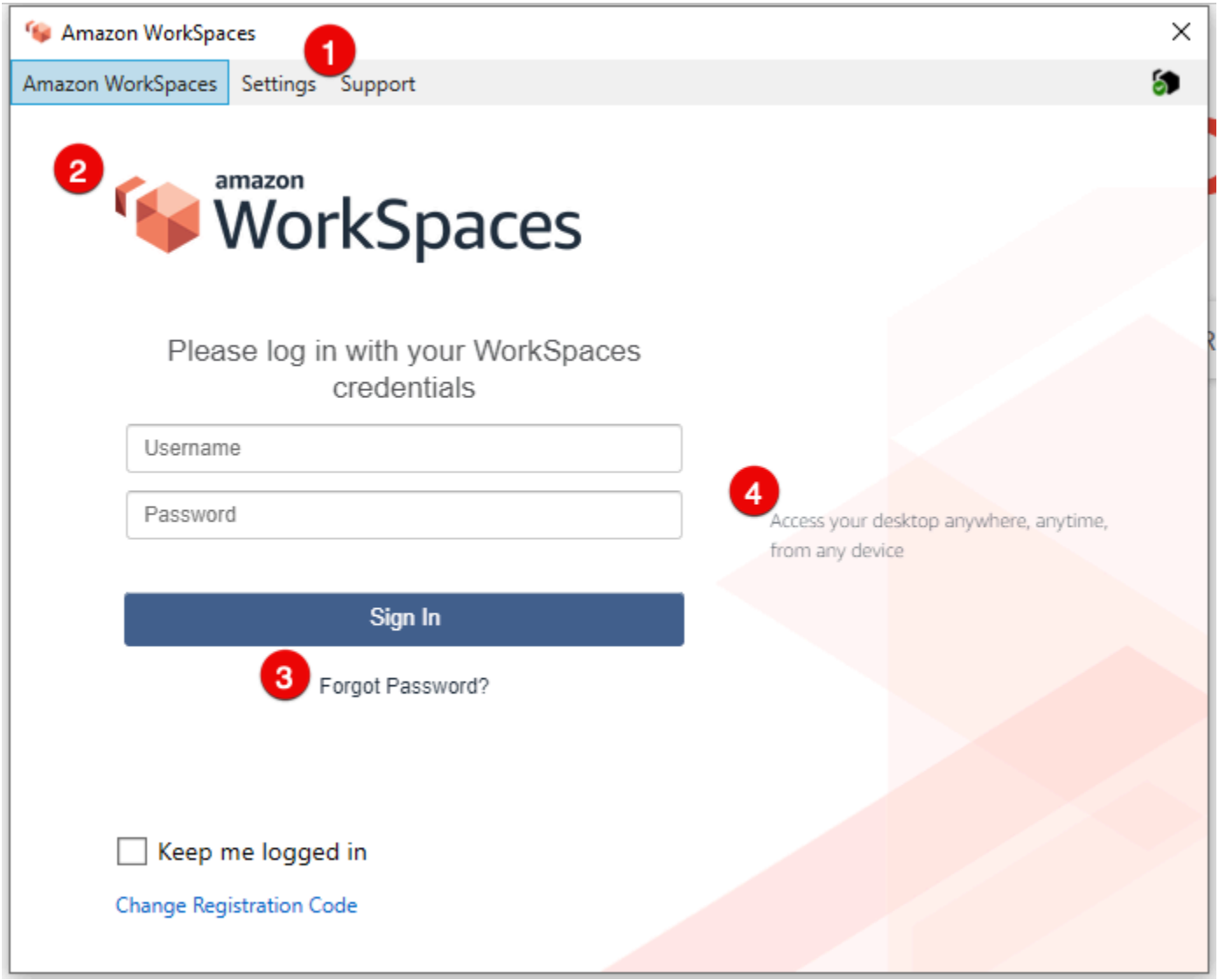
- Windows
- Linux
- Android
- MacOS
- iOS
- Web Access

> **Note**
>
> Para modificar elementos de marca usando as ClientBranding APIs noAWS GovCloud (US) Region, use uma versão de WorkSpaces cliente que seja 5.10.0.

Importar marca personalizada

Para importar a personalização de marca do cliente, use a ação `ImportClientBranding`, que inclui os elementos a seguir. Consulte a referência ImportClientBranding da API para obter mais informações.

> **Important**
>
> Os atributos da marca do cliente são voltados para o público. Não inclua informações confidenciais.



1. Link de suporte
2. Logo
3. Link de esquecimento de senha
4. Mensagem de login

Elementos de marca personalizados

Elemento da marca	Descrição	Requisitos e recomendações
Link de suporte	Permite que você especifique um link de e-mail de suporte para os usuários entrarem em contato para obter ajuda WorkSpaces. Você pode usar o atributo `SupportEmail` ou fornecer um link para a página de suporte usando o atributo `SupportLink` .	• Para cada tipo de plataforma, os parâmetros `SupportEmail` e `SupportLink` são mutuamente exclusivos. Você pode especificar um único parâmetro para cada tipo de plataforma, mas não para ambos. • O e-mail padrão é `workspaces-feedback@amazon.com` . • Restrições de tamanho: tamanho mínimo 1. Comprimento máximo de 200.

Logo	Permite que você personalize o logotipo da organização usando o atributo `Logo`.	• O único formato de imagem aceito é um objeto de dados binários que é convertido de um arquivo `.png`.
		• Resoluções recomendadas:
		  • Android: 978 x 190
		  • Área de trabalho: 319 x 55
		  • iOS@2x: 110 x 200
		  • iOS@3x: 1650 x 300

Link de esquecimento de senha	Permite adicionar um endereço da web usando o ForgotPasswordLink atributo que os usuários podem	Restrições de comprimento: comprimento mínimo 1. Comprimento máximo de 200.

Elemento da marca	Descrição	Requisitos e recomendações
	acessar se esquecerem a senha WorkSpace.	
Mensagem de login	Permite que você personalize uma mensagem usando o atributo `LoginMessage` na tela de login.	• Restrições de tamanho: tamanho mínimo 0. Tamanho máximo de 2.000 caracteres para integração com etiquetas HTML e tamanhos de fonte diferentes. Para casos padrão sem etiquetas HTML, é recomendável manter a mensagem de login com menos de 600 caracteres. • Etiquetas HTML compatíveis: `a, b, blockquote, br, cite, code, dd, dl, dt, div, em, i, li, ol, p, pre, q, small, span, strike, strong, sub, sup, u, ul`

Veja a seguir exemplos de trechos de código para uso. ImportClientBranding

CLI da AWS versão 2

> **Warning**
>
> A importação de marcas personalizadas substitui os atributos, dentro da plataforma, que você especifica com seus dados personalizados. Ela também substitui os atributos que você

não especifica pelos valores padrão de atributos de marca personalizados. Você deve incluir os dados de qualquer atributo que não deseja substituir.

```
aws workspaces import-client-branding \
--cli-input-json file://~/Downloads/import-input.json \
--region us-west-2
```

O arquivo JSON de importação deve ter uma aparência semelhante à seguinte amostra de código:

```
{
    "ResourceId": "<directory-id>",
    "DeviceTypeOsx": {
        "Logo":
 "iVBORw0KGgoAAAANSUhEUgAAAAIAAAACCAYAAABytg0kAAAAC0lEQVR42mNgQAcAABIAAeRVjecAAAAASUVORK5CYII="
        "ForgotPasswordLink": "https://amazon.com/",
        "SupportLink": "https://amazon.com/",
        "LoginMessage": {
            "en_US": "Hello!!"
        }
    }
}
```

O exemplo de trecho de código Java a seguir converte a imagem do logotipo em uma string codificada em base64:

```
// Read image as BufferImage
BufferedImage bi = ImageIO.read(new File("~/Downloads/logo.png"));

// convert BufferedImage to byte[]
ByteArrayOutputStream baos = new ByteArrayOutputStream();
ImageIO.write(bi, "png", baos);
byte[] bytes = baos.toByteArray();

//convert byte[] to base64 format and print it
String bytesBase64 = Base64.encodeBase64String(bytes);
System.out.println(bytesBase64);
```

O exemplo de trecho de código Python a seguir converte a imagem do logotipo em uma string codificada em base64:

```
# Read logo into base64-encoded string
with open("~/Downloads/logo.png", "rb") as image_file:
    f = image_file.read()
    base64_string = base64.b64encode(f)
    print(base64_string)
```

Java

> **Warning**
>
> A importação de marcas personalizadas substitui os atributos, dentro da plataforma, que você especifica com seus dados personalizados. Ela também substitui os atributos que você não especifica pelos valores padrão de atributos de marca personalizados. Você deve incluir os dados de qualquer atributo que não deseja substituir.

```
// Create WS Client
WorkSpacesClient client = WorkSpacesClient.builder().build();

// Read image as BufferImage
BufferedImage bi = ImageIO.read(new File("~/Downloads/logo.png"));

// convert BufferedImage to byte[]
ByteArrayOutputStream baos = new ByteArrayOutputStream();
ImageIO.write(bi, "png", baos);
byte[] bytes = baos.toByteArray();

// Create import attributes for the plateform
DefaultImportClientBrandingAttributes attributes =
        DefaultImportClientBrandingAttributes.builder()
                .logo(SdkBytes.fromByteArray(bytes))
                .forgotPasswordLink("https://aws.amazon.com/")
                .supportLink("https://aws.amazon.com/")
                .build();

// Create import request
ImportClientBrandingRequest request =
        ImportClientBrandingRequest.builder()
                .resourceId("<directory-id>")
                .deviceTypeOsx(attributes)
                .build();
```

```
// Call ImportClientBranding API
ImportClientBrandingResponse response = client.importClientBranding(request);
```

Python

> **Warning**
>
> A importação de marcas personalizadas substitui os atributos, dentro da plataforma, que você especifica com seus dados personalizados. Ela também substitui os atributos que você não especifica pelos valores padrão de atributos de marca personalizados. Você deve incluir os dados de qualquer atributo que não deseja substituir.

```
import boto3

# Read logo into bytearray
with open("~/Downloads/logo.png", "rb") as image_file:
    f = image_file.read()
    bytes = bytearray(f)

# Create WorkSpaces client
client = boto3.client('workspaces')

# Call import API
response = client.import_client_branding(
    ResourceId='<directory-id>',
    DeviceTypeOsx={
        'Logo': bytes,
        'SupportLink': 'https://aws.amazon.com/',
        'ForgotPasswordLink': 'https://aws.amazon.com/',
        'LoginMessage': {
            'en_US': 'Hello!!'
        }
    }
)
```

PowerShell

```
#Requires -Modules @{ ModuleName="AWS.Tools.WorkSpaces"; ModuleVersion="4.1.56"}
```

```
# Specify Image Path
$imagePath = "~/Downloads/logo.png"

# Create Byte Array from image file
$imageByte = ([System.IO.File]::ReadAllBytes($imagePath))

# Call import API
Import-WKSClientBranding -ResourceId <directory-id> `
    -DeviceTypeLinux_LoginMessage @{en_US="Hello!!"} `
    -DeviceTypeLinux_Logo $imageByte `
    -DeviceTypeLinux_ForgotPasswordLink "https://aws.amazon.com/" `
    -DeviceTypeLinux_SupportLink "https://aws.amazon.com/"
```

Para visualizar a página de login, inicie o WorkSpaces aplicativo ou a página de login na web.

> **Note**
>
> As alterações podem levar até um minuto para serem exibidas.

Descreva a marca personalizada

Para ver os detalhes da personalização da marca do cliente que você tem atualmente, use a ação `DescribeCustomBranding`. Veja a seguir um exemplo de script para uso DescribeClientBranding. Consulte a referência DescribeClientBranding da API para obter mais informações.

```
aws workspaces describe-client-branding \
--resource-id <directory-id> \
--region us-west-2
```

Excluir marca personalizada

Para excluir a personalização da marca do cliente, use a ação `DeleteCustomBranding`. Veja a seguir um exemplo de script para uso DeleteClientBranding. Consulte a referência DeleteClientBranding da API para obter mais informações.

```
aws workspaces delete-client-branding \
--resource-id <directory-id> \
--platforms DeviceTypeAndroid DeviceTypeIos \
--region us-west-2
```

> **Note**
>
> As alterações podem levar até um minuto para serem exibidas.

Marcar recursos do WorkSpaces

Você pode organizar e gerenciar os recursos do WorkSpaces atribuindo seus próprios metadados a cada recurso na forma de tags. Você especifica uma chave e um valor para cada tag. Uma chave pode ser uma categoria geral, como "projeto", "proprietário" ou "ambiente", com valores específicos associados. O uso de tags é uma forma simples, mas eficiente, de gerenciar os recursos da AWS e organizar os dados, incluindo dados de faturamento.

Quando você adicionar tags a um recurso existente, essas tags não serão exibidas no relatório de alocação de custos até o primeiro dia do mês seguinte. Por exemplo, se você adicionar tags a um WorkSpace existente em 15 de julho, elas serão exibidas no relatório de alocação de custos em 1º de agosto. Para obter mais informações, consulte Usar tags de alocação de custos no Guia do usuário do AWS Billing.

> **Note**
>
> Para visualizar etiquetas de recursos do WorkSpaces no Explorador de Custos, você precisa ativar as etiquetas que foram aplicadas aos recursos do WorkSpaces seguindo as instruções em Ativar tags de alocação de custos definidas pelo usuário no Guia do usuário do AWS Billing.
>
> Embora as tags apareçam 24 horas após a ativação, pode levar de quatro a cinco dias para que os valores associados a essas tags apareçam no Cost Explorer. Além disso, para que apareçam e forneçam dados de custo no Explorador de Custos, os recursos do WorkSpaces que foram marcados com etiquetas devem incorrer em cobranças durante esse período. O Cost Explorer mostra apenas os dados de custo do momento em que as tags foram ativadas em diante. Não há dados de histórico disponíveis no momento.

Recursos que você pode marcar com tags

- Você pode adicionar etiquetas aos seguintes recursos ao criá-los: WorkSpaces, imagens importadas e grupos de controle de acesso de IP.

- Você pode adicionar etiquetas a recursos existentes dos seguintes tipos: WorkSpaces, diretórios registrados, pacotes personalizados, imagens e grupos de controle de acesso de IP.

Restrições de tags

- Número máximo de tags por recurso: 50
- Comprimento máximo da chave: 127 caracteres Unicode
- Comprimento máximo de valor: 255 caracteres Unicode
- As chaves e os valores de tags diferenciam maiúsculas de minúsculas. Os caracteres permitidos são letras, espaços e números representáveis em UTF-8, além dos seguintes caracteres especiais: + - = . _ : / @. Não use espaços no início nem no fim.
- Não use os prefixo `aws:` ou `aws:workspaces:` no nome nem no valor de suas tags, pois eles são reservados para uso do AWS. Não é possível editar nem excluir nomes ou valores de tag com esses prefixos.

Como atualizar as etiquetas de um recurso existente usando o console (diretórios, WorkSpaces ou grupos de controle de acesso de IP)

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, escolha um dos seguintes tipos de recurso: Diretórios, WorkSpaces ou Controles de acesso do IP.
3. Selecione o recurso para abrir a página de detalhes dele.
4. Faça uma ou mais das coisas a seguir:
   - Para atualizar uma tag, edite os valores de Chave e Valor.
   - Para adicionar uma tag, escolha Adicionar tag e, em seguida, edite os valores de Chave e Valor.
   - Para excluir uma tag, escolha o ícone de exclusão (X) ao lado da tag.
5. Ao finalizar a atualização de tags, escolha Salvar.

Como atualizar as etiquetas de um recurso existente usando o console (imagens ou pacotes)

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, escolha um dos seguintes tipos de recursos: Pacotes ou Imagens.

3. Escolha o recurso para abrir a página de detalhes dele.
4. Em Tags, selecione Manage tags (Gerenciar tags).
5. Faça uma ou mais das coisas a seguir:
   - Para atualizar uma tag, edite os valores de Chave e Valor.
   - Para adicionar uma tag, escolha Adicionar nova tag e, em seguida, edite os valores de Chave e Valor.
   - Para excluir uma tag, escolha Remover ao lado da tag.
6. Ao concluir a atualização de tags, selecione Salvar alterações.

Para atualizar as tags de um recurso existente usando a AWS CLI

Use os comandos create-tags e delete-tags.

Manutenção do WorkSpace

Recomendamos que faça a manutenção do WorkSpaces regularmente. O WorkSpaces agenda janelas de manutenção padrão para seus WorkSpaces. Durante a janela de manutenção, o WorkSpace instala atualizações importantes no Amazon WorkSpaces e reinicia conforme necessário. Se disponíveis, as atualizações do sistema operacional também serão instaladas no servidor de atualização do sistema operacional que o WorkSpace está configurado para usar. Durante a manutenção, os WorkSpaces podem ficar indisponíveis.

Por padrão, os WorkSpaces do Windows são configurados para receber atualizações do Windows Update. Para configurar seus próprios mecanismos de atualização automática para o Windows, consulte a documentação do Windows Server Update Services (WSUS) e do Configuration Manager.

Requisito

Os WorkSpaces devem ter acesso à Internet para que seja possível instalar atualizações no sistema operacional e implantar aplicativos. Para obter mais informações, consulte the section called “Acesso à Internet”.

Janelas de manutenção para WorkSpaces no modo AlwaysOn

Para WorkSpaces AlwaysOn, a janela de manutenção é determinada pelas configurações do sistema operacional. O padrão é um período de quatro horas das 0h às 4h, no fuso horário do

WorkSpace, todo domingo de manhã. Por padrão, o fuso horário de um WorkSpace no modo AlwaysOn corresponde ao fuso horário da região da AWS do WorkSpace. No entanto, se você se conectar de outra região com o redirecionamento de fuso horário habilitado e se desconectar, o fuso horário do WorkSpace será atualizado para o fuso horário da região em que estiver conectado.

É possível desativar o redirecionamento do fuso horário para WorkSpaces do Windows usando a política de grupo. Você pode desativar o redirecionamento de fuso horário para WorkSpaces do Linux usando a configuração do agente PCoIP.

Para WorkSpaces do Windows, é possível configurar a janela de manutenção usando políticas de grupo. Consulte Definir configurações de políticas de grupo para atualizações automáticas. Não é possível configurar a janela de manutenção para WorkSpaces do Linux.

Janelas de manutenção para WorkSpaces no modo AutoStop

Os WorkSpaces AutoStop são executados automaticamente uma vez por mês para instalar atualizações importantes. A partir da terceira segunda-feira de cada mês, e por até duas semanas, a janela de manutenção abre todo dia das 0h às 5h, no fuso horário da região da AWS do WorkSpace. A manutenção do WorkSpace pode ser feita em qualquer dia da janela de manutenção. Durante essa janela, somente será feita a manutenção de WorkSpaces com mais de 7 dias.

Durante o período em que o WorkSpace está passando por manutenção, o estado do WorkSpace é definido como `MAINTENANCE`.

Embora não seja possível modificar o fuso horário usado para manter os WorkSpaces AutoStop, é possível desativar a janela de manutenção dos WorkSpaces AutoStop conforme mostrado a seguir. Se você desabilitar o modo de manutenção, seus WorkSpaces não serão reinicializados e não entrarão no estado `MAINTENANCE`.

Como desabilitar o modo de manutenção

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione Directories (Diretórios).
3. Selecione o diretório e escolha Actions (Ações), Update Details (Atualizar detalhes).
4. Expanda Modo de manutenção.
5. Para habilitar as atualizações automáticas, escolha Enabled (Ativado). Se você preferir gerenciar as atualizações manualmente, escolha Disabled (Desativado).
6. Escolha Atualizar e sair.

Manutenção manual

Se preferir, você pode fazer a manutenção de seus WorkSpaces em seu próprio cronograma. Quando você executar tarefas de manutenção, recomendamos que altere o status do WorkSpace para Manutenção. Ao concluir, altere o status do WorkSpace para Disponível.

Quando um WorkSpace está no status de Manutenção, ocorre o seguinte comportamento:

- O WorkSpace não responde a solicitações de reinicialização, interrupção, inicialização ou recriação.
- Os usuários não conseguem fazer login no WorkSpace.
- Um AutoStop WorkSpace não entra em hibernação.

Para alterar o estado do WorkSpace usando o console

> **Note**
>
> Para alterar o estado de um WorkSpace, o WorkSpace deve estar no status de Disponível. A configuração Modificar estado não estará disponível quando um WorkSpace estiver no status de Disponível.

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione WorkSpaces.
3. Selecione seu WorkSpace e escolha Ações, Modificar status.
4. Em Modificar status, escolha Disponível ou Manutenção.
5. Escolha Save (Salvar).

Para alterar o estado do WorkSpace usando a AWS CLI

Use o comando modify-workspace-state.

Encriptado WorkSpaces

WorkSpaces está integrado com o AWS Key Management Service (AWS KMS). Isso permite que você criptografe volumes de armazenamento WorkSpaces usando o AWS KMS Key. Ao iniciar um WorkSpace, você pode criptografar o volume raiz (para Microsoft Windows, a unidade C; para

Linux,/) e o volume do usuário (para Windows, a unidade D; para Linux, /home). Isso garante que os dados armazenados em repouso, E/S do disco para o volume e snapshots criados a partir dos volumes sejam todos criptografados.

> **Note**
>
> Além de criptografar seu WorkSpaces, você também pode usar a criptografia de endpoint FIPS em determinadas AWS regiões dos EUA. Para ter mais informações, consulte Configurar o Amazon WorkSpaces para a autorização do FedRAMP ou a conformidade com o SRG do DoD.

Conteúdo

Pré-requisitos

Você precisa de uma AWS KMS chave antes de começar o processo de criptografia. Essa chave KMS pode ser a chave KMS AWS gerenciada pela Amazon WorkSpaces (aws/workspaces) ou uma chave KMS simétrica gerenciada pelo cliente.

- AWS Chaves KMS gerenciadas — Na primeira vez que você executa uma chave não criptografada a WorkSpace partir do WorkSpaces console em uma região, a Amazon cria WorkSpaces automaticamente uma chave KMS AWS gerenciada (aws/workspaces) em sua conta. Você pode selecionar essa chave KMS AWS gerenciada para criptografar os volumes raiz e de usuário do seu. WorkSpace Para obter detalhes, consulte Visão geral da WorkSpaces criptografia usando AWS KMS.

  Você pode visualizar essa chave KMS AWS gerenciada, incluindo suas políticas e concessões, e pode rastrear seu uso em AWS CloudTrail registros, mas não pode usar ou gerenciar essa chave

KMS. WorkSpaces A Amazon cria e gerencia essa chave KMS. Somente a Amazon WorkSpaces pode usar essa chave KMS e WorkSpaces pode usá-la somente para criptografar WorkSpaces recursos em sua conta.

AWS As chaves KMS gerenciadas, incluindo a que a Amazon WorkSpaces suporta, são trocadas a cada três anos. Para obter detalhes, consulte AWS KMS Chave rotativa no Guia do AWS Key Management Service desenvolvedor.

- Chave KMS gerenciada pelo cliente — Como alternativa, você pode selecionar uma chave KMS simétrica gerenciada pelo cliente que você criou usando. AWS KMSÉ possível visualizar, usar e gerenciar essa chave do KMS, além de definir suas políticas. Para obter mais informações sobre como criar chaves do KMS, consulte Criar chaves no Guia do desenvolvedor do AWS Key Management Service . Para obter mais informações sobre a criação de chaves KMS usando a AWS KMS API, consulte Como trabalhar com chaves no Guia do AWS Key Management Service desenvolvedor.

  As chaves do KMS gerenciadas pelo cliente não são alternadas automaticamente, a menos que você decida habilitar a alternância automática de chaves. Para obter detalhes, consulte AWS KMS Chaves rotativas no Guia do AWS Key Management Service desenvolvedor.

> **Important**
>
> Ao girar manualmente as chaves KMS, você deve manter a chave KMS original e a nova chave KMS ativadas para que AWS KMS possa descriptografar a chave KMS original criptografada WorkSpaces . Se você não quiser manter a chave KMS original ativada, você deve recriá-la WorkSpaces e criptografá-la usando a nova chave KMS.

Você deve atender aos seguintes requisitos para usar uma AWS KMS chave para criptografar seu WorkSpaces:

- A chave do KMS deve ser simétrica. A Amazon WorkSpaces não oferece suporte a chaves KMS assimétricas. Para obter informações sobre a distinção entre chaves do KMS simétricas e assimétricas, consulte Identifying Symmetric and Asymmetric KMS Keys no Guia do desenvolvedor do AWS Key Management Service .
- A chave do KMS deve estar habilitada. Para determinar se uma chave do KMS está habilitada, consulte Displaying KMS Key Details no Guia do desenvolvedor do AWS Key Management Service .

- Você deve ter as permissões e políticas corretas associadas à chave do KMS. Para ter mais informações, consulte Parte 2: Conceda permissões adicionais WorkSpaces aos administradores usando uma política do IAM.

Limites

- Você não pode criptografar um existente WorkSpace. Você deve criptografar um WorkSpace ao iniciá-lo.
- Não WorkSpace há suporte para criar uma imagem personalizada a partir de uma imagem criptografada.
- A desativação da criptografia para um criptografado não WorkSpace é suportada atualmente.
- WorkSpaces lançado com a criptografia de volume raiz ativada, pode levar até uma hora para ser provisionado.
- Para reinicializar ou reconstruir um criptografado WorkSpace, primeiro verifique se a AWS KMS chave está ativada; caso contrário, WorkSpace ela se tornará inutilizável. Para determinar se uma chave do KMS está habilitada, consulte Displaying KMS Key Details no Guia do desenvolvedor do AWS Key Management Service .

Visão geral da WorkSpaces criptografia usando AWS KMS

Quando você cria WorkSpaces com volumes criptografados, WorkSpaces usa o Amazon Elastic Block Store (Amazon EBS) para criar e gerenciar esses volumes. O Amazon EBS criptografa os volumes com uma chave de dados usando o algoritmo AES-256 padrão do setor. Tanto o Amazon EBS quanto a Amazon WorkSpaces usam sua chave KMS para trabalhar com os volumes criptografados. Para obter mais informações sobre a criptografia de volume do EBS, consulte Amazon EBS Encryption no Guia do usuário do Amazon EC2.

Quando você inicia WorkSpaces com volumes criptografados, o end-to-end processo funciona assim:

1. Você especifica a chave KMS a ser usada para criptografia, bem como o usuário e o diretório do WorkSpace. Essa ação cria uma concessão que permite WorkSpaces usar sua chave KMS somente para isso, ou WorkSpace seja, somente para a WorkSpace associada ao usuário e diretório especificados.
2. WorkSpaces cria um volume do EBS criptografado para o WorkSpace e especifica a chave KMS a ser usada, bem como o usuário e o diretório do volume. Essa ação cria uma concessão que permite que o Amazon EBS use sua chave KMS somente para essa chave WorkSpace e para

o volume, ou seja, somente para o WorkSpace associado ao usuário e diretório especificados e somente para o volume especificado.

3. O Amazon EBS solicita uma chave de dados de volume que é criptografada sob sua chave KMS e especifica o identificador de segurança do Active Directory (SID) e o ID do AWS Directory Service diretório do WorkSpace usuário, bem como o ID do volume do Amazon EBS como contexto de criptografia.
4. AWS KMS cria uma nova chave de dados, a criptografa sob sua chave KMS e, em seguida, envia a chave de dados criptografada para o Amazon EBS.
5. WorkSpaces usa o Amazon EBS para anexar o volume criptografado ao seu WorkSpace. O Amazon EBS envia a chave de dados criptografada para AWS KMS com uma `Decrypt`solicitação e especifica o SID do WorkSpace usuário, o ID do diretório e o ID do volume, que é usado como contexto de criptografia.
6. AWS KMS usa sua chave KMS para descriptografar a chave de dados e, em seguida, envia a chave de dados em texto simples para o Amazon EBS.
7. O Amazon EBS usa a chave de dados em texto simples para criptografar todos os dados enviados e recebidos do volume criptografado. O Amazon EBS mantém a chave de dados de texto simples na memória enquanto o volume estiver conectado ao WorkSpace.
8. O Amazon EBS armazena a chave de dados criptografada (recebida emStep 4) com os metadados do volume para uso futuro, caso você reinicie ou reconstrua o. WorkSpace
9. Quando você usa o AWS Management Console para remover uma WorkSpace (ou usa a `TerminateWorkspaces`ação na WorkSpaces API), WorkSpaces o Amazon EBS retira as concessões que permitiram que eles usassem sua chave KMS para isso. WorkSpace

WorkSpaces contexto de criptografia

WorkSpaces não usa sua chave KMS diretamente para operações criptográficas (como `Encrypt`,,, etc.) `DecryptGenerateDataKey`, o que significa que WorkSpaces não envia solicitações AWS KMS que incluam um contexto de criptografia. No entanto, quando o Amazon EBS solicita uma chave de dados criptografada para os seus volumes criptografados WorkSpaces (Step 3noVisão geral da WorkSpaces criptografia usando AWS KMS) e quando solicita uma cópia em texto simples dessa chave de dados (Step 5), ele inclui o contexto de criptografia na solicitação.

O contexto de criptografia fornece dados autenticados adicionais (AAD) que são AWS KMS usados para garantir a integridade dos dados. O contexto de criptografia também é gravado em seus

arquivos de AWS CloudTrail log, o que pode ajudar você a entender por que uma determinada chave KMS foi usada. O Amazon EBS usa o seguinte como contexto de criptografia:

- O identificador de segurança (SID) do usuário do Active Directory associado ao WorkSpace
- O ID do AWS Directory Service diretório associado ao WorkSpace
- O ID do volume do Amazon EBS do volume criptografado

O exemplo a seguir mostra uma representação JSON do contexto de criptografia usado pelo Amazon EBS:

```
{
  "aws:workspaces:sid-directoryid":
 "[S-1-5-21-277731876-1789304096-451871588-1107]@[d-1234abcd01]",
  "aws:ebs:id": "vol-1234abcd"
}
```

Conceda WorkSpaces permissão para usar uma chave KMS em seu nome

Você pode proteger seus WorkSpace dados com a chave KMS AWS gerenciada para WorkSpaces (aws/workspaces) ou com uma chave KMS gerenciada pelo cliente. Se você usa uma chave KMS gerenciada pelo cliente, precisa conceder WorkSpaces permissão para usar a chave KMS em nome dos WorkSpaces administradores da sua conta. A chave KMS AWS gerenciada para WorkSpaces tem as permissões necessárias por padrão.

Para preparar sua chave KMS gerenciada pelo cliente para uso com WorkSpaces, use o procedimento a seguir.

1. Adicione seus WorkSpaces administradores à lista de usuários-chave na política de chaves do KMS
2. Dê aos seus WorkSpaces administradores permissões adicionais com uma política do IAM

Seus WorkSpaces administradores também precisam de permissão para usar WorkSpaces. Para obter mais informações sobre essas permissões, acesse Gerenciamento de identidade e acesso para o WorkSpaces.

Parte 1: Adicionar WorkSpaces administradores como usuários-chave

Para dar aos WorkSpaces administradores as permissões de que eles precisam, você pode usar a AWS Management Console ou a AWS KMS API.

Para adicionar WorkSpaces administradores como usuários-chave de uma chave KMS (console)

1. Faça login AWS Management Console e abra o console AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, escolha Chaves gerenciadas pelo cliente.
4. Escolha o ID de chave ou alias da sua chave do KMS gerenciada pelo cliente preferida
5. Selecione a guia Key policy (Política de chaves). Em Key users (Usuários de chaves), escolhaAdd (Adicionar).
6. Na lista de usuários e funções do IAM, selecione os usuários e funções que correspondem aos seus WorkSpaces administradores e, em seguida, escolha Adicionar.

Para adicionar WorkSpaces administradores como usuários-chave de uma chave KMS (API)

1. Use a operação GetKeyPolítica para obter a política de chaves existente e, em seguida, salve o documento de política em um arquivo.
2. Abra o documento de política no editor de texto de sua preferência. Adicione os usuários e funções do IAM que correspondem aos seus WorkSpaces administradores às declarações de política que dão permissão aos principais usuários. Salve o arquivo.
3. Use a operação PutKeyPolítica para aplicar a política de chaves à Chave KMS.

Parte 2: Conceda permissões adicionais WorkSpaces aos administradores usando uma política do IAM

Se você selecionar uma chave KMS gerenciada pelo cliente para usar para criptografia, deverá estabelecer políticas do IAM que permitam WorkSpaces à Amazon usar a chave KMS em nome de um usuário do IAM em sua conta que inicia a criptografia. WorkSpaces Esse usuário também precisa de permissão para usar a Amazon WorkSpaces. Para obter mais informações sobre como criar e editar políticas de usuários do IAM, consulte Gerenciamento de políticas do IAM no Guia do usuário do IAM e em Gerenciamento de identidade e acesso para o WorkSpaces.

WorkSpaces a criptografia requer acesso limitado à chave KMS. Veja a seguir um exemplo de política de chaves que pode ser usada. Essa política separa as entidades principais que podem gerenciar a chave do AWS KMS daquelas que podem usá-la. Antes de usar esse exemplo de política de chaves, substitua o exemplo de ID da conta e o nome de usuário do IAM pelos valores reais da sua conta.

A primeira declaração corresponde à política de AWS KMS chaves padrão. Isso concede à sua conta permissão para usar políticas do IAM para controlar o acesso à chave do KMS. A segunda e a terceira declarações definem quais AWS diretores podem gerenciar e usar a chave, respectivamente. A quarta declaração permite que os AWS serviços integrados AWS KMS usem a chave em nome do principal especificado. Essa declaração permite que os serviços da AWS criem e gerenciem concessões. A declaração usa um elemento condicional que limita as concessões da chave KMS às concedidas por AWS serviços em nome dos usuários em sua conta.

> **Note**
>
> Se seus WorkSpaces administradores usarem o AWS Management Console para criar WorkSpaces com volumes criptografados, eles precisarão de permissão para listar aliases e chaves de lista (as permissões `"kms:ListAliases"` e`"kms:ListKeys"`). Se seus WorkSpaces administradores usarem somente a WorkSpaces API da Amazon (não o console), você poderá omitir as permissões `"kms:ListAliases"` e. `"kms:ListKeys"`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:root"},
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:Create*",
        "kms:Describe*",
        "kms:Enable*",
        "kms:List*",
```

```
        "kms:Put*",
        "kms:Update*",
        "kms:Revoke*",
        "kms:Disable*",
        "kms:Get*",
        "kms:Delete*"
       ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": "*",
      "Condition": {"Bool": {"kms:GrantIsForAWSResource": "true"}}
    }
  ]
}
```

A política do IAM para um usuário ou função que está criptografando um WorkSpace deve incluir permissões de uso na chave KMS gerenciada pelo cliente, bem como acesso a. WorkSpaces Para conceder WorkSpaces permissões a um usuário ou função do IAM, você pode anexar o exemplo de política a seguir ao usuário ou função do IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "ds:*",
                "ds:DescribeDirectories",
                "workspaces:*",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:CreateWorkspaces",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaces",
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces"
            ],
            "Resource": "*"
        }
    ]
}
```

A política do IAM a seguir é exigida pelo usuário para usar o AWS KMS. Ela concede ao usuário acesso somente leitura à chave do KMS juntamente com a capacidade de criar concessões.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:Describe*",
                "kms:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Se você quiser especificar a chave do KMS em sua política, use uma política do IAM semelhante ao exemplo a seguir. Substitua o ARN da chave do KMS de exemplo por um válido.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kms:CreateGrant",
      "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource": "*"
    }
  ]
}
```

Criptografar um WorkSpace

Para criptografar um WorkSpace

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. Escolha Iniciar WorkSpaces e conclua as três primeiras etapas.
3. Para a etapa WorkSpaces de configuração, faça o seguinte:

    a. Selecione os volumes a serem criptografados: Volume raiz, Volume de usuário ou os dois volumes.

    b. Para Chave de criptografia, selecione uma AWS KMS chave, seja a chave KMS AWS gerenciada criada pela Amazon WorkSpaces ou uma chave KMS que você criou. A chave do KMS que você seleciona deve ser simétrica. A Amazon WorkSpaces não oferece suporte a chaves KMS assimétricas.

    c. Escolha Next Step.
4. Escolha Iniciar WorkSpaces.

Visualização criptografada WorkSpaces

Para ver quais volumes WorkSpaces e volumes foram criptografados no WorkSpaces console, escolha na barra WorkSpacesde navegação à esquerda. A coluna Criptografia de volume mostra se

cada uma WorkSpace tem a criptografia ativada ou desativada. Para ver quais volumes específicos foram criptografados, expanda a WorkSpace entrada para ver o campo Volumes criptografados.

Reinicie um WorkSpace

Ocasionalmente, talvez seja necessário reinicializar (reiniciar) WorkSpace manualmente. A reinicialização de um WorkSpace desconecta o usuário e, em seguida, executa o desligamento e a reinicialização do. WorkSpace Para evitar perda de dados, certifique-se de que o usuário salve todos os documentos abertos e outros arquivos do aplicativo antes de reinicializar o. WorkSpace Os dados de usuário, o sistema operacional e as configurações do sistema não são afetados.

> **Warning**
>
> Para reinicializar um criptografado WorkSpace, primeiro verifique se a AWS KMS chave está ativada; caso contrário, WorkSpace ela se tornará inutilizável. Para determinar se uma chave do KMS está habilitada, consulte Displaying KMS Key Details no Guia do desenvolvedor do AWS Key Management Service.

Para reinicializar um WorkSpace

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione WorkSpaces.
3. Selecione a opção WorkSpaces para reinicializar e escolha Ações, WorkSpacesReinicializar.
4. Quando solicitada a confirmação, escolha WorkSpacesReinicializar.

Para reinicializar um WorkSpace usando o AWS CLI

Use o comando reboot-workspaces.

Para reinicializar em massa WorkSpaces

Use amazon-workspaces-admin-moduleo.

Reconstrua um WorkSpace

A reconstrução de um WorkSpace recria o volume raiz da imagem mais recente do pacote a partir do qual o WorkSpace foi lançado, seu volume de usuário e sua interface primária de elastic

network. Reconstruir um WorkSpace exclui mais dados do que restaurar um WorkSpace, mas requer apenas que você tenha um instantâneo do volume do usuário. Para restaurar um WorkSpace, consulteRestaurar um WorkSpace.

A reconstrução de um WorkSpace faz com que ocorra o seguinte:

- O volume raiz (para Microsoft Windows, unidade C; para Linux,/) é atualizado com a imagem mais recente do pacote a partir do qual o WorkSpace foi criado. Todos os aplicativos que foram instalados ou as configurações do sistema que foram alteradas após a WorkSpace criação são perdidos.
- O volume do usuário (para Microsoft Windows, a unidade D; para Linux, /home) é recriado a partir do snapshot mais recente. O conteúdo atual do volume do usuário é substituído.

  Os instantâneos automáticos para uso na reconstrução de um WorkSpace são programados a cada 12 horas. Esses instantâneos do volume do usuário são tirados independentemente da integridade do WorkSpace. Quando você escolhe Ações, Reconstruir/Restaurar WorkSpace, a data e a hora do instantâneo mais recente são mostradas.

  Quando você reconstrói um WorkSpace, novos instantâneos também são tirados logo após a conclusão da reconstrução (geralmente em 30 minutos).
- A interface de rede elástica principal é recriada. O WorkSpace recebe um novo endereço IP privado.

> **Important**
>
> Depois de 14 de janeiro de 2020, WorkSpaces criado a partir de um pacote público do Windows 7 não poderá mais ser reconstruído. Talvez você queira considerar a migração do Windows 7 WorkSpaces para o Windows 10. Para ter mais informações, consulte Migre um WorkSpace.

Você pode reconstruir um WorkSpace somente se as seguintes condições forem atendidas:

- Eles WorkSpace devem ter um estado de`AVAILABLE`,`ERROR`,`UNHEALTHY`,`STOPPED`, ou`REBOOTING`. Para reconstruir um WorkSpace no `REBOOTING` estado, você deve usar a operação de RebuildWorkspacesAPI ou o comando AWS CLI rebuild-workspaces.
- Deve existir um snapshot do volume do usuário.

Para reconstruir um WorkSpace

> **Warning**
>
> Para reconstruir um criptografado WorkSpace, primeiro certifique-se de que a AWS KMS chave esteja ativada; caso contrário, WorkSpace ela se tornará inutilizável. Para determinar se uma chave do KMS está habilitada, consulte Displaying KMS Key Details no Guia do desenvolvedor do AWS Key Management Service .

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, escolha WorkSpaces.
3. Selecione a opção WorkSpace para reconstruir e escolha Ações, Reconstruir/Restaurar. WorkSpace
4. Em Snapshot, selecione a data e hora do snapshot.
5. Escolha Rebuild.

Para reconstruir um WorkSpace usando o AWS CLI

Use o comando rebuild-workspaces.

Solução de problemas

Se você reconstruir um WorkSpace após alterar o atributo de nomeação de AccountNameusuário SaM do usuário no Active Directory, poderá receber a seguinte mensagem de erro:

```
"ErrorCode": "InvalidUserConfiguration.Workspace"
"ErrorMessage": "The user was either not found or is misconfigured."
```

Para contornar esse problema, reverta para o atributo de nome de usuário original e reinicie a reconstrução ou crie um novo para esse usuário. WorkSpace

Restaurar um WorkSpace

Restaurar um WorkSpace recriará o volume raiz e o volume do usuário com base nos snapshots mais recentes desses volumes que foram criados quando o WorkSpace estava íntegro. A restauração de um WorkSpace exclui menos dados do que a recompilação de um WorkSpace. No

entanto, isso exige que você tenha snapshots do volume raiz e do volume do usuário, enquanto a recompilação de um WorkSpace requer apenas um snapshot do volume do usuário. Para recompilar um WorkSpace, consulte Reconstrua um WorkSpace.

Restaurar um WorkSpace causa o seguinte:

- O volume raiz (para Microsoft Windows, unidade C; para Linux, /) é restaurado para o snapshot mais recente. Todos os aplicativos que foram instalados ou as configurações do sistema que foram alteradas após a criação do snapshot mais recente são perdidos.
- O volume do usuário (para Microsoft Windows, a unidade D; para Linux, /home) é recriado a partir do snapshot mais recente. O conteúdo atual do volume do usuário é substituído.

Quando os snapshots são tirados

Os snapshots do volume raiz e do usuário são tirados da forma a seguir. Quando você seleciona Ações e Recompilar/Restaurar WorkSpace, a data e a hora dos snapshots mais recentes são mostradas.

- Depois que um WorkSpace é criado pela primeira vez: normalmente, os snapshots iniciais dos volumes raiz e do usuário são tirados logo após a criação do WorkSpace (geralmente em 30 minutos). Em algumas regiões da AWS, pode levar várias horas para tirar os snapshots iniciais após a criação de um WorkSpace.

  Se um WorkSpace se tornar não íntegro antes que os snapshots iniciais sejam tirados, ele não poderá ser restaurado. Nesse caso, você pode tentar recompilar o WorkSpace ou entrar em contato com o AWS Support para obter ajuda.
- Durante o uso regular: os snapshots automáticos para uso durante a restauração de um WorkSpace são programados a cada 12 horas. Se o WorkSpace estiver íntegro, os snapshots do volume raiz e do volume do usuário serão criados ao mesmo tempo. Se o WorkSpace não estiver íntegro, os snapshots serão criados somente para o volume do usuário.
- Depois que um WorkSpace é restaurado: quando você restaura um WorkSpace, novos snapshots são tirados logo após a conclusão da restauração (geralmente em 30 minutos). Em algumas regiões da AWS, pode levar várias horas para tirar esses snapshots após a restauração de um WorkSpace.

  Após a restauração de um WorkSpace, se o WorkSpace se tornar não íntegro antes que novos snapshots possam ser tirados, ele não poderá ser restaurado novamente. Nesse caso, você pode tentar recompilar o WorkSpace ou entrar em contato com o AWS Support para obter ajuda.

Você pode restaurar um WorkSpace somente se as seguintes condições forem atendidas:

- O WorkSpace deve estar no estado `AVAILABLE`, `ERROR`, `UNHEALTHY` ou `STOPPED`.
- Devem existir snapshots dos volumes raiz e do usuário.

Como restaurar um WorkSpace

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione WorkSpaces.
3. Selecione o WorkSpace a ser restaurado e clique em Ações, Recompilar/Restaurar WorkSpace.
4. Em Snapshot, selecione a data e hora do snapshot.
5. Escolha Restore.

Como restaurar um WorkSpace usando o AWS CLI

Use o comando restore-workspace.

Traga sua própria licença (BYOL) do Microsoft 365

A Amazon WorkSpaces permite que você traga suas próprias licenças do Microsoft 365 se elas atenderem aos requisitos de licenciamento da Microsoft. Essas licenças permitem que você instale e ative os aplicativos Microsoft 365 para software corporativo WorkSpaces que são alimentados pelos seguintes sistemas operacionais:

- Windows 10 (Traga sua própria licença)
- Windows 11 (Traga sua própria licença)
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Para usar o Microsoft 365 Apps for enterprise on WorkSpaces, você deve ter uma assinatura do Microsoft 365 E3/E5, Microsoft 365 A3/A5 ou Microsoft 365 Business Premium.

Na Amazon, WorkSpaces você pode usar suas licenças do Microsoft 365 para instalar e ativar os aplicativos Microsoft 365 para empresas, incluindo o seguinte:

- Microsoft Word
- Microsoft Excel
- Microsoft PowerPoint
- Microsoft Outlook
- Microsoft OneDrive

Para obter mais informações, consulte a lista completa do Microsoft 365 Apps para Grandes Empresas.

Você também pode instalar aplicativos da Microsoft não incluídos no Microsoft 365, como o Microsoft Project, o Microsoft Visio e o Microsoft Power Automate, WorkSpaces mas precisa trazer suas próprias licenças adicionais.

Você pode instalar e usar o Microsoft 365 e outros aplicativos da Microsoft no sistema primário WorkSpaces e no failover WorkSpaces usando a resiliência multirregional.

Conteúdo

Crie WorkSpaces com o Microsoft 365 Apps para empresas

Para criar WorkSpaces com o Microsoft 365 Apps for enterprise, você deve criar uma imagem personalizada com os aplicativos instalados e usá-la para criar um pacote personalizado. Você pode usar o pacote para lançar novos WorkSpaces que tenham os aplicativos instalados. WorkSpaces não fornece pacotes públicos com o Microsoft 365 Apps for enterprise.

Para criar WorkSpaces com o Microsoft 365 Apps para empresas:

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. Inicie uma WorkSpace que você deseja usar como imagem para outro aplicativo da Microsoft WorkSpaces. É nele que você instalará as aplicações da Microsoft. Para obter mais informações sobre como iniciar um WorkSpace, consulte Iniciar uma área de trabalho virtual usando WorkSpaces.

3. Inicie a aplicação cliente em https://clients.amazonworkspaces.com/, insira o código de registro presente no e-mail de convite e clique em Registrar.
4. Quando for necessário fazer login, insira as credenciais de login do usuário e clique em Fazer login.
5. Instale e configure o Microsoft 365 Apps para Grandes Empresas.
6. Crie uma imagem personalizada a WorkSpace partir do e use-a para criar um pacote personalizado. Para obter mais informações sobre a criação de imagens e pacotes personalizados, consulte Criar uma WorkSpaces imagem e um pacote personalizados.
7. Inicie WorkSpaces usando o pacote personalizado que você criou. Eles WorkSpaces têm o Microsoft 365 Apps para empresas instalado.

Migre seus aplicativos existentes WorkSpaces para usar o Microsoft 365 para empresas

Se você WorkSpaces não tiver uma licença do Microsoft OfficeAWS, você pode instalar e configurar o Microsoft 365 Apps for enterprise em seu WorkSpaces.

Se você tiver uma licença WorkSpaces do Microsoft OfficeAWS, primeiro cancele o registro da licença do Microsoft Office antes de instalar o Microsoft 365 Apps for enterprise.

Important

A desinstalação dos aplicativos do Microsoft Office do seu WorkSpaces não cancela o registro das licenças. Para evitar a cobrança pelas licenças do Microsoft Office, cancele o registro de seus aplicativos do WorkSpaces Microsoft Office AWS fazendo o seguinte:

- Gerenciar aplicativos (recomendado) — Você pode desinstalar o Microsoft Office 2016 e 2019 do seu WorkSpaces. Para obter mais informações, consulte Manage applications. Depois de desinstalar, você pode instalar o Microsoft 365 Apps for enterprise no seu WorkSpaces.
- Migrar um WorkSpace — Você pode migrar um WorkSpace de um pacote para outro enquanto retém os dados no volume do usuário.
  - Migre sua WorkSpaces para um pacote com uma imagem que não tenha uma assinatura do Microsoft Office. Depois que a migração for concluída, você poderá instalar o Microsoft 365 Apps for enterprise no seu WorkSpaces.

- Ou crie uma WorkSpaces imagem e um pacote personalizados que já tenham o Microsoft 365 Apps for enterprise instalados na imagem e, em seguida, migre os seus WorkSpaces para esse novo pacote personalizado. Depois que a migração for concluída, seus WorkSpaces usuários poderão começar a usar o Microsoft 365 Apps for enterprise.
- Para obter mais informações sobre como migrar WorkSpaces, consulte Migrar a. WorkSpace

Atualize seus aplicativos Microsoft 365 para empresas em WorkSpaces

Por padrão, sua WorkSpaces execução no sistema operacional Microsoft Windows está configurada para receber atualizações do Windows Update. No entanto, as atualizações do Microsoft 365 Apps para Grandes Empresas não estão disponíveis no Windows Update. Configure as atualizações para serem executadas automaticamente pela CDN do Office ou use o Windows Server Update Services (WSUS) com o Microsoft Configuration Manager para atualizar o Microsoft 365 Apps para Grandes Empresas. Para obter mais informações, consulte Manage updates to Microsoft 365 Apps with Microsoft Configuration Manager. Para definir a frequência das atualizações do aplicativo Microsoft 365, especifique um canal de atualização e defina-o como Empresa atual ou mensal para estar em conformidade com a política de WorkSpaces licenciamento do Microsoft 365.

Atualize o Windows BYOL WorkSpaces

Em seu Windows Bring Your Own License (BYOL) WorkSpaces, você pode atualizar para uma versão mais recente do Windows usando o processo de atualização no local. Siga as instruções neste tópico para fazer a atualização.

O processo de atualização in-loco se aplica somente ao WorkSpaces BYOL do Windows 10 e 11.

Important

Não execute o Sysprep em um upgrade. WorkSpace Se você fizer isso, poderá ocorrer um erro que impede a conclusão do Sysprep. Se você planeja executar o Sysprep, faça isso somente em um WorkSpace que não tenha sido atualizado.

> **Note**
>
> Você pode usar esse processo para atualizar o Windows 10 e 11 WorkSpaces para uma versão mais recente. No entanto, esse processo não pode ser usado para atualizar seu Windows 10 WorkSpaces para o Windows 11.

Conteúdos

Pré-requisitos

- Se você adiou ou pausou as atualizações do Windows 10 e 11 usando a Política de Grupo ou o System Center Configuration Manager (SCCM), habilite as atualizações do sistema operacional para o Windows 10 e 11. WorkSpaces
- Se WorkSpace for um AutoStop WorkSpace, altere-o para um AlwaysOn WorkSpace antes do processo de atualização local para que ele não pare automaticamente enquanto as atualizações estiverem sendo aplicadas. Para ter mais informações, consulte Modificar o modo de execução. Se você preferir manter a WorkSpace configuração AutoStop, altere o AutoStop tempo para três horas ou mais enquanto a atualização ocorre.
- O processo de atualização local recria o perfil do usuário fazendo uma cópia de um perfil especial chamado Default User (`C:\Users\Default`). Não use esse perfil de usuário padrão para fazer personalizações. Recomendamos fazer personalizações no perfil do usuário por meio de GPOs (Objetos de política de grupo). As personalizações feitas por meio de GPOs podem ser facilmente modificadas ou revertidas e são menos propensas a erros.
- O processo de atualização no local pode fazer backup e recriar somente um perfil de usuário. Se você tiver vários perfis de usuário na unidade D, exclua todos os perfis, exceto aquele que você precisa.

Considerações

O processo de atualização no local usa dois scripts de registro (`enable-inplace-upgrade.ps1eupdate-pvdrivers.ps1`) para fazer as alterações necessárias no seu WorkSpaces que permitem a execução do processo do Windows Update. Essas alterações envolvem a criação de um perfil de usuário (temporário) na unidade C em vez de na unidade D. Se já existir um perfil de usuário na unidade D, os dados nesse perfil original permanecerão na unidade D.

Por padrão, WorkSpaces cria o perfil do usuário em`D:\Users\%USERNAME%`. O script `enable-inplace-upgrade.ps1` configura o Windows para criar um perfil de usuário em `C:\Users\%USERNAME%` e redireciona as pastas do shell do usuário para `D:\Users\%USERNAME%`. Esse perfil de usuário é criado quando um usuário faz login pela primeira vez.

Após a atualização in-loco, você tem a opção de deixar seus perfis de usuário na unidade C para permitir que seus usuários utilizem o processo do Windows Update para atualizar seus computadores no futuro. No entanto, lembre-se de que, WorkSpaces com os perfis armazenados na unidade C, não é possível recriar ou migrar sem perder todos os dados no perfil do usuário, a menos que você mesmo faça backup e restaure esses dados. Se você decidir deixar os perfis na unidade C, poderá usar a chave do UserShellFoldersRedirectionregistro para redirecionar as pastas do shell do usuário para a unidade D, conforme explicado posteriormente neste tópico.

Para garantir que você possa reconstruir ou migrar sua pasta WorkSpaces e evitar possíveis problemas com o redirecionamento da pasta shell do usuário, recomendamos que você opte por restaurar seus perfis de usuário na unidade D após a atualização local. Você pode fazer isso usando a chave de registro PostUpgradeRestoreProfileOnD, conforme explicado posteriormente neste tópico.

Limitações conhecidas

- A alteração da localização do perfil do usuário da unidade D para a unidade C não acontece durante WorkSpace reconstruções ou migrações. Se você realizar uma atualização local em um BYOL do Windows 10 ou 11 WorkSpace e depois reconstruí-lo ou migrá-lo, o novo WorkSpace terá o perfil de usuário na unidade D.

  > **Warning**
  >
  > Se você deixar o perfil de usuário na unidade C após a atualização in-loco, os dados do perfil armazenados na unidade C serão perdidos durante reconstruções ou migrações, a menos que você faça backup manualmente dos dados do perfil de usuário antes de recriar

ou migrar e, depois, restaure manualmente os dados do perfil após executar o processo de recriação ou migração.

- Se o pacote BYOL padrão contiver uma imagem baseada em uma versão anterior do Windows 10 e 11, você deverá realizar a atualização local novamente após a recriação ou WorkSpace migração.

Resumo das configurações da chave do registro

Para habilitar o processo de atualização in-loco e especificar o local do perfil de usuário após a atualização, é necessário definir uma série de chaves do registro.

Caminho de registro: HKL M:\Software\Amazon\WorkSpacesConfig\ .ps1 enable-inplace-upgrade

Chave do registro	Tipo	Valores
Ativado	DWORD	0: (padrão) desativa a atualização in-loco 1: permite a atualização in-loco
PostUpgradeRestoreProfileOnD	DWORD	0: (padrão) não tenta restaurar o caminho do perfil do usuário após a atualização in-loco 1 — Restaura o caminho do perfil do usuário (ProfileImagePath) após a atualização in-loco
UserShellFoldersRedirection	DWORD	0: não habilita o redirecionamento de pastas do shell do usuário 1: (padrão) habilita o redirecionamento de pastas do shell do usuário para `D:\Users\%USERNAME%` depois que

Chave do registro	Tipo	Valores
		o perfil do usuário é gerado novamente em `C:\Users\%USERNAME%`
NoReboot	DWORD	0: (padrão) permite controlar quando ocorre uma reinicialização após modificar o registro para o perfil de usuário 1 — Não permite que o script reinicie o WorkSpace após modificar o registro do perfil do usuário

Caminho de registro: HKL M:\Software\Amazon\WorkSpacesConfig\ update-pvdrivers.ps1

Chave do registro	Tipo	Valores
Ativado	DWORD	0 — (Padrão) Desativa a atualização de drivers AWS fotovoltaicos 1 — Permite a atualização de drivers AWS fotovoltaicos

Realizar uma atualização no local

Para habilitar atualizações in-loco do Windows em seu BYOL WorkSpaces, você deve definir determinadas chaves de registro, conforme descrito no procedimento a seguir. Também é preciso definir determinadas chaves do registo para indicar a unidade (C ou D) onde os perfis de usuário deverão estar depois de concluídas as atualizações in-loco.

É possível fazer essas alterações de registro manualmente. Se você tiver vários WorkSpaces para atualizar, poderá usar a Política de Grupo ou o SCCM para enviar um PowerShell script. Para obter

um exemplo de PowerShell script, consulteAtualize seu WorkSpace registro usando um PowerShell script.

Para realizar uma atualização local do Windows 10 e 11

1. Anote qual versão do Windows está sendo executada atualmente no BYOL do Windows 10 e 11 WorkSpaces que você está atualizando e, em seguida, reinicie-as.
2. Atualize as seguintes chaves do registro do sistema Windows para alterar os dados de valor de Enabled (Habilitado) de 0 para 1. Essas alterações no registro permitem atualizações locais para o. WorkSpace

   - HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\\ .ps1 WorkSpacesConfig enable-inplace-upgrade
   - HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\\ update-pvdrivers.ps1 WorkSpacesConfig

   > **Note**
   >
   > Se essas chaves não existirem, reinicie o. WorkSpace As chaves devem ser adicionadas quando o sistema for reiniciado.

   (Opcional) Se você estiver usando um fluxo de trabalho gerenciado, como as sequências de tarefas do SCCM, para realizar a atualização, defina o seguinte valor de chave como 1 para impedir que o computador seja reinicializado:

   HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\\ .ps1\ WorkSpacesConfig enable-inplace-upgrade NoReboot
3. Decida em qual unidade os perfis de usuário deverão estar após o processo de atualização in-loco (para obter mais informações, consulte Considerações) e defina as chaves de registo da seguinte forma:

   - Configurações se o local do perfil de usuário precisar ser a unidade C após a atualização:

     HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\\ .ps1 WorkSpacesConfig enable-inplace-upgrade

     Nome da chave: PostUpgradeRestoreProfileOnD

Valor da chave: 0

Nome da chave: UserShellFoldersRedirection

Valor da chave: 1

- Configurações se o local do perfil de usuário precisar ser a unidade D após a atualização:

  HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\\ .ps1 WorkSpacesConfig enable-inplace-upgrade

  Nome da chave: PostUpgradeRestoreProfileOnD

  Valor da chave: 1

  Nome da chave: UserShellFoldersRedirection

  Valor da chave: 0

4. Depois de salvar as alterações no registro, reinicie WorkSpace novamente para que as alterações sejam aplicadas.

> **Note**
>
> - Após a reinicialização, o login no WorkSpace cria um novo perfil de usuário. É possível ver os ícones de espaço reservado no menu Start (Iniciar). Esse comportamento é resolvido automaticamente após a conclusão da atualização no local.
> - Aguarde 10 minutos para garantir que WorkSpace esteja desbloqueado.

(Opcional) Confirme se o valor da chave a seguir está definido como 1, o que desbloqueia o WorkSpace para atualização:

HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\\ .ps1\ Excluído WorkSpacesConfig enable-inplace-upgrade profileImagePath

5. Execute a atualização local. Você pode usar qualquer método que desejar, como SCCM, ISO ou Windows Update (WU). Dependendo da versão original do Windows 10 e 11 e de quantos aplicativos foram instalados, esse processo pode levar de 40 a 120 minutos.

   > **Note**
   >
   > O processo de atualização in-loco pode levar pelo menos uma hora. O status da WorkSpace instância pode aparecer como `UNHEALTHY` durante a atualização.

6. Depois que o processo de atualização for concluído, confirme se a versão do Windows foi atualizada.

   > **Note**
   >
   > Se a atualização in-loco falhar, o Windows reverte automaticamente para usar a versão do Windows 10 e 11 que estava em vigor antes de você iniciar a atualização. Para obter mais informações sobre a solução de problemas, consulte a documentação da Microsoft.

   (Opcional) Para confirmar que os scripts de atualização foram executados com êxito, verifique se o seguinte valor da chave está configurado como 1:

   HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\\ .ps1\ WorkSpacesConfig enable-inplace-upgrade scriptExecutionComplete

7. Se você modificou o modo de execução do WorkSpace definindo-o AlwaysOn ou alterando o período de AutoStop tempo para que o processo de atualização no local pudesse ser executado sem interrupção, redefina o modo de execução para as configurações originais. Para ter mais informações, consulte Modificar o modo de execução.

Se você não tiver definido a chave de registro PostUpgradeRestoreProfileOnD como 1, o perfil do usuário será regenerado pelo Windows e inserido `C:\Users\%USERNAME%` após a atualização local, para que você não precise seguir as etapas acima novamente para futuras atualizações in-loco do Windows 10 e 11. Por padrão, o script `enable-inplace-upgrade.ps1` redireciona as seguintes pastas do shell para a unidade D:

- `D:\Users\%USERNAME%\Downloads`
- `D:\Users\%USERNAME%\Desktop`

- `D:\Users\%USERNAME%\Favorites`
- `D:\Users\%USERNAME%\Music`
- `D:\Users\%USERNAME%\Pictures`
- `D:\Users\%USERNAME%\Videos`
- `D:\Users\%USERNAME%\Documents`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Network Shortcuts`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Printer Shortcuts`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\SendTo`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Templates`

Se você redirecionar as pastas do shell para outros locais em sua WorkSpaces, execute as operações necessárias WorkSpaces após as atualizações no local.

Solução de problemas

Se você tiver problemas com a atualização, verifique os seguintes itens para auxiliar na solução de problemas:

- Logs do Windows, que, por padrão, estão localizados nos seguintes locais:

  `C:\Program Files\Amazon\WorkSpacesConfig\Logs\`

  `C:\Program Files\Amazon\WorkSpacesConfig\Logs\TRANSMITTED`

- Visualizador de eventos do Windows

  Logs do Windows > Aplicativo > Fonte: Amazon WorkSpaces

> **Tip**
>
> Durante o processo de atualização no local, se você perceber que alguns atalhos de ícones na área de trabalho não funcionam mais, é porque WorkSpaces move qualquer perfil de usuário localizado na unidade D para a unidade C para se preparar para a atualização. Depois de concluída a atualização, os atalhos funcionarão conforme o esperado.

Atualize seu WorkSpace registro usando um PowerShell script

Você pode usar o seguinte exemplo de PowerShell script para atualizar o registro no seu e WorkSpaces permitir atualizações no local. Siga aRealizar uma atualização no local, mas use esse script para atualizar o registro em cada um WorkSpace.

```
# AWS WorkSpaces 1.28.20
# Enable In-Place Update Sample Scripts
# These registry keys and values will enable scripts to run on the next reboot of the
 WorkSpace.

$scriptlist = ("update-pvdrivers.ps1","enable-inplace-upgrade.ps1")
$wsConfigRegistryRoot="HKLM:\Software\Amazon\WorkSpacesConfig"
$Enabled = 1
$script:ErrorActionPreference = "Stop"

foreach ($scriptName in $scriptlist)
{
    $scriptRegKey = "$wsConfigRegistryRoot\$scriptName"

    try
    {
        if (-not(Test-Path $scriptRegKey))
        {
            Write-Host "Registry key not found. Creating registry key '$scriptRegKey'
 with 'Update' enabled."
            New-Item -Path $wsConfigRegistryRoot -Name $scriptName | Out-Null
            New-ItemProperty -Path $scriptRegKey -Name Enabled -PropertyType DWord -
Value $Enabled | Out-Null
            Write-Host "Value created. '$scriptRegKey' Enabled='$((Get-ItemProperty -
Path $scriptRegKey).Enabled)'"
        }
        else
```

```
        {
            Write-Host "Registry key is already present with value '$scriptRegKey'
 Enabled='$((Get-ItemProperty -Path $scriptRegKey).Enabled)'"
            if((Get-ItemProperty -Path $scriptRegKey).Enabled -ne $Enabled)
            {
                Set-ItemProperty -Path $scriptRegKey -Name Enabled -Value $Enabled
                Write-Host "Value updated. '$scriptRegKey' Enabled='$((Get-ItemProperty
 -Path $scriptRegKey).Enabled)'"
            }
        }
    }
    catch
    {
        write-host "Stopping script, the following error was encountered:" `r`n$_ -
ForegroundColor Red
        break
    }
}
```

Migre um WorkSpace

> **Note**
>
> Se você quiser cancelar a assinatura ou desinstalar as licenças da versão do Microsoft Office por meio AWS do seu WorkSpace, recomendamos o uso de Gerenciar aplicativos.

Você pode migrar um WorkSpace de um pacote para outro, mantendo os dados no volume do usuário. Estes são cenários de exemplo:

- Você pode migrar WorkSpaces da experiência de desktop do Windows 7 para a experiência da área de trabalho do Windows 10.
- Você pode migrar WorkSpaces do protocolo PCoIP para o WorkSpaces Streaming Protocol (WSP).
- Você pode migrar WorkSpaces do pacote Microsoft Office de 32 bits no Windows Server 2016 WorkSpaces para os pacotes do Microsoft Office de 64 bits no Windows Server 2019 e Windows Server 2022. WorkSpaces
- Você pode migrar WorkSpaces de um pacote público ou personalizado para outro. Por exemplo, você pode migrar de uma placa de vídeo habilitada para GPU (Graphics.G4DN).

GraphicsPro.g4dn, Graphics e GraphicsPro) se agrupam em pacotes não habilitados para GPU, bem como na outra direção.

- Você pode migrar WorkSpaces do Windows 10 BYOL para o Windows 11 BYOL, mas a migração do Windows 11 para o Windows 10 não é suportada.
- Pacotes de valor não são compatíveis com o Windows 11. Para migrar seu pacote de valor do Windows 7 ou 10 WorkSpaces para o Windows 11, você precisa primeiro mudar seu Value WorkSpaces para uma oferta de pacote maior.
- Antes WorkSpaces de migrar do Windows 7 para o Windows 11, você precisa migrá-lo para o Windows 10. Faça login no Windows 10 pelo WorkSpace menos uma vez antes de migrá-lo para o Windows 11. A migração do Windows 7 WorkSpaces diretamente para o Windows 11 não é suportada.
- Você pode migrar o Windows WorkSpaces que usa o Microsoft Office AWS para um WorkSpaces pacote personalizado com aplicativos do Microsoft 365. Após a migração, sua WorkSpaces assinatura do Microsoft Office será cancelada.
- Você pode migrar o Windows WorkSpaces que usa o Microsoft Office AWS para um WorkSpaces pacote sem assinatura do Office 2016/2019. Após a migração, sua WorkSpaces assinatura do Microsoft Office será cancelada.

Para obter mais informações sobre os WorkSpaces pacotes da Amazon, consulteWorkSpace pacotes e imagens.

O processo de migração recria o WorkSpace usando um novo volume raiz da imagem do pacote de destino e o volume do usuário do último instantâneo disponível do original. WorkSpace Um novo perfil de usuário é gerado durante a migração para melhor compatibilidade. O perfil de usuário antigo é renomeado e, depois, determinados arquivos no perfil de usuário antigo são movidos para o novo perfil de usuário. (Para obter detalhes sobre o que é movido, consulte O que acontece durante a migração.)

O processo de migração leva até uma hora por WorkSpace. Quando você inicia o processo de migração, um novo WorkSpace é criado. Se ocorrer um erro que impeça a migração bem-sucedida, o original WorkSpace será recuperado e retornado ao estado original, e o novo WorkSpace será encerrado.

Sumário

- O que acontece durante a migração
- Práticas recomendadas
- Solução de problemas
- Como a cobrança é afetada
- Migrando um WorkSpace

Limites de migração

- Não é possível migrar para um pacote de experiência de desktop do Windows 7 público ou personalizado. Você também não pode migrar para pacotes do Windows 7 Traga sua própria licença (BYOL).
- Você pode migrar o BYOL WorkSpaces somente para outros pacotes BYOL. Para migrar um BYOL WorkSpace do PCoIP para o WSP, você deve primeiro criar um pacote BYOL com o protocolo WSP. Em seguida, você pode migrar seu PCoIP BYOL WorkSpaces para esse pacote WSP BYOL.
- Você não pode migrar um pacote WorkSpace criado de pacotes públicos ou personalizados para um pacote BYOL.
- Graphics.g4dn, GraphicsPro .g4dn, Graphics e GraphicsPro bundles estão disponíveis somente para o protocolo PCoIP no momento, portanto, Graphics.g4dn, .g4dn, Graphics e Graphics ainda não podem ser migrados para o WSP. GraphicsPro GraphicsPro WorkSpaces
- Atualmente, a migração do Linux não WorkSpaces é suportada.
- Em AWS regiões que oferecem suporte a mais de um idioma, você pode migrar WorkSpaces entre pacotes de idiomas.
- Os pacotes de origem e destino devem ser diferentes. (No entanto, em regiões que oferecem suporte a mais de um idioma, é possível migrar para o mesmo pacote do Windows 10, desde que os idiomas sejam diferentes.) Se você quiser atualizar seu WorkSpace usando o mesmo pacote, reconstrua o em vez disso. WorkSpace
- Você não pode migrar WorkSpaces entre regiões.
- Em alguns casos, se não for possível concluir a migração com êxito, talvez você não receba uma mensagem de erro e pode parecer que o processo de migração não foi iniciado. Se o WorkSpace pacote permanecer o mesmo uma hora após a tentativa de migração, a migração não será bem-sucedida. Entre em contato com o AWS Support Center para obter assistência.

Cenários de migração

A tabela a seguir mostra quais cenários de migração estão disponíveis:

SO de origem	SO de destino	Disponível?
Pacote público ou personalizado do Windows 7	Pacote público ou personalizado do Windows 10	Sim
Pacote personalizado do Windows 7	Pacote público do Windows 7	Não
Pacote personalizado do Windows 7	Pacote personalizado do Windows 7	Não
Pacote público do Windows 7	Pacote personalizado do Windows 7	Não
Pacote público ou personalizado do Windows 10	Pacote público ou personalizado do Windows 7	Não
Pacote público ou personalizado do Windows 10	Pacote personalizado do Windows 10	Sim
Pacote BYOL do Windows 7	Pacote BYOL do Windows 7	Não
Pacote BYOL do Windows 7	Pacote BYOL do Windows 10	Sim
Pacote BYOL do Windows 10	Pacote BYOL do Windows 7	Não
Pacote BYOL do Windows 10	Pacote BYOL do Windows 10	Sim
Pacote público do Windows 10 baseado em Windows Server 2016	Pacote público do Windows 10 baseado em Windows Server 2019 	Sim

SO de origem	SO de destino	Disponível?
Pacote público do Windows 10 baseado em Windows Server 2019 	Pacote público do Windows 10 baseado em Windows Server 2016	Sim
Pacote BYOL do Windows 10	Pacote BYOL do Windows 11	Sim
Pacote BYOL do Windows 11	Pacote BYOL do Windows 10	Não
Pacote personalizado do Windows 10 baseado em Windows Server 2016	Pacote público do Windows 10 baseado em Windows Server 2019	Sim
Pacote personalizado do Windows 10 baseado em Windows Server 2016	Pacote público do Windows 10 baseado em Windows Server 2022	Sim
Pacote personalizado do Windows 10 baseado em Windows Server 2019	Pacote público do Windows 10 baseado em Windows Server 2022	Sim

Note

O Acesso via Web não está disponível para a ramificação PCoIP do pacote público do Windows 10 baseado em Windows Server 2019.

Important

O pacote público do Windows 10 Plus baseado em Windows Server 2016 inclui o Microsoft Office 2016 e o Worry-Free Business Security Services do Trend Micro. O pacote público do Windows 10 Plus baseado em Windows Server 2019 inclui apenas o Microsoft Office 2019, sem nenhum serviço do Trend Micro.

O que acontece durante a migração

Durante a migração, os dados no volume do usuário (unidade D) são preservados, mas todos os dados no volume raiz (unidade C) são perdidos. Isso significa que nenhum dos aplicativos instalados, configurações e alterações no registro são preservados. A pasta de perfil de usuário antiga é renomeada com o sufixo `.NotMigrated` e um perfil de usuário é criado.

O processo de migração recria a unidade D com base no último snapshot do volume do usuário original. Durante a primeira inicialização do novo WorkSpace, o processo de migração move a `D:\Users\%USERNAME%` pasta original para uma pasta chamada`D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated`. Uma nova pasta `D:\Users\%USERNAME%\` é gerada pelo novo sistema operacional.

Depois que o perfil de usuário é criado, os arquivos nas seguintes pastas do shell de usuário são movidos do perfil `.NotMigrated` antigo para o novo perfil:

- `D:\Users\%USERNAME%\Desktop`
- `D:\Users\%USERNAME%\Documents`
- `D:\Users\%USERNAME%\Downloads`
- `D:\Users\%USERNAME%\Favorites`
- `D:\Users\%USERNAME%\Music`
- `D:\Users\%USERNAME%\Pictures`
- `D:\Users\%USERNAME%\Videos`

Important

O processo de migração tenta mover os arquivos do perfil de usuário antigo para o novo perfil. Todos os arquivos que não foram movidos durante a migração permanecem na pasta `D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated`. Se a migração for bem-sucedida, você poderá ver quais arquivos foram movidos em `C:\Program Files\Amazon\WorkspacesConfig\Logs\MigrationLogs`. É possível mover manualmente todos os arquivos que não foram movidos automaticamente.

Por padrão, os pacotes públicos têm a indexação de pesquisa local desabilitada. Se você quiser habilitá-la, o padrão será pesquisar `C:\Users` e não `D:\Users`, portanto, será necessário ajustar isso também. Se você definiu a indexação de pesquisa local especificamente para `D:\Users\`*`username`* e não para `D:\Users`, então ela pode não

funcionar após a migração para arquivos de usuário que estejam na pasta `D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated`.

Todas as tags atribuídas ao original WorkSpace são transferidas durante a migração e o modo de execução do WorkSpace é preservado. No entanto, o novo WorkSpace recebe um novo WorkSpace ID, nome do computador e endereço IP.

Práticas recomendadas

Antes de migrar um WorkSpace, faça o seguinte:

- Faça backup de todos os dados importantes na unidade C para outro local. Todos os dados na unidade C são apagados durante a migração.
- Certifique-se de que o que está WorkSpace sendo migrado tenha pelo menos 12 horas, para garantir que um instantâneo do volume do usuário tenha sido criado. Na WorkSpaces página Migrate no WorkSpaces console da Amazon, você pode ver a hora do último snapshot. Todos os dados criados após o último snapshot são perdidos durante a migração.
- Para evitar possíveis perdas de dados, certifique-se de que seus usuários se desconectem WorkSpaces e não façam login novamente até que o processo de migração seja concluído. Observe que WorkSpaces não podem ser migrados quando estão no `ADMIN_MAINTENANCE` modo.
- Certifique-se de que o que WorkSpaces você deseja migrar tenha o status de `AVAILABLE`, `STOPPED`, ou `ERROR`.
- Verifique se você tem endereços IP suficientes para o WorkSpaces que você está migrando. Durante a migração, novos endereços IP serão alocados para o. WorkSpaces
- Se você estiver usando scripts para migrar WorkSpaces, migre-os em lotes de no máximo 25 por WorkSpaces vez.

Solução de problemas

- Se os usuários relatarem arquivos ausentes após a migração, verifique se seus arquivos de perfil de usuário não foram movidos durante o processo de migração. É possível ver quais arquivos foram movidos em `C:\Program Files\Amazon\WorkspacesConfig\Logs\MigrationLogs`. Os arquivos que não foram movidos estarão localizados na pasta `D:\Users`

`\%USERNAME%MMddyyTHHmmss%.NotMigrated`. É possível mover manualmente todos os arquivos que não foram movidos automaticamente.

- Se você estiver usando a API para migrar WorkSpaces e a migração não for bem-sucedida, a WorkSpace ID de destino retornada pela API não será usada e ela ainda WorkSpace terá a WorkSpace ID original.
- Se uma migração não for concluída com êxito, verifique o Active Directory para ver se ele foi limpo adequadamente. Talvez seja necessário remover manualmente o WorkSpaces que não é mais necessário.

Como a cobrança é afetada

Durante o mês em que a migração ocorre, são cobrados valores rateados tanto pelo novo quanto pelo original. WorkSpaces Por exemplo, se você migrar WorkSpace de A para WorkSpace B em 10 de maio, você será WorkSpace cobrado por A de 1º de maio a 10 de maio e por WorkSpace B de 11 a 30 de maio.

> **Note**
>
> Se você estiver migrando um WorkSpace para um tipo de pacote diferente (por exemplo, de Desempenho para Potência ou Valor para Padrão), o tamanho do volume raiz (unidade C) e do volume do usuário (unidade D) poderá aumentar durante o processo de migração. Se necessário, o volume raiz aumentará para corresponder ao tamanho padrão do volume raiz para o novo pacote. No entanto, se você já tiver especificado um tamanho (maior ou menor) para o volume do usuário diferente do padrão para o pacote original, esse mesmo tamanho de volume de usuário será mantido durante o processo de migração. Caso contrário, o processo de migração usa o maior tamanho do volume WorkSpace do usuário de origem e o tamanho padrão do volume do usuário para o novo pacote.

Migrando um WorkSpace

Você pode migrar WorkSpaces por meio do WorkSpaces console da Amazon, do AWS CLI ou da WorkSpaces API da Amazon.

Para migrar um WorkSpace

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.

2. No painel de navegação, selecione WorkSpaces.
3. Selecione seu WorkSpace e escolha Ações, Migrar. WorkSpaces
4. Em Pacotes, selecione o pacote para o qual você gostaria de migrar. WorkSpace

> **Note**
>
> Para migrar um BYOL WorkSpace do PCoIP para o WSP, você deve primeiro criar um pacote BYOL com o protocolo WSP. Em seguida, você pode migrar seu PCoIP BYOL WorkSpaces para esse pacote WSP BYOL.

5. Escolha Migrar. WorkSpaces

   Um novo WorkSpace com o status de `PENDING` aparece no WorkSpaces console da Amazon. Quando a migração é concluída, o original WorkSpace é encerrado e o status do novo WorkSpace é definido como. `AVAILABLE`
6. (Opcional) Para excluir quaisquer pacotes personalizados e imagens que não são mais necessários, consulte Excluir um WorkSpaces pacote ou imagem personalizada.

Para migrar WorkSpaces peloAWS CLI, use o comando migrate-workspace. Para migrar WorkSpaces pela WorkSpaces API da Amazon, consulte a Referência MigrateWorkSpaceda WorkSpaces API da Amazon.

Excluir um WorkSpace

Quando não precisar mais de um WorkSpace, você poderá excluí-lo. Você também pode excluir os recursos relacionados.

> **Warning**
>
> A exclusão de um WorkSpace é uma ação permanente e não pode ser desfeita. Os dados do usuário do WorkSpace não são persistidos e são destruídos. Para obter ajuda para fazer backup dos dados do usuário, entre em contato com o AWS Support.

> **Note**
>
> O Simple AD e o AD Connector estão disponíveis gratuitamente para uso com os WorkSpaces. Se não houver WorkSpaces sendo usados com o diretório do Simple AD ou do AD Connector por 30 dias consecutivos, o registro desse diretório será automaticamente cancelado para uso com o Amazon WorkSpaces, e você será cobrado por esse diretório de acordo com os Preços do AWS Directory Service.
> Para excluir diretórios vazios, consulte Excluir o diretório dos WorkSpaces. Se você excluir o diretório do Simple AD ou do AD Connector, sempre poderá criar um novo quando quiser começar a usar o WorkSpaces novamente.

Para excluir um WorkSpace

Você pode excluir um WorkSpace que esteja em qualquer estado, exceto Suspenso.

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione WorkSpaces.
3. Selecione seu WorkSpace e clique em Excluir.
4. Quando a confirmação for solicitada, clique em Excluir. A exclusão de um WorkSpace leva aproximadamente 5 minutos. Durante a exclusão, o status do WorkSpace é definido como Encerrando. Quando a exclusão for concluída, o WorkSpace desaparecerá do console.
5. (Opcional) Para excluir todos os pacotes personalizados e imagens que não serão mais usados, consulte Excluir um WorkSpaces pacote ou imagem personalizada.
6. (Opcional) Depois de excluir todos os WorkSpaces em um diretório, você pode excluir o diretório. Para obter mais informações, consulte Excluir o diretório dos WorkSpaces.
7. (Opcional) Depois de excluir todos os recursos na rede virtual privada (VPC) para seu diretório, você pode excluir a VPC e liberar o endereço IP elástico usado para o gateway NAT. Para obter mais informações, consulte Deleting your VPC e Trabalhar com endereços IP elásticos no Guia do usuário do Amazon VPC.

Como excluir um WorkSpace usando o AWS CLI

Use o comando terminate-workspaces.

WorkSpace pacotes e imagens

Um WorkSpace pacote é uma combinação de um sistema operacional e recursos de armazenamento, computação e software. Ao lançar um WorkSpace, você seleciona o pacote que atende às suas necessidades. Os pacotes padrão disponíveis para WorkSpaces são chamados de pacotes públicos. Para obter mais informações sobre os vários pacotes públicos disponíveis WorkSpaces, consulte Amazon WorkSpaces Bundles.

Se você lançou um Windows ou Linux WorkSpace e o personalizou, você pode criar uma imagem personalizada a partir disso WorkSpace.

Uma imagem personalizada contém somente o sistema operacional, o software e as configurações do WorkSpace. Um pacote personalizado é uma combinação dessa imagem personalizada e do hardware a partir do qual um WorkSpace pode ser iniciado.

Depois de criar uma imagem personalizada, você pode criar um pacote personalizado que combina a WorkSpace imagem personalizada e a configuração subjacente de computação e armazenamento selecionada. Em seguida, você pode especificar esse pacote personalizado ao iniciar um novo WorkSpaces para garantir que o novo WorkSpaces tenha a mesma configuração consistente (hardware e software).

Se precisar realizar atualizações de software ou instalar software adicional no seu WorkSpaces, você pode atualizar seu pacote personalizado e usá-lo para reconstruir seu. WorkSpaces

WorkSpaces suporta vários sistemas operacionais (OS), protocolos de streaming e pacotes diferentes. A tabela a seguir fornece informações sobre licenciamento, protocolos de streaming e pacotes compatíveis com cada sistema operacional.

Sistema operacional	Licenças	Protocolos de streaming	Pacotes compatíveis	Política de ciclo de vida/ data de aposentadoria
Windows Server 2016	Incluído	WSP, PCoIP	Valor, padrão, desempenho, potência, gráficos (obsoleto	12 de janeiro de 2027

Sistema operacional	Licenças	Protocolos de streaming	Pacotes compatíveis	Política de ciclo de vida/ data de aposentadoria
			s) PowerPro, gráficos.g4dn GraphicsPro, .g4dn GraphicsPro	
Windows Server 2019	Incluído	WSP, PCoIP	Valor, padrão, desempenho, potência, gráficos (obsoletos) PowerPro, gráficos.g4dn GraphicsPro, .g4dn GraphicsPro	9 de janeiro de 2029
Windows Server 2022	Incluído	WSP, PCoIP	Padrão, Desempenho, Potência, Gráficos (descontinuados) PowerPro, Gráficos.g4dn GraphicsPro, .g4dn GraphicsPro	14 de outubro de 2013
Windows 10	Traga a sua própria licença (BYOL)	WSP, PCoIP	Valor, padrão, desempenho, potência, gráficos (obsoletos) PowerPro, gráficos.g4dn GraphicsPro, .g4dn GraphicsPro	Em apoio
Windows 11	Traga a sua própria licença (BYOL)	VESPA	Padrão, desempenho, potência, PowerPro	Em apoio
Amazon Linux 2	Incluído	WSP, PCoIP	Valor, padrão, desempenho, potência, PowerPro	30 de junho de 2025

Sistema operacional	Licenças	Protocolos de streaming	Pacotes compatíveis	Política de ciclo de vida/ data de aposentadoria
Ubuntu 22.04 LTS	Incluído	VESPA	Valor, padrão, desempenho, potência e PowerPro gráficos. G4dn, .g4dn GraphicsPro	Junho de 2032

> **Note**
>
> - As versões do sistema operacional que não são mais suportadas pelo fornecedor não têm garantia de funcionamento e não são suportadas pelo AWS suporte.
> - Para WorkSpaces execução no sistema operacional Windows, os pacotes gráficos suportam apenas o protocolo de streaming PCoIP.

Conteúdo

Opções de pacote

Antes de selecionar um pacote, garanta que ele é compatível com o protocolo, o sistema operacional, a rede e o tipo de computação do seu WorkSpaces. Para obter mais informações sobre

protocolos, consulte Protocolos do Amazon WorkSpaces. Para obter mais informações sobre redes, consulte Requisitos de rede do cliente do Amazon WorkSpaces.

> **Note**
>
> - Recomendamos não exceder a latência máxima de rede de 250 ms para WorkSpaces que utilizam PCoIP. Para obter a melhor experiência do usuário com WorkSpaces que utilizam PCoIP, recomendamos manter a latência da rede abaixo de 100 ms. Quando o tempo de ida e volta (RTT) exceder 375 ms, a conexão do cliente do WorkSpaces será encerrada. Para obter a melhor experiência do usuário com o WorkSpaces Streaming Protocol (WSP), recomendamos manter o RTT abaixo de 250 ms. Se o RTT estiver entre 250 ms e 400 ms, o usuário poderá acessar o WorkSpace, mas a performance diminuirá significativamente.
> - Recomendamos testar a performance dos pacotes que você deseja escolher em um ambiente de teste, executando e usando aplicações que repliquem as tarefas diárias dos usuários.

> **Important**
>
> - O pacote Graphics deixará de receber suporte a partir de 30 de novembro de 2023. Recomendamos mudar para o pacote Graphics.g4dn para WorkSpaces que usam o pacote Graphics.
> - Os pacotes Graphics e GraphicsPro ainda não estão disponíveis na região Ásia-Pacífico (Mumbai).

O WorkSpaces oferece os pacotes a seguir. Para obter informações sobre pacotes do WorkSpaces, consulte Pacotes do Amazon WorkSpaces.

Pacote Value

Esse pacote é ideal para:

- Edição básica de texto e entrada de dados
- Navegação na web com uso leve
- Mensagens instantâneas

Esse pacote não é recomendado para processamento de texto, audioconferência, videoconferência, compartilhamento de tela, ferramenta de desenvolvimento de software, aplicações de business intelligence e aplicações gráficas.

Pacote Standard

Esse pacote é ideal para:

- Edição básica de texto e entrada de dados
- Navegação na web
- Mensagens instantâneas
- E-mail

Esse pacote não é recomendado para audioconferência, videoconferência, compartilhamento de tela, processamento de texto, ferramenta de desenvolvimento de software, aplicações de business intelligence e aplicações gráficas

Pacote Performance

Esse pacote é ideal para:

- Navegação na web
- Processamento de texto
- Mensagens instantâneas
- E-mail
- Planilhas
- Processamento de áudio
- Material didático eletrônico

Esse pacote não é recomendado para videoconferência, compartilhamento de tela, ferramenta de desenvolvimento de software, aplicações de business intelligence e aplicações gráficas

Pacote Power

Esse pacote é ideal para:

- Navegação na web

- Processamento de texto
- E-mail
- Mensagens instantâneas
- Planilhas
- Processamento de áudio
- Desenvolvimento de software (ambiente de desenvolvimento integrado [IDE])
- Processamento de dados em nível básico e médio
- Audioconferência e videoconferência

Esse pacote não é recomendado para compartilhamento de tela, ferramenta de desenvolvimento de software, aplicações de business intelligence e aplicações gráficas.

Pacote PowerPro

Esse pacote é ideal para:

- Navegação na web
- Processamento de texto
- E-mail
- Mensagens instantâneas
- Planilhas
- Processamento de áudio
- Desenvolvimento de software (ambiente de desenvolvimento integrado [IDE])
- Data warehousing
- Aplicações de business intelligence
- Audioconferência e videoconferência

Esse pacote não é recomendado para treinamento de modelos de machine learning e aplicações gráficas

Pacote GraphicsPro

Esse pacote oferece um nível básico de performance gráfica e alto nível de performance de CPU e memória para WorkSpaces. Ele é ideal para:

- Navegação na web
- Processamento de texto
- E-mail
- Mensagens instantâneas
- Planilhas
- Audioconferência
- Desenvolvimento de software (ambiente de desenvolvimento integrado [IDE])
- Data warehousing
- Aplicações de business intelligence
- Design gráfico
- Processamento de imagens

Este pacote não é recomendado para audioconferência, videoconferência, renderização em 3D e design fotorrealista

Pacote Graphics.g4dn

Esse pacote oferece um alto nível de performance gráfica e um nível moderado de performance de CPU e memória para WorkSpaces, sendo ideal para:

- Navegação na web
- Processamento de texto
- E-mail
- Planilhas
- Mensagens instantâneas
- Audioconferência
- Desenvolvimento de software (ambiente de desenvolvimento integrado [IDE])
- Processamento de dados em nível básico e médio
- Data warehousing
- Aplicações de business intelligence
- Design gráfico
- CAD/CAM (projeto auxiliado por computador/manufatura auxiliada por computador)

Esse pacote não é recomendado para audioconferência, videoconferência, renderização 3D, design fotorrealista e treinamento de modelos de machine learning

GraphicsPro.g4dn

Pacote GraphicsPro.g4dn

Esse pacote oferece um alto nível de performance gráfica, performance de CPU e memória para WorkSpaces, sendo ideal para:

- Navegação na web
- Processamento de texto
- E-mail
- Planilhas
- Mensagens instantâneas
- Audioconferência
- Desenvolvimento de software (ambiente de desenvolvimento integrado [IDE])
- Processamento de dados em nível básico e médio
- Data warehousing
- Aplicações de business intelligence
- Design gráfico
- CAD/CAM (projeto auxiliado por computador/manufatura auxiliada por computador)
- Transcodificação de vídeo
- Renderização 3D
- Design fotorrealista
- Streaming de jogos
- Treinamento de modelos de machine learning (ML) inferência de ML

Esse pacote não é recomendado para audioconferência e videoconferência.

Crie uma WorkSpaces imagem e um pacote personalizados

Se você lançou um Windows ou Linux WorkSpace e o personalizou, você pode criar uma imagem personalizada e pacotes personalizados a partir disso WorkSpace.

Uma imagem personalizada contém somente o sistema operacional, o software e as configurações do WorkSpace. Um pacote personalizado é uma combinação dessa imagem personalizada e do hardware a partir do qual um WorkSpace pode ser iniciado.

> **Note**
>
> Certifique-se de esperar pelo menos 2 horas após excluir um pacote antes de criar um novo pacote com o mesmo nome.

Depois de criar uma imagem personalizada, será possível criar um pacote personalizado que combine a imagem personalizada e a configuração de computação e armazenamento subjacente selecionada. Em seguida, você pode especificar esse pacote personalizado ao iniciar um novo WorkSpaces para garantir que o novo WorkSpaces tenha a mesma configuração consistente (hardware e software).

É possível usar a mesma imagem personalizada para criar vários pacotes personalizados selecionando diferentes opções de computação e armazenamento para cada pacote.

> **Important**
>
> - Se você planeja criar uma imagem a partir do Windows 10 WorkSpace, observe que a criação de imagens não é suportada nos sistemas Windows 10 que foram atualizados de uma versão do Windows 10 para uma versão mais recente do Windows 10 (uma atualização de recurso/versão do Windows). No entanto, as atualizações cumulativas ou de segurança do Windows são suportadas pelo processo de criação de WorkSpaces imagens.
> - Depois de 14 de janeiro de 2020, as imagens não podem ser criadas de pacotes públicos do Windows 7. Talvez você queira considerar a migração do Windows 7 WorkSpaces para o Windows 10. Para ter mais informações, consulte Migre um WorkSpace.
> - O pacote Graphics deixará de receber suporte a partir de 30 de novembro de 2023. Recomendamos migrar seu pacote para o WorkSpaces Graphics.g4dn. Para ter mais informações, consulte Migre um WorkSpace.
> - No momento, gráficos e GraphicsPro pacotes não estão disponíveis na região Ásia-Pacífico (Mumbai).

- Os volumes de armazenamento de pacotes personalizados não podem ser menores que os volumes de armazenamento de imagens.

Os pacotes personalizados custam o mesmo que os pacotes públicos pelos quais são criados. Para obter mais informações sobre preços, consulte Amazon WorkSpaces Pricing.

Conteúdo

Requisitos para criar imagens personalizadas do Windows

> **Note**
>
> Atualmente, o Windows define 1 GB como 1.073.741.824 bytes. Os clientes precisarão garantir que tenham mais de 12.884.901.888 bytes (ou 12 GiB) livres na unidade C e que o perfil do usuário tenha menos de 10.737.418.240 bytes (ou 10 GiB) para criar uma imagem de a. WorkSpace

- O status do WorkSpace deve ser Disponível e seu estado de modificação deve ser Nenhum.
- Todos os aplicativos e perfis de usuário em WorkSpaces imagens devem ser compatíveis com o Microsoft Sysprep.
- Todas as aplicações a serem incluídas na imagem devem ser instaladas na unidade `C`.
- Para o Windows 7 WorkSpaces, e seu tamanho total (arquivos e dados) deve ser menor que 10 GB.
- Para o Windows 7 WorkSpaces, a `C` unidade deve ter pelo menos 12 GB de espaço disponível.

- Todos os serviços de aplicativos executados no WorkSpace devem usar uma conta do sistema local em vez de credenciais de usuário do domínio. Por exemplo, você não pode ter uma instalação do Microsoft SQL Server Express em execução com as credenciais de um usuário do domínio.
- Eles não WorkSpace devem ser criptografados. A criação de imagens a partir de uma imagem criptografada não WorkSpace é suportada atualmente.
- Os componentes a seguir são necessários em uma imagem. Sem esses componentes, o WorkSpaces que você inicia a partir da imagem não funcionará corretamente. Para ter mais informações, consulte the section called “Configuração necessária”.
  - Windows PowerShell versão 3.0 ou posterior
  - Serviços de desktop remoto
  - AWS Controladores fotovoltaicos
  - Gerenciamento remoto do Windows (WinRM)
  - Agentes e drivers do Teradici PCoIP
  - Agentes e drivers do STXHD
  - AWS e WorkSpaces certificados
  - Agente do Skylight

Requisitos para criar imagens personalizadas do Linux

- O status do WorkSpace deve ser Disponível e seu estado de modificação deve ser Nenhum.
- Todas as aplicações a serem incluídas na imagem devem ser instaladas fora do volume do usuário (o diretório `/home`).
- O volume raiz (/) deve estar com menos de 97% de sua capacidade ocupada.
- Eles não WorkSpace devem ser criptografados. A criação de imagens a partir de uma imagem criptografada não WorkSpace é suportada atualmente.
- Os componentes a seguir são necessários em uma imagem. Sem esses componentes, o WorkSpaces que você inicia a partir da imagem não funcionará corretamente:
  - Cloud-init
  - Agentes e drivers do Teradici PCoIP ou WSP
  - Agente do Skylight

Práticas recomendadas

Antes de criar uma imagem a partir de um WorkSpace, faça o seguinte:

- Use uma VPC separada que não esteja conectada ao ambiente de produção.
- Implemente o WorkSpace em uma sub-rede privada e use uma instância NAT para tráfego de saída.
- Use um pequeno diretório do Simple AD.
- Use o menor tamanho de volume para a fonte e WorkSpace, em seguida, ajuste o tamanho do volume conforme necessário ao criar o pacote personalizado.
- Instale todas as atualizações do sistema operacional (exceto as atualizações de recursos/versões do Windows) e todas as atualizações de aplicativos no. WorkSpace Para obter mais informações, consulte a Observação importante no início deste tópico.
- Exclua dados em cache do WorkSpace que não devem ser incluídos no pacote (por exemplo, histórico do navegador, arquivos em cache e cookies do navegador).
- Exclua as configurações WorkSpace que não devem ser incluídas no pacote (por exemplo, perfis de e-mail).
- Alterne para configurações de endereço IP dinâmico usando DHCP.
- Verifique se você não excedeu sua cota de WorkSpace imagens permitidas em uma região. Por padrão, você tem permissão para 40 WorkSpace imagens por região. Se você atingiu essa cota, ocorrerão falhas em novas tentativas de criar uma imagem. Para solicitar um aumento de cota, use o formulário WorkSpaces Limites.
- Verifique se você não está tentando criar uma imagem a partir de uma imagem criptografada WorkSpace. A criação de imagens a partir de uma imagem criptografada não WorkSpace é suportada atualmente.
- Se você estiver executando algum software antivírus no WorkSpace, desative-o enquanto estiver tentando criar uma imagem.
- Se você tiver um firewall habilitado no seu WorkSpace, certifique-se de que ele não esteja bloqueando nenhuma porta necessária. Para ter mais informações, consulte Requisitos de endereço IP e porta para WorkSpaces.
- Para Windows WorkSpaces, não configure nenhum Objeto de Política de Grupo (GPOs) antes da criação da imagem.
- Para Windows WorkSpaces, não personalize o perfil de usuário padrão (`C:\Users\Default`) antes de criar uma imagem. Recomendamos fazer personalizações no perfil do usuário por meio

de GPOs e aplicá-los após a criação da imagem. Os GPOs podem ser facilmente modificados ou revertidos e, portanto, são menos propensos a erros do que as personalizações feitas no perfil do usuário padrão.

- Para Linux WorkSpaces, consulte também o whitepaper "Best Practices to Prepare Your Amazon WorkSpaces for Linux Images".
- Se você quiser usar cartões inteligentes no Linux WorkSpaces com o protocolo de WorkSpaces streaming (WSP) ativado, consulte Usar cartões inteligentes para autenticação as personalizações que você deve fazer no Linux WorkSpace antes de criar sua imagem.
- Certifique-se de atualizar os drivers de dependência de rede, como ENA, NVMe e drivers PV, no seu. WorkSpaces Você deve fazer isso pelo menos uma vez a cada 6 meses. Para obter mais informações, consulte Instalar ou atualizar o driver do Elastic Network Adapter (ENA)Drivers do AWS NVMe para instâncias do Windows e Atualizar os drivers fotovoltaicos nas instâncias do Windows.
- Certifique-se de atualizar periodicamente os agentes EC2Config, EC2Launch e EC2Launch V2 para as versões mais recentes. Você deve fazer isso pelo menos uma vez a cada 6 meses. Para obter mais informações, consulte Atualizar EC2Config e EC2Launch.

(Opcional) Etapa 1: Especificar um formato de nome de computador personalizado para a imagem

Para as imagens WorkSpaces lançadas a partir de suas imagens personalizadas ou Bring Your Own License (BYOL), você pode especificar um prefixo personalizado para o formato do nome do computador em vez de usar o formato padrão do nome do computador. Para especificar um prefixo personalizado, siga o procedimento adequado para seu tipo de imagem.

Como especificar um formato de nome de computador personalizado para imagens personalizadas

> **Note**
>
> Por padrão, o formato do nome do computador para o Windows 10 WorkSpaces é `DESKTOP-XXXXX` e para o Windows 11 WorkSpaces,`WORKSPA-XXXXX`.

1. No WorkSpace que você está usando para criar sua imagem personalizada, abra `C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xml` no Bloco de notas ou em outro editor de texto. Para obter mais informações sobre como trabalhar com o

arquivo `Unattend.xml`, consulte Arquivos de resposta (unattend.xml) na documentação da Microsoft.

> **Note**
>
> Para acessar a unidade C: a partir do Explorador de Arquivos do Windows em seu WorkSpace, insira **`C:\`** na barra de endereço.

2. Na seção `<settings pass="specialize">`, verifique se `<ComputerName>` está definido como um asterisco (`*`). Se `<ComputerName>` estiver definido com qualquer outro valor, as configurações personalizadas do nome do computador serão ignoradas. Para obter mais informações sobre a `<ComputerName>` configuração, consulte ComputerNamea documentação da Microsoft.
3. Na seção `<settings pass="specialize">`, defina `<RegisteredOrganization>` e `<RegisteredOwner>` com seus valores de preferência.

   Durante o Sysprep, os valores especificados para `<RegisteredOwner>` e `<RegisteredOrganization>` são concatenados, e os primeiros sete caracteres da string combinada são usados para criar o nome do computador. *Por exemplo, se você especificar* ***Amazon.com*** *para <RegisteredOrganization> e* ***EC2*** *para<RegisteredOwner>, os nomes dos computadores WorkSpaces criados a partir do seu pacote personalizado começarão com EC2AMAZ- xxxxxxx.*

   > **Note**
   >
   > Os valores `<RegisteredOrganization>` e `<RegisteredOwner>` na seção `<settings pass="oobeSystem">` são ignorados pelo Sysprep.

4. Salve as alterações no arquivo `Unattend.xml`.

Como especificar um formato de nome de computador personalizado para imagens BYOL

1. Se você estiver usando o Windows 10, abra `C:\Program Files\Amazon\Ec2ConfigService\Sysprep2008.xml` no Bloco de notas ou em outro editor de texto. Se você estiver usando o Windows 11, abra `C:\ProgramData\Amazon\EC2Launch\sysprep\OOBE_unattend.xml`.

2. Na seção `<settings pass="specialize">`, remova o comentário `<ComputerName>*</ComputerName>` e garanta que `<ComputerName>` está definido como um asterisco (*). Se `<ComputerName>` estiver definido com qualquer outro valor, as configurações personalizadas do nome do computador serão ignoradas. Para obter mais informações sobre a `<ComputerName>` configuração, consulte ComputerNamea documentação da Microsoft.
3. Na seção `<settings pass="specialize">`, defina `<RegisteredOrganization>` e `<RegisteredOwner>` com seus valores de preferência.

   Durante o Sysprep, os valores especificados para `<RegisteredOwner>` e `<RegisteredOrganization>` são concatenados, e os primeiros sete caracteres da string combinada são usados para criar o nome do computador. *Por exemplo, se você especificar **Amazon.com** para <RegisteredOrganization> e **EC2** para<RegisteredOwner>, os nomes dos computadores WorkSpaces criados a partir do seu pacote personalizado começarão com EC2AMAZ- xxxxxxx.*

   > **Note**
   >
   > Os valores `<RegisteredOrganization>` e `<RegisteredOwner>` na seção `<settings pass="oobeSystem">` são ignorados pelo Sysprep.

4. Se você estiver usando o Windows 10, salve as alterações no arquivo `Sysprep2008.xml`. Se você estiver usando o Windows 11, salve as alterações em `OOBE_unattend.xml`

Etapa 2: Executar o Verificador de Imagens

> **Note**
>
> O Image Checker está disponível somente para Windows WorkSpaces. Se você estiver criando uma imagem a partir de um Linux WorkSpace, vá paraEtapa 3: Criar uma imagem e um pacote personalizados.

Para confirmar se o Windows WorkSpace atende aos requisitos de criação de imagens, recomendamos executar o Verificador de Imagem. O Image Checker executa uma série de testes sobre o WorkSpace que você deseja usar para criar sua imagem e fornece orientação sobre como resolver quaisquer problemas encontrados.

> **Important**
>
> - Eles WorkSpace devem passar por todos os testes executados pelo Image Checker antes de poder usá-lo para criar imagens.
> - Antes de executar o Image Checker, verifique se as atualizações cumulativas e de segurança mais recentes do Windows estão instaladas no seu. WorkSpace

Para obter o Verificador de Imagens, siga um destes procedimentos:

- Reinicie seu. WorkSpace O Verificador de imagens é baixado automaticamente durante a reinicialização e instalado em `C:\Program Files\Amazon\ImageChecker.exe`.
- Faça o download do Amazon WorkSpaces Image Checker em https://tools.amazonworkspaces.com/ ImageChecker .zip e extraia o arquivo. `ImageChecker.exe` Copie esse arquivo em `C:\Program Files\Amazon\`.

Como executar o Verificador de Imagens

1. Abra o arquivo `C:\Program Files\Amazon\ImageChecker.exe`.
2. Na caixa de diálogo Amazon WorkSpaces Image Checker, escolha Executar.
3. Após a conclusão de cada teste, você pode visualizar o status do teste.

   Para qualquer teste com o status FAILED (Com falha), selecione Info (Informações) para exibir informações sobre como resolver o problema que provocou a falha. Para obter mais informações sobre como resolver esses problemas, consulte Dicas para resolver problemas detectados pelo Verificador de Imagens.

   Se algum teste exibir o status WARNING (Aviso), selecione o botão Fix all warnings (Corrigir todos os avisos).

   A ferramenta gera um arquivo de log de saída no mesmo diretório onde o Verificador de Imagens está localizado. Por padrão, esse arquivo está localizado em `C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log`.

> **Tip**
>
> Não exclua esse arquivo de log. Se ocorrer um problema, esse arquivo de log poderá ser útil na solução de problemas.

4. Se aplicável, resolva quaisquer problemas que causem falhas e avisos no teste e repita o processo de execução do Image Checker até que WorkSpace ele passe em todos os testes. Todas as falhas e avisos devem ser resolvidos para que você possa criar uma imagem.
5. Depois de WorkSpace passar em todos os testes, você verá uma mensagem de validação bem-sucedida. Agora você está pronto para criar um pacote personalizado.

Dicas para resolver problemas detectados pelo Verificador de Imagens

Além de consultar as dicas a seguir para resolver problemas detectados pelo Verificador de imagens, verifique o arquivo de log do Verificador de imagens em `C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log`.

PowerShell a versão 3.0 ou posterior deve ser instalada

Instale a versão mais recente do Microsoft Windows PowerShell.

> **Important**
>
> A política de PowerShell execução de um WorkSpace deve ser definida para permitir RemoteSignedscripts. Para verificar a política de execução, execute o ExecutionPolicy PowerShell comando Get-. Se a política de execução não estiver definida como Irrestrita ou RemoteSigned, execute o ExecutionPolicy RemoteSigned comando Set- ExecutionPolicy — para alterar o valor da política de execução. A RemoteSignedconfiguração permite a execução de scripts na Amazon WorkSpaces, o que é necessário para criar uma imagem.

Somente as unidades C e D podem estar presentes

Somente as `D` unidades `C` e podem estar presentes em uma WorkSpace que é usada para geração de imagens. Remova todas as outras unidades, incluindo unidades virtuais.

Nenhuma reinicialização pendente devido às atualizações do Windows pode ser detectada

- O processo de criação de imagem não pode ser executado até que o Windows seja reinicializado para concluir a instalação de atualizações de segurança ou cumulativas. Reinicie o Windows para aplicar essas atualizações e certifique-se de que nenhuma outra atualização de segurança ou cumulativa do Windows precise ser instalada.
- Não há suporte para a criação de imagens nos sistemas Windows 10 que foram atualizados de uma versão do Windows 10 para uma mais recente (uma atualização de recurso/versão do Windows). No entanto, as atualizações cumulativas ou de segurança do Windows são suportadas pelo processo de criação de WorkSpaces imagens.

O arquivo Sysprep deve existir e não pode estar em branco

Se houver problemas com o arquivo Sysprep, entre em contato com o AWS Support Center para reparar seu EC2Config ou EC2Launch.

O tamanho do perfil do usuário deve ser inferior a 10 GB

Para o Windows 7 WorkSpaces, o perfil do usuário (`D:\Users\`*`username`*) deve ter menos de 10 GB no total. Remova os arquivos conforme necessário para reduzir o tamanho do perfil do usuário.

A unidade C deve ter espaço livre suficiente

Para o Windows 7 WorkSpaces, você deve ter pelo menos 12 GB de espaço livre na unidade`C`. Remova os arquivos conforme necessário para liberar espaço na unidade `C`. Para o Windows 10 WorkSpaces, ignore se você receber uma `FAILED` mensagem e o espaço em disco estiver acima de 2 GB.

Nenhum serviço pode estar em execução em uma conta de domínio

Para executar o processo de criação de imagem, nenhum serviço no WorkSpace pode ser executado em uma conta de domínio. Todos os serviços devem estar em execução em uma conta local.

Como executar serviços em uma conta local

1. Abra `C:\Program Files\Amazon\ImageChecker_`*`yyyyMMddhhmmss`*`.log` e localize a lista de serviços que estão em execução em uma conta de domínio.
2. Na caixa de pesquisa do Windows, digite **`services.msc`** para abrir o Gerenciador de Serviços do Windows.

3. Em Log On As (Fazer login como), procure os serviços que estão em execução em contas de domínio. (Os serviços executados como Local System (Sistema local), Local Service (Serviço local) ou Network Service (Serviço de rede) não interferem na criação de imagens.)
4. Selecione um serviço que esteja em execução em uma conta de domínio e escolha Action (Ação), Properties (Propriedades).
5. Abra a guia Log On (Fazer login). Em Log on as (Fazer login como), escolha Local System account (Conta do sistema local).
6. Escolha OK.

O WorkSpace deve ser configurado para usar DHCP

Você deve configurar todos os adaptadores de rede no WorkSpace para usar DHCP em vez de endereços IP estáticos.

Como definir todos os adaptadores de rede para usar DHCP

1. Na caixa de pesquisa do Windows, digite **`control panel`** para abrir o Painel de Controle.
2. Escolha Rede e Internet.
3. Escolha Central de Rede e Compartilhamento.
4. Escolha Alterar as configurações do adaptador e selecione um adaptador.
5. Escolha Alterar as configurações desta conexão.
6. Na guia Rede selecione Protocolo TCP/IP Versão 4 (TCP/IPv4) e, depois, escolha Propriedades.
7. Na caixa de diálogo Propriedades de Protocolo TCP/IP Versão 4 (TCP/IPv4) selecione Obter um endereço IP automaticamente.
8. Escolha OK.
9. Repita esse processo para todos os adaptadores de rede no WorkSpace.

Os Serviços de área de trabalho remota devem estar habilitados

O processo de criação de imagem requer que os Serviços de área de trabalho remota sejam habilitados.

Como habilitar os Serviços de área de trabalho remota

1. Na caixa de pesquisa do Windows, digite **`services.msc`** para abrir o Gerenciador de Serviços do Windows.

2. Na coluna Name (Nome) localize Remote Desktop Services (Serviços de área de trabalho remota).
3. Selecione Remote Desktop Services (Serviços de área de trabalho remota) e, depois, escolha Action (Ação), Properties (Propriedades).
4. Na guia General (Geral), em Startup type (Tipo de inicialização), escolha Manual ou Automatic (Automático).
5. Escolha OK.

Deve existir um perfil do usuário

O WorkSpace que você está usando para criar imagens deve ter um perfil de usuário (`D:\Users\username`). Se ocorrer uma falha nesse teste, entre em contato com o AWS Support Center para obter assistência.

O caminho da variável de ambiente deve ser configurado corretamente

O caminho da variável de ambiente para a máquina local não tem entradas para System32 e para Windows PowerShell. Essas entradas são necessárias para a execução do processo de criação de imagem.

Como configurar o caminho da variável de ambiente

1. Na caixa de pesquisa do Windows, insira **`environment variables`** e escolha Edit the system environment variables (Editar as variáveis de ambiente do sistema).
2. Na caixa de diálogo System Properties (Propriedades do sistema), abra a guia Advanced (Avançado) e escolha Environment Variables (Variáveis de ambiente).
3. Na caixa de diálogo Environment Variables (Variáveis de ambiente), em System variables (Variáveis de sistema), selecione a entrada Path (Caminho) e escolha Edit (Editar).
4. Escolha New (Novo) e adicione o seguinte caminho:

   ```
   C:\Windows\System32
   ```

5. Escolha New (Novo) novamente e adicione o seguinte caminho:

   ```
   C:\Windows\System32\WindowsPowerShell\v1.0\
   ```

6. Escolha OK.
7. Reinicie WorkSpace o.

> **Tip**
>
> A ordem em que os itens aparecem no caminho da variável de ambiente é importante. Para determinar a ordem correta, talvez você queira comparar o caminho da sua variável de ambiente WorkSpace com um de uma instância recém-criada WorkSpace ou nova do Windows.

O instalador de módulos do Windows deve estar habilitado

O processo de criação de imagem requer que o serviço Instalador de módulos do Windows esteja habilitado.

Como habilitar o serviço Instalador de módulos do Windows

1. Na caixa de pesquisa do Windows, digite **`services.msc`** para abrir o Gerenciador de Serviços do Windows.
2. Na coluna Name (Nome), localize Windows Modules Installer (Instalador de módulos do Windows).
3. Selecione Windows Modules Installer (Instalador de módulos do Windows) e, depois, escolha Action (Ação), Properties (Propriedades).
4. Na guia General (Geral), em Startup type (Tipo de inicialização), escolha Manual ou Automatic (Automático).
5. Escolha OK.

O Amazon SSM Agent deve ser desativado

O processo de criação de imagem requer que o serviço Amazon SSM Agent seja desativado.

Como desativar o serviço Amazon SSM Agent

1. Na caixa de pesquisa do Windows, digite **`services.msc`** para abrir o Gerenciador de Serviços do Windows.
2. Na coluna Name (Nome), localize o Amazon SSM Agent.
3. Selecione Amazon SSM Agent e, depois, escolha Action (Ação), Properties (Propriedades).
4. Na guia General (Geral), em Startup type (Tipo de inicialização), escolha Disabled (Desativado).

5. Escolha OK.

O SSL3 e o TLS versão 1.2 devem estar habilitados

Para configurar o SSL/TLS para Windows, consulte Como habilitar o TLS 1.2 na documentação do Microsoft Windows.

Somente um perfil de usuário pode existir no WorkSpace

Só pode haver um perfil de WorkSpaces usuário (`D:\Users\username`) no WorkSpace que você está usando para criar imagens. Exclua todos os perfis de usuário que não pertençam ao usuário pretendido do WorkSpace.

Para que a criação de imagens funcione, você só WorkSpace pode ter três perfis de usuário nela:

- O perfil de usuário do usuário pretendido do WorkSpace (`D:\Users\username`)
- O perfil do usuário padrão (também conhecido como perfil padrão)
- O perfil do usuário Administrador

Se houver perfis do usuário adicionais, será possível excluí-los por meio das propriedades avançadas do sistema no Painel de Controle do Windows.

Como excluir um perfil do usuário

1. Para acessar as propriedades avançadas do sistema, siga um destes procedimentos:
   - Pressione a tecla Windows+Pause Break e escolha Advanced system settings (Configurações avançadas do sistema) no painel esquerdo da caixa de diálogo Control Panel (Painel de Controle) > System and Security (Sistema e Segurança) > System (Sistema).
   - Na caixa de pesquisa do Windows, digite **`control panel`**. No Painel de Controle, escolha System and Security (Sistema e Segurança), escolha System (Sistema) e, depois, selecione Advanced system settings (Configurações avançadas do sistema) no painel esquerdo da caixa de diálogo Control Panel (Painel de Controle) > System and Security (Sistema e Segurança) > System (Sistema).
2. Na caixa de diálogo System Properties (Propriedades do sistema) na guia Advanced (Avançado) escolha Settings (Configurações) em User Profiles (Perfis do usuário).
3. Se houver algum perfil listado que não seja o perfil do administrador, o perfil padrão e o perfil do WorkSpaces usuário pretendido, selecione esse perfil adicional e escolha Excluir.

4. Quando perguntado se deseja excluir o perfil, escolha Yes (Sim).
5. Se necessário, repita as etapas 3 e 4 para remover quaisquer outros perfis que não pertençam ao WorkSpace.
6. Escolha OK duas vezes e feche o Painel de Controle.
7. Reinicie WorkSpace o.

Nenhum pacote AppX pode estar em um estado de preparo

Um ou mais pacotes AppX estão em um estado de preparo. Isso pode causar um erro de Sysprep durante a criação da imagem.

Como remover todos os pacotes do AppX preparados

1. Na caixa de pesquisa do Windows, digite **`powershell`**. Escolha Executar como administrador.
2. Quando perguntado “Deseja permitir que este aplicativo faça alterações no dispositivo?”, escolha Sim.
3. Na PowerShell janela do Windows, insira os seguintes comandos para listar todos os pacotes AppX preparados e pressione Enter após cada um.

```
$workSpaceUserName = $env:username
```

```
$allAppxPackages = Get-AppxPackage -AllUsers
```

```
$packages = $allAppxPackages |    Where-Object { `
                                 (($_.PackageUserInformation -like "*S-1-5-18*" -
and !($_.PackageUserInformation -like "*$workSpaceUserName*")) -and `
                                 ($_.PackageUserInformation -like "*Staged*" -or
 $_.PackageUserInformation -like "*Installed*")) -or `
                                 ((!($_.PackageUserInformation -like "*S-1-5-18*") -
and $_.PackageUserInformation -like "*$workSpaceUserName*") -and `
                                 $_.PackageUserInformation -like "*Staged*")
                                 }
```

4. Digite o comando a seguir para remover todos os pacotes AppX preparados e pressione Enter.

```
$packages | Remove-AppxPackage -ErrorAction SilentlyContinue
```

5. Execute o Verificador de imagens novamente. Se este teste ainda falhar, digite os comandos a seguir para remover todos os pacotes AppX e pressione Enter após cada um.

```
Get-AppxProvisionedPackage -Online | Remove-AppxProvisionedPackage -Online -
ErrorAction SilentlyContinue
```

```
Get-AppxPackage -AllUsers | Remove-AppxPackage -ErrorAction SilentlyContinue
```

O Windows não pode ter sido atualizado de uma versão anterior

Não há suporte para a criação de imagens nos sistemas Windows que foram atualizados de uma versão do Windows 10 para uma mais recente (atualização de um recurso/versão do Windows).

Para criar imagens, use uma WorkSpace que não tenha passado por uma atualização de recurso/versão do Windows.

A contagem de rearmação do Windows não deve ser 0

O recurso rearmar permite que você estenda o período de ativação para a versão de avaliação do Windows. O processo de criação de imagem requer que a contagem de rearmação seja um valor diferente de 0.

Como verificar a contagem de rearmação do Windows

1. No menu Start (Iniciar) do Windows, escolha Windows System (Sistema Windows) e selecione Command Prompt (Prompt de comando).
2. Na janela Command Prompt (Prompt de comando), digite o comando a seguir e depois pressione Enter.

```
cscript C:\Windows\System32\slmgr.vbs /dlv
```

Para redefinir a contagem de rearmação como um valor diferente de 0, consulte Sysprep (Generalize) uma instalação do Windows na documentação do Microsoft Windows.

Outras dicas de solução de problemas

Se você WorkSpace passar em todos os testes executados pelo Image Checker, mas ainda não conseguir criar uma imagem a partir do WorkSpace, verifique os seguintes problemas:

- Certifique-se de que WorkSpace não esteja atribuído a um usuário dentro de um grupo de convidados do domínio. Para verificar se há alguma conta de domínio, execute o PowerShell comando a seguir.

```
Get-WmiObject -Class Win32_Service | Where-Object { $_.StartName -like "*
$env:USERDOMAIN*" }
```

- WorkSpaces Somente para Windows 7: se ocorrerem problemas durante a cópia do perfil do usuário durante a criação da imagem, verifique os seguintes problemas:
  - Caminhos de perfil longos podem causar erros de criação de imagem. Certifique-se de que os caminhos de todas as pastas dentro do perfil do usuário tenham menos de 261 caracteres.
  - Certifique-se de conceder permissões totais na pasta de perfil para o sistema e todos os pacotes de aplicativos.
  - Se algum arquivo no perfil do usuário estiver bloqueado por um processo ou estiver em uso durante a criação da imagem, poderá ocorrer uma falha na cópia do perfil.
- Alguns GPOs (Objetos de política de grupo) restringem o acesso à impressão digital do certificado RDP quando ela é solicitada pelo serviço EC2Config ou pelos scripts EC2Launch durante a configuração da instância do Windows. Antes de tentar criar uma imagem, mova-a WorkSpace para uma nova unidade organizacional (OU) com herança bloqueada e sem GPOs aplicados.
- Verifique se o serviço Gerenciamento Remoto do Windows (WinRM) está configurado para ser iniciado automaticamente. Faça o seguinte:
  1. Na caixa de pesquisa do Windows, digite **`services.msc`** para abrir o Gerenciador de Serviços do Windows.
  2. Na coluna Nome localize Gerenciamento Remoto do Windows (WS-Management).
  3. Selecione Gerenciamento Remoto do Windows (WS-Management) e escolha Ação, Propriedades.
  4. Na guia Geral, em Tipo de inicialização, escolha Automático.
  5. Escolha OK.

Etapa 3: Criar uma imagem e um pacote personalizados

Depois de validar sua WorkSpace imagem, você pode continuar com a criação da imagem personalizada e do pacote personalizado.

Como criar uma imagem e um pacote personalizados

1. Se você ainda estiver conectado ao WorkSpace, desconecte escolhendo Amazon WorkSpaces e Disconnect no aplicativo WorkSpaces cliente.
2. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
3. No painel de navegação, escolha WorkSpaces.
4. Selecione a WorkSpace para abrir sua página de detalhes e escolha Criar imagem. Se o status do WorkSpace for Parado, você deverá iniciá-lo primeiro (escolha Ações, Iniciar WorkSpaces) antes de escolher Ações, Criar imagem.

   > **Note**
   >
   > Para criar uma imagem programaticamente, use a ação da CreateWorkspaceImage API. Para obter mais informações, consulte CreateWorkspaceImagea Amazon WorkSpaces API Reference.

5. Uma mensagem é exibida solicitando que você reinicie (reinicie) o seu WorkSpace antes de continuar. Reiniciando suas WorkSpace atualizações, seu WorkSpaces software Amazon para a versão mais recente.

   Reinicie o seu WorkSpace fechando a mensagem e seguindo as etapas emReinicie um WorkSpace. Quando terminar, repita a Step 4 desse procedimento, mas desta vez selecione Próximo quando a mensagem de reinicialização for exibida. Para criar uma imagem, o status do WorkSpace deve ser Disponível e seu estado de modificação deve ser Nenhum.
6. Insira um nome de imagem e uma descrição que o ajudarão a identificar a imagem e escolha Create Image (Criar imagem). Enquanto a imagem está sendo criada, o status do WorkSpace é Suspenso e não WorkSpace está disponível.

   > **Note**
   >
   > Ao inserir uma descrição de imagem, certifique-se de não usar o caractere especial “-” ou você receberá um erro.

7. No painel de navegação, selecione Images (Imagens). A imagem estará completa quando o status das WorkSpace alterações for alterado para Disponível (isso pode levar até 45 minutos).
8. Selecione a imagem e escolha Ações, Criar pacote.

> **Note**
>
> Para criar um pacote de forma programática, use a ação da API CreateWorkspaceBundle. Para obter mais informações, consulte CreateWorkspaceBundlea Amazon WorkSpaces API Reference.

9. Insira o nome de um pacote e uma descrição. Depois, faça o seguinte:

   - Para o tipo de hardware de pacote, escolha o hardware a ser usado ao iniciar WorkSpaces a partir desse pacote personalizado.
   - Em Configurações de armazenamento, selecione uma das combinações padrão para o volume raiz e o tamanho do volume do usuário. Você também pode selecionar Personalizado e inserir valores (até 2.000 GB) para o Tamanho do volume raiz e o Tamanho do volume do usuário.

     Os tamanhos disponíveis padrão para combinações do volume raiz (para Microsoft Windows, a unidade `C` e, para Linux, /) e o volume do usuário (para Windows, a unidade `D` e, para Linux, /home) são:

     - Raiz: 80 GB, usuário: 10 GB, 50 GB ou 100 GB
     - Raiz: 175 GB, usuário: 100 GB
     - Somente para Graphics.g4dn, GraphicsPro .g4dn, Graphics e GraphicsPro WorkSpaces somente: Raiz: 100 GB, Usuário: 100 GB

     Também é possível expandir os volumes raiz e do usuário para até 2.000 GB cada um.

     > **Note**
     >
     > Para garantir que seus dados sejam preservados, você não pode diminuir o tamanho dos volumes raiz ou do usuário depois de iniciar um WorkSpace. Em vez disso, certifique-se de especificar os tamanhos mínimos para esses volumes ao lançar um WorkSpace. Você pode iniciar um Value, Standard, Performance, Power ou PowerPro WorkSpace com um mínimo de 80 GB para o volume raiz e 10 GB para o volume do usuário. Você pode iniciar um Graphics.G4dn, GraphicsPro .g4dn, Graphics ou GraphicsPro WorkSpace com um mínimo de 100 GB para o volume raiz e 100 GB para o volume do usuário.

10. Escolha Criar pacote.

11. Para confirmar que o pacote foi criado, escolha Pacotes e verifique se o pacote está listado.

O que está incluído nas imagens WorkSpaces personalizadas do Windows

Quando você cria uma imagem a partir de um Windows 7, Windows 10 ou Windows 11 WorkSpace, todo o conteúdo da `C` unidade é incluído.

Para o Windows 10 ou 11 WorkSpaces, o perfil do usuário em não `D:\Users\`*`username`* está incluído na imagem personalizada.

Para o Windows 7 WorkSpaces, todo o conteúdo do perfil do usuário `D:\Users\`*`username`* está incluído, exceto o seguinte:

- Contatos
- Downloads
- Música
- Imagens
- Jogos salvos
- Vídeos
- Podcasts
- Máquinas virtuais
- .virtualbox
- Rastreamento
- appdata\local\temp
- appdata\roaming\apple computer\mobilesync\
- appdata\roaming\apple computer\logs\
- appdata\roaming\apple computer\itunes\iphone software updates\
- appdata\roaming\macromedia\flash player\macromedia.com\support\flashplayer\sys\
- appdata\roaming\macromedia\flash player\#sharedobjects\
- appdata\roaming\adobe\flash player\assetcache\
- appdata\roaming\microsoft\windows\recent\
- appdata\roaming\microsoft\office\recent\

- appdata\roaming\microsoft office\live meeting
- appdata\roaming\microsoft shared\livemeeting shared\
- appdata\roaming\mozilla\firefox\crash reports\
- appdata\roaming\mcafee\common framework\
- appdata\local\microsoft\feeds cache
- appdata\local\microsoft\windows\temporary internet files\
- appdata\local\microsoft\windows\history\
- appdata\local\microsoft\internet explorer\domstore\
- appdata\local\microsoft\internet explorer\imagestore\
- appdata\locallow\microsoft\internet explorer\iconcache\
- appdata\locallow\microsoft\internet explorer\domstore\
- appdata\locallow\microsoft\internet explorer\imagestore\
- appdata\local\microsoft\internet explorer\recovery\
- appdata\local\mozilla\firefox\profiles\

O que está incluído nas imagens WorkSpace personalizadas do Linux

Quando você cria uma imagem a partir de um Amazon Linux WorkSpace, todo o conteúdo do volume do usuário (/home) é removido. O conteúdo do volume raiz (/) é incluído, exceto as seguintes pastas e chaves aplicáveis, que são removidas:

- /tmp
- /var/spool/mail
- /var/tmp
- /var/lib/dhcp
- /var/lib/cloud
- /var/cache
- /var/backups
- /etc/sudoers.d
- /etc/udev/rules.d/70-persistent-net.rules
- /etc/network/interfaces.d/50-cloud-init.cfg

- /var/log/amazon/ssm
- /var/log/pcoip-agent
- /var/log/skylight
- /var/lock/.skylight.domain-join.lock
- /var/lib/skylight/domain-join-status
- /var/lib/skylight/configuration-data
- /var/lib/skylight/config-data.json
- /home
- /etc/default/grub.d/zz-hibernation.cfg
- /etc/netplan/zz-workspaces-domain.yaml
- /etc/netplan/yy-workspaces-base.yaml
- /var/lib/ /usuários AccountsService

As seguintes chaves são destruídas durante a criação da imagem personalizada:

- /etc/ssh/ssh_host_*_key
- /etc/ssh/ssh_host_*_key.pub
- /var/lib/skylight/tls.*
- /var/lib/skylight/private.key
- /var/lib/skylight/public.key

Atualizar um pacote personalizado de WorkSpaces

É possível atualizar um pacote de WorkSpaces personalizados existente modificando um WorkSpace com base no pacote, criando uma imagem do WorkSpace e atualizando o pacote com a nova imagem. Você pode ativar novos WorkSpaces usando o pacote atualizado.

> **Important**
>
> Os WorkSpaces existentes não são atualizados automaticamente quando você atualiza o pacote no qual eles são baseados. Para atualizar os WorkSpaces existentes baseados em um pacote que você atualizou, você deve recriar os WorkSpaces ou excluí-los e recriá-los.

Como atualizar um pacote usando o console

1. Conecte-se a um WorkSpace com base no pacote e faça as alterações desejadas. Por exemplo, você pode aplicar os patches mais recentes do sistema operacional e dos aplicativos e instalar aplicativos adicionais.

   Você também pode criar um WorkSpace com o mesmo pacote de software base (Plus ou Standard) que a imagem usada para criar o pacote e fazer alterações.
2. Se ainda estiver conectado ao WorkSpace, desconecte-se selecionando Amazon WorkSpaces e Desconectar na aplicação cliente do WorkSpaces.
3. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
4. No painel de navegação, selecione WorkSpaces.
5. Selecione o WorkSpace e escolha Actions (Ações), Create Image (Criar imagem). Se o status do WorkSpace for `STOPPED`, você deverá iniciá-lo primeiro (selecione Ações, Iniciar WorkSpaces) antes de selecionar Ações, Criar imagem.
6. Insira um nome de imagem e uma descrição, e escolha Create Image (Criar imagem). O WorkSpace permanece indisponível enquanto a imagem está sendo criada. Para obter informações detalhadas sobre o processo de criação de imagens, consulte Crie uma WorkSpaces imagem e um pacote personalizados.
7. No painel de navegação, selecione Pacotes.
8. Selecione o pacote para abrir a página de detalhes dele e, em Imagem de origem, selecione Editar.
9. Na página Atualizar imagem de origem, selecione a imagem que você criou e selecione Atualizar pacote.
10. Conforme necessário, atualize todos os WorkSpaces existentes baseados no pacote recriando os WorkSpaces ou excluindo-os e recriando-os. Para obter mais informações, consulte Reconstrua um WorkSpace.

Como atualizar um pacote de forma programática

Para atualizar um pacote de forma programática, use a ação da API UpdateWorkspaceBundle. Para obter mais informações, consulte UpdateWorkspaceBundle na Referência da API do Amazon WorkSpaces.

Copiar uma imagem personalizada do WorkSpaces

Você pode copiar uma imagem personalizada do WorkSpaces em uma região ou entre regiões da AWS. A cópia de uma imagem resulta na criação de uma imagem idêntica, mas com seu próprio identificador exclusivo.

É possível copiar uma imagem BYOL (Bring Your Own License) para outra região, desde que a região de destino esteja habilitada para BYOL. O BYOL deve estar habilitado para todas as contas e regiões envolvidas.

> **Note**
>
> Na região China (Ningxia), só é possível copiar imagens dentro da mesma região.
> Nas regiões AWS GovCloud (EUA), para copiar imagens de e para outras regiões da AWS, entre em contato com o AWS Support.
> Em regiões Opt-in, para copiar imagens para outras regiões, entre em contato com o AWS Support. Para obter mais informações sobre as regiões Opt-in disponíveis, consulte a Regiões disponíveis.

Também é possível copiar uma imagem que tenha sido compartilhada com você por outra conta da AWS. Para obter mais informações sobre imagens compartilhadas, consulte Compartilhar ou cancelar o compartilhamento de uma imagem personalizada do WorkSpaces.

Não há cobrança adicional para a cópia de imagens dentro ou entre regiões. No entanto, é aplicada a cota de número de imagens na região de destino. Para obter mais informações sobre cotas do Amazon WorkSpaces, consulte WorkSpaces Cotas da Amazon.

Permissões do IAM para a cópia de imagens

Se você usar um usuário do IAM para copiar uma imagem, o usuário deverá ter permissões para `workspaces:DescribeWorkspaceImages` e `workspaces:CopyWorkspaceImage`.

A política de exemplo a seguir permite que o usuário copie a imagem especificada para a conta especificada na região especificada.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeWorkspaceImages",
        "workspaces:CopyWorkspaceImage"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:123456789012:workspaceimage/wsi-a1bcd2efg"
      ]
    }
  ]
}
```

Important

Se você estiver criando uma política do IAM para copiar imagens compartilhadas para contas que não possuem as imagens, não é possível especificar um ID de conta no ARN. Em vez disso, você deve usar * como o ID da conta, conforme exibido no exemplo de política a seguir.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeWorkspaceImages",
        "workspaces:CopyWorkspaceImage"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:*:workspaceimage/wsi-a1bcd2efg"
      ]
    }
  ]
}
```

É possível especificar um ID de conta no ARN somente quando essa conta possui as imagens a serem copiadas.

Para obter mais informações sobre como trabalhar com o IAM, consulte Gerenciamento de identidade e acesso para o WorkSpaces.

Cópia de imagens em massa

É possível copiar imagens uma a uma usando o console. Para copiar imagens em massa, use a operação de API CopyWorkspaceImage ou o comando copy-workspace-image no AWS Command Line Interface (AWS CLI). Para obter mais informações, consulte CopyWorkspaceImage na Referência da API do Amazon WorkSpaces ou consulte copy-workspace-image na Referência de comando da AWS CLI.

> **Important**
>
> Antes de copiar uma imagem compartilhada, verifique se ela foi compartilhada da conta da AWS correta. Para determinar se uma imagem foi compartilhada e ver o ID da conta da AWS que possui uma imagem, use as operações da API DescribeWorkSpaceImages e DescribeWorkspaceImagePermissions ou os comandos describe-workspace-images and describe-workspace-image-permissions na AWS CLI.

Como copiar uma imagem usando o console

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione Images (Imagens).
3. Selecione a imagem e escolha Ações, Copiar imagem.
4. Em Selecionar destino, selecione a região da AWS para a qual você deseja copiar a imagem.
5. Em Nome da cópia, insira o novo nome para a imagem copiada e, em Descrição, insira uma descrição para ela.
6. (Opcional) Em Tags, insira etiquetas para a imagem copiada. Para obter mais informações, consulte Marcar recursos do WorkSpaces.
7. Escolha Copiar imagem.

Compartilhar ou cancelar o compartilhamento de uma imagem personalizada do WorkSpaces

É possível compartilhar imagens personalizadas do WorkSpaces entre contas da AWS dentro da mesma região da AWS. Após compartilhar uma imagem, a conta do destinatário poderá copiar a imagem para outras regiões da AWS conforme necessário. Para obter mais informações sobre cópia de imagens, consulte Copiar uma imagem personalizada do WorkSpaces.

> **Note**
>
> Na região China (Ningxia), só é possível copiar imagens dentro da mesma região.
> Nas regiões AWS GovCloud (EUA), para copiar imagens de e para outras regiões da AWS, entre em contato com o AWS Support.

Não há cobranças adicionais pelo compartilhamento de uma imagem. No entanto, é aplicada a cota de número de imagens na região da AWS. Uma imagem compartilhada não conta na cota da conta do destinatário até que o destinatário copie a imagem. Para obter mais informações sobre cotas do Amazon WorkSpaces, consulte WorkSpaces Cotas da Amazon.

Para excluir uma imagem compartilhada, você deve cancelar o compartilhamento antes de excluí-la.

Compartilhar imagens do tipo traga a sua própria licença

Você só pode compartilhar imagens do tipo traga a sua própria licença (BYOL) com contas da AWS habilitadas para BYOL. A conta da AWS com a qual deseja compartilhar imagens de BYOL também deve fazer parte da sua organização (na mesma conta do pagante).

> **Note**
>
> No momento, o compartilhamento de imagens BYOL entre contas da AWS não é compatível com as regiões do AWS GovCloud (Oeste dos EUA) e do AWS GovCloud (Leste dos EUA). Para compartilhar imagens BYOL entre contas nas regiões do AWS GovCloud (Oeste dos EUA) e do AWS GovCloud (Leste dos EUA), entre em contato com o AWS Support.

Imagens compartilhadas com você

Se imagens forem compartilhadas com você, você poderá copiá-las. Dessa forma, você poderá usar suas cópias das imagens compartilhadas para criar pacotes e iniciar novos WorkSpaces.

> **Important**
>
> Antes de copiar uma imagem compartilhada, verifique se ela foi compartilhada da conta da AWS correta. Para determinar de maneira programática se uma imagem foi compartilhada, use as operações de API DescribeWorkSpaceImages e

DescribeWorkspaceImagePermissions ou os comandos describe-workspace-images e describe-workspace-image-permissions na AWS Command Line Interface (CLI).

A data de criação mostrada para uma imagem que foi compartilhada com você é a data em que a imagem foi criada originalmente, não a data em que a imagem foi compartilhada com você.

Se uma imagem foi compartilhada com você, você não poderá mais compartilhá-la com outras contas.

Como compartilhar uma imagem

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione Images (Imagens).
3. Escolha a imagem para abrir sua página de detalhes.
4. Na página de detalhes da imagem, na seção Contas compartilhadas, selecione Adicionar conta.
5. Na página Adicionar conta, em Adicionar conta para compartilhar, insira o ID da conta com a qual você deseja compartilhar a imagem.

   Important

   Antes de compartilhar a imagem, confirme se você está compartilhando com o ID da conta da AWS correto.

6. Clique em Compartilhar imagem.

   Note

   Para usar a imagem compartilhada, a conta do destinatário deve primeiro copiar a imagem. Dessa forma, a conta de destinatário poderá usar a cópia da imagem compartilhada para criar pacotes e iniciar novos WorkSpaces.

Como interromper o compartilhamento de uma imagem

1. Abra o console do WorkSpaces em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione Images (Imagens).
3. Escolha a imagem para abrir sua página de detalhes.

4. Na página de detalhes da imagem, na seção Contas compartilhadas, selecione a conta da AWS com a qual você deseja interromper o compartilhamento e clique em Cancelar compartilhamento.
5. Quando solicitado a confirmar o cancelamento do compartilhamento da imagem, clique em Cancelar compartilhamento.

> **Note**
>
> Se quiser excluir a imagem depois de cancelar o compartilhamento, você deve primeiro cancelar o compartilhamento dela de todas as contas com as quais ela foi compartilhada.

Depois de cancelar o compartilhamento de uma imagem, a conta de destinatário não poderá mais fazer cópias dessa imagem. No entanto, todas as cópias de imagens compartilhadas que já estão na conta de destinatário permanecerão nessa conta e novos WorkSpaces poderão ser executados com essas cópias.

Como compartilhar ou cancelar o compartilhamento de imagens de forma programática

Para compartilhar ou cancelar o compartilhamento de imagens de forma programática, use a operação da API UpdateWorkspaceImagePermission ou o comando update-workspace-image-permission do AWS Command Line Interface (AWS CLI). Para determinar se uma imagem foi compartilhada, use a operação da API DescribeWorkspaceImagePermissions ou o comando describe-workspace-image-permissions da CLI.

Excluir um WorkSpaces pacote ou imagem personalizada

Você pode excluir imagens ou pacotes personalizados não utilizados conforme necessário.

Excluir um pacote

Para excluir um pacote, você deve primeiro excluir todos os WorkSpaces que são baseados no pacote.

Como excluir um pacote usando o console

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.

2. No painel de navegação, selecione Pacotes.
3. Selecione o pacote e clique em Excluir.
4. Quando a confirmação for solicitada, escolha Excluir.

Como excluir um pacote de forma programática

Para excluir um pacote de forma programática, use a ação da API DeleteWorkspaceBundle. Para obter mais informações, consulte DeleteWorkspaceBundle a Amazon WorkSpaces API Reference.

> **Note**
>
> Certifique-se de esperar pelo menos 2 horas após excluir um pacote antes de criar um novo pacote com o mesmo nome.

Excluir uma imagem

Depois de excluir um pacote personalizado, é possível excluir a imagem que usou para criar ou atualizar o pacote.

Para excluir uma imagem, você deve primeiro excluir todos os bundles associados à imagem ou atualizá-los para usar outra imagem de origem. Você também deve cancelar o compartilhamento da imagem se ela for compartilhada com outras contas. A imagem também não pode estar no estado Pendente ou Validando.

Como excluir uma imagem usando o console

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione Images (Imagens).
3. Selecione a imagem e clique em Excluir.
4. Quando a confirmação for solicitada, escolha Excluir.

Como excluir uma imagem de forma programática

Para excluir uma imagem de forma programática, use a ação da API DeleteWorkspaceImage. Para obter mais informações, consulte DeleteWorkspaceImage a Amazon WorkSpaces API Reference.

Traga suas próprias licenças da área de trabalho do Windows

Se o seu contrato de licenciamento com a Microsoft permitir, você poderá trazer e implantar seu desktop Windows 10 ou 11 no seu WorkSpaces. Para fazer isso, é necessário habilitar o traga a sua própria licença (BYOL) e fornecer uma licença do Windows 10 ou 11 que atenda aos requisitos a seguir. Para obter mais informações sobre como usar o software da Microsoft em AWS, consulte Amazon Web Services e Microsoft.

Para manter a conformidade com os termos de licenciamento da Microsoft, AWS execute seu BYOL WorkSpaces em hardware dedicado a você na nuvem. AWS Ao trazer sua própria licença, você pode proporcionar uma experiência consistente para os seus usuários. Para obter mais informações, consulte WorkSpaces Preços.

> **Important**
>
> A criação de imagens não é suportada em sistemas Windows 10 ou 11 que foram atualizados de uma versão do Windows 10 ou 11 para uma versão mais recente do Windows 10 ou 11 (uma atualização de recurso/versão do Windows). No entanto, as atualizações cumulativas ou de segurança do Windows são suportadas pelo processo de criação de WorkSpaces imagens.

Conteúdo

- Etapa 8: registrar um diretório dedicado para WorkSpaces
- Etapa 9: Inicie seu BYOL WorkSpaces
- Vincular contas BYOL

Requisitos

Antes de começar, verifique o seguinte:

- Seu contrato de licenciamento da Microsoft permite que o Windows seja executado em um ambiente de host virtual.
- Se você estiver usando pacotes não habilitados para GPU (pacotes diferentes de Graphics.g4dn, GraphicsPro .g4dn, Graphics e GraphicsPro), verifique se você usará no mínimo 100 por região. WorkSpaces Esses 100 WorkSpaces podem ser qualquer mistura de AlwaysOn AutoStop WorkSpaces e. Usar um mínimo de 100 WorkSpaces por região é um requisito para executar seu WorkSpaces próprio hardware dedicado. É necessário executar WorkSpaces seu próprio hardware dedicado para cumprir os requisitos de licenciamento da Microsoft. O hardware dedicado é provisionado na AWS lateral, para que sua VPC possa permanecer na locação padrão.

  Se você planeja usar pacotes habilitados para GPU (Graphics.g4dn, GraphicsPro .g4dn, Graphics e GraphicsPro), verifique se você executará no mínimo 4 AlwaysOn ou 20 habilitados para GPU em uma região por mês em hardware dedicado. AutoStop WorkSpaces

  > **Note**
  >
  > - Gráficos.g4dn, GraphicsPro .g4dn, gráficos e GraphicsPro pacotes só podem ser criados para o protocolo PCoIP no momento.
  > - O pacote Graphics deixará de receber suporte a partir de 30 de novembro de 2023. Recomendamos migrar seu pacote para o WorkSpaces Graphics.g4dn. Para ter mais informações, consulte Migre um WorkSpace.
  > - No momento, gráficos e GraphicsPro pacotes não estão disponíveis na região Ásia-Pacífico (Mumbai).
  > - Gráficos.g4dn, GraphicsPro .g4dn, gráficos e GraphicsPro pacotes não estão disponíveis atualmente na região da África (Cidade do Cabo).
  > - Para executar o seu WorkSpaces na região da África (Cidade do Cabo), você deve executar no mínimo 400 WorkSpaces na região da África (Cidade do Cabo).
  > - Os pacotes do Windows 11 só podem ser criados para o protocolo WSP.

- No momento, os pacotes Graphics.g4dn GraphicsPro e.g4dn não estão disponíveis para o Windows 11.
- Gráficos e GraphicsPro pacotes não são compatíveis com o Windows 11.
- Os pacotes de valor não estão disponíveis para o Windows 11. Para obter mais informações sobre como migrar seu pacote WorkSpaces de valores existente, consulte. Migre um WorkSpace
- Para obter a melhor experiência de videoconferência, recomendamos o uso de Power ou pacotes PowerPro
- O Windows 11 requer o modo de inicialização Unified Extensible Firmware Interface (UEFI) para funcionar. Certifique-se de especificar o `--boot-mode` parâmetro opcional como UEFI para importar com sucesso sua VM.

- WorkSpaces pode usar uma interface de gerenciamento no intervalo de endereços IP /16. A interface de gerenciamento está conectada a uma rede WorkSpaces de gerenciamento segura usada para streaming interativo. Isso WorkSpaces permite gerenciar seu WorkSpaces. Para ter mais informações, consulte Interfaces de rede. É necessário reservar uma máscara de rede /16 de pelo menos um dos seguintes intervalos de endereços IP para este fim:
  - 10.0.0.0/8
  - 100.64.0.0/10
  - 172.16.0.0/12
  - 192.168.0.0/16
  - 198.18.0.0/15

  Note
  - Conforme você adota o WorkSpaces serviço, os intervalos de endereços IP da interface de gerenciamento disponíveis mudam com frequência. Para determinar quais intervalos estão disponíveis atualmente, execute o comando list-available-management-cidr-ranges AWS Command Line Interface (AWS CLI).
  - Além do bloco CIDR /16 selecionado, o intervalo de endereços IP 54.239.224.0/20 é usado para o tráfego da interface de gerenciamento em todas as regiões. AWS
- Verifique se você abriu as portas da interface de gerenciamento necessárias para a ativação do Microsoft Windows e do Microsoft Office KMS para WorkSpaces BYOL. Para ter mais informações, consulte Portas de interface de gerenciamento.

- Você tem uma máquina virtual (VM) que executa uma versão de 64 bits do Windows. Para obter uma lista de versões compatíveis, consulte a próxima seção deste tópico, Versões do Windows compatíveis com BYOL. A VM também deve atender a estes requisitos:
  - O sistema operacional Windows precisa estar ativado em relação aos servidores de gerenciamento de chaves.
  - O sistema operacional Windows deve ter English (United States) [inglês (Estados Unidos)] como o idioma principal.
  - Nenhum software além dos fornecidos com o Windows pode ser instalado na VM. Você pode adicionar outros softwares, como uma solução antivírus, ao criar uma imagem personalizada posteriormente.
  - Não personalize o perfil do usuário padrão (`C:\Users\Default`) nem faça outras personalizações antes de criar uma imagem. Todas as personalizações devem ser feitas após a criação da imagem. Recomendamos fazer personalizações no perfil do usuário por meio de GPOs (Objetos de política de grupo) e aplicá-los após a criação da imagem. Isso ocorre porque as personalizações feitas por meio de GPOs podem ser facilmente modificadas ou revertidas e são menos propensas a erros do que as personalizações feitas no perfil do usuário padrão.
  - Você deve criar uma conta WorkSpaces_BYOL com acesso de administrador local antes de compartilhar a imagem. A senha para essa conta pode ser necessária mais tarde, portanto, anote-a.
  - A VM deve estar em um único volume com um tamanho máximo de 70 GB e pelo menos 10 GB de espaço livre. Se você também planeja assinar o Microsoft Office para sua imagem BYOL, a VM deve estar em um único volume com um tamanho máximo de 70 GB e, pelo menos, 20 GB de espaço livre. O DISCO no qual o volume raiz está não pode exceder 70 GB.
  - Sua VM deve executar o Windows PowerShell versão 4 ou posterior.
- Verifique se você instalou os patches mais recentes do Microsoft Windows antes de executar o script de verificação BYOL na Etapa 3: Executar o PowerShell script BYOL Checker em uma VM do Windows.

> **Note**
>
> - Para o BYOL AutoStop WorkSpaces, um grande número de logins simultâneos pode resultar em um aumento significativo no tempo de disponibilidade WorkSpaces . Se você espera que muitos usuários acessem seu BYOL AutoStop WorkSpaces ao mesmo tempo, consulte seu gerente de conta para obter orientação.

- As AMIs criptografadas não são compatíveis com o processo de importação. Desative a instância usada para criar a AMI do EC2 com criptografia EBS. A criptografia pode ser ativada após o provisionamento final WorkSpaces .

Versões do Windows compatíveis com BYOL

A VM deve executar uma das seguintes versões do Windows:

- Windows 10 versão 21H2 (atualização de dezembro de 2021)
- Windows 10 versão 22H2 (atualização de novembro de 2022)
- Windows 10 Enterprise LTSC 2019 (1809)
- Windows 10 Enterprise LTSC 2021 (21H2)
- Windows 11 Enterprise 23H2 (versão de outubro de 2023)
- Windows 11 Enterprise 22H2 (versão de outubro de 2022)

Todas as versões de sistema operacional compatíveis oferecem suporte a todos os tipos de computação disponíveis na AWS região em que você está usando WorkSpaces. As versões do Windows que não são mais suportadas pela Microsoft não têm garantia de funcionamento e não são suportadas pelo AWS Support.

> **Note**
>
> No momento, as versões Windows 10 N e Windows 11 N não têm compatibilidade com BYOL.

Adicionar o Microsoft Office a uma imagem BYOL

Durante o processo de ingestão de imagens BYOL, se você estiver usando o Windows 10, você tem a opção de assinar o Microsoft Office Professional 2016 (32 bits) ou 2019 (64 bits) por meio de. AWS Se você estiver usando o Windows 11, poderá assinar o Microsoft Office Professional 2019 (64 bits). Se você escolher uma dessas opções, o Microsoft Office será pré-instalado em sua imagem BYOL e incluído em qualquer uma WorkSpaces que você iniciar a partir dessa imagem.

Se você optar por assinar o Office por meio de AWS, cobranças adicionais serão aplicadas. Para obter mais informações, consulte WorkSpaces Preços.

Important

- Se o Microsoft Office já estiver instalado na VM que você está usando para criar sua imagem BYOL, você deverá desinstalá-la da VM se quiser assinar o Office por meio de. AWS
- Se você planeja assinar o Office por meio de AWS, certifique-se de que sua VM tenha pelo menos 20 GB de espaço livre em disco.
- Durante a importação de imagens, você pode assinar o Office 2016 ou 2019, mas não o Office 2021. Para o Office 2021 e outras aplicações, como o Microsoft Visio 2021 e o Microsoft Project 2021, consulte Manage applications.
- Para trazer suas próprias licenças do Microsoft 365 para aplicativos baseados em navegador e desktop na Amazon, WorkSpaces instale os aplicativos Microsoft 365 em sua imagem BYOL após a conclusão do processo de ingestão de imagens BYOL.

Note

As imagens BYOL Graphics.g4dn e GraphicsPro .g4dn oferecem suporte somente ao Office 2019 e não ao Office 2016.

Se você optar por assinar o Office, o processo de ingestão de imagens BYOL levará no mínimo três horas.

Para obter detalhes sobre a assinatura do Office durante o processo de ingestão BYOL, consulte Etapa 6: criar uma imagem BYOL usando o console WorkSpaces .

Configurações de idioma do Office

Escolhemos o idioma usado para sua assinatura do Office com base na AWS região em que você está realizando a ingestão de imagens BYOL. Por exemplo, se você estiver realizando a ingestão de imagens BYOL na região Ásia-Pacífico (Tóquio), a assinatura do Office terá o japonês como idioma.

Por padrão, instalamos vários pacotes de idiomas do Office usados com frequência em seu WorkSpaces. Se o pacote de idiomas desejado não estiver instalado, é possível baixar pacotes de idiomas adicionais da Microsoft. Para obter mais informações, consulte Pacote de acessórios de idioma para o Office na documentação da Microsoft.

Para alterar o idioma do Office, você pode:

Opção 1: permitir que usuários individuais personalizem suas configurações de idioma do Office

Usuários individuais podem ajustar as configurações de idioma do Office em seus WorkSpaces. Para obter mais informações, consulte Como adicionar um idioma de edição ou criação ou definir preferências de idioma no Office na documentação da Microsoft.

Opção 2: usar modelos administrativos do GPO (.admx/.adml) para impor as configurações padrão de idioma do Office para todos os seus usuários WorkSpaces

Você pode usar as configurações de Objeto de Política de Grupo (GPO) para impor as configurações padrão de idioma do Office para seus WorkSpaces usuários.

> **Note**
>
> Seus WorkSpaces usuários não poderão substituir as configurações de idioma impostas pelo GPO.

Para obter mais informações sobre como usar o GPO para definir o idioma do Office, consulte Como personalizar a definição e as configurações de idioma do Office na documentação da Microsoft. O Office 2016 e o Office 2019 usam as mesmas configurações de GPO (identificadas com o Office 2016).

Para trabalhar com GPOs, você deve instalar as ferramentas de administração do Active Directory. Para obter informações sobre como usar as ferramentas de administração do Active Directory para trabalhar com GPOs, consulte Configurar as ferramentas de administração do Active Directory para WorkSpaces.

Antes de definir as configurações de política do Office 2016 ou do Office 2019, você deve baixar os arquivos de modelo administrativo (.admx/.adml) para o Office na Central de Download da Microsoft. Depois de baixar os arquivos de modelo administrativo, você deve adicionar os `office16.adml` arquivos `office16.admx` e ao Armazenamento Central do controlador de domínio do seu WorkSpaces diretório. (Os arquivos `office16.admx` e `office16.adml` se aplicam ao Office 2016 e ao Office 2019.) Para obter mais informações sobre como trabalhar com os arquivos `.admx` e `.adml`, consulte Como criar e gerenciar o armazenamento central de modelos administrativos de política de grupo no Windows na documentação da Microsoft.

O procedimento a seguir descreve como criar o repositório central e adicionar os arquivos de modelo administrativo a ele. Execute o procedimento a seguir em uma administração de diretório WorkSpace ou instância do Amazon EC2 que esteja associada ao seu WorkSpaces diretório.

Como instalar os arquivos de modelo administrativo de política de grupo no Office

1. Baixe os arquivos de modelo administrativo (.admx/.adml) do Office na Central de Download da Microsoft.
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra o Windows File Explorer e, na barra de endereço, insira o nome de domínio totalmente qualificado (FQDN) da sua organização, como. `\\example.com`
3. Abra a pasta `SYSVOL`.
4. Abra a pasta com o nome *FQDN*.
5. Abra a pasta `Policies`. O endereço agora deve ser `\\`*FQDN*`\SYSVOL\`*FQDN*`\Policies`.
6. Se ele ainda não existir, crie uma pasta chamada `PolicyDefinitions`.
7. Abra a pasta `PolicyDefinitions`.
8. Copie o arquivo `office16.admx` na pasta `\\`*FQDN*`\SYSVOL\`*FQDN*`\Policies\PolicyDefinitions`.
9. Crie uma pasta chamada `en-US` na pasta `PolicyDefinitions`.
10. Abra a pasta `en-US`.
11. Copie o arquivo `office16.adml` na pasta `\\`*FQDN*`\SYSVOL\`*FQDN*`\Policies\PolicyDefinitions\en-US`.

Como definir as configurações de idioma do GPO para o Office

1. Na administração do seu diretório WorkSpace ou na instância do Amazon EC2 que está associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management ()gpmc.msc.
2. Expanda a floresta (Floresta: ***FQDN***).
3. Expanda os Domínios.
4. Expanda o FQDN (por exemplo, `example.com`).
5. Selecione o FQDN, abra o menu de contexto (clique com o botão direito do mouse) ou abra o menu Ação e selecione Criar um GPO neste domínio e vinculá-lo aqui.
6. Nomeie o GPO (por exemplo, **`Office`**).

7. Selecione o GPO, abra o menu de contexto (clique com o botão direito do mouse) ou abra o menu Ação e selecione Editar.
8. No Editor de gerenciamento de políticas de grupo, selecione Configuração do usuário, Políticas, Definições de política do modelo administrativo (arquivos ADMX) recuperadas do computador local, Microsoft Office 2016 e Preferências de idioma.

   > **Note**
   >
   > O Office 2016 e o Office 2019 usam as mesmas configurações de GPO (identificadas com o Office 2016). Se você não encontrar Definições de política do modelo administrativo (arquivos ADMX) recuperadas do computador local em Configuração do usuário, Políticas, os arquivos `office16.admx` e `office16.adml` não foram instalados corretamente no controlador de domínio.

9. Em Preferências de idioma, especifique o idioma desejado para as configurações a seguir. Defina cada configuração como Habilitada e selecione o idioma desejado em Opções. Escolha OK para salvar cada configuração.

   - Idioma de exibição > Exibir ajuda em
   - Idioma de exibição > Exibir menus e caixas de diálogo em
   - Idiomas de edição > Idioma de edição principal

10. Feche a ferramenta de Gerenciamento de política de grupo quando terminar.
11. As alterações nas configurações da Política de Grupo entram em vigor após a próxima atualização da Política de Grupo WorkSpace e após a reinicialização da WorkSpace sessão. Para aplicar as alterações de política de grupo, execute um destes procedimentos:

    - Reinicie o WorkSpace (no WorkSpaces console da Amazon, selecione o e, em seguida WorkSpace, escolha Ações, Reinicialização WorkSpaces).
    - Em um prompt de comando administrativo, insira gpupdate /force.

Opção 3: Atualizar as configurações do registro de idiomas do Office em seu WorkSpaces

Para definir as configurações de idioma do Office por meio do registro, atualize as seguintes configurações do registro:

- HKEY_CURRENT_USER\ SOFTWARE\ Microsoft\ Office\ 16.0\ Common\\ UI Language LanguageResources

- HKEY_CURRENT_USER\ SOFTWARE\ Microsoft\ Office\ 16.0\ Comum\\ LanguageResources HelpLanguage

Para essas configurações, adicione um valor de chave DWORD com o ID de localidade do Office (LCID) adequado. Por exemplo, o LCID para inglês (EUA) é 1033. Como os LCIDs são valores decimais, você deve definir a opção Base para o valor DWORD como Decimal. Para obter uma lista dos LCIDs do Office, consulte Identificadores de idioma e valores de OptionState ID no Office 2016 na documentação da Microsoft.

Você pode aplicar essas configurações de registro às suas WorkSpaces por meio de configurações de GPO ou de um script de logon.

Para obter mais informações sobre como usar as configurações de idioma do Office, consulte Como personalizar a definição e as configurações de idioma do Office na documentação da Microsoft.

Adicione o Office ao seu BYOL existente WorkSpaces

Você também pode adicionar uma assinatura do Office ao seu BYOL existente WorkSpaces fazendo o seguinte.

- Gerenciar aplicativos (recomendado) - Você pode instalar e configurar o Microsoft Office, o Microsoft Visio ou o Microsoft Project 2021 no seu. WorkSpaces Para obter mais informações, consulte Manage applications.
- Migrar um WorkSpace - Depois de ter um pacote BYOL com o Office instalado, você pode usar o recurso de WorkSpaces migração para migrar seu BYOL existente para o pacote BYOL WorkSpaces que está inscrito no Office. Para ter mais informações, consulte Migre um WorkSpace.

> **Note**
>
> A opção gerenciar aplicativos está disponível para instalar o Microsoft Office 2021 e outros aplicativos, como o Microsoft Visio 2021 e o Microsoft Project 2021 no seu WorkSpaces. Para instalar o Microsoft Office 2016 ou 2019 em seu WorkSpaces, useMigre um WorkSpace.

Migrar entre versões do Microsoft Office

Para migrar de uma versão do Microsoft Office para outra, você tem as seguintes opções:

- Gerenciar aplicativos (recomendado) — Você pode desinstalar a versão original do Office e instalar o Office 2021 e outros aplicativos, como o Microsoft Visio 2021 e o Microsoft Project 2021, no seu aplicativo existente WorkSpaces. Por exemplo, para migrar do Microsoft Office 2019 para o Microsoft Office 2021, use o fluxo de trabalho de gerenciamento de aplicações para desinstalar o Microsoft Office 2019 e instalar o Microsoft Office 2021. Para obter mais informações, consulte Manage applications.
- Migrar um WorkSpace — Para migrar do Microsoft Office 2016 para o Microsoft Office 2019 ou do Microsoft Office 2019 para o Microsoft Office 2016, você deve criar um pacote BYOL que esteja inscrito na versão do Office para a qual você deseja migrar. Em seguida, use o recurso de WorkSpaces migração para migrar seu BYOL existente WorkSpaces que está inscrito no Office para o pacote BYOL que está inscrito na versão do Office para a qual você deseja migrar. Por exemplo, para migrar do Microsoft Office 2016 para o Microsoft Office 2019, crie um pacote BYOL que esteja inscrito no Microsoft Office 2019. Em seguida, use o recurso de WorkSpaces migração para migrar seu BYOL existente WorkSpaces que está inscrito no Office 2016 para o pacote BYOL que está inscrito no Office 2019. Para obter mais informações, consulte Migrar a. WorkSpace

Você pode usar essas opções para migrar os WorkSpaces que estão inscritos no Microsoft Office para os aplicativos do AWS Microsoft 365. No entanto, gerenciar aplicativos se limita à desinstalação do Microsoft Office do seu WorkSpace. Você deve trazer suas próprias ferramentas e instaladores para instalar os aplicativos Microsoft 365 em seu WorkSpaces.

> **Note**
>
> Usando aplicativos de gerenciamento, você pode instalar ou desinstalar o Microsoft Office, o Microsoft Visio ou MicrosoftProject 2021 no seu WorkSpaces. Para as versões do Microsoft Office 2016 ou 2019, você só pode removê-las do seu WorkSpaces. Para instalar o Microsoft Office 2016 ou 2019 no seu WorkSpaces, migre um WorkSpace.

Para obter mais informações sobre o processo de migração, consulte Migre um WorkSpace.

Cancelar a assinatura do Office

As opções a seguir descrevem como cancelar a assinatura do Office.

- Gerenciar aplicativos (recomendado) - Você pode desinstalar o Microsoft Office e outros aplicativos, como o Microsoft Visio e o Microsoft Project, do seu WorkSpaces. Para obter mais informações, consulte Manage applications.
- Migrar um WorkSpace - Você pode criar um pacote BYOL que não esteja inscrito no Office. Em seguida, use o recurso de WorkSpaces migração para migrar seu BYOL existente WorkSpaces para o pacote BYOL que não está inscrito no Office. Para ter mais informações, consulte Migre um WorkSpace.

Atualizações do Office

Se você se inscreveu no Office por meio de AWS, as atualizações do Office são incluídas como parte de suas atualizações regulares do Windows. Para ficar em dia sobre todos os patches e atualizações de segurança, recomendamos que você atualize periodicamente as imagens BYOL base.

Etapa 1: verifique a elegibilidade da sua conta para BYOL usando o console da Amazon WorkSpaces

Antes de habilitar sua conta para BYOL, você deve passar por um processo de verificação para confirmar sua elegibilidade para o BYOL. Até que você passe por esse processo, a opção Enable BYOL não estará disponível no WorkSpaces console da Amazon.

> **Note**
>
> O processo de verificação leva pelo menos um dia útil. Se quiser aplicar o intervalo CIDR e as configurações de BYOL de uma AWS conta existente a uma conta diferente, você pode vinculá-las para usar o mesmo hardware subjacente. Para vincular suas AWS contas, você não precisa enviar um ticket de suporte. Você pode usar APIs, como CreateAccountLinkInvitationse AcceptAccountLinkInvitationpara conectar suas AWS contas. Para ter mais informações, consulte Vincular contas BYOL.

Para verificar a elegibilidade da sua conta para BYOL usando o console da Amazon WorkSpaces

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, escolha Configurações da conta e, em Traga sua própria licença (BYOL), escolha Exibir configurações de WorkSpaces BYOL. Se sua conta não estiver qualificada para BYOL, uma mensagem apresenta orientações para as próximas etapas. Para

começar, entre em contato com seu gerente de AWS conta ou representante de vendas, ou entre em contato com o AWS Support Centro. Seu contato verificará sua elegibilidade para BYOL.

Para determinar sua elegibilidade para o BYOL, seu contato precisará de algumas informações. Por exemplo, talvez seja necessário responder às perguntas a seguir.

- Você revisou e aceitou os requisitos de BYOL listados anteriormente?
- Em quais AWS regiões você precisa ativar sua conta para BYOL?
- Quantos BYOL WorkSpaces você planeja implantar por AWS região?
- Qual é o seu plano de crescimento?
- Você está comprando WorkSpaces de um revendedor?
- Quais tipos de pacote você precisa para BYOL?
- Sua organização tem outras AWS contas habilitadas para BYOL na mesma região? Se sim, você deseja vincular essas contas para que elas usem o mesmo hardware subjacente?

  Se as contas estiverem vinculadas, o número total de contas WorkSpaces implantadas nessas contas será agregado para determinar sua elegibilidade para BYOL. Se a resposta para essas duas perguntas for sim, você pode vincular suas contas. Você pode usar APIs, como CreateAccountLinkInvitationse AcceptAccountLinkInvitationpara conectar suas AWS contas. Se você quiser vincular outras contas habilitadas para BYOL, mas quiser usar uma configuração BYOL diferente (intervalo e imagem do CIDR), entre em contato com o AWS Support para habilitar sua nova conta para BYOL.

3. Depois que sua elegibilidade for confirmada para o BYOL, você poderá prosseguir para a próxima etapa, na qual habilitará o BYOL para sua conta no console da Amazon. WorkSpaces

Etapa 2: Habilite o BYOL para sua conta de BYOL usando o console da Amazon WorkSpaces

Para habilitar o BYOL na sua conta, você deve especificar uma interface de rede de gerenciamento. Essa interface está conectada a uma rede de WorkSpaces gerenciamento segura da Amazon. Ele é usado para streaming interativo do WorkSpace desktop para WorkSpaces clientes da Amazon e para permitir que WorkSpaces a Amazon gerencie WorkSpace o.

> **Note**
>
> Você precisa realizar as etapas presentes neste procedimento apenas uma vez por região para habilitar o BYOL na sua conta.

Para habilitar o BYOL para sua conta usando o console da Amazon WorkSpaces

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, escolha Configurações da conta e, em Traga sua própria licença (BYOL), escolha Exibir configurações de WorkSpaces BYOL.
3. Na página Configurações da conta, em Traga a sua própria licença (BYOL), selecione Habilitar BYOL.

   Se a opção Habilitar BYOL não estiver presente, isso significa que sua conta não está atualmente qualificada para BYOL. Para ter mais informações, consulte Etapa 1: verifique a elegibilidade da sua conta para BYOL usando o console da Amazon WorkSpaces .
4. Em Bring Your Own License (BYOL) (Traga sua própria licença), na área Management network interface IP address range (Intervalo de endereços IP da rede de gerenciamento), escolha um intervalo de endereços IP e selecione Display available CIDR blocks (Exibir blocos CIDR disponíveis).

   WorkSpaces A Amazon pesquisa e exibe os intervalos de endereços IP disponíveis como blocos IPv4 Classless Inter-Domain Routing (CIDR), dentro do intervalo que você especificar. Se você precisar de um intervalo de endereços IP determinado, pode editar o intervalo de pesquisa.

   > **Important**
   >
   > Depois de especificar um intervalo de endereços IP, você não poderá modificá-lo. Lembre-se de especificar um intervalo de endereços IP que não entre em conflito com os intervalos usados em sua rede interna. Se você tiver alguma dúvida sobre qual faixa especificar, entre em contato com seu gerente de AWS conta ou representante de vendas, ou entre em contato com o AWS Support Centro antes de continuar.
5. Escolha o bloco CIDR que você deseja na lista de resultados e, em seguida, escolha Enable BYOL (Ativar BYOL).

Esse processo pode levar várias horas. Enquanto WorkSpaces estiver habilitando sua conta para BYOL, vá para a próxima etapa.

Etapa 3: Executar o PowerShell script BYOL Checker em uma VM do Windows

Depois de habilitar o BYOL para a sua conta, você deve confirmar se a VM atende aos requisitos de BYOL. Para fazer isso, execute estas etapas para baixar e executar o script WorkSpaces BYOL Checker PowerShell . O script executa uma série de testes na VM que você planeja usar para criar sua imagem.

> **Important**
>
> A VM deve passar em todos os testes para que você possa usá-la para BYOL.

Para fazer o download do script BYOL Checker

Antes de fazer download e executar o script BYOL Checker, verifique se as atualizações de segurança do Windows mais recentes estão instaladas na sua VM. Enquanto o script é executado, ele desativa o serviço Windows Update.

1. Baixe o arquivo.zip do script BYOL Checker de https://tools.amazonworkspaces.com/BYOLChecker.zip para sua pasta. `Downloads`
2. Na pasta `Downloads`, crie uma pasta `BYOL`.
3. Extraia os arquivos de `BYOLChecker.zip` e copie-os na pasta `Downloads\BYOL`.
4. Exclua a pasta `Downloads\BYOLChecker.zip` para que apenas os arquivos extraídos permaneçam.

Realize essas etapas para executar o script BYOL Checker.

Para executar o script BYOL Checker

1. Na área de trabalho do Windows, abra o Windows PowerShell. Escolha o botão Iniciar do Windows, clique com o botão direito do mouse em Windows PowerShell e escolha Executar

como administrador. Se você for solicitado pelo Controle de Conta de Usuário a escolher se deseja PowerShell fazer alterações em seu dispositivo, escolha Sim.

2. No prompt de PowerShell comando, vá para o diretório em que o script BYOL Checker está localizado. Por exemplo, se o script estiver localizado no diretório `Downloads\BYOL`, insira o seguinte comando e pressione Enter:

   ```
   cd C:\Users\username\Downloads\BYOL
   ```

3. Digite o comando a seguir para atualizar a política de PowerShell execução no computador. Isso permite que o script BYOL Checker execute:

   ```
   Set-ExecutionPolicy AllSigned
   ```

4. Quando solicitado a confirmar se deseja alterar a política de PowerShell execução, insira A para especificar Sim para Todos.

5. Insira o comando a seguir para executar o script BYOL Checker.

   ```
   .\BYOLChecker.ps1
   ```

6. Se uma notificação de segurança for exibida, pressione a tecla R para executar uma vez.

7. Na caixa de diálogo Validação de WorkSpaces imagem, escolha Iniciar testes.

8. Após a conclusão de cada teste, você pode visualizar o status do teste. Para qualquer teste com o status FAILED (Com falha), selecione Info (Informações) para exibir informações sobre como resolver o problema que provocou a falha. Se algum teste exibir o status WARNING (Aviso), selecione o botão Fix all warnings (Corrigir todos os avisos).

9. Se aplicável, resolva qualquer problema que causam avisos e falhas de teste e repita Step 7 e Step 8 até que a VM passe em todos os testes. Todas as falhas e avisos devem ser resolvidos antes de exportar a VM.

10. O script do BYOL Checker gera dois arquivos de registro, `BYOLPrevalidationlog`*`YYYY-MM-DD_HHmmss`*`.txt` e `ImageInfo.text`. Esses arquivos estão localizados no diretório que contém os arquivos do script BYOL Checker.

    > **Tip**
    >
    > Não exclua esses arquivos. Se ocorrer algum problema, eles poderão ajudar a resolver.

11. Depois que sua VM é aprovada em todos os testes, você recebe a mensagem Validation Successful (Validação bem-sucedida). Revise as configurações regionais da VM exibidas na

ferramenta. Para atualizar as configurações regionais, siga estas instruções na documentação da Microsoft e execute o script BYOL Checker novamente.

12. Desligue a VM e crie um snapshot dela.
13. Inicie a VM novamente. Escolha Run Sysprep (Executar o Sysprep). Se o Sysprep for bem-sucedido, a VM exportada após Step 12 poderá ser importada para o Amazon Elastic Compute Cloud (Amazon EC2). Caso contrário, revise os logs do Sysprep, reverta para o snapshot criado em Step 12, resolva os problemas relatados, crie um snapshot e execute o script do BYOL Checker novamente.

    O motivo mais comum para o Sysprep falhar é que os pacotes Modern AppX não estão desinstalados para todos os usuários. Use o Remove-AppxPackage PowerShell cmdlet para remover os pacotes AppX.
14. Depois de criar sua imagem com sucesso, você pode remover a conta WorkSpaces_BYOL.

Lista de mensagens de erro e correções de erros

A importação de BYOL requer o Powershell 4.0 ou superior. A versão instalada do não PowerShell é suportada.

PowerShell a versão 4.0 ou posterior deve ser instalada. Para obter mais informações, consulte Microsoft Windows PowerShell.

A importação de BYOL não é compatível com sistemas que têm uma instalação ativa do Microsoft Office.

O Microsoft Office deve ser desinstalado antes da importação. Para obter mais informações, consulte Como desinstalar o Office de um PC.

A importação de BYOL requer um sistema sem um agente PCoIP.

Desinstale o agente PCoIP. Para obter informações sobre como desinstalar o agente PCoIP, consulte Como desinstalar o cliente de software Teradici PCoIP para Mac

A importação de BYOL requer que as atualizações do Windows estejam desabilitadas.

Saiba como desabilitar as atualizações do Windows seguindo as seguintes etapas:

1. Pressione a tecla Windows + R. Digite `services.msc` e, em seguida, pressione Enter.

2. Clique com o botão direito do mouse em Windows Update e selecione Propriedades.
3. Na guia Geral, defina o Tipo de inicialização como Desativado.
4. Escolha Parar.
5. Clique em Aplicar e, em seguida, em OK.
6. Reinicie o computador.

A importação de BYOL exige que a montagem automática esteja habilitada.

Você deve ativar a montagem automática. Execute o seguinte comando no PowerShell como administrador:

```
C:\> diskpart
DISKPART> automount enable
```

A montagem automática de novos volumes foi ativada.

A importação de BYOL exige que a conta WorkSpaces _BYOL esteja ativada

WorkSpacesA conta _BYOL deve estar ativada. Para obter mais informações, consulte Habilitar BYOL para sua conta de BYOL usando o console da Amazon WorkSpaces .

A importação de BYOL exige que a interface de rede use DHCP para atribuir automaticamente um endereço IP. No momento, a interface de rede está usando um endereço IP estático.

A interface de rede deve ser alterada para usar DHCP. Para obter mais informações, consulte Como alterar as configurações de TCP/IP.

A importação de BYOL requer mais de 20 GB de espaço no disco local.

O disco local deve ter espaço suficiente e exige que você libere 20 GB ou mais.

A importação de BYOL requer sistemas com uma unidade local. Existem unidades locais, removíveis ou de rede adicionais.

Somente as unidades C e D podem estar presentes em uma WorkSpace que é usada para importar uma imagem. Remova todas as outras unidades, incluindo unidades virtuais.

A importação de BYOL requer o Windows 10 ou o Windows 11.

Use um sistema operacional Windows 10 ou Windows 11.

A importação de BYOL requer sistemas que não estejam associados a um domínio do AD.

O sistema deve ser desassociado do domínio do AD. Para obter mais informações, consulte Perguntas frequentes sobre o gerenciamento de dispositivos do Azure Active Directory.

A importação de BYOL requer sistemas que não estejam associados a um domínio do Azure.

O sistema deve ser desassociado do domínio Azure. Para obter mais informações, consulte Perguntas frequentes sobre o gerenciamento de dispositivos do Azure Active Directory.

A importação de BYOL exige que o firewall público do Windows esteja desabilitado.

O perfil do firewall público deve estar desabilitado. Para obter mais informações, consulte Como habilitar ou desabilitar o Microsoft Defender Firewall.

A importação de BYOL requer um sistema sem ferramentas da VMware.

As ferramentas da VMware devem ser desinstaladas. Para obter mais informações, consulte Como desinstalar e instalar manualmente o VMware Tools no VMware Fusion (1014522).

A importação de BYOL exige que o disco local seja inferior a 80 GB.

O arquivo deve ter menos de 80 GB. Reduza o tamanho do disco.

A importação de BYOL requer menos de duas partições na unidade local. Além disso, todas as partições do Windows 10 devem ser separadas por MBR e todas as partições do Windows 11 devem ser separadas por GPT.

Os volumes devem ser separados por MBR para o Windows 10 e por GPT para o Windows 11. Para obter mais informações, consulte Como gerenciar discos.

A importação de BYOL requer a conclusão de todas as atualizações pendentes que exigem reinicializações.

Instale todas as atualizações e reinicie o sistema operacional.

A importação de BYOL exige que AutoLogon esteja desativada.

Para desativar o AutoLogon registro:

1. Pressione a tecla Windows +R e digite `Regedit.exe` o prompt de comando.
2. Role para baixo até `HKEY_LOCAL_Machine\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon`.

3. Adicione um valor para `DontDisplayLastUserName`.
4. Em Tipo, insira `REG_SZ`.
5. Em Valor, insira `0`.

> **Note**
>
> - O valor `DontDisplayLastUserName` determina se a caixa de diálogo de login exibe o nome de usuário do último usuário que fez login no PC.
> - O valor não existe por padrão. Se existir, você deve defini-lo como `0` ou o valor de `DefaultUser` será apagado e AutoLogon falhará.

A importação de BYOL requer que **`RealTimeIsUniversal`** esteja habilitada.

RealTimeUniversal A chave do registro deve estar ativada. Para obter mais informações, consulte Como configurar as definições de horário para o Windows Server 2008 e posterior.

A importação de BYOL requer um sistema com uma partição inicializável.

O número de partições inicializáveis não deve exceder um.

Como remover partições adicionais

1. Pressione as teclas de logo do Windows + R para abrir a caixa Executar. Digite `msconfig` e pressione Enter no teclado para abrir a janela Configuração do Sistema.
2. Selecione a guia Inicialização na janela e verifique se o sistema operacional que você deseja usar está definido como Sistema Operacional atual; Sistema Operacional padrão. Se não estiver definido, escolha o sistema operacional desejado na janela e clique em Definir como padrão na mesma janela.
3. Para excluir outra partição, selecione essa partição e clique em Excluir, Aplicar, OK.

Se o erro persistir, reinicialize o computador a partir do disco de instalação ou de reparo e siga estas etapas.

1. Ignore a tela inicial de idiomas e escolha Reparar o computador na tela de instalação principal.
2. Na tela Escolher uma opção, escolha Solucionar problemas.

3. Na tela Opções avançadas, escolha Prompts de comando.
4. No prompt de comando, digite `bootrec.exe /fixmbr` e pressione Enter.

A importação de BYOL requer um sistema de 64 bits.

Uma imagem de sistema operacional de 64 bits deve ser usada. Para obter mais informações, consulte Versões do Windows compatíveis com o BYOL.

A importação de BYOL requer um sistema que não tenha sido rearmado.

A contagem de rearmação de imagem não deve ser 0. O recurso rearmar permite que você estenda o período de ativação para a versão de avaliação do Windows. O processo de criação de imagem requer que a contagem de rearmação seja um valor diferente de 0.

Como verificar a contagem de rearmação do Windows

1. No menu Iniciar do Windows, escolha Sistema Windows e selecione Prompt de Comando.
2. Em Prompt de Comando, digite `cscript C:\Windows\System32\slmgr.vbs /dlv` e pressione Enter.
3. Para redefinir a contagem de rearmação para um valor diferente de 0. Para obter mais informações, consulte Sysprep (Generalize) uma instalação do Windows.

A importação de BYOL requer um sistema que não foi atualizado no local. Este sistema foi atualizado no local.

O Windows não pode ter sido atualizado de uma versão anterior.

A importação de BYOL requer que nenhum antivírus esteja instalado no sistema.

Você deve desinstalar o software de antivírus. Execute o BYOLChecker para obter detalhes sobre a desinstalação do software de antivírus.

A importação de BYOL requer que os sistemas Windows 10 tenham um modo de inicialização herdado.

O BIOS antigo BootMode deve ser usado para o Windows 10. Para obter mais informações, consulte Modos de inicialização.

Etapa 4: Exportar a VM do ambiente de virtualização

Para criar uma imagem para BYOL, você deve primeiro exportar a VM do seu ambiente de virtualização. A VM deve estar em um único volume com um tamanho máximo de 70 GB e pelo menos 10 GB de espaço livre. Para obter mais informações, consulte a documentação do seu ambiente de virtualização e exporte sua VM a partir do ambiente de virtualização no guia do usuário sobre importação e exportação da VM.

O Windows 11 define novos requisitos de hardware para suporte a Unified Extensible Firmware Interface (UEFI), Trusted Platform Module (TPM) 2.0 e Secure Boot. Exclusivo para importações do Windows 11, o VM Import/Export automaticamente habilita o UEFI Secure Boot usando as teclas da Microsoft e o NitroTPM. Para obter mais informações, consulte Trazendo sua imagem do Windows 11 para AWS com o VM Import/Export.

Etapa 5: Importar a VM como uma imagem para o Amazon EC2

Depois de exportar a VM, analise os requisitos de importação de sistemas operacionais Windows de uma VM. Tome ações conforme necessário. Para obter mais informações, consulte Requisitos do VM Import/Export.

> **Note**
>
> A importação de uma VM com um disco criptografado não é compatível. Se você optou pela criptografia padrão para os volumes do Amazon Elastic Block Store (Amazon EBS), você deve desmarcar essa opção antes de importar a VM.

Importe a VM para o Amazon EC2 como uma imagem de máquina da Amazon (AMI). Use um dos seguintes métodos:

- Use o comando import-image com a AWS CLI. Para obter mais informações, consulte import-image na Referência de comandos da AWS CLI .
- Use a operação de API ImportImage. Para obter mais informações, consulte a ImportImageReferência de API do Amazon EC2.

Para obter mais informações, consulte Como importar uma VM como uma imagem no guia do usuário sobre importação e exportação de VM.

Etapa 6: criar uma imagem BYOL usando o console WorkSpaces

Execute essas etapas para criar uma imagem WorkSpaces BYOL.

> **Note**
>
> Para realizar esse procedimento, verifique se você tem permissões AWS Identity and Access Management (IAM) para:
>
> - Ligue WorkSpaces **`ImportWorkspaceImage`**.
> - Chamar o **`DescribeImages`** do Amazon EC2 na imagem do EC2 que você deseja usar para criar a imagem BYOL.
> - Chamar o **`ModifyImageAttribute`** do Amazon EC2 na imagem do EC2 que você deseja usar para criar a imagem BYOL. Garanta que as permissões de execução na imagem do Amazon EC2 não sejam restritas. A imagem deve ser compartilhável durante todo o processo de criação da imagem BYOL.
>
> Para ver um exemplo de política do IAM específica para BYOL WorkSpaces, consulteGerenciamento de identidade e acesso para o WorkSpaces. Para obter mais informações sobre como usar permissões do IAM, consulte Como alterar permissões para um usuário do IAM no Guia do usuário do IAM.
> Para criar um Graphics.G4dn, GraphicsPro .g4dn, Graphics ou um GraphicsPro pacote a partir da sua imagem, entre em contato com o AWS Support Centro para que sua conta seja adicionada à lista de permissões. Depois que sua conta estiver na lista de permissões, você poderá usar o AWS CLI import-workspace-image comando para ingerir os gráficos.g4dn, GraphicsPro .g4dn, gráficos ou imagem. GraphicsPro Para obter mais informações, consulte import-workspace-image na Referência de comandos da AWS CLI .

Para criar uma imagem a partir da VM do Windows

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecione Images (Imagens).
3. Escolha Criar imagem BYOL.
4. Na página Criar imagem BYOL, faça o seguinte:

- Para AMI ID, escolha o link do console EC2 e escolha a imagem do Amazon EC2 que você importou conforme descrito na seção anterior (Etapa 5: Importar a VM como uma imagem para o Amazon EC2). O nome da imagem deve começar com `ami-` e ser seguido pelo identificador da AMI (por exemplo, `ami-1234567e`).
- Em Nome de imagem, insira um nome exclusivo para a imagem.
- Em Descrição da imagem, insira uma descrição que ajude a identificar rapidamente a imagem.
- Em Tipo de instância, escolha o tipo de pacote apropriado (Regular, Graphics.G4dn, Graphics ou GraphicsPro), dependendo do protocolo que você deseja usar para sua imagem, seja PCoIP ou Streaming Protocol (WSP). WorkSpaces Se você quiser criar um pacote GraphicsPro .g4dn, escolha Graphics.g4dn. Para pacotes não habilitados para GPU (pacotes diferentes de Graphics.g4dn, .g4dn, Graphics ou), escolha Regular. GraphicsPro GraphicsPro

  > **Note**
  >
  > - Gráficos.g4dn, GraphicsPro .g4dn, gráficos e GraphicsPro imagens só podem ser criados para o protocolo PCoIP no momento.
  > - As imagens do Windows 11 só podem ser criadas para o protocolo WSP.
  > - No momento, os pacotes Graphics.g4dn GraphicsPro e.g4dn não estão disponíveis para o Windows 11.
  > - Gráficos e GraphicsPro imagens não são compatíveis com o Windows 11.

- (Opcional) Em Selecionar aplicações, escolha qual versão do Microsoft Office você deseja assinar. Para ter mais informações, consulte Adicionar o Microsoft Office a uma imagem BYOL.
- (Opcional) Em Tags, escolha Adicionar nova tag para associar etiquetas a essa imagem. Para ter mais informações, consulte Marcar recursos do WorkSpaces.

5. Escolha Criar imagem BYOL.

   Enquanto a imagem estiver sendo criada, o status dela na página Imagens do console aparece como Pendente. O processo de ingestão do BYOL leva no mínimo 90 minutos. Se você também se inscreveu no Office, o processo deve levar no mínimo três horas.

   Se a validação da imagem não for bem-sucedida, o console exibirá um código de erro. Quando a criação da imagem estiver concluída, o status muda para Available (Disponível).

Etapa 7: Criar um pacote personalizado com base na imagem BYOL

Depois que sua imagem de BYOL estiver criada, você pode usá-la para criar um pacote personalizado. Para obter mais informações, consulte Crie uma WorkSpaces imagem e um pacote personalizados.

Etapa 8: registrar um diretório dedicado para WorkSpaces

Para usar imagens BYOL para WorkSpaces, você deve registrar um diretório para essa finalidade.

Para registrar um diretório para WorkSpaces

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, selecionar Diretórios.
3. Selecione o diretório e escolha Actions (Ações), Register (Registro).
4. Na caixa de diálogo Registrar diretório, em Ativar dedicado WorkSpaces, escolha Sim.
5. Escolha Register.

Se você já registrou um AWS Managed Microsoft AD diretório ou um diretório do AD Connector WorkSpaces que não é executado em hardware dedicado, você pode configurar um novo AWS Managed Microsoft AD diretório ou diretório do AD Connector para essa finalidade. Você também pode cancelar o registro do diretório e depois registrá-lo novamente como um diretório dedicado. WorkSpaces Para fazer isso, siga estas etapas.

> **Note**
>
> Você só poderá executar esse procedimento se nenhum WorkSpaces estiver associado ao diretório.

Para cancelar o registro de um diretório e registrá-lo novamente para um diretório dedicado WorkSpaces

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. Encerrar o existente WorkSpaces.
3. No painel de navegação, selecionar Diretórios.
4. Selecione o diretório e escolha Ações, Cancelar o registro.

5. Quando a confirmação for solicitada, escolha Cancelar registro.
6. Selecione o diretório novamente e selecione Actions (Ações), Register (Registro).
7. Na caixa de diálogo Registrar diretório, em Ativar dedicado WorkSpaces, escolha Sim.
8. Escolha Register.

Etapa 9: Inicie seu BYOL WorkSpaces

Depois de registrar um diretório para dedicado WorkSpaces, você pode iniciar seu BYOL WorkSpaces nesse diretório. Para obter informações sobre como iniciar WorkSpaces, consulteInicializar uma área de trabalho virtual usando WorkSpaces.

Vincular contas BYOL

Você pode usar a vinculação BYOL para vincular contas e compartilhar configurações de BYOL. As configurações de BYOL incluem o intervalo CIDR usado por suas contas e as imagens que você usa para criar WorkSpaces com sua licença do Windows. Todas as contas vinculadas compartilham a mesma infraestrutura de hardware subjacente.

A conta habilitada para vinculação BYOL é a proprietária principal da infraestrutura de hardware subjacente e é chamada de conta de origem. A conta Source gerencia o acesso à infraestrutura de hardware subjacente. As contas de destino são as contas vinculadas à conta de origem.

> **Important**
>
> No momento, as APIs para vinculação de contas BYOL não estão disponíveis no. AWS GovCloud (US) Region

> **Note**
>
> As AWS contas às quais você deseja se vincular devem fazer parte da sua organização e estar na mesma conta pagante. Você só pode vincular contas dentro da mesma região.

Para vincular as contas de origem e de destino

1. Envie um link de convite da sua conta do Source para a conta do Target usando a CreateAccountLinkInvitationAPI.

2. Aceite o link pendente da sua conta do Target usando a AcceptAccountLinkInvitationAPI.
3. Verifique se o link foi estabelecido usando a API GetAccountLinkou ListAccountLinks.

Monitore seu WorkSpaces

Você pode usar os seguintes recursos para monitorar seu WorkSpaces.

CloudWatch métricas

A Amazon WorkSpaces publica pontos de dados na Amazon CloudWatch sobre você WorkSpaces. CloudWatch permite que você recupere estatísticas sobre esses pontos de dados como um conjunto ordenado de dados de séries temporais, conhecido como métricas. Você pode usar essas métricas para verificar WorkSpaces se o desempenho é o esperado. Para ter mais informações, consulte Monitore suas CloudWatch métricas de WorkSpaces uso.

CloudWatch Eventos

A Amazon WorkSpaces pode enviar eventos para o Amazon CloudWatch Events quando os usuários fazem login no seu WorkSpace. Isso permite que você responda quando o evento ocorrer. Para ter mais informações, consulte Monitore seu WorkSpaces uso da Amazon EventBridge.

CloudTrail troncos

O AWS CloudTrail fornece um registro das ações executadas por um usuário, uma função ou um serviço da AWS no WorkSpaces. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita WorkSpaces, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais. Para obter mais informações, consulte Registrar chamadas de WorkSpaces API usando CloudTrail. AWS CloudTrailregistra eventos de login bem-sucedidos e malsucedidos para usuários de cartões inteligentes. Para ter mais informações, consulte Noções básicas de eventos de login da AWS para usuários de cartão inteligente.

CloudWatch Monitor de Internet

O Amazon CloudWatch Internet Monitor fornece visibilidade sobre como os problemas da Internet afetam o desempenho e a disponibilidade entre seus aplicativos hospedados AWS e seus usuários finais. Você também pode usar o CloudWatch Internet Monitor para:

- Crie monitores para um ou mais WorkSpace diretórios.
- Monitorar a performance da internet.
- Receba alarmes para problemas entre a rede municipal de seus usuários finais, incluindo sua localização e o ASN, que normalmente é o provedor de serviços de Internet (ISP), e suas regiões. WorkSpace

O Monitor de Internet usa os dados de conectividade que a AWS captura de sua rede global para calcular uma linha de base de performance e de disponibilidade para tráfego voltado para a Internet. Atualmente, o Monitor de Internet não fornece performance de internet para usuários finais individuais, mas consegue fornecer para cidades e ISPs.

Monitore sua WorkSpaces saúde usando o painel CloudWatch automático

Você pode monitorar WorkSpaces usando o painel CloudWatch automático, que coleta dados brutos e os processa em métricas legíveis, quase em tempo real. As métricas são mantidas por 15 meses para acessar informações históricas e monitorar o desempenho do seu aplicativo ou serviço web. Você também pode definir alarmes que observam determinados limites e enviam notificações ou realizam ações quando esses limites são atingidos. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.

O CloudWatch painel é criado automaticamente quando você usa sua AWS conta para configurar seu WorkSpaces. O painel permite que você monitore suas WorkSpaces métricas, como a saúde e o desempenho, em todas as regiões. Você também pode usar o painel para as seguintes finalidades:

- Identifique WorkSpace instâncias não íntegras.
- Identifique modos de execução, protocolos e sistemas operacionais que têm WorkSpace instâncias não íntegras.
- Visualize a utilização crítica de recursos ao longo do tempo.
- Identifique anomalias para ajudar na solução de problemas.

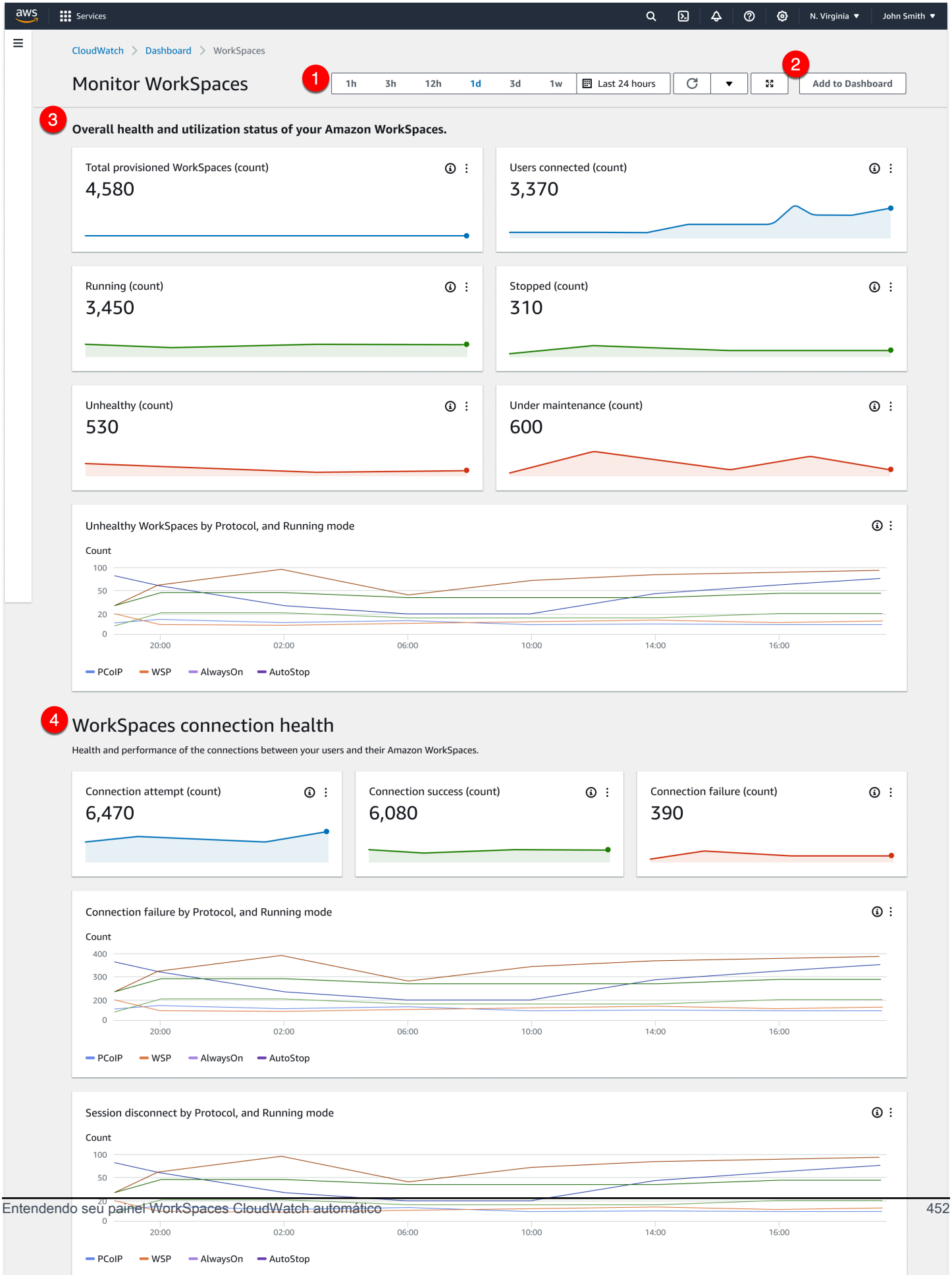
WorkSpaces CloudWatch painéis automáticos estão disponíveis em todas as regiões AWS comerciais.

Para usar o painel WorkSpaces CloudWatch automático

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, escolha Painéis.
3. Escolha a guia Painéis automáticos.
4. Escolha WorkSpaces.

Entendendo seu painel WorkSpaces CloudWatch automático

O painel CloudWatch automático permite que você obtenha informações sobre o desempenho de seus WorkSpaces recursos e ajuda a identificar problemas de desempenho.


aws
Services
N. Virginia
John Smith
CloudWatch > Dashboard > WorkSpaces
Monitor WorkSpaces
1
1h 3h 12h 1d 3d 1w
Last 24 hours
2
Add to Dashboard
3
Overall health and utilization status of your Amazon WorkSpaces.
Total provisioned WorkSpaces (count)
4,580
Users connected (count)
3,370
Running (count)
3,450
Stopped (count)
310
Unhealthy (count)
530
Under maintenance (count)
600
Unhealthy WorkSpaces by Protocol, and Running mode
Count
100
50
20
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop
4
WorkSpaces connection health
Health and performance of the connections between your users and their Amazon WorkSpaces.
Connection attempt (count)
6,470
Connection success (count)
6,080
Connection failure (count)
390
Connection failure by Protocol, and Running mode
Count
400
300
200
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop
Session disconnect by Protocol, and Running mode
Count
100
50
20
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop

O painel consiste nos seguintes recursos:

1. Visualize dados históricos usando controles de intervalo de data e hora.
2. Adicione uma visualização personalizada do painel aos painéis CloudWatch personalizados.
3. Monitore a integridade geral e o status de utilização do seu WorkSpaces fazendo o seguinte:
    a. Veja o número total de instâncias provisionadas WorkSpaces, o número de usuários conectados e o número de instâncias não íntegras e íntegras. WorkSpace
    b. Visualize não WorkSpaces íntegros e suas diferentes variáveis, como protocolo e modo de computação.
    c. Passe o mouse sobre o gráfico de linhas para ver o número de WorkSpace instâncias íntegras ou não íntegras de um protocolo e modo de execução específicos durante um período de tempo.
    d. Escolha o menu de reticências e, em seguida, escolha Exibir em métricas para visualizar as métricas em um gráfico de escala de tempo.
4. Visualize suas métricas de conexão e suas diferentes variáveis, como número de tentativas de conexão, conexões bem-sucedidas e conexões com falha em seu WorkSpaces ambiente a qualquer momento.
5. Visualize InSession as latências que afetam a experiência do usuário, como o tempo de ida e volta (RTT), para determinar a integridade da conexão e a perda de pacotes para monitorar a integridade da rede.
6. Visualize o desempenho do host e a utilização de recursos para identificar e solucionar possíveis problemas de desempenho.

Monitore suas CloudWatch métricas de WorkSpaces uso

WorkSpaces e a Amazon CloudWatch estão integradas, para que você possa reunir e analisar métricas de desempenho. Você pode monitorar essas métricas usando o CloudWatch console, a interface da linha de CloudWatch comando ou programaticamente usando a CloudWatch API. CloudWatch também permite definir alarmes quando você atinge um limite especificado para uma métrica.

Para obter mais informações sobre uso CloudWatch e alarmes, consulte o Guia do CloudWatch usuário da Amazon.

Pré-requisitos

Para obter CloudWatch métricas, habilite o acesso na porta 443 no AMAZON subconjunto na us-east-1Região. Para ter mais informações, consulte Requisitos de endereço IP e porta para WorkSpaces.

Conteúdo

WorkSpaces métricas

O namespace AWS/WorkSpaces inclui as métricas a seguir.

Métrica	Descrição	Dimensões	Statistics	Unidades
Available [1]	O número deles WorkSpaces retornou um status saudável.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Média, soma, máximo, mínimo, amostragens de dados	Contagem
Unhealthy [1]	O número WorkSpaces que retornou um status insalubre.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	Média, soma, máximo, mínimo, amostragens de dados	Contagem

Métrica	Descrição	Dimensões	Statistics	Unidades
		UserName		
ConnectionAttempt [2]	O número de tentativas de conexão.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Média, soma, máximo, mínimo, amostragens de dados	Contagem
ConnectionSuccess [2]	O número de conexões bem-sucedidas.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Média, soma, máximo, mínimo, amostragens de dados	Contagem

Métrica	Descrição	Dimensões	Statistics	Unidades

`ConnectionFailure` [2]	O número de conexões com falha.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
			Média, soma, máximo, mínimo, amostragens de dados	Contagem

`SessionLaunchTime` [2, 6]	A quantidade de tempo necessária para iniciar uma WorkSpaces sessão.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
			Média, soma, máximo, mínimo, amostragens de dados	Segundos (tempo)

`InSessionLatency` [2, 6]	O tempo de ida e volta entre o WorkSpaces cliente e o WorkSpace.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
			Média, soma, máximo, mínimo, amostragens de dados	Milissegundos (tempo)

Métrica	Descrição	Dimensões	Statistics	Unidades

`SessionDisconnect` [2, 6]	O número de conexões que foram fechadas, incluindo conexões com falha e iniciadas pelo usuário.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
			Média, soma, máximo, mínimo, amostragens de dados	Contagem

`UserConnected` [3]	O número WorkSpaces que tem um usuário conectado.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
			Média, soma, máximo, mínimo, amostragens de dados	Contagem

`Stopped`	O número deles WorkSpaces está parado.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
			Média, soma, máximo, mínimo, amostragens de dados	Contagem

Métrica	Descrição	Dimensões	Statistics	Unidades

`Maintenance` [4]	O número deles WorkSpaces está em manutenção.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
			Média, soma, máximo, mínimo, amostragens de dados	Contagem

`TrustedDeviceValidationAttempt` [5, 6]	O número de tentativas de validação da assinatura de autenticação do dispositivo.	`DirectoryId`	Média, soma, máximo, mínimo, amostragens de dados	Contagem
`TrustedDeviceValidationSuccess` [5, 6]	O número de validações da assinatura de autenticação do dispositivo bem-sucedidas.	`DirectoryId`	Média, soma, máximo, mínimo, amostragens de dados	Contagem
`TrustedDeviceValidationFailure` [5, 6]	O número de validações da assinatura de autenticação do dispositivo com falha.	`DirectoryId`	Média, soma, máximo, mínimo, amostragens de dados	Contagem

Métrica	Descrição	Dimensões	Statistics	Unidades
`TrustedDeviceCertificateDaysBeforeExpiration` [6]	Dias restantes até que o certificado raiz associado ao diretório expire.	`CertificateId`	Média, soma, máximo, mínimo, amostragens de dados	Contagem

`CPUUsage`	A porcentagem do recurso de CPU usado.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
			Média, Máxima, Mínima	Porcentagem

`MemoryUsage`	A porcentagem da memória da máquina usada.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
			Média, Máxima, Mínima	Porcentagem

Métrica	Descrição	Dimensões	Statistics	Unidades
RootVolumeDiskUsage	A porcentagem do volume do disco raiz usado.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Média, Máxima, Mínima	Porcentagem
UserVolumeDiskUsage	A porcentagem do volume de disco do usuário usado.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Média, Máxima, Mínima	Porcentagem
UDPPacketLossRate [7]	A porcentagem de pacotes descartados entre o cliente e o gateway.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Média, Máxima, Mínima, Amostras de Dados	Porcentagem

Métrica	Descrição	Dimensões	Statistics	Unidades

`UpTime`	O tempo desde a última reinicialização de um WorkSpace.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
			Média, Máxima, Mínima, Amostras de Dados	Segundos

[1] envia WorkSpaces periodicamente solicitações de status para um WorkSpace. A WorkSpace é marcado `Available` quando responde a essas solicitações e `Unhealthy` quando não responde a essas solicitações. Essas métricas estão disponíveis em um nível de granularidade por WorkSpace nível e também são agregadas para todos WorkSpaces em uma organização.

[2] WorkSpaces registros de métricas sobre as conexões feitas com cada um WorkSpace. Essas métricas são emitidas depois que um usuário se autentica com sucesso por meio do WorkSpaces cliente e o cliente inicia uma sessão. As métricas estão disponíveis em um nível de granularidade por WorkSpace nível e também são agregadas para todas WorkSpaces em um diretório.

[3] envia WorkSpaces periodicamente solicitações de status de conexão para WorkSpace a. Os usuários são reportados como conectados quando estão utilizando ativamente suas sessões. Essa métrica está disponível em um WorkSpace nível de granularidade por nível e também é agregada para todos WorkSpaces em uma organização.

[4] Essa métrica se aplica aos WorkSpaces que estão configurados com um modo de AutoStop execução. Se você tiver a manutenção ativada para o seu WorkSpaces, essa métrica captura o número de pessoas WorkSpaces que estão atualmente em manutenção. Essa métrica está disponível em um WorkSpace nível de granularidade por nível, que descreve quando uma WorkSpace entrou em manutenção e quando foi removida.

[5] Se o recurso de dispositivos confiáveis estiver habilitado para o diretório, a Amazon WorkSpaces usará a autenticação baseada em certificado para determinar se um dispositivo é confiável.

Quando os usuários tentam acessar suas WorkSpaces, essas métricas são emitidas para indicar a autenticação bem-sucedida ou malsucedida do dispositivo confiável. Essas métricas estão disponíveis em um nível de granularidade por diretório e somente para os aplicativos clientes Amazon Windows WorkSpaces e macOS.

[6] Não disponível no WorkSpaces Web Access.

[7] Essa métrica mede a perda média de pacotes.

- No PCoIP: mede a perda média de pacotes no gateway do cliente.
- No WSP: mede a perda média de pacotes do cliente em relação ao gateway.

Dimensões para WorkSpaces métricas

Para filtrar os dados das métricas, use as dimensões a seguir.

Dimensão	Descrição
`DirectoryId`	Filtra os dados métricos para o WorkSpaces no diretório especificado. O formato do ID do diretório é `d-XXXXXXXXXX` .
`WorkspaceId`	Filtra os dados métricos de acordo com o especificado WorkSpace. A forma do WorkSpace ID é `ws-XXXXXXXXXX` .
`CertificateId`	Filtra os dados de métricas para o certifica do raiz especificado associado ao diretório. O formato do ID do certificado é `wsc-XXXXX XXXX` .
`RunningMode`	Filtra os dados métricos de acordo WorkSpace s com seu modo de execução. A forma do modo de execução é AutoStop ou AlwaysOn.
`BundleId`	Filtra os dados métricos de WorkSpaces acordo com o protocolo. A forma do pacote é `wsb-XXXXXXXXXX` .

Dimensão	Descrição
`ComputeType`	Filtra os dados métricos de acordo WorkSpaces com o tipo de computação.
`Protocol`	Filtra os dados métricos de acordo WorkSpaces com o tipo de protocolo.
`UserName`	Filtra os dados métricos WorkSpaces pelo nome do usuário.

Exemplo de monitoramento

O exemplo a seguir demonstra como você pode usar o AWS CLI para responder a um CloudWatch alarme e determinar quais WorkSpaces em um diretório tiveram falhas de conexão.

Para responder a um CloudWatch alarme

1. Determine o diretório ao qual o alarme se aplica usando o comando describe-alarms.

```
aws cloudwatch describe-alarms --state-value "ALARM"

{
  "MetricAlarms": [
    {
      ...
      "Dimensions": [
        {
          "Name": "DirectoryId",
          "Value": "directory_id"
        }
      ],
      ...
    }
  ]
}
```

2. Obtenha a lista de WorkSpaces no diretório especificado usando o comando describe-workspaces.

```
aws workspaces describe-workspaces --directory-id directory_id

{
  "Workspaces": [
    {
      ...
      "WorkspaceId": "workspace1_id",
      ...
    },
    {
      ...
      "WorkspaceId": "workspace2_id",
      ...
    },
    {
      ...
      "WorkspaceId": "workspace3_id",
      ...
    }
  ]
}
```

3. Obtenha as CloudWatch métricas de cada uma WorkSpace no diretório usando o comando get-metric-statistics.

```
aws cloudwatch get-metric-statistics \
--namespace AWS/WorkSpaces \
--metric-name ConnectionFailure \
--start-time 2015-04-27T00:00:00Z \
--end-time 2015-04-28T00:00:00Z \
--period 3600 \
--statistics Sum \
--dimensions "Name=WorkspaceId,Value=workspace_id"

{
  "Datapoints" : [
    {
      "Timestamp": "2015-04-27T00:18:00Z",
      "Sum": 1.0,
      "Unit": "Count"
    },
    {
```

```
      "Timestamp": "2014-04-27T01:18:00Z",
      "Sum": 0.0,
      "Unit": "Count"
    }
  ],
  "Label" : "ConnectionFailure"
}
```

Monitore seu WorkSpaces uso da Amazon EventBridge

Você pode usar eventos da Amazon WorkSpaces para visualizar, pesquisar, baixar, arquivar, analisar e responder a logins bem-sucedidos em seu WorkSpaces. Por exemplo, é possível usar eventos para as seguintes finalidades:

- Armazene ou arquive eventos de WorkSpaces login como registros para futura referência, analise os registros para procurar padrões e tome medidas com base nesses padrões.
- Use o endereço IP da WAN para determinar de onde os usuários estão conectados e, em seguida, use políticas para permitir que os usuários acessem somente arquivos ou dados WorkSpaces que atendam aos critérios de acesso encontrados no tipo de evento de`WorkSpaces Access`.
- Analise os dados de login e execute ações automatizadas usando AWS Lambda.
- Usar controles de política para bloquear o acesso a arquivos e aplicativos de endereços IP não autorizados.
- Descubra a versão WorkSpaces do cliente usada para se conectar WorkSpaces.

A Amazon WorkSpaces emite esses eventos com base no melhor esforço. Os eventos são entregues quase EventBridge em tempo real. Com EventBridge, você pode criar regras que acionam ações programáticas em resposta a um evento. Por exemplo, é possível configurar uma regra que invoque um tópico do SNS para enviar uma notificação por e-mail ou que invoque uma função do Lambda para realizar alguma ação. Para obter mais informações, consulte o Guia EventBridge do usuário da Amazon.

WorkSpaces Acesse eventos

WorkSpaces aplicativos clientes enviam `WorkSpaces Access` eventos quando um usuário faz login com sucesso em um WorkSpace. Todos os WorkSpaces clientes enviam esses eventos.

Os eventos emitidos para WorkSpaces usar o WorkSpaces Streaming Protocol (WSP) exigem a versão 4.0.1 ou posterior do aplicativo WorkSpaces cliente.

Os eventos são representados como objetos JSON. A seguir, um exemplo de dados para um evento de `WorkSpaces Access`.

```
{
    "version": "0",
    "id": "64ca0eda-9751-dc55-c41a-1bd50b4fc9b7",
    "detail-type": "WorkSpaces Access",
    "source": "aws.workspaces",
    "account": "123456789012",
    "time": "2023-04-05T16:13:59Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "clientIpAddress": "192.0.2.3",
        "actionType": "successfulLogin",
        "workspacesClientProductName": "WorkSpacesWebClient",
        "loginTime": "2023-04-05T16:13:37.603Z",
        "clientPlatform": "Windows",
        "directoryId": "domain/d-123456789",
        "clientVersion": "5.7.0.3472",
        "workspaceId": "ws-xyskdga"
    }
}
```

Campos específicos de eventos

`clientIpAddress`

O endereço IP da WAN do aplicativo cliente. Para clientes zero PCoIP, este é o endereço IP do cliente de autenticação Teradici.

`actionType`

Esse valor é sempre `successfulLogin`.

`workspacesClientProductName`

Os valores a seguir diferenciam maiúsculas de minúsculas.

- `WorkSpaces Desktop client`: clientes Windows, macOS e Linux
- `Amazon WorkSpaces Mobile client`: cliente iOS

- `WorkSpaces Mobile Client`: cliente Android
- `WorkSpaces Chrome Client`: cliente Chromebook
- `WorkSpacesWebClient`: cliente do Acesso via Web
- `AmazonWorkSpacesThinClient`— Dispositivo Amazon WorkSpaces Thin Client
- `Teradici PCoIP Zero Client, Teradici PCoIP Desktop Client, or Dell Wyse PCoIP Client` : cliente Zero

`loginTime`

A hora em que o usuário fez login no WorkSpace.

`clientPlatform`

- `Android`
- `Chrome`
- `iOS`
- `Linux`
- `OSX`
- `Windows`
- `Teradici PCoIP Zero Client and Tera2`
- `Web`

`directoryId`

O identificador do diretório para WorkSpace o. Você deve acrescentar `domain/` antes do identificador do diretório. Por exemplo, `"domain/d-123456789"`.

`clientVersion`

A versão do cliente usada para se conectar WorkSpaces a.

`workspaceId`

O identificador da WorkSpace.

Crie uma regra para lidar com WorkSpaces eventos

Use o procedimento a seguir para criar uma regra para lidar com os WorkSpaces eventos.

Pré-requisito

Para receber notificações por e-mail, crie um tópico do Amazon Simple Notification Service.

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. No painel de navegação, escolha Tópicos.
3. Escolha Criar tópico.
4. Em Tipo, escolha Padrão.
5. Em Name (Nome), digite um nome para o tópico.
6. Escolha Criar tópico.
7. Selecione Criar assinatura.
8. Em Protocolo, escolha Email.
9. Em Endpoint, insira o endereço de e-mail que receberá as notificações.
10. Selecione Criar assinatura.
11. Você receberá uma mensagem de e-mail com esta linha de assunto: AWS Notification - Subscription Confirmation. Siga as instruções para confirmar sua assinatura.

Para criar uma regra para lidar com WorkSpaces eventos

1. Abra o EventBridge console da Amazon em https://console.aws.amazon.com/events/.
2. Escolha a opção Criar regra.
3. Em Name (Nome), insira um nome para a regra.
4. Em Rule type (Tipo de regra), selecione Rule with an event pattern (Regra com um padrão de evento).
5. Selecione Next (Próximo).
6. Em Event pattern (Padrão de evento), faça o seguinte:
    a. Em Event source, escolha Serviços da AWS.
    b. Para AWS service (Serviço da AWS), escolha WorkSpaces.
    c. Em Tipo de evento, escolha WorkSpacesAcesso.
    d. Por padrão, enviamos notificações para cada evento. Se preferir, você pode criar um padrão de evento que filtra eventos para clientes ou espaços de trabalho específicos.
7. Escolha Próximo.

8. Especifique um destino desta forma:
    a. Em Target types (Tipos de destino), escolha AWS service (Serviço da AWS).
    b. Em Select a target (Selecionar um destino), escolha SNS topic (Tópico do SNS).
    c. Em Tópico, escolha o tópico do SNS que você criou para as notificações.
9. Escolha Próximo.
10. (Opcional) Adicione etiquetas à regra.
11. Escolha Próximo.
12. Escolha a opção Criar regra.

Noções básicas de eventos de login da AWS para usuários de cartão inteligente

O AWS CloudTrail registra em log eventos de login com e sem sucesso para usuários de cartões inteligentes. Isso inclui eventos de login que são capturados sempre que um usuário é solicitado a resolver um desafio ou fator específico de credencial, bem como o status dessa solicitação específica de verificação de credencial. Um usuário é conectado somente após concluir todos os desafios de credenciais necessários, o que resulta no registro em log de um evento `UserAuthentication`.

A tabela a seguir captura cada um dos nomes de eventos de login do CloudTrail e suas finalidades.

Nome do evento	Objetivo do evento
`CredentialChallenge`	Notifica que o login da AWS solicitou que o usuário resolva um desafio de credencial específico e especifica o `CredentialType` necessário (por exemplo, SMARTCARD).
`CredentialVerification`	Notifica que o usuário tentou resolver uma solicitação `CredentialChallenge` específica e especifica se a credencial foi bem-sucedida ou falhou.
`UserAuthentication`	Notifica que todos os requisitos de autenticação pelos quais o usuário foi desafiado foram concluídos e que o usuário foi conectado com sucesso. Quando os usuários não conseguem concluir com sucesso os desafios

Nome do evento	Objetivo do evento
	de credenciais necessários, nenhum evento `UserAuthentication` é registrado em log.

A tabela a seguir captura outros campos úteis de dados de eventos contidos em eventos específicos de login do CloudTrail.

Nome do evento	Objetivo do evento	Aplicabilidade do evento de login	Exemplos de valores
`AuthWorkflowID`	Correlaciona todos os eventos emitidos em toda a sequência de login. Para cada login de usuário, vários eventos podem ser emitidos pelo login da AWS.	`CredentialChallenge` , `CredentialVerification` , `UserAuthentication`	“AuthWorkflowID”: “9de74b32-8362-4a01-a524-de21df59fd83”
`CredentialType`	Notifica que o usuário tentou resolver uma solicitação `CredentialChallenge` específica e especifica se a credencial foi bem-sucedida ou falhou.	`CredentialChallenge` , `CredentialVerification` , `UserAuthentication`	“CredentialType”: “SMARTCARD” (valores possíveis hoje: SMARTCARD)
`LoginTo`	Notifica que todos os requisitos de autenticação pelos quais o usuário foi desafiado foram concluídos e que o usuário foi conectado com sucesso. Quando os usuários não conseguem concluir com sucesso os desafios de credencia	`UserAuthentication`	“LoginTo”: “https://skylight.local”

Nome do evento	Objetivo do evento	Aplicabilidade do evento de login	Exemplos de valores
	is necessários, nenhum evento `UserAuthentication` é registrado em log.		

Exemplos de eventos para cenários de login da AWS

Os exemplos a seguir mostram a sequência esperada de eventos do CloudTrail para diferentes cenários de login.

Índice

Login bem-sucedido ao autenticar com cartão inteligente

A sequência de eventos a seguir captura um exemplo de login bem-sucedido com cartão inteligente.

CredentialChallenge


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:29Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialChallenge",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
```

```
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "65551a6d-654a-4be8-90b5-bbfef7187d3a",
    "eventID": "fb603838-f119-4304-9fdc-c0f947a82116",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialChallenge": "Success"
    }
}
```

CredentialVerification bem-sucedida

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:39Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialVerification",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
```

```
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "81869203-1404-4bf2-a1a4-3d30aa08d8d5",
    "eventID": "84c0a2ff-413f-4d0f-9108-f72c90a41b6c",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialVerification": "Success"
    }
}
```

UserAuthentication bem-sucedida

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:39Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "UserAuthentication",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "LoginTo": "https://skylight.local",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "81869203-1404-4bf2-a1a4-3d30aa08d8d5",
```

```
    "eventID": "acc0dba8-8e8b-414b-a52d-6b7cd51d38f6",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        UserAuthentication": "Success"
    }
}
```

Falha no login ao autenticar com cartão inteligente

A sequência de eventos a seguir captura um exemplo de falha no login com cartão inteligente.

CredentialChallenge

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:06Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialChallenge",
    "awaRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "73dfd26b-f812-4bd2-82e9-0b2abb358cdb",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "73eb499d-91a8-4c18-9c5d-281fd45ab50a",
```

```
    "eventID": "f30a50ec-71cf-415a-a5ab-e287edc800da",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialChallenge": "Success"
    }
}
```

Falha na CredentialVerification

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:13Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialVerification",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "73dfd26b-f812-4bd2-82e9-0b2abb358cdb",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "051ca316-0b0d-4d38-940b-5fe5794fda03",
    "eventID": "4e6fbfc7-0479-48da-b7dc-e875155a8177",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
```

```
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialVerification": "Failure"
    }
}
```

Continuidade de negócios para a Amazon WorkSpaces

A Amazon WorkSpaces se baseia na infraestrutura AWS global, que é organizada em AWS regiões e zonas de disponibilidade. Essas regiões e zonas de disponibilidade fornecem resiliência em termos de isolamento físico e redundância de dados. Para ter mais informações, consulte Resiliência no Amazon WorkSpaces.

A Amazon WorkSpaces também fornece redirecionamento entre regiões, um recurso que funciona com suas políticas de roteamento do Sistema de Nomes de Domínio (DNS) para redirecionar seus WorkSpaces usuários para uma alternativa WorkSpaces quando a principal não está disponível. WorkSpaces Por exemplo, usando políticas de roteamento de failover de DNS, você pode conectar seus usuários à sua WorkSpaces região de failover especificada quando eles não puderem acessar a WorkSpaces região primária.

Você pode usar o redirecionamento entre regiões para obter resiliência regional e alta disponibilidade. Você também pode usá-lo para outros fins, como distribuição de tráfego ou fornecimento de alternativas WorkSpaces durante os períodos de manutenção. Se você usa o Amazon Route 53 para sua configuração de DNS, você pode aproveitar as verificações de saúde que monitoram os alarmes da Amazon CloudWatch .

O Amazon WorkSpaces Multi-Region Resilience fornece infraestrutura de desktop virtual automatizada e redundante em uma WorkSpace região secundária e simplifica o processo de redirecionamento de usuários para a região secundária quando a região primária está inacessível devido a interrupções.

Você pode usar a resiliência WorkSpaces multirregional com redirecionamento entre regiões para implantar uma infraestrutura redundante de desktop virtual em uma WorkSpace região secundária e projetar uma estratégia de failover entre regiões em preparação para eventos disruptivos. Você também pode usar essa solução para outros fins, como distribuição de tráfego ou fornecimento de alternativas WorkSpaces durante os períodos de manutenção. Se você usa o Route 53 para sua configuração de DNS, pode aproveitar as verificações de saúde que monitoram os CloudWatch alarmes.

Conteúdo

Redirecionamento entre regiões para a Amazon WorkSpaces

Com o recurso de redirecionamento entre regiões na Amazon WorkSpaces, você pode usar um nome de domínio totalmente qualificado (FQDN) como código de registro para seu. WorkSpaces O redirecionamento entre regiões funciona com suas políticas de roteamento do Sistema de Nomes de Domínio (DNS) para redirecionar seus WorkSpaces usuários para uma alternativa WorkSpaces quando a principal não está disponível. WorkSpaces Por exemplo, usando políticas de roteamento de failover de DNS, você pode conectar seus usuários à sua WorkSpaces AWS região de failover especificada quando eles não conseguem acessar a WorkSpaces região primária.

Use o redirecionamento entre regiões junto com as políticas de roteamento por failover de DNS para obter resiliência regional e alta disponibilidade. Você também pode usar esse recurso para outros fins, como distribuição de tráfego ou fornecimento de alternativas WorkSpaces durante os períodos de manutenção. Se você usa o Amazon Route 53 para sua configuração de DNS, você pode aproveitar as verificações de saúde que monitoram os alarmes da Amazon CloudWatch .

Para usar esse recurso, você deve configurar WorkSpaces para seus usuários em duas (ou mais) AWS regiões. Também é necessário criar códigos de registro especiais baseados em FQDN, denominados aliases de conexão. Esses aliases de conexão substituem os códigos de registro específicos da região para seus usuários. WorkSpaces (Os códigos de registro específicos da região permanecem válidos. No entanto, para que o redirecionamento entre regiões funcione, os usuários devem usar o FQDN como o código de registro.)

Para criar um alias de conexão, especifique uma string de conexão, que é o FQDN, como `www.example.com` ou `desktop.example.com`. Para usar esse domínio para redirecionamento entre regiões, registre-o em um registrador de domínio e configure o serviço de DNS para o domínio.

Depois de criar seus aliases de conexão, você os associa aos seus WorkSpaces diretórios em diferentes regiões para criar pares de associação. Cada par de associação tem uma região principal e uma ou mais regiões de failover. Se ocorrer uma interrupção na região primária, suas políticas de roteamento de failover de DNS redirecionarão seus WorkSpaces usuários para WorkSpaces aquela que você configurou para eles na região de failover.

Para designar as regiões primária e de failover, defina a prioridade da região (primária ou secundária) ao configurar as políticas de roteamento por failover de DNS.

Conteúdos

- Etapa 1: Criar aliases de conexão
- (Opcional) Etapa 2: Compartilhar um alias de conexão com outra conta
- Etapa 3: Associar aliases de conexão a diretórios em cada região
- Etapa 4: Configurar o serviço de DNS e definir políticas de roteamento de DNS
- Etapa 5: enviar a string de conexão para seus WorkSpaces usuários
- Diagrama da arquitetura de redirecionamento entre regiões
- Iniciar o redirecionamento entre regiões
- O que acontece durante o redirecionamento entre regiões
- Desassociar um alias de conexão de um diretório
- Cancelar o compartilhamento de um alias de conexão
- Excluir um alias de conexão
- Permissões do IAM para associar e desassociar aliases de conexão
- Considerações de segurança se você parar de usar o redirecionamento entre regiões

Pré-requisitos

- Você deve possuir e registrar o domínio que deseja usar como o FQDN nos aliases de conexão. Se você ainda não estiver usando outro registrador de domínio, poderá usar o Amazon Route 53 para registrar o domínio. Para obter mais informações, consulte Registrar e gerenciar novos domínios com o Amazon Route 53 no Guia do desenvolvedor do Amazon Route 53.

  > **Important**
  >
  > Você deve ter todos os direitos necessários para usar qualquer nome de domínio usado em conjunto com a Amazon WorkSpaces. Você concorda que o nome de domínio não viola nem infringe os direitos legais de terceiros nem viola a legislação aplicável.

  O tamanho total do nome de domínio não pode exceder 255 caracteres. Para obter mais informações sobre nomes de domínio, consulte Formato de nome de domínio DNS no Guia do desenvolvedor do Amazon Route 53.

  O redirecionamento entre regiões funciona com nomes de domínio público e nomes de domínio em zonas DNS privadas. Se você estiver usando uma zona DNS privada, deverá fornecer

uma conexão de rede privada virtual (VPN) à nuvem privada virtual (VPC) que contém sua. WorkSpaces Se seus WorkSpaces usuários tentarem usar um FQDN privado da Internet pública, os aplicativos WorkSpaces cliente retornarão a seguinte mensagem de erro:

```
"We're unable to register the WorkSpace because of a DNS server issue.
Contact your administrator for help."
```

- Você deve configurar o serviço de DNS e as políticas de roteamento de DNS necessárias. O redirecionamento entre regiões funciona em conjunto com suas políticas de roteamento de DNS para redirecionar seus usuários conforme necessário. WorkSpaces
- Em cada região primária e de failover em que você deseja configurar o redirecionamento entre regiões, crie WorkSpaces para seus usuários. Certifique-se de usar os mesmos nomes de usuário em cada WorkSpaces diretório em cada região. Para manter seus dados de usuário do Active Directory sincronizados, recomendamos usar o AD Connector para apontar para o mesmo Active Directory em cada região em que você configurou WorkSpaces para seus usuários. Para obter mais informações sobre criação WorkSpaces, consulte Launch WorkSpaces.

> **Important**
>
> Se você configurar seu diretório AWS gerenciado do Microsoft AD para replicação em várias regiões, somente o diretório na região principal poderá ser registrado para uso com a Amazon. WorkSpaces As tentativas de registrar o diretório em uma região replicada para uso com a Amazon WorkSpaces falharão. A replicação multirregional com o AWS Microsoft AD gerenciado não é suportada para uso com a Amazon WorkSpaces em regiões replicadas.

Ao concluir a configuração do redirecionamento entre regiões, verifique se WorkSpaces os usuários estão usando o código de registro baseado em FQDN em vez do código de registro baseado em região (por exemplo,) para sua região principal. `WSpdx+ABC12D` Para fazer isso, envie um e-mail com a string de conexão FQDN usando o procedimento presente na Etapa 5: enviar a string de conexão para seus WorkSpaces usuários.

> **Note**
>
> Se você criar seus usuários no WorkSpaces console em vez de criá-los no Active Directory, WorkSpaces enviará automaticamente um e-mail de convite para seus usuários com um código de registro baseado em região sempre que você iniciar um novo.

WorkSpace Isso significa que, quando você configura WorkSpaces para seus usuários na região de failover, seus usuários também receberão automaticamente e-mails sobre esses failover WorkSpaces. Instrua os usuários a ignorar e-mails com códigos de registro baseados em região.

Limitações

- O redirecionamento entre regiões não verifica automaticamente se as conexões com a região principal falharam e, em seguida, transfere você WorkSpaces para outra região. Em outras palavras: não ocorre failover automático.

  Para implementar um cenário de failover automático, você deve usar outro mecanismo em conjunto com o redirecionamento entre regiões. Por exemplo, você pode usar uma política de roteamento de DNS de failover do Amazon Route 53 combinada com uma verificação de integridade do Route 53 que monitora um CloudWatch alarme na região primária. Se o CloudWatch alarme na região principal for acionado, sua política de roteamento de failover de DNS redirecionará seus WorkSpaces usuários para WorkSpaces aquela que você configurou para eles na região de failover.
- Quando você usa o redirecionamento entre regiões, os dados do usuário não são mantidos entre WorkSpaces regiões diferentes. Para garantir que os usuários possam acessar seus arquivos de diferentes regiões, recomendamos que você configure a Amazon WorkDocs para seus WorkSpaces usuários, se a Amazon WorkDocs tiver suporte em suas regiões primária e de failover. Para obter mais informações sobre a Amazon WorkDocs, consulte Amazon WorkDocs Drive no Guia de WorkDocs Administração da Amazon. Para obter mais informações sobre como habilitar WorkDocs a Amazon para seus WorkSpace usuários, consulte Registrar um diretório com o WorkSpaces Habilitar o Amazon WorkDocs para o AWS Managed Microsoft AD e. Para obter informações sobre como WorkSpaces os usuários podem configurar a Amazon WorkDocs em seus WorkSpaces, consulte Integrar com WorkDocs no Guia WorkSpaces do usuário da Amazon.
- O redirecionamento entre regiões é suportado somente na versão 3.0.9 ou posterior dos aplicativos cliente Linux, macOS e Windows. WorkSpaces Você também pode usar o redirecionamento entre regiões com o Acesso via Web.
- O redirecionamento entre regiões está disponível em todas as AWSregiões em que a Amazon WorkSpaces está disponível, exceto nas regiões AWS GovCloud (US) Region s e China (Ningxia).

Etapa 1: Criar aliases de conexão

Usando a mesma conta da AWS, crie um alias de conexão em cada região primária e de failover em que deseja configurar o redirecionamento entre regiões.

Como criar um alias de conexão

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No canto superior direito do console, selecione a AWS região principal para o seu. WorkSpaces
3. No painel de navegação, selecione Account Settings (Configurações da conta).
4. Em Redirecionamento entre regiões, selecione Criar um alias de conexão.
5. Em String de conexão, insira um FQDN, como `www.example.com` ou `desktop.example.com`. Uma string de conexão pode ter no máximo 255 caracteres. Ela pode incluir apenas letras (A–Z, a–z), números (0–9) e os seguintes caracteres: .-

   > **Important**
   >
   > Depois de criar uma string de conexão, ela sempre estará associada à sua conta da AWS. Não é possível recriar a mesma string de conexão com outra conta, mesmo que você tenha excluído todas as instâncias dela da conta original. A string de conexão é reservada globalmente para sua conta.

6. (Opcional) Em Tags, especifique as etiquetas que você deseja associar ao alias de conexão.
7. Escolha Criar conexão.
8. Repita essas etapas, mas emStep 2, certifique-se de selecionar a região de failover para sua WorkSpaces. Se você tiver mais de uma região de failover, repita essas etapas para cada uma delas. Use a mesma conta da AWS para criar o alias de conexão em cada região de failover.

(Opcional) Etapa 2: Compartilhar um alias de conexão com outra conta

É possível compartilhar um alias de conexão com outra conta da AWS na mesma região da AWS. Compartilhar um alias de conexão com outra conta concede a essa conta permissão para associar ou desassociar o alias de um diretório de propriedade da conta, apenas na mesma região. Somente a conta que possui um alias de conexão pode exclui-lo.

> **Note**
>
> Um alias de conexão pode ser associado a apenas um diretório por região da AWS. Se você compartilhar um alias de conexão com outra conta da AWS, somente uma conta (a sua conta ou a conta compartilhada) poderá associar o alias a um diretório nessa região.

Como compartilhar um alias de conexão com outra conta da AWS

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No canto superior direito do console, selecione a região da AWS na qual você quer compartilhar o alias de conexão com outra conta da AWS.
3. No painel de navegação, selecione Account Settings (Configurações da conta).
4. Em Associações de redirecionamento entre regiões, selecione a string de conexão e, em seguida, escolha Ações, Compartilhar/cancelar compartilhamento do alias de conexão.

   Você também pode compartilhar um alias na página de detalhes do alias de conexão. Para fazer isso, em Conta compartilhada, escolha Compartilhar alias de conexão.
5. Na página Compartilhar/cancelar compartilhamento do alias de conexão, em Compartilhar com uma conta, insira o ID da conta da AWS com a qual você deseja compartilhar o alias de conexão nesta região da AWS.
6. Escolha Compartilhar.

Etapa 3: Associar aliases de conexão a diretórios em cada região

Associar o mesmo alias de conexão a um WorkSpaces diretório em duas ou mais regiões cria um par de associação entre os diretórios. Cada par de associação tem uma região principal e uma ou mais regiões de failover.

Por exemplo, se sua região principal for a região Oeste dos EUA (Oregon), você pode emparelhar seu WorkSpaces diretório na região Oeste dos EUA (Oregon) com um WorkSpaces diretório na região Leste dos EUA (Norte da Virgínia). Se ocorrer uma interrupção na região principal, o redirecionamento entre regiões funciona em conjunto com suas políticas de roteamento de failover de DNS e quaisquer verificações de saúde que você tenha implementado na região Oeste dos EUA (Oregon) para redirecionar seus usuários para a região que WorkSpaces você configurou para eles na região Leste dos EUA (Norte da Virgínia). Para obter mais informações sobre a experiência de redirecionamento entre regiões, consulte O que acontece durante o redirecionamento entre regiões.

> **Note**
>
> Se seus WorkSpaces usuários estiverem localizados a uma distância significativa da região de failover (por exemplo, a milhares de quilômetros de distância), a WorkSpaces experiência deles poderá ser menos responsiva do que o normal. Para verificar o tempo de ida e volta (RTT) para as várias AWS regiões de sua localização, use o Amazon Connection WorkSpaces Health Check.

Como associar um alias de conexão a um diretório

É possível associar um alias de conexão com apenas um diretório por região da AWS. Se você tiver compartilhado um alias de conexão com outra conta da AWS, somente uma conta (a sua conta ou a conta compartilhada) poderá associar o alias a um diretório nessa região.

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No canto superior direito do console, selecione a AWS região principal para o seu. WorkSpaces
3. No painel de navegação, selecione Account Settings (Configurações da conta).
4. Em Associações de redirecionamento entre regiões, selecione a string de conexão e, em seguida, escolha Ações, Associar/desassociar.

   Também é possível associar um alias de conexão a um diretório na página de detalhes do alias de conexão. Para fazer isso, em Diretório associado, escolha Associar diretório.
5. Na página Associar/desassociar, em Associar a um diretório, selecione o diretório ao qual você deseja associar o alias de conexão nesta região da AWS.

   > **Note**
   >
   > Se você configurar seu diretório AWS gerenciado do Microsoft AD para replicação em várias regiões, somente o diretório na região principal poderá ser usado com a Amazon. WorkSpaces As tentativas de usar o diretório em uma região replicada com a Amazon WorkSpaces falharão. A replicação multirregional com o AWS Microsoft AD gerenciado não é suportada para uso com a Amazon WorkSpaces em regiões replicadas.
6. Selecione Associar.

7. Repita essas etapas, mas emStep 2, certifique-se de selecionar a região de failover para sua WorkSpaces. Se você tiver mais de uma região de failover, repita essas etapas para cada uma delas. Associe o mesmo alias de conexão a um diretório em cada região de failover.

Etapa 4: Configurar o serviço de DNS e definir políticas de roteamento de DNS

Depois de criar aliases de conexão e pares de associação de alias de conexão, você poderá configurar o serviço de DNS para o domínio que você usou nas strings de conexão. Você pode usar qualquer provedor de serviços de DNS para essa finalidade. Se você não tiver um provedor de serviços de DNS de preferência, poderá usar o Amazon Route 53. Para obter mais informações, consulte Como configurar o Amazon Route 53 como o serviço de DNS no Guia do desenvolvedor do Amazon Route 53.

Depois de configurar o serviço de DNS para o domínio, configure as políticas de roteamento de DNS que deseja usar para o redirecionamento entre regiões. Por exemplo, você pode usar as verificações de saúde do Amazon Route 53 para determinar se seus usuários podem se conectar a eles WorkSpaces em uma região específica. Se os usuários não conseguirem se conectar, você pode usar uma política de failover de DNS para rotear o tráfego de DNS de uma região para outra.

Para obter mais informações sobre a política de roteamento de DNS, consulte Como escolher uma política de roteamento no Guia do desenvolvedor do Amazon Route 53. Para obter mais informações sobre as verificações de integridade do Amazon Route 53, consulte Como o Amazon Route 53 verifica a integridade de seus recursos no Guia do desenvolvedor do Amazon Route 53.

Ao configurar suas políticas de roteamento de DNS, você precisará do identificador de conexão para a associação entre o alias de conexão e o WorkSpaces diretório na região primária. Você também precisará do identificador de conexão para a associação entre o alias de conexão e o WorkSpaces diretório em sua região ou regiões de failover.

> **Note**
>
> O identificador da conexão não é o mesmo que o ID do alias da conexão. O ID do alias da conexão começa com `wsca-`.

Como encontrar o identificador de conexão para uma associação de alias de conexão

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No canto superior direito do console, selecione a AWS região principal para o seu. WorkSpaces
3. No painel de navegação, selecione Account Settings (Configurações da conta).
4. Em Associações de redirecionamento entre regiões, selecione o texto da string de conexão (o FQDN) para exibir a página de detalhes do alias de conexão.
5. Na página de detalhes do alias de conexão, em Diretório associado, anote o valor exibido para o Identificador de conexão.
6. Repita essas etapas, mas emStep 2, certifique-se de selecionar a região de failover para sua WorkSpaces. Se você tiver mais de uma região de failover, repita essas etapas para encontrar o identificador de conexão para cada uma delas.

Exemplo: como configurar uma política de roteamento por failover de DNS usando o Route 53

O exemplo a seguir configura uma zona hospedada para o domínio. No entanto, é possível configurar uma zona hospedada pública ou privada. Para obter mais informações sobre como configurar uma zona hospedada, consulte Como trabalhar com zonas hospedadas privadas no Guia do desenvolvedor do Amazon Route 53.

Esse exemplo também usa uma política de roteamento por failover. Você pode usar outros tipos de política de roteamento para sua estratégia de redirecionamento entre regiões. Para obter mais informações sobre a política de roteamento de DNS, consulte Como escolher uma política de roteamento no Guia do desenvolvedor do Amazon Route 53.

Ao configurar uma política de roteamento por failover no Route 53, é necessário realizar uma verificação de integridade na região primária. Para obter mais informações sobre a como criar uma verificação de integridade no Route 53, consulte Como criar de verificações de integridade e configurar o failover de DNS no Amazon Route 53 e Como criar, atualizar e excluir verificações de integridade no Guia do desenvolvedor do Amazon Route 53.

Se você quiser usar um CloudWatch alarme da Amazon com sua verificação de saúde do Route 53, você também precisará configurar um CloudWatch alarme para monitorar os recursos em sua região principal. Para obter mais informações sobre CloudWatch, consulte O que é a Amazon CloudWatch? no Guia do CloudWatch usuário da Amazon. Para obter mais informações sobre como o Route 53 usa CloudWatch alarmes em suas verificações de saúde, consulte Como o Route 53 determina

o status das verificações de saúde que monitoram CloudWatch alarmes e Monitoramento de um CloudWatch alarme no Amazon Route 53 Developer Guide.

Para configurar uma política de roteamento por failover de DNS no Route 53, primeiro você precisa criar uma zona hospedada para o domínio.

1. Abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Zonas hospedadas e, em seguida, escolha Criar zona hospedada.
3. Na página Zona hospedada criada, insira o nome de domínio (como `example.com`) em Nome do domínio.
4. Em Tipo, escolha Zona hospedada pública.
5. Escolha Create hosted zone (Criar zona hospedada).

Depois, crie uma verificação de integridade para a região primária.

1. Abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Verificações de integridade e, em seguida, escolha Criar verificação de integridade.
3. Na página Configurar verificação de integridade, insira um nome para a verificação de integridade.
4. Em O que monitorar, selecione Endpoint, Status de outras verificações de saúde (verificação de saúde calculada) ou Estado do CloudWatch alarme.
5. Dependendo da seleção na etapa anterior, configure a verificação de integridade e escolha Avançar.
6. Na página Receber notificações quando a verificação de integridade falhar, em Criar alarme, escolha Sim ou Não.
7. Selecione Criar verificação de integridade.

Depois de criar a verificação de integridade, é possível criar os registros de failover de DNS.

1. Abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Zonas hospedadas.
3. Na página Zonas hospedadas, selecione o nome do domínio.
4. Na página de detalhes do nome de domínio, escolha Criar registro.

5. Na página Escolher política de roteamento, escolha Failover e, em seguida, Próximo.
6. Na página Configurar registro, em Configuração básica, insira o nome do subdomínio em Nome do registro. Por exemplo, se o FQDN for `desktop.example.com`, insira **`desktop`**.

> **Note**
>
> Se você quiser usar o domínio raiz, deixe o campo Nome do registro em branco. No entanto, recomendamos o uso de um subdomínio, como `desktop` ou`workspaces`, a menos que você tenha configurado o domínio exclusivamente para uso com seu WorkSpaces.

7. Em Tipo de registro, selecione TXT: usado para verificar remetentes de e-mail e valores específicos da aplicação.
8. Deixe as configurações de Segundos TTL como padrão.
9. Em Registros de failover para adicionar ao ***`your_domain_name`***, escolha Definir registro de failover.

Agora é necessário configurar os registros de failover para as regiões primária e de failover.

Exemplo: como configurar o registro de failover para a região primária

1. Na caixa de diálogo Definir registro de failover, em Valor/rotear tráfego para, selecione Endereço IP ou outro valor, dependendo do tipo de registro.
2. Uma caixa de diálogo é aberta para você inserir as entradas de texto de amostra. Insira o identificador de conexão para a associação de alias de conexão para a região primária.
3. Em Tipo de registro de failover, selecione Primário.
4. Em Verificação de integridade, selecione uma verificação de integridade que você criou para a região primária.
5. Em ID do registro, insira uma descrição para identificar esse registro.
6. Escolha Definir registro de failover. O novo registro de failover é exibido em Registros de failover para adicionar ao ***`your_domain_name`***.

Exemplo: como configurar o registro de failover para a região de failover

1. Em Registros de failover para adicionar ao ***`your_domain_name`***, escolha Definir registro de failover.

2. Na caixa de diálogo Definir registro de failover, em Valor/rotear tráfego para, selecione Endereço IP ou outro valor, dependendo do tipo de registro.
3. Uma caixa de diálogo é aberta para você inserir as entradas de texto de amostra. Insira o identificador de conexão para a associação de alias de conexão para a região de failover.
4. Em Tipo de registro de failover, selecione Secundário.
5. (Opcional) Em Verificação de integridade, insira uma verificação de integridade criada para a região de failover.
6. Em ID do registro, insira uma descrição para identificar esse registro.
7. Escolha Definir registro de failover. O novo registro de failover é exibido em Registros de failover para adicionar ao ***your_domain_name***.

Se a verificação de saúde que você configurou para sua região principal falhar, sua política de roteamento de failover de DNS redirecionará seus WorkSpaces usuários para sua região de failover. O Route 53 continua monitorando a verificação de saúde da sua região principal e, quando a verificação de saúde da sua região primária não falha mais, o Route 53 redireciona automaticamente seus WorkSpaces usuários de volta para a WorkSpaces região primária.

Para obter informações sobre como criar registros de DNS, consulte Como criar registros usando o console do Amazon Route 53 no Guia do desenvolvedor do Amazon Route 53. Para obter informações sobre como configurar registros TXT de DNS, consulte Tipos de registro TXT no Guia do desenvolvedor do Amazon Route 53.

Etapa 5: enviar a string de conexão para seus WorkSpaces usuários

Para garantir que seus usuários WorkSpaces sejam redirecionados conforme necessário durante uma interrupção, você deve enviar a string de conexão (FQDN) aos seus usuários. Se você já emitiu códigos de registro baseados na região (por exemplo,`WSpdx+ABC12D`) para seus WorkSpaces usuários, esses códigos permanecem válidos. No entanto, para que o redirecionamento entre regiões funcione, seus WorkSpaces usuários devem usar a cadeia de conexão como código de registro ao registrá-los WorkSpaces no WorkSpaces aplicativo cliente.

> **Important**
>
> Se você criar seus usuários no WorkSpaces console em vez de criá-los no Active Directory, enviará WorkSpaces automaticamente um e-mail de convite para seus usuários com um código de registro baseado em região (por exemplo,`WSpdx+ABC12D`) sempre que você

iniciar um novo. WorkSpace Mesmo que você já tenha configurado o redirecionamento entre regiões, o e-mail de convite enviado automaticamente para novos WorkSpaces contém esse código de registro baseado na região em vez da sua cadeia de conexão.
Para garantir que seus WorkSpaces usuários estejam usando a cadeia de conexão em vez do código de registro baseado na região, você deve enviar a eles outro e-mail com a cadeia de conexão usando o procedimento abaixo.

Para enviar a cadeia de conexão aos seus WorkSpaces usuários

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No canto superior direito do console, selecione a AWS região principal para o seu. WorkSpaces
3. No painel de navegação, selecione WorkSpaces.
4. Na WorkSpacespágina, use a caixa de pesquisa para pesquisar um usuário para o qual você deseja enviar um convite e selecione o correspondente nos resultados WorkSpace da pesquisa. Você pode selecionar somente um por WorkSpace vez.
5. Escolha Actions (Ações), Invite User (Convidar usuário).
6. Na WorkSpaces página Convidar usuários para seus usuários, você verá um modelo de e-mail para enviar aos seus usuários.
7. (Opcional) Se houver mais de um alias de conexão associado ao seu WorkSpaces diretório, selecione a cadeia de conexão que você deseja que seus usuários usem na lista Cadeia de caracteres do alias de conexão. O modelo de e-mail é atualizado para exibir a sequência de caracteres que você escolheu.
8. Copie o texto do modelo do e-mail e cole em um e-mail para os usuários usando a sua própria aplicação de e-mail. Na aplicação de e-mail, é possível modificar o texto conforme necessário. Quando o convite por e-mail estiver pronto, envie-o para os usuários.

Diagrama da arquitetura de redirecionamento entre regiões

O diagrama a seguir descreve o processo de implantação do redirecionamento entre regiões.

> **Note**
>
> O redirecionamento entre regiões facilita apenas o failover e o fallback entre regiões. Isso não facilita a criação e a manutenção WorkSpaces na região secundária e não permite a

replicação de dados entre regiões. WorkSpaces nas regiões primária e secundária devem ser gerenciadas separadamente.

Iniciar o redirecionamento entre regiões

No caso de uma interrupção, você pode atualizar os registros DNS manualmente ou usar políticas de roteamento automatizadas com base nas verificações de saúde, que determinam a região de failover. Recomendamos seguir os mecanismos de recuperação de desastres descritos em Criação de mecanismos de recuperação de desastres usando o Amazon Route 53.

O que acontece durante o redirecionamento entre regiões

Durante o failover da região, seus WorkSpaces usuários são desconectados da WorkSpaces região primária. Quando eles tentam se reconectar, recebem a seguinte mensagem de erro:

```
We can't connect to your WorkSpace. Check your network connection, and then try again.
```

Então, eles são solicitados a fazer login novamente. Se eles estiverem usando o FQDN como código de registro, quando fizerem login novamente, suas políticas de roteamento de failover de DNS os redirecionarão para o WorkSpaces que você configurou para eles na região de failover.

> **Note**
>
> Em alguns casos, os usuários podem não conseguir se reconectar ao fazer login novamente. Se esse comportamento ocorrer, eles deverão fechar e reiniciar o aplicativo WorkSpaces cliente e, em seguida, tentar fazer login novamente.

Desassociar um alias de conexão de um diretório

Somente a conta que possui um diretório pode desassociar um alias de conexão do diretório.

Se você tiver compartilhado um alias de conexão com outra conta e essa conta tiver associado o alias de conexão a um diretório de propriedade da conta, essa mesma conta deverá ser usada para desassociar o alias de conexão do diretório.

Como desassociar um alias de conexão de um diretório

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No canto superior direito do console, selecione a região da AWS que contém o alias de conexão que você deseja desassociar.
3. No painel de navegação, selecione Account Settings (Configurações da conta).
4. Em Associações de redirecionamento entre regiões, selecione a string de conexão e, em seguida, escolha Ações, Associar/desassociar.

   Você também pode desassociar um alias de conexão na página de detalhes do alias de conexão. Para fazer isso, em Diretório associado, escolha Desassociar.
5. Na página Associar/desassociar, escolha Desassociar.
6. Na caixa de diálogo que solicita a confirmação da dissociação, escolha Desassociar.

Cancelar o compartilhamento de um alias de conexão

Somente o proprietário de um alias de conexão pode cancelar o compartilhamento do alias. Se você cancelar o compartilhamento de um alias de conexão com uma conta, essa conta não poderá mais associar o alias de conexão a um diretório.

Como cancelar o compartilhamento de um alias de conexão

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No canto superior direito do console do, selecione a região da AWS que contém o alias de conexão que você deseja cancelar compartilhamento.
3. No painel de navegação, selecione Account Settings (Configurações da conta).
4. Em Associações de redirecionamento entre regiões, selecione a string de conexão e, em seguida, escolha Ações, Compartilhar/cancelar compartilhamento do alias de conexão.

   Você também pode cancelar o compartilhamento de um alias de conexão na página de detalhes do alias de conexão. Para fazer isso, em Conta compartilhada, escolha Cancelar compartilhamento.
5. Na página Compartilhar/cancelar compartilhamento do alias de conexão, escolha Cancelar compartilhamento.
6. Na caixa de diálogo que solicita que você confirme o cancelamento do compartilhamento do alias de conexão, escolha Cancelar compartilhamento.

Excluir um alias de conexão

Só é possível excluir um alias de conexão se ele pertencer à sua conta e não estiver associado a um diretório.

Se você tiver compartilhado um alias de conexão com outra conta e essa conta tiver associado o alias de conexão a um diretório de propriedade da conta, essa conta deverá primeiro desassociar o alias de conexão do diretório antes que você possa excluir o alias de conexão.

Important

Depois de criar uma string de conexão, ela sempre estará associada à sua conta da AWS. Não é possível recriar a mesma string de conexão com outra conta, mesmo que você tenha excluído todas as instâncias dela da conta original. A string de conexão é reservada globalmente para sua conta.

Warning

Se você não usar mais um FQDN como código de registro para seus WorkSpaces usuários, deverá tomar algumas precauções para evitar possíveis problemas de segurança. Para ter mais informações, consulte Considerações de segurança se você parar de usar o redirecionamento entre regiões.

Como excluir um alias de conexão

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No canto superior direito do console do, selecione a região da AWS que contém o alias de conexão que você deseja excluir.
3. No painel de navegação, selecione Account Settings (Configurações da conta).
4. Em Associações de redirecionamento entre regiões, selecione a string de conexão e escolha Excluir.

   Você também pode excluir um alias de conexão na página de detalhes do alias de conexão. Para fazer isso, no canto superior direito da página, escolha Excluir.

> **Note**
>
> Se o botão Excluir estiver desabilitado, verifique se o alias está sob sua propriedade e se ele não está associado a um diretório.

5. Na caixa de diálogo que confirma a exclusão, escolha Excluir.

Permissões do IAM para associar e desassociar aliases de conexão

Se você usa um usuário do IAM para associar ou desassociar aliases de conexão, o usuário deve ter permissões para `workspaces:AssociateConnectionAlias` e `workspaces:DisassociateConnectionAlias`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:AssociateConnectionAlias",
        "workspaces:DisassociateConnectionAlias"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:123456789012:connectionalias/wsca-a1bcd2efg"
      ]
    }
  ]
}
```

> **Important**
>
> Se você estiver criando uma política do IAM para associar ou desassociar aliases de conexão para contas que não possuem os aliases de conexão, não é possível especificar um ID de conta no ARN. Em vez disso, você deve usar * como o ID da conta, conforme exibido no exemplo de política a seguir.
>
> ```
> {
>   "Version": "2012-10-17",
>   "Statement": [
> ```

```
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:AssociateConnectionAlias",
        "workspaces:DisassociateConnectionAlias"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:*:connectionalias/wsca-a1bcd2efg"
      ]
    }
  ]
}
```

Você pode especificar um ID de conta no ARN somente quando essa conta possui o alias de conexão a ser associado ou desassociado.

Para obter mais informações sobre como trabalhar com o IAM, consulte Gerenciamento de identidade e acesso para o WorkSpaces.

Considerações de segurança se você parar de usar o redirecionamento entre regiões

Se você não usar mais um FQDN como código de registro para seus WorkSpaces usuários, deverá tomar as seguintes precauções para evitar possíveis problemas de segurança:

- Certifique-se de emitir aos WorkSpaces usuários o código de registro específico da região (por exemplo,`WSpdx+ABC12D`) para o WorkSpaces diretório e instruí-los a parar de usar o FQDN como código de registro.
- Se você ainda possui esse domínio, atualize o registro TXT do DNS para removê-lo para que ele não possa ser explorado em um ataque de phishing. Se você remover esse domínio do seu registro DNS TXT e seus WorkSpaces usuários tentarem usar o FQDN como código de registro, as tentativas de conexão falharão inofensivamente.
- Se você não é mais proprietário desse domínio, seus WorkSpaces usuários devem usar o código de registro específico da região. Se eles continuarem tentando usar o FQDN como o código de registro, as tentativas de conexão poderão ser redirecionadas para um site mal-intencionado.

Resiliência multirregional para a Amazon WorkSpaces

O Amazon WorkSpaces Multi-Region Resilience (MRR) permite que você redirecione usuários para uma região secundária quando sua WorkSpaces região principal estiver inacessível devido a eventos disruptivos, sem exigir que seus usuários troquem os códigos de registro ao se conectarem ao modo de espera. WorkSpaces O Standby WorkSpaces é um recurso do Amazon WorkSpaces Multi-Region Resilience que simplifica a criação e o gerenciamento da implantação em espera. Depois de configurar um diretório de usuários na sua região secundária, selecione aquele WorkSpace em sua região principal para o qual você deseja criar um modo de WorkSpace espera. O sistema espelha automaticamente as imagens do WorkSpace pacote primário para a região secundária. Em seguida, ele provisiona automaticamente um novo modo de espera WorkSpace em sua região secundária.

A resiliência WorkSpaces multirregional da Amazon se baseia no redirecionamento entre regiões que aproveita os recursos de verificação de integridade e failover do DNS. Ele permite que você use um nome de domínio totalmente qualificado (FQDN) como seu código de WorkSpaces registro. Quando seus usuários fazem login WorkSpaces, você pode redirecioná-los para as WorkSpaces regiões suportadas com base nas políticas do seu Sistema de Nomes de Domínio (DNS) para o FQDN. Se você usa o Amazon Route 53, recomendamos o uso de verificações de saúde que monitorem CloudWatch os alarmes da Amazon ao criar uma estratégia de redirecionamento entre regiões para. WorkSpaces Para obter mais informações, consulte Criação de verificações de saúde do Amazon Route 53 e configuração do failover de DNS no Guia do desenvolvedor do Amazon Route 53.

A replicação de dados é um recurso complementar do modo de espera WorkSpaces que replica dados unidirecionais da região primária para a região secundária. Depois de habilitar a replicação de dados, os snapshots do EBS dos volumes do sistema e do usuário são feitos a cada 12 horas. A resiliência multirregional verifica regularmente se há novos instantâneos. Quando os instantâneos são encontrados, ele inicia uma cópia para a região secundária. Quando as cópias chegam à região secundária, elas são usadas para atualizar a secundária WorkSpace.

Conteúdos

- Replicação de dados unidirecional para espera WorkSpaces
- Planeje reservar a capacidade do Amazon EC2 para recuperação

Pré-requisitos

- Você deve criar WorkSpaces para seus usuários na região principal antes de criar o modo de espera WorkSpaces. Para obter mais informações sobre a criação WorkSpaces, consulteInicializar uma área de trabalho virtual usando WorkSpaces.
- Para habilitar a replicação de dados em espera WorkSpaces, você deve ter um Active Directory autogerenciado ou um AWS Microsoft AD gerenciado configurado para replicar em suas regiões em espera. Para obter mais informações, consulte Criar seu diretório AWS gerenciado do Microsoft AD e Adicionar uma região replicada.
- Certifique-se de atualizar os drivers de dependência de rede, como ENA, NVMe e drivers PV, em sua rede primária. WorkSpaces Você deve fazer isso pelo menos uma vez a cada 6 meses. Para obter mais informações, consulte Instalar ou atualizar o driver do Elastic Network Adapter (ENA)Drivers do AWS NVMe para instâncias do Windows e Atualizar os drivers fotovoltaicos nas instâncias do Windows.
- Certifique-se de atualizar periodicamente os agentes EC2Config, EC2Launch e EC2Launch V2 para as versões mais recentes. Você deve fazer isso pelo menos uma vez a cada 6 meses. Para obter mais informações, consulte Atualizar EC2Config e EC2Launch.
- Para garantir a replicação adequada dos dados, certifique-se de que os Active Directories nas regiões primária e secundária estejam sincronizados com o FQDN, a OU e o SID do usuário.
- A cota padrão (limite) para espera WorkSpaces é 0. Você precisa solicitar um aumento da cota de serviço antes de criar um modo de espera WorkSpace. Para ter mais informações, consulte WorkSpaces Cotas da Amazon.
- Verifique se você está usando chaves gerenciadas pelo cliente para criptografar tanto a chave primária quanto a de espera WorkSpaces. Você pode usar chaves de região única ou chaves de várias regiões para criptografar suas chaves primárias e de espera. WorkSpaces

Limitações

- O modo de espera copia WorkSpaces somente a imagem do pacote primário WorkSpaces , mas não copia o volume do sistema (unidade C) nem o volume do usuário (unidade D) do seu principal. WorkSpaces Para copiar o volume do sistema (unidade C) ou o volume do usuário (unidade D) do

principal WorkSpaces para o modo de espera WorkSpaces, você precisa ativar a replicação de dados.

- Você não pode modificar, reconstruir, restaurar ou migrar diretamente um standby. WorkSpace
- O failover para redirecionamento entre regiões é controlado pelas configurações de DNS. Para implementar um cenário de failover automático, use um mecanismo diferente em conjunto com o redirecionamento entre regiões. Por exemplo, você pode usar uma política de roteamento de DNS de failover do Amazon Route 53 combinada com uma verificação de integridade do Route 53 que monitora um CloudWatch alarme na região primária. Se o CloudWatch alarme na região principal for invocado, sua política de roteamento de failover de DNS redirecionará seus WorkSpaces usuários para WorkSpaces aquela que você configurou para eles na região de failover.
- A replicação de dados ocorre apenas de uma maneira, copiando dados da região primária para a região secundária. Durante o WorkSpaces failover em espera, você pode acessar os dados e o aplicativo entre 12 e 24 horas. Depois de uma interrupção, faça backup manual de todos os dados que você criou no secundário WorkSpace e saia. Recomendamos salvar seu trabalho em unidades externas, como sua unidade de rede, para que você possa acessar seus dados a partir da unidade primária WorkSpace.
- A replicação de dados não oferece suporte ao AWS Simple AD.
- Quando você ativa a replicação de dados em espera WorkSpaces, os snapshots do EBS do primário WorkSpaces (volumes raiz e do sistema) são tirados a cada 12 horas. O instantâneo inicial de um determinado volume de dados está cheio e os instantâneos subsequentes são incrementais. Como resultado, a primeira replicação de uma determinada WorkSpace levará mais tempo do que as subsequentes. Os instantâneos são iniciados em uma programação interna WorkSpaces e você não pode controlar o tempo.
- Se o principal WorkSpace e o standby WorkSpace se unirem usando o mesmo domínio, recomendamos que você se conecte somente ao primário WorkSpace ou ao standby WorkSpace em um determinado momento para evitar a perda da conexão com o controlador de domínio.
- Se você configurar sua AWS Managed Microsoft AD para replicação multirregional, somente o diretório na região primária poderá ser registrado para uso com. WorkSpaces Se você tentar registrar o diretório em uma região replicada para uso com WorkSpaces, ele falhará. A replicação multirregional com AWS Managed Microsoft AD não é suportada para uso em regiões WorkSpaces replicadas.
- Se você já configurou o redirecionamento entre regiões e criou WorkSpaces nas regiões primária e secundária sem usar o modo de espera WorkSpaces, não é possível converter o existente WorkSpace na região secundária em um modo de espera diretamente. WorkSpace Em vez disso, você precisa desligar a WorkSpace na sua região secundária, selecionar aquela WorkSpace na

sua região primária para a qual deseja criar uma espera e usar WorkSpaces a espera WorkSpace para criar a espera. WorkSpace

- Depois de uma interrupção, faça backup manual de todos os dados que você criou no secundário WorkSpace e saia. Recomendamos salvar seu trabalho em unidades externas, como sua unidade de rede, para que você possa acessar seus dados a partir da unidade primária WorkSpace.
- WorkSpaces Atualmente, a resiliência multirregional está disponível nas seguintes regiões:
  - Região Leste dos EUA (N. da Virgínia)
  - Região Oeste dos EUA (Oregon)
  - Região Europa (Frankfurt)
  - Região Europa (Irlanda)
- WorkSpaces A resiliência multirregional só é suportada na versão 3.0.9 ou posterior dos aplicativos cliente Linux, macOS e Windows. WorkSpaces Você também pode usar a Resiliência Multirregional com o Acesso via Web.
- WorkSpaces A resiliência multirregional é compatível com Windows e Bring Your Own License (BYOL). WorkSpaces Ele não é compatível com Amazon Linux, Ubuntu ou GPU WorkSpaces (por exemplo WorkSpaces, Graphics, GraphicsPro Graphics.g4dn ou .g4dn). GraphicsPro
- Após a conclusão do failover ou do failback, aguarde de 15 a 30 minutos antes de se conectar ao seu. WorkSpace

Configure seu modo de espera de resiliência multirregional WorkSpace

Para configurar seu modo de espera de resiliência multirregional WorkSpace

1. Configure diretórios de usuários nas regiões primária e secundária. Certifique-se de usar os mesmos nomes de usuário em cada WorkSpaces diretório em cada região.

   Para manter seus dados de usuário do Active Directory sincronizados, recomendamos usar o AD Connector para apontar para o mesmo Active Directory em cada região em que você configurou WorkSpaces para seus usuários. Para obter mais informações sobre como criar um diretório, consulte Registrar um diretório com WorkSpaces.

   > **Important**
   >
   > Se você configurar seu AWS Managed Microsoft AD diretório para replicação multirregional, somente o diretório na região primária poderá ser registrado para uso

com. WorkSpaces As tentativas de registrar o diretório em uma região replicada para uso com ela WorkSpaces falharão. A replicação multirregional com AWS Managed Microsoft AD não é suportada para uso em regiões WorkSpaces replicadas.

2. Crie WorkSpaces para seus usuários na região principal. Para obter mais informações sobre criação WorkSpaces, consulte Launch WorkSpaces.
3. Crie um standby WorkSpace na região secundária. Para obter mais informações sobre como criar uma espera WorkSpace, consulte Criar uma espera WorkSpace.
4. Crie e associe cadeias de conexão (FQDN) a diretórios de usuários nas regiões primária e secundária.

   Você deve ativar o redirecionamento entre regiões em sua conta porque o modo de espera se WorkSpaces baseia no redirecionamento entre regiões. Siga as etapas 1 a 3 das instruções para redirecionamento entre regiões para a Amazon. WorkSpaces
5. Configure o serviço DNS e configure as políticas de roteamento de DNS.

   Você deve configurar seu serviço DNS e configurar as políticas de roteamento de DNS necessárias. O redirecionamento entre regiões funciona em conjunto com suas políticas de roteamento de DNS para redirecionar seus usuários conforme necessário. WorkSpaces
6. Ao concluir a configuração do redirecionamento entre regiões, envie um e-mail ao usuário com uma cadeia de conexão FQDN. Para obter mais informações, consulte Etapa 5: Enviar a cadeia de conexão para seus WorkSpaces usuários. Certifique-se de que seus WorkSpaces usuários estejam usando o código de registro baseado em FQDN em vez do código de registro baseado em região (por exemplo, WSPDx+ABC12d) para sua região principal.

   ⚠ Important

   - Se você criar seus usuários no WorkSpaces console em vez de criá-los no Active Directory, WorkSpaces enviará automaticamente um e-mail de convite para seus usuários com um código de registro baseado em região sempre que você iniciar um novo. WorkSpace Isso significa que quando você configura WorkSpaces para seus usuários na região secundária, seus usuários também receberão automaticamente e-mails para esses usuários secundários WorkSpaces. Instrua os usuários a ignorar e-mails com códigos de registro baseados em região.

- Os códigos de registro específicos da região permanecem válidos; no entanto, para que o redirecionamento entre regiões funcione, seus usuários devem usar o FQDN como código de registro.

Crie um modo de espera WorkSpace

Antes de criar um modo de espera WorkSpace, certifique-se de ter cumprido os pré-requisitos, incluindo a criação de um diretório de usuários nas regiões primária e secundária, o provisionamento WorkSpaces para seus usuários na sua região primária, a configuração do redirecionamento entre regiões em sua conta e a solicitação de aumento do limite de espera por meio da cota de serviço. WorkSpaces

Para criar um modo de espera WorkSpace

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No canto superior direito do console, selecione a AWS região principal para sua. WorkSpaces
3. No painel de navegação, escolha WorkSpaces.
4. Selecione um para o qual WorkSpace você deseja criar um modo de WorkSpace espera.
5. Escolha Ações e, em seguida, escolha Criar espera WorkSpace.
6. Selecione a região secundária, onde você criará seu modo de espera WorkSpace e escolha Avançar.
7. Selecione o diretório de usuário na região secundária e selecione Próximo.
8. (Opcional) Adicione a chave de criptografia, ative a criptografia de dados e gerencie as tags.
   - Para adicionar uma chave de criptografia, insira-a em Chave de criptografia de entrada.
   - Para ativar a replicação de dados, escolha Habilitar replicação de dados. Em seguida, marque a caixa de seleção para confirmar que você autoriza a cobrança mensal adicional.
   - Para adicionar uma tag, selecione Adicionar nova tag.

   Em seguida, escolha Próximo.

> **Note**
>
> - Se o original WorkSpace estiver criptografado, esse campo será preenchido previamente. No entanto, você pode optar por substituí-la por sua própria chave de criptografia.
> - A atualização do status da replicação de dados leva alguns minutos.
> - Depois que o modo de espera WorkSpace for atualizado com êxito com os instantâneos do primário WorkSpace, você poderá encontrar os carimbos de data e hora dos instantâneos em Recovery Snapshot.

9. Revise as configurações do seu modo de espera WorkSpaces e escolha Criar.

> **Note**
>
> - Para ver informações sobre sua espera WorkSpaces, acesse a página de WorkSpace detalhes principal.
> - O modo de espera copia WorkSpace somente a imagem do pacote primário WorkSpace , mas não copia o volume do sistema (unidade C) nem o volume do usuário (unidade D) do sistema primário. WorkSpaces Por padrão, a replicação de dados está desativada. Para copiar o volume do sistema (unidade C) ou o volume do usuário (unidade D) do principal WorkSpaces para o modo de espera WorkSpaces, você precisa ativar a replicação de dados.

Gerenciar um modo de espera WorkSpace

Você não pode modificar, reconstruir, restaurar ou migrar diretamente um standby. WorkSpace

Para habilitar a replicação de dados para seu modo de espera WorkSpace

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. Vá para sua região principal e selecione o WorkSpace ID principal.
3. Role para baixo até a WorkSpace seção Em espera e escolha Editar em espera WorkSpace.
4. Escolha Habilitar replicação de dados. Em seguida, marque a caixa de seleção para confirmar que você autoriza a cobrança mensal adicional. Selecione Salvar.

Note

- O modo de espera WorkSpaces não pode hibernar. Se você interromper o modo de espera WorkSpace, ele não preservará seu trabalho não salvo. Recomendamos que os usuários sempre salvem seus trabalhos antes de sair do modo de espera WorkSpaces.
- Para habilitar a replicação de dados em espera WorkSpaces, você deve ter um Active Directory autogerenciado ou um AWS Microsoft AD gerenciado configurado para replicar em suas regiões em espera. Para configurar seus diretórios, siga as etapas de 1 a 3 na seção Passo a passo de Criação para continuidade de negócios com a WorkSpaces Amazon AWS e os Serviços de Diretório ou consulte Usando o Active Directory gerenciado em AWS várias regiões com a Amazon. WorkSpaces A replicação multirregional só é compatível com a Enterprise Edition do Managed AWS Microsoft AD.
- A atualização do status da replicação de dados leva alguns minutos.
- Depois que o modo de espera WorkSpace for atualizado com êxito com os instantâneos do primário WorkSpace, você poderá encontrar os carimbos de data e hora dos instantâneos em Recovery Snapshot.

Excluir um modo de espera WorkSpace

Você pode encerrar um modo de espera WorkSpace da mesma forma que encerra um normal. WorkSpace

Para excluir um standby WorkSpace

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No canto superior direito do console, selecione a AWS região principal para sua. WorkSpaces
3. No painel de navegação, escolha WorkSpaces.
4. Selecione o modo de espera WorkSpace e escolha Excluir. Demora aproximadamente 5 minutos para excluir um modo de espera WorkSpace. Durante a exclusão, o status do modo de espera WorkSpace será definido como Encerrando. Quando a exclusão for concluída, o modo de espera WorkSpace desaparecerá do console.

> **Note**
>
> A exclusão de um modo de espera WorkSpace é uma ação permanente e não pode ser desfeita. Os dados WorkSpace do usuário em espera não persistem e são destruídos. Para obter ajuda com o backup dos dados do usuário, entre em contato com o AWS Support.

Replicação de dados unidirecional para espera WorkSpaces

Habilitar a replicação de dados na resiliência multirregional permite replicar dados de uma região primária para uma região secundária. Durante o estado estacionário, a resiliência multirregional captura instantâneos do sistema (unidade C) e dos dados (unidade D) do sistema primário a cada 12 horas. WorkSpaces Esses instantâneos são transferidos para a região secundária e usados para atualizar o modo de espera WorkSpaces. Por padrão, a replicação de dados está desativada para espera WorkSpaces.

Depois que a replicação de dados é ativada para o modo de espera WorkSpaces, o instantâneo inicial de um determinado volume de dados é concluído, enquanto os instantâneos subsequentes são incrementais. Como consequência, a primeira replicação de uma determinada WorkSpace levará mais tempo do que as subsequentes. Os instantâneos são acionados em intervalos predeterminados WorkSpaces e o tempo não pode ser controlado pelos usuários.

Durante o failover, quando os usuários são redirecionados para a região secundária, eles podem acessar o modo de espera WorkSpaces com dados e aplicativos com idade entre 12 e 24 horas. Enquanto os usuários estiverem usando o modo de espera WorkSpaces, a resiliência multirregional não os forçará a sair do modo de espera WorkSpaces nem a atualizar o modo de espera WorkSpaces com os instantâneos da região principal.

Após uma interrupção, os usuários devem fazer backup manual de todos os dados que criaram no secundário WorkSpaces antes de sair do modo de espera WorkSpaces. Quando fizerem login novamente, serão direcionados para a região principal e sua principal WorkSpaces.

Planeje reservar a capacidade do Amazon EC2 para recuperação

O Amazon Multi-Region Resilience (MRR) depende, por padrão, dos pools sob demanda do Amazon EC2. Se um tipo específico de instância do Amazon EC2 não estiver disponível para apoiar sua recuperação, o MRR tentará automaticamente escalar a instância repetidamente até que um tipo

de instância disponível seja encontrado, mas em circunstâncias extremas, as instâncias podem nem sempre estar disponíveis. Para melhorar a disponibilidade dos tipos de instância necessários para as mais críticas WorkSpaces, entre em contato com o AWS Support e nós o ajudaremos no planejamento da capacidade.

Segurança no Amazon WorkSpaces

A segurança para com a nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você 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 isso como a segurança da nuvem e a 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 aplicáveis ao WorkSpaces, consulte Serviços da AWS no escopo por programa de conformidade.
- Segurança na nuvem: sua responsabilidade é determinada pelo serviço da AWS que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade dos dados, os requisitos da empresa e as leis e os regulamentos aplicáveis

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o WorkSpaces. Ela mostra como configurar o WorkSpaces para atender aos objetivos de segurança e conformidade. Você também aprende a usar outros serviços da AWS que ajudam a monitorar e proteger os recursos do WorkSpaces.

Índice

Proteção de dados na Amazon WorkSpaces

O modelo de responsabilidade AWS compartilhada de se aplica à proteção de dados na Amazon WorkSpaces. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as Perguntas Frequentes sobre Privacidade de Dados.. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS LGPD e Modelo de Responsabilidade Compartilhada no AWS Blog de Segurança.

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com WorkSpaces ou Serviços da AWS usa o console, a API ou AWS os SDKs. AWS CLI Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico.

Se você fornecer um URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Para obter mais informações sobre a criptografia de endpoint FIPS WorkSpaces e a criptografia, consulte. Configurar o Amazon WorkSpaces para a autorização do FedRAMP ou a conformidade com o SRG do DoD

Criptografia em repouso

Você pode criptografar os volumes de armazenamento para você WorkSpaces usando o AWS KMS Key from AWS Key Management Service. Para ter mais informações, consulte Encriptado WorkSpaces.

Quando você cria WorkSpaces com volumes criptografados, WorkSpaces usa o Amazon Elastic Block Store (Amazon EBS) para criar e gerenciar esses volumes. O EBS criptografa os volumes com uma chave de dados usando o algoritmo AES-256 padrão do setor. Para obter mais informações, consulte Amazon EBS Encryption no Guia do usuário do Amazon EC2.

Criptografia em trânsito

Para o PCoIP, os dados em trânsito são criptografados usando a criptografia TLS 1.2 e a assinatura de solicitação SigV4. O protocolo PCoIP usa tráfego UDP criptografado, com criptografia AES, para streaming de pixels. A conexão de streaming, usando a porta 4172 (TCP e UDP), é criptografada usando cifras AES-128 e AES-256, mas o padrão de criptografia é de 128 bits. Você pode alterar esse padrão para 256 bits usando a configuração de política de grupo Configurar configurações de segurança PCoIP para Windows WorkSpaces ou modificando as configurações de segurança PCoIP no arquivo para Amazon Linux. `pcoip-agent.conf` WorkSpaces

Para saber mais sobre a administração de políticas de grupo para a Amazon WorkSpaces, consulte Definir configurações de segurança do PCoIP emGerencie seu Windows WorkSpaces. Para saber mais sobre a modificação do arquivo `pcoip-agent.conf`, consulte Controle o comportamento do agente PCoIP no Amazon Linux WorkSpaces e PCoIP Security Settings na documentação do Teradici.

Para o WorkSpaces Streaming Protocol (WSP), os dados de streaming e controle em trânsito são criptografados usando criptografia DTLS 1.2 para tráfego UDP e criptografia TLS 1.2 para tráfego TCP, com cifras AES-256.

Gerenciamento de identidade e acesso para o WorkSpaces

Por padrão, os usuários do IAM não têm permissões para recursos e operações do WorkSpaces. Para permitir que os usuários do IAM gerenciem os recursos do WorkSpaces, é necessário criar uma política do IAM que conceda explicitamente permissões a eles e vincular a política aos usuários ou grupos do IAM que precisam dessas permissões.

Para fornecer o acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos no AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em Create a permission set (Criação de um conjunto de permissões) no Guia do usuário do AWS IAM Identity Center.
- Usuários gerenciados no IAM usando um provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criar um perfil para um provedor de identidades de terceiros (federação) no Guia do usuário do IAM.
- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Creating a role for an IAM user (Criação de um perfil para um usuário do IAM) no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Para obter mais informações gerais sobre as políticas do IAM, consulte Permissões e políticas no Guia do usuário do IAM.

O WorkSpaces também cria um perfil do IAM, `workspaces_DefaultRole`, que permite que o serviço WorkSpaces acesse os recursos necessários.

Para obter mais informações sobre o IAM, consulte Identity and Access Management (IAM) e o Guia do usuário do IAM. É possível encontrar recursos, ações e chaves de contexto de condição específicos do WorkSpaces para uso nas políticas de permissão do IAM em Ações, recursos e chaves de condição para o Amazon WorkSpaces no Guia do usuário do IAM.

Para obter uma ferramenta que ajuda a criar políticas do IAM, consulte o AWS Policy Generator. Também é possível usar o simulador de políticas do IAM para testar se uma política permitiria ou negaria uma solicitação específica à AWS.

> **Note**
>
> O Amazon WorkSpaces não oferece suporte ao provisionamento de credenciais do IAM em um WorkSpace (como com um perfil de instância).

Índice

Exemplo de políticas

Os exemplos a seguir mostram declarações de políticas que é possível usar para controlar as permissões que os usuários do IAM têm para o Amazon WorkSpaces.

Example 1: executar todas as tarefas do WorkSpaces

A declaração de política a seguir concede a um usuário do IAM permissão para executar todas as tarefas do WorkSpaces, incluindo a criação e o gerenciamento de diretórios. Ela também concede permissão para executar o procedimento de configuração rápida.

Embora o Amazon WorkSpaces ofereça suporte total aos elementos `Action` e `Resource` ao usar a API e ferramentas de linha de comando, para usar o Amazon WorkSpaces a partir do AWS Management Console, um usuário do IAM deve ter permissões para as seguintes ações e recursos:

- Ações: `"workspaces:*"` e `"ds:*"`
- Recursos: `"Resource": "*"`

O exemplo de política a seguir mostra como permitir que um usuário do IAM use o Amazon WorkSpaces a partir do AWS Management Console.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:GetRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:CreatePolicy",
        "iam:AttachRolePolicy",
        "iam:ListRoles",
        "kms:ListAliases",
        "kms:ListKeys",
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:CreateNetworkInterface",
        "ec2:CreateInternetGateway",
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateTags",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "workdocs:RegisterDirectory",
        "workdocs:DeregisterDirectory",
        "workdocs:AddUserToGroup"
      ],
      "Resource": "*"
    },
    {
      "Sid": "iamPassRole",
```

```
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "workspaces.amazonaws.com"
        }
      }
    }
  ]
}
```

Example 2: executar tarefas específicas do WorkSpace

A declaração de política a seguir concede a um usuário do IAM permissão para executar tarefas específicas do WorkSpace, como executar e remover WorkSpaces. Na declaração de política, a ação `ds:*` concede permissões amplas - controle total sobre todos os objetos do Directory Services na conta.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:PutRolePolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Para também conceder ao usuário a capacidade de habilitar o Amazon WorkDocs para usuários no WorkSpaces, adicione a operação `workdocs`, conforme mostrado no exemplo a seguir.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Action": [
        "workspaces:*",
        "ds:*",
        "workdocs:AddUserToGroup"
      ],
      "Resource": "*"
    }
  ]
}
```

Para também conceder ao usuário a capacidade de usar o assistente de inicialização do WorkSpaces, adicione as operações kms conforme exibido no exemplo a seguir.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "workdocs:AddUserToGroup",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource": "*"
    }
  ]
}
```

Example 3: executar todas as tarefas do WorkSpaces para o BYOL WorkSpaces

A declaração de política a seguir concede a um usuário do IAM permissão para realizar todas as tarefas do WorkSpaces, incluindo as tarefas do Amazon EC2 necessárias para criar traga a sua própria licença (BYOL) WorkSpaces.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
```

```
        "workspaces:*",
        "ds:*",
        "iam:GetRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "kms:ListAliases",
        "kms:ListKeys",
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:CreateNetworkInterface",
        "ec2:CreateInternetGateway",
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateTags",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeImages",
        "ec2:ModifyImageAttribute",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "workdocs:RegisterDirectory",
        "workdocs:DeregisterDirectory",
        "workdocs:AddUserToGroup"
      ],
      "Resource": "*"
    },
    {
      "Sid": "iamPassRole",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
```

```
        "StringEquals": {
          "iam:PassedToService": "workspaces.amazonaws.com"
        }
      }
    }
  ]
}
```

Especificar recursos do WorkSpaces em uma política do IAM

Para especificar um recurso do WorkSpaces no elemento `Resource` da declaração de política, use o nome do recurso da Amazon (ARN) do recurso. Você controla o acesso aos recursos do WorkSpaces permitindo ou negando permissões para usar as ações de API especificadas no elemento `Action` da declaração de política do IAM. O WorkSpaces define ARNs para WorkSpaces, pacotes, grupos de IP e diretórios.

ARN do WorkSpace

Um ARN do WorkSpace tem a sintaxe mostrada no exemplo a seguir.

```
arn:aws:workspaces:region:account_id:workspace/workspace_identifier
```

region

A região em que o WorkSpace está (por exemplo, `us-east-1`).

account_id

O ID da conta da AWS, sem hífens (por exemplo, `123456789012`).

workspace_identifier

O ID do WorkSpace (por exemplo, `ws-a1bcd2efg`).

Veja a seguir o formato do elemento `Resource` de uma declaração de política que identifica um WorkSpace específico.

```
"Resource": "arn:aws:workspaces:region:account_id:workspace/workspace_identifier"
```

É possível usar o caractere curinga * para especificar todos os WorkSpaces que pertencem a uma conta específica em determinada região.

ARN de imagem

Um ARN de imagem do WorkSpace tem a sintaxe mostrada no exemplo a seguir.

```
arn:aws:workspaces:region:account_id:workspaceimage/image_identifier
```

region

A região em que a imagem do WorkSpace está (por exemplo, `us-east-1`).

account_id

O ID da conta da AWS, sem hífens (por exemplo, `123456789012`).

bundle_identifier

O ID da imagem do WorkSpace (por exemplo, `wsi-a1bcd2efg`).

Veja a seguir o formato do elemento `Resource` de uma declaração de política que identifica uma imagem específica.

```
"Resource": "arn:aws:workspaces:region:account_id:workspaceimage/image_identifier"
```

É possível usar o caractere curinga * para especificar todas as imagens que pertencem a uma conta específica em determinada região.

ARN de pacote

Um ARN de pacote tem a sintaxe mostrada no exemplo a seguir.

```
arn:aws:workspaces:region:account_id:workspacebundle/bundle_identifier
```

region

A região em que o WorkSpace está (por exemplo, `us-east-1`).

account_id

O ID da conta da AWS, sem hífens (por exemplo, `123456789012`).

bundle_identifier

O ID do pacote do WorkSpace (por exemplo, `wsb-a1bcd2efg`).

Veja a seguir o formato do elemento `Resource` de uma declaração de política que identifica um pacote específico.

```
"Resource": "arn:aws:workspaces:region:account_id:workspacebundle/bundle_identifier"
```

É possível usar o caractere curinga * para especificar todos os pacotes que pertencem a uma conta específica em determinada região.

ARN do grupo de IP

Um ARN de grupo IP tem a sintaxe mostrada no exemplo a seguir.

```
arn:aws:workspaces:region:account_id:workspaceipgroup/ipgroup_identifier
```

region

A região em que o WorkSpace está (por exemplo, `us-east-1`).

account_id

O ID da conta da AWS, sem hífens (por exemplo, `123456789012`).

ipgroup_identifier

O ID do grupo de IP (por exemplo, `wsipg-a1bcd2efg`).

Veja a seguir o formato do elemento `Resource` de uma declaração de política que identifica um grupo de IP específico.

```
"Resource": "arn:aws:workspaces:region:account_id:workspaceipgroup/ipgroup_identifier"
```

É possível usar o caractere curinga * para especificar todos os grupos de IP que pertencem a uma conta específica determinada região.

ARN do diretório

Um ARN de diretório tem a sintaxe mostrada no exemplo a seguir.

```
arn:aws:workspaces:region:account_id:directory/directory_identifier
```

region

A região em que o WorkSpace está (por exemplo, `us-east-1`).

account_id

O ID da conta da AWS, sem hífens (por exemplo, `123456789012`).

directory_identifier

O ID do diretório (por exemplo, `d-12345a67b8`).

Veja a seguir o formato do elemento `Resource` de uma declaração de política que identifica um diretório específico.

```
"Resource": "arn:aws:workspaces:region:account_id:directory/directory_identifier"
```

É possível usar o caractere curinga * para especificar todos os diretórios que pertencem a uma conta específica em determinada região.

ARN de alias de conexão

Um ARN de alias de conexão tem a sintaxe mostrada no exemplo a seguir.

```
arn:aws:workspaces:region:account_id:connectionalias/connectionalias_identifier
```

region

A região em que o alias da conexão está (por exemplo, `us-east-1`).

account_id

O ID da conta da AWS, sem hífens (por exemplo, `123456789012`).

connectionalias_identifier

O ID do alias de conexão (por exemplo, `wsca-12345a67b8`).

Veja a seguir o formato do elemento `Resource` de uma declaração de política que identifica um alias de conexão específico.

```
"Resource":
 "arn:aws:workspaces:region:account_id:connectionalias/connectionalias_identifier"
```

É possível usar o caractere curinga * para especificar todos os alias de conexão que pertencem a uma conta específica em determinada região.

Ações da API sem suporte de permissões no nível de recurso

Você não pode especificar um ARN de recurso com as seguintes ações de API:

- `AssociateIpGroups`
- `CreateIpGroup`
- `CreateTags`
- `DeleteTags`
- `DeleteWorkspaceImage`
- `DescribeAccount`
- `DescribeAccountModifications`
- `DescribeIpGroups`
- `DescribeTags`
- `DescribeWorkspaceDirectories`
- `DescribeWorkspaceImages`
- `DescribeWorkspaces`
- `DescribeWorkspacesConnectionStatus`
- `DisassociateIpGroups`
- `ImportWorkspaceImage`
- `ListAvailableManagementCidrRanges`
- `ModifyAccount`

Para ações de API que não oferecem suporte a permissões no nível de recurso, é necessário especificar a instrução de recurso mostrada no exemplo a seguir.

```
"Resource": "*"
```

Ações de API que não oferecem suporte a restrições no nível de conta em recursos compartilhados

Para as seguintes ações da API, você não pode especificar um ID de conta no ARN do recurso quando o recurso não é de propriedade da conta:

- `AssociateConnectionAlias`
- `CopyWorkspaceImage`
- `DisassociateConnectionAlias`

Para essas ações da API, você pode especificar um ID de conta no ARN do recurso somente quando essa conta é a proprietária dos recursos a serem usados. Quando a conta não é a proprietária dos recursos, você deve especificar * para o ID da conta, conforme mostrado no exemplo a seguir.

```
"arn:aws:workspaces:region:*:resource_type/resource_identifier"
```

Criar o perfil workspaces_DefaultRole

Antes de registrar um diretório usando a API, você deve verificar se existe um perfil chamado `workspaces_DefaultRole`. Esse perfil é criado pela Configuração Rápida ou se você iniciar um WorkSpace usando o AWS Management Console, e ela concede permissão ao Amazon WorkSpaces para acessar recursos AWS específicos em seu nome. Se esse perfil não existir, você poderá criá-lo usando o procedimento a seguir.

Como criar a função workspaces_DefaultRole

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação à esquerda, escolha Roles (Funções).
3. Selecione Create role (Criar função).
4. Em Selecionar tipo de entidade confiável, selecione Outra conta da AWS.
5. Em Account ID (ID da conta), insira seu ID de conta sem hífens ou espaços.
6. Em Options (Opções), não especifique a autenticação multifator (MFA).
7. Escolha Next: Permissions (Próximo: permissões).
8. Na página Anexar políticas de permissões, selecione as políticas gerenciadas pela AWS AmazonWorkSpacesServiceAccess e AmazonWorkSpacesSelfServiceAccess.

9. Em Definir limite de permissões, recomendamos que você não use um limite de permissões devido ao potencial para conflitos com as políticas anexadas à esse perfil. Tais conflitos podem bloquear determinadas permissões necessárias para a função.
10. Escolha Next: Tags (Próximo: tags).
11. Na página Add tags (optional) (Adicionar tags (opcional)), adicione tags se necessário.
12. Escolha Next: Review (Próximo: revisar).
13. Na página Review (Revisar), em Role name (Nome da função), insira **`workspaces_DefaultRole`**.
14. (Opcional) Em Role description (Descrição da função), insira uma descrição.
15. Selecione Create Role (Criar função).
16. Na página Summary (Resumo) da função workspaces_DefaultRole, escolha a guia Trust relationships (Relações de confiança).
17. Na guia Trust relationships (Relações de confiança), escolha Edit trust relationship (Editar relação de confiança).
18. Na página Edit Trust Relationship (Editar relação de confiança), substitua a declaração de política existente pela declaração a seguir.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

19. Escolha Update Trust Policy.

Criar o perfil de serviço AmazonWorkSpacesPCAAccess

Antes que os usuários possam fazer login usando a autenticação baseada em certificado, você deve verificar se existe um perfil chamado `AmazonWorkSpacesPCAAccess`. Esse perfil é criado quando você habilita a autenticação baseada em certificado em um diretório usando o AWS Management

Console. Ele concede permissão ao Amazon WorkSpaces para acessar recursos do AWS Private CA em seu nome. Se esse perfil não existir porque você não está usando o console para gerenciar a autenticação baseada em certificado, você poderá criá-lo usando o procedimento a seguir.

Como criar o perfil de serviço AmazonWorkSpacesPCAAccess usando a AWS CLI

1. Crie um arquivo JSON denominado `AmazonWorkSpacesPCAAccess.json` com o texto a seguir.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "prod.euc.ecm.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

2. Ajuste o caminho `AmazonWorkSpacesPCAAccess.json` conforme necessário e execute os comandos AWS CLI a seguir para criar o perfil de serviço e anexar a política gerenciada AmazonWorkspacesPCAAccess.

```
aws iam create-role --path /service-role/ --role-name AmazonWorkSpacesPCAAccess --
assume-role-policy-document file://AmazonWorkSpacesPCAAccess.json
```

```
aws iam attach-role-policy –role-name AmazonWorkSpacesPCAAccess –policy-arn
 arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess
```

Políticas gerenciadas pela AWS para o WorkSpaces

O uso de políticas gerenciadas pela AWS torna a adição de permissões a usuários, grupos e perfis mais fácil do que a criação de políticas por conta própria. É necessário tempo e experiência para criar políticas gerenciadas pelo cliente do IAM que fornecem à sua equipe apenas as permissões de que precisam. Use as políticas gerenciadas da AWS para começar rapidamente. Essas políticas abrangem casos de uso comuns e estão disponíveis na sua conta da AWS. Para obter mais

informações sobre políticas gerenciadas pela AWS, consulte Políticas gerenciadas pela AWS no Guia do usuário do IAM.

Os serviços da AWS mantêm e atualizam políticas gerenciadas pela AWS. Não é possível alterar as permissões em políticas gerenciadas pela AWS. Os serviços podem ocasionalmente acrescentar permissões adicionais a uma política gerenciada pela AWS para oferecer suporte a novos recursos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e funções) em que a política está anexada. É mais provável que os serviços atualizem uma política gerenciada pela AWS quando um novo recurso for iniciado ou novas operações se tornarem disponíveis. Os serviços não removem permissões de uma política gerenciada por AWS, portanto, as atualizações de políticas não suspendem suas permissões existentes.

Além disso, a AWS oferece suporte a políticas gerenciadas para funções de trabalho que abrangem vários serviços. Por exemplo, a política gerenciada `ReadOnlyAccess` AWS concede acesso somente leitura a todos os serviços e recursos da AWS. Quando um serviço inicia um novo atributo, a AWS adiciona permissões somente leitura para novas operações e recursos. Para obter uma lista e descrições das políticas de funções de trabalho, consulte Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.

Política gerenciada pela AWS: AmazonWorkSpacesAdmin

Esta política fornece acesso às ações administrativas do Amazon WorkSpaces. Ela fornece as seguintes permissões:

- `workspaces`: permite o acesso para realizar ações administrativas nos recursos do WorkSpaces.
- `kms`: permite o acesso para listar e descrever chaves do KMS, bem como listar aliases.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListAliases",
                "kms:ListKeys",
                "workspaces:CreateTags",
                "workspaces:CreateWorkspaces",
                "workspaces:CreateWorkspaceImage",
                "workspaces:DeleteTags",
```

```
                "workspaces:DescribeTags",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaces",
                "workspaces:DescribeWorkspacesConnectionStatus",
                "workspaces:ModifyCertificateBasedAuthProperties",
                "workspaces:ModifyWorkspaceProperties",
                "workspaces:ModifySamlProperties",
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces",
                "workspaces:RestoreWorkspaces",
                "workspaces:StartWorkspaces",
                "workspaces:StopWorkspaces",
                "workspaces:TerminateWorkspaces"
            ],
            "Resource": "*"
        }
    ]
}
```

Política gerenciada pela AWS: AmazonWorkspacesPCAAccess

Esta política gerenciada fornece acesso aos recursos do Private Certificate Authority (Private CA) do AWS Certificate Manager em sua conta da AWS para autenticação baseada em certificado. Ela está incluída no perfil AmazonWorkspacesPCAAccess e fornece as seguintes permissões:

- `acm-pca`: permite acesso ao Private CA da AWS para gerenciar a autenticação baseada em certificados.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource": "arn:*:acm-pca:*:*:*",
      "Condition": {
        "StringLike": {
```

```
          "aws:ResourceTag/euc-private-ca": "*"
        }
      }
    }
  ]
}
```

Política gerenciada pela AWS: AmazonWorkspacesSelfServiceAccess

Esta política fornece acesso ao serviço do Amazon WorkSpaces para realizar ações de autoatendimento do WorkSpaces iniciadas por um usuário. Ela está incluída no perfil `workspaces_DefaultRole` e fornece as seguintes permissões:

- `workspaces`: permite acesso aos recursos de gerenciamento de WorkSpaces de autoatendimento para usuários.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces",
                "workspaces:ModifyWorkspaceProperties"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Política gerenciada pela AWS: AmazonWorkspacesServiceAccess

Esta política fornece acesso à conta do cliente ao serviço do Amazon WorkSpaces para iniciar um Workspace. Ela está incluída no perfil `workspaces_DefaultRole` e fornece as seguintes permissões:

- `ec2`: permite o acesso para gerenciar recursos do Amazon EC2 associados a um WorkSpace, como interfaces de rede.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Atualizações do WorkSpaces para políticas gerenciadas pela AWS

Visualize detalhes sobre atualizações em políticas gerenciadas pela AWS para o WorkSpaces desde que esse serviço começou a rastrear essas alterações.

Alteração	Descrição	Data
the section called “AmazonWorkSpacesAdmin”: política atualizada	O WorkSpaces adicionou a ação `workspaces:RestoreWorkspace` à política gerenciada AmazonWorkSpacesAdmin, concedendo aos administradores acesso para restaurar WorkSpaces.	25 de junho de 2023
the section called “AmazonWorkspacesPCAAccess”: nova política adicionada	O WorkSpaces adicionou uma nova política gerenciada para conceder permissão ao `acm-pca` para gerenciar o Private CA da AWS para gerenciar a autenticação baseada em certificados.	18 de novembro de 2022

Alteração	Descrição	Data
O WorkSpaces começou a monitorar alterações	O WorkSpaces começou a monitorar as alterações das políticas gerenciadas pelo WorkSpaces.	1º de março de 2021

Validação de conformidade para o Amazon WorkSpaces

Auditores externos avaliam a segurança e a conformidade do Amazon WorkSpaces como parte de vários programas de conformidade da AWS. Isso inclui SOC, PCI, FedRAMP, HIPAA e outros.

Para obter uma lista de serviços da AWS no escopo de programas de conformidade específicos, consulte Serviços da AWS no escopo por programa de conformidade. 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 Fazer download de relatórios no AWS Artifact.

Para obter mais informações sobre o WorkSpaces e o FedRAMP, consulte Configurar o Amazon WorkSpaces para a autorização do FedRAMP ou a conformidade com o SRG do DoD.

Sua responsabilidade com relação à conformidade ao usar o WorkSpaces 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 a manter a conformidade:

- Guias de início rápido de segurança e compatibilidade: estes guias de implantação abordam as considerações de arquitetura e fornecem etapas para implantação de ambientes de linha de base focados em compatibilidade e segurança na AWS.
- Architecting for HIPAA Security and Compliance on Amazon Web Services (Arquitetura para segurança e conformidade com HIPAA na Amazon Web Services): esse whitepaper descreve como as empresas podem usar a AWS para criar aplicativos em conformidade com os padrões 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 Guia do desenvolvedor: AWS Config; avalia como suas configurações de recursos estão em conformidade com práticas internas, diretrizes do setor e regulamentos.
- AWS Security Hub: esse serviço da AWS fornece uma visão abrangente do estado de sua segurança na AWS que ajuda você a conferir sua conformidade com padrões e práticas recomendadas de segurança do setor.

Resiliência no Amazon WorkSpaces

A infraestrutura global da AWS é criada com base em regiões e zonas de disponibilidade da AWS. As regiões fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, que são conectadas com baixa latência, alta throughput e redes altamente redundantes. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

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

O Amazon WorkSpaces também fornece redirecionamento entre regiões, um recurso que funciona com as políticas de roteamento por failover do Sistema de Nomes de Domínio (DNS) para redirecionar os usuários do WorkSpaces para WorkSpaces alternativos em outra região da AWS quando os WorkSpaces primários não estão disponíveis. Para obter mais informações, consulte Redirecionamento entre regiões para a Amazon WorkSpaces.

Segurança da infraestrutura no Amazon WorkSpaces

Como um serviço gerenciado, o Amazon WorkSpaces é protegido pela segurança da rede global da AWS. Para obter informações sobre serviços de segurança da AWS e como a AWS protege a infraestrutura, consulte Segurança na Nuvem AWS. Para projetar seu ambiente da AWS usando as práticas recomendadas de segurança de infraestrutura, consulte Proteção de infraestrutura em Pilar segurança: AWS Well-Architected Framework.

Você usa chamadas de API publicadas pela AWS para acessar o WorkSpaces por meio da rede. Os clientes devem oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.

- Conjuntos de criptografia com Perfect Forward Secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, suporta 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.

Isolamento de rede

Uma nuvem virtual privada (VPC) é uma rede virtual na área isolada logicamente na Nuvem AWS. Você pode implantar o WorkSpaces em uma sub-rede privada na VPC. Para obter mais informações, consulte Configurar uma VPC para WorkSpaces.

Para permitir o tráfego somente em intervalos de endereços específicos (por exemplo, da rede corporativa), atualize o grupo de segurança para a VPC ou use um grupo de controle de acesso IP.

Você pode restringir o acesso ao WorkSpace a dispositivos confiáveis com certificados válidos. Para obter mais informações, consulte Restrinja o WorkSpaces acesso a dispositivos confiáveis.

Isolamento em hosts físicos

WorkSpaces diferentes no mesmo host físico são isolados uns dos outros por meio do hipervisor. É como se estivessem em hosts físicos separados. Quando um WorkSpace é excluído, a memória alocada para ele será removida (definida como 0) pelo hipervisor antes de ser alocada para outro WorkSpace.

Autorização de usuários corporativos

Com o WorkSpaces, os diretórios são gerenciados pelo AWS Directory Service. É possível criar um diretório gerenciado autônomo para os usuários. Ou é possível integrar com seu ambiente do Active Directory existente para que os usuários possam usar suas credenciais atuais para obter acesso contínuo aos recursos corporativos. Para obter mais informações, consulte Gerenciar diretórios para WorkSpaces.

Para controlar ainda mais o acesso aos WorkSpaces, use a autenticação multifator. Para obter mais informações, consulte How to Enable Multi-Factor Authentication for AWS Services.

Fazer solicitações de API do Amazon WorkSpaces por um endpoint de interface da VPC

É possível se conectar diretamente a endpoints de API do Amazon WorkSpaces por meio de um endpoint de interface em sua nuvem privada virtual (VPC) em vez de se conectar pela internet. Quando você usa um endpoint de interface da VPC, a comunicação entre a VPC e o endpoint de API do Amazon WorkSpaces é realizada inteiramente e com segurança na rede da AWS.

> **Note**
>
> Esse recurso pode ser usado somente para conexão com endpoints de API do WorkSpaces. Para se conectar ao WorkSpaces usando os clientes do WorkSpaces, é necessária conectividade com a Internet, conforme descrito em Requisitos de endereço IP e porta para WorkSpaces.

Os endpoints de API do Amazon WorkSpaces são compatíveis com os endpoints de interface do Amazon Virtual Private Cloud (Amazon VPC) baseados no AWS PrivateLink. Cada VPC endpoint é representado por uma ou mais interfaces de rede (também conhecidas como interfaces de rede elástica ou ENIs) com endereços IP privados nas sub-redes da VPC.

O endpoint de interface da VPC conecta a VPC diretamente ao endpoint de API do Amazon WorkSpaces sem um gateway da Internet, um dispositivo NAT, uma conexão VPN ou uma conexão do AWS Direct Connect. As instâncias na VPC não precisam de endereços IP públicos para a comunicação com o endpoint de API do Amazon WorkSpaces.

É possível criar um endpoint de interface para se conectar ao Amazon WorkSpaces com o AWS Management Console ou os comandos do AWS Command Line Interface (AWS CLI). Para obter instruções, consulte Criar um endpoint de interface.

Depois que criar um endpoint da VPC, você poderá usar os seguintes comandos da CLI de exemplo que usam o parâmetro `endpoint-url` para especificar endpoints de interface para o endpoint da API do Amazon WorkSpaces:

```
aws workspaces copy-workspace-image --endpoint-
url VPC_Endpoint_ID.workspaces.Region.vpce.amazonaws.com

aws workspaces delete-workspace-image --endpoint-
url VPC_Endpoint_ID.api.workspaces.Region.vpce.amazonaws.com
```

```
aws workspaces describe-workspace-bundles --endpoint-
url VPC_Endpoint_ID.workspaces.Region.vpce.amazonaws.com  \
   --endpoint-name Endpoint_Name \
   --body "Endpoint_Body" \
   --content-type "Content_Type" \
       Output_File
```

Se você habilitar nomes de hosts DNS privados para seu VPC endpoint, não precisará especificar a URL do endpoint. O nome de host DNS da API do Amazon WorkSpaces que a CLI e o SDK do Amazon WorkSpaces usam por padrão (https://api.workspaces.*Região*.amazonaws.com) é resolvido para seu endpoint da VPC.

O endpoint da API do Amazon WorkSpaces é compatível com os endpoints da VPC em todas as regiões da AWS em que o Amazon VPC e o Amazon WorkSpaces estão disponíveis. O Amazon WorkSpaces é compatível com chamadas para todas suas APIs públicas dentro da VPC.

Para saber mais sobre o AWS PrivateLink, consulte a documentação do AWS PrivateLink. Para obter o preço dos VPC endpoints, consulte a Definição de preço da VPC. Para saber mais sobre VPC e endpoints, consulte Amazon VPC.

Para ver uma lista de endpoints de API do Amazon WorkSpaces por região, consulte WorkSpaces API Endpoints.

> **Note**
>
> Os endpoints de API do Amazon WorkSpaces com AWS PrivateLink não são compatíveis com endpoints de API do Amazon WorkSpaces do Padrão de Processamento de Informações Federal (FIPS).

Criar uma política de endpoint da VPC para o Amazon WorkSpaces

É possível criar uma política de endpoints do Amazon VPC para o Amazon WorkSpaces a fim de especificar o seguinte:

- A entidade principal que pode executar ações.
- As ações que podem ser executadas.
- Os recursos sobre os quais as ações podem ser realizadas.

Para obter mais informações, consulte Controlar o acesso a serviços com VPC endpoints no Manual do usuário da Amazon VPC.

> **Note**
>
> As políticas de endpoint da VPC não são compatíveis com os endpoints do Amazon WorkSpaces do Padrão de Processamento de Informações Federal (FIPS).

O exemplo de política de endpoint da VPC a seguir especifica que todos os usuários com acesso ao endpoint de interface da VPC têm permissão para invocar o endpoint hospedado do Amazon WorkSpaces, denominado `ws-f9abcdefg`.

```
{
     "Statement": [
         {
             "Action": "workspaces:*",
             "Effect": "Allow",
             "Resource": "arn:aws:workspaces:us-west-2:1234567891011:workspace/ws-
f9abcdefg",
             "Principal": "*"
         }
     ]
}
```

Neste exemplo, as seguintes ações são negadas:

- Invocar endpoints hospedados do Amazon WorkSpaces que não sejam `ws-f9abcdefg`.
- Executar uma ação em qualquer recurso além da especificada (ID do WorkSpace: `ws-f9abcdefg`).

> **Note**
>
> Neste exemplo, os usuários ainda podem realizar outras ações da API do Amazon WorkSpaces de fora da VPC. Para restringir chamadas de API para esses de dentro da VPC, consulte Gerenciamento de identidade e acesso para o WorkSpaces para obter informações sobre como usar políticas baseadas em identidade para controlar o acesso a endpoints de API do Amazon WorkSpaces.

Conectar uma rede privada a uma VPC

Para chamar a API do Amazon WorkSpaces por meio da VPC, é necessário se conectar de uma instância que esteja dentro da VPC ou conectar sua rede privada à sua VPC usando o AWS Virtual Private Network (AWS VPN) ou o AWS Direct Connect. Para obter mais informações, consulte Conexões VPN no Guia do usuário do Amazon Virtual Private Cloud. Para obter informações sobre a AWS Direct Connect, consulte Criar uma conexão no Manual do usuário da AWS Direct Connect.

Gerenciamento de atualizações em WorkSpaces

Recomendamos que você corrija, atualize e proteja regularmente o sistema operacional e os aplicativos do seu WorkSpaces. Você pode configurar seu WorkSpaces para ser atualizado WorkSpaces durante uma janela de manutenção regular ou você mesmo pode atualizá-lo. Para ter mais informações, consulte Manutenção do WorkSpace.

Para aplicativos em seu WorkSpaces, você pode usar qualquer serviço de atualização automática fornecido ou seguir as recomendações de instalação de atualizações fornecidas pelo fornecedor do aplicativo.

Solucionar problemas WorkSpaces

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

Habilitar o registro em log avançado

Para ajudar a solucionar problemas que seus usuários possam enfrentar, você pode ativar o registro avançado em qualquer WorkSpaces cliente da Amazon.

O registro em log avançado gera arquivos de log que contêm informações de diagnóstico e detalhes no nível da depuração, incluindo dados de desempenho detalhados. Para os clientes 1.0+ e 2.0+, esses arquivos de registro avançados são automaticamente enviados para um banco de dados em. AWS

> **Note**
>
> Para obter AWS uma análise dos arquivos de registro avançados e receber suporte técnico para problemas com seus WorkSpaces clientes, entre em contato com AWS Support. Para obter mais informações, consulte o AWS Support Center.

Como habilitar o registro em log avançado para o Acesso via Web

Como habilitar o registro em log avançado para o Acesso via Web

1. Abra seu cliente Amazon WorkSpaces Web Access.
2. Na parte superior da página de WorkSpaces login, escolha Registro de diagnóstico.
3. Na caixa de diálogo pop-up, verifique se o Registro em log de diagnóstico está habilitado.
4. Em Nível de registro, escolha Registro em log avançado.

Como acessar arquivos de log no Google Chrome, no Microsoft Edge e no Firefox

1. Abra o menu de contexto (clique com o botão direito do mouse) nos navegadores ou pressione Ctrl + Shift + I (em computadores Mac, command + option + I) no teclado para abrir o painel de ferramentas do desenvolvedor.
2. No painel de ferramentas do desenvolvedor, escolha a guia Console para exibir os arquivos de log.

Como acessar arquivos de log no Safari

1. Escolha Safari, Configurações.
2. Na janela Preferências, escolha a guia Avançado.
3. Escolha Mostrar menu Desenvolvedor na barra de menus.
4. Na guia Desenvolvedor na barra de menus, escolha Desenvolvedor > Conectar Inspetor Web.
5. No painel do Inspetor Web do Safari, escolha a guia Console para exibir os arquivos de log.

Como habilitar o registro em log avançado em clientes 4.0+

Os logs de cliente no Windows são armazenados no local a seguir:

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\logs
```

Como habilitar o log avançado para clientes no Windows

1. Feche o WorkSpaces cliente da Amazon.
2. Abra o aplicativo de prompt de comando.
3. Inicie o WorkSpaces cliente com a `-l3` bandeira.

   ```
   c:

   cd "C:\Program Files\Amazon Web Services, Inc\Amazon WorkSpaces"

   workspaces.exe -l3
   ```

   > **Note**
   >
   > Se WorkSpaces estiver instalado para um usuário e não para todos os usuários, use os seguintes comandos:
   >
   > ```
   > c:
   > cd "%LocalAppData%\Programs\Amazon Web Services, Inc\Amazon WorkSpaces"
   > workspaces.exe -l3
   > ```

Os logs do cliente no macOS são armazenados no local a seguir:

```
~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/
logs
```

Como habilitar o registro em log avançado para clientes no macOS

1. Feche o WorkSpaces cliente da Amazon.
2. Abra o terminal.
3. Execute o seguinte comando .

   ```
   open -a workspaces --args -l3
   ```

Como habilitar o registro em log avançado em clientes para Android

1. Feche o WorkSpaces cliente da Amazon.
2. Abra o menu do cliente Android.
3. Selecione Suporte.
4. Selecione Configurações de registro em log.
5. Selecione Ativar registro em log avançado.

Para recuperar logs de clientes Android depois de ativar o registro em log avançado:

- Selecione Extrair log para salvar os logs compactados localmente.

Os logs de cliente no Linux são armazenados no local a seguir:

```
~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs
```

Como habilitar o log avançado para clientes no Linux

1. Feche o WorkSpaces cliente da Amazon.
2. Abra o terminal.
3. Execute o seguinte comando .

   ```
   /opt/workspacesclient/workspacesclient -l3
   ```

Como habilitar o registro em log avançado em clientes 3.0

Os logs de cliente no Windows são armazenados no local a seguir:

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\logs
```

Como habilitar o log avançado para clientes no Windows

1. Feche o WorkSpaces cliente da Amazon.
2. Abra o aplicativo de prompt de comando.
3. Inicie o WorkSpaces cliente com a `-l3` bandeira.

   ```
   c:

   cd "C:\Program Files (x86)\Amazon Web Services, Inc\Amazon WorkSpaces"

   workspaces.exe -l3
   ```

   > **Note**
   >
   > Se WorkSpaces estiver instalado para um usuário e não para todos os usuários, use os seguintes comandos:
   >
   > ```
   > c:
   > cd "%LocalAppData%\Programs\Amazon Web Services, Inc\Amazon WorkSpaces"
   > workspaces.exe -l3
   > ```

Os logs do cliente no macOS são armazenados no local a seguir:

```
~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/logs
```

Como habilitar o registro em log avançado para clientes no macOS

1. Feche o WorkSpaces cliente da Amazon.
2. Abra o terminal.
3. Execute o seguinte comando .

   ```
   open -a workspaces --args -l3
   ```

Como habilitar o registro em log avançado em clientes para Android

1. Feche o WorkSpaces cliente da Amazon.
2. Abra o menu do cliente Android.
3. Selecione Suporte.
4. Selecione Configurações de registro em log.
5. Selecione Ativar registro em log avançado.

Para recuperar logs de clientes Android depois de ativar o registro em log avançado:

- Selecione Extrair log para salvar os logs compactados localmente.

Os logs de cliente no Linux são armazenados no local a seguir:

```
~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs
```

Como habilitar o log avançado para clientes no Linux

1. Feche o WorkSpaces cliente da Amazon.
2. Abra o terminal.
3. Execute o seguinte comando .

   ```
   /opt/workspacesclient/workspacesclient -l3
   ```

Como habilitar o log avançado para clientes do 1.0 e posterior e do 2.0 e posterior

1. Abra o WorkSpaces cliente.
2. Escolha o ícone de engrenagem no canto superior direito do aplicativo cliente.
3. Escolha Advanced Settings.
4. Marque a caixa de seleção Enable Advanced Logging (Habilitar o registro em log avançado).
5. Escolha Salvar.

Os logs de cliente no Windows são armazenados no local a seguir:

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\1.0\Logs
```

Os logs do cliente no macOS são armazenados no local a seguir:

```
~/Library/Logs/Amazon Web Services/Amazon WorkSpaces/1.0
```

Solucionar problemas específicos

As informações a seguir podem ajudá-lo a solucionar problemas específicos com seu WorkSpaces.

Problemas

- Não consigo criar um Amazon Linux WorkSpace porque há caracteres inválidos no nome de usuário
- Eu mudei o shell do meu Amazon Linux WorkSpace e agora não consigo provisionar uma sessão de PCoIP
- Meu Amazon Linux WorkSpaces não inicia
- O lançamento WorkSpaces no meu diretório conectado geralmente falha
- O lançamento WorkSpaces falha com um erro interno
- Quando tento registrar um diretório, o registro falha e deixa o diretório em um estado de ERRO
- Meus usuários não conseguem se conectar a um Windows WorkSpace com um banner de logon interativo
- Meus usuários não conseguem se conectar a um Windows WorkSpace
- Meus usuários estão tendo problemas quando tentam se conectar a WorkSpaces partir do WorkSpaces Web Access
- O WorkSpaces cliente da Amazon exibe uma tela cinza “Carregando...” por um tempo antes de retornar à tela de login. Nenhuma outra mensagem de erro é exibida.
- Meus usuários recebem a mensagem "WorkSpace Status: Insalubre. Não foi possível conectar você ao seu WorkSpace. Tente novamente em alguns minutos”.
- Meus usuários recebem a mensagem “Este dispositivo não está autorizado a acessar WorkSpace o. Entre em contato com o administrador para obter ajuda”.
- Meus usuários recebem a mensagem “Sem rede. Conexão de rede perdida. Verifique a conexão de rede ou entre em contato com o administrador para obter ajuda.” ao tentar se conectar a um WSP WorkSpace
- O WorkSpaces cliente dá aos meus usuários um erro de rede, mas eles podem usar outros aplicativos habilitados para rede em seus dispositivos

- Meus WorkSpace usuários veem a seguinte mensagem de erro: “O dispositivo não consegue se conectar ao serviço de registro. Verifique suas configurações de rede."
- Meus usuários de cliente zero PCoIP estão recebendo o erro "The supplied certificate is invalid due to timestamp" (O certificado fornecido é inválido devido ao time stamp)
- Impressoras USB e outros periféricos compatíveis com USB não estão funcionando para clientes zero PCoIP
- Meus usuários ignoraram a atualização dos aplicativos cliente Windows ou macOS e não foram solicitados a instalar a versão mais recente
- Meus usuários não conseguem instalar o aplicativo cliente Android em seus Chromebooks
- Meus usuários não estão recebendo e-mails de convite nem e-mails de redefinição de senha
- Meus usuários não veem a opção Esqueceu sua senha? na tela de login do cliente
- Eu recebo a mensagem “O administrador do sistema definiu políticas para impedir essa instalação” quando tento instalar aplicativos em um Windows WorkSpace
- Não WorkSpaces , no meu diretório, posso me conectar à internet
- Meu WorkSpace perdeu o acesso à Internet
- Eu recebo um erro de "DNS indisponível" quando tento me conectar ao meu diretório on-premises
- Eu recebo um erro "Problemas de conectividade detectados" quando tento me conectar ao meu diretório on-premises
- Eu recebo um erro "Registro SRV" quando tento me conectar ao meu diretório on-premises
- Meu Windows WorkSpace adormece quando fica ocioso
- Um dos meus WorkSpaces tem um estado de UNHEALTHY
- Meu WorkSpace está travando ou reiniciando inesperadamente
- O mesmo nome de usuário tem mais de um WorkSpace, mas o usuário só pode fazer login em um dos WorkSpaces
- Estou tendo problemas para usar o Docker com a Amazon WorkSpaces
- Eu recebo ThrottlingException erros em algumas das minhas chamadas de API
- Meu WorkSpace continua se desconectando quando eu o deixo rodar em segundo plano
- A federação SAML 2.0 não está funcionando. Meus usuários não estão autorizados a transmitir seus WorkSpaces desktops.
- Meus usuários são desconectados da WorkSpaces sessão a cada 60 minutos.

- Meus usuários recebem um erro de redirecionamento de URI quando se federam usando o fluxo iniciado pelo provedor de identidade (IdP) SAML 2.0 ou uma instância adicional do aplicativo WorkSpaces cliente é iniciada toda vez que meus usuários tentam fazer login a partir do cliente após a federação no IdP.
- Meus usuários recebem a mensagem “Algo deu errado: ocorreu um erro ao iniciar seu WorkSpace” quando tentam entrar no aplicativo WorkSpaces cliente após a federação no IdP.
- Meus usuários recebem a mensagem “Não é possível validar as tags” quando tentam entrar no aplicativo WorkSpaces cliente após a federação no IdP.
- Meus usuários recebem a mensagem: “O cliente e o servidor não conseguem se comunicar porque não possuem um algoritmo comum”.
- Meu microfone ou webcam não está funcionando no Windows WorkSpaces.
- Meus usuários não conseguem fazer login usando a autenticação baseada em certificado e a senha é solicitada no WorkSpaces cliente ou na tela de login do Windows quando se conectam à sessão do desktop.
- Estou tentando fazer algo que requer mídia de instalação do Windows, mas WorkSpaces não a fornece.
- Quero iniciar WorkSpaces com um diretório AWS gerenciado existente criado em uma WorkSpaces região sem suporte.
- Quero atualizar o Firefox no Amazon Linux 2.
- Meu usuário consegue redefinir sua senha usando o WorkSpaces cliente, ignorando a configuração Fine Grained Password Policy (FFGP) que está configurada. AWS Managed Microsoft AD
- Meus usuários recebem a mensagem de erro “Este sistema operacional não está autorizado a acessar seu WorkSpace” ao tentar acessar o WorkSpace Windows/Linux usando o Web Access

Não consigo criar um Amazon Linux WorkSpace porque há caracteres inválidos no nome de usuário

Para Amazon Linux WorkSpaces, nomes de usuário:

- Podem conter 20 caracteres no máximo
- Podem conter letras, espaços e números que são representáveis em UTF-8
- Podem incluir os seguintes caracteres especiais: _.-#

- Não é possível começar com um símbolo de traço (-) como o primeiro caractere do nome de usuário

> **Note**
>
> Essas limitações não se aplicam ao Windows WorkSpaces. O Windows WorkSpaces suporta os símbolos @ e - para todos os caracteres no nome do usuário.

Eu mudei o shell do meu Amazon Linux WorkSpace e agora não consigo provisionar uma sessão de PCoIP

Para substituir o shell padrão para Linux WorkSpaces, consulteSubstitua o shell padrão para Amazon Linux WorkSpaces.

Meu Amazon Linux WorkSpaces não inicia

A partir de 20 de julho de 2020, o Amazon Linux WorkSpaces usará novos certificados de licença. Esses novos certificados são compatíveis somente com as versões 2.14.1.1, 2.14.7, 2.14.9 e 20.10.6 ou posteriores do agente PCoIP.

Se você estiver usando uma versão não compatível do agente PCoIP, atualize-a para a versão mais recente (20.10.6), que contém as correções mais recentes e os aprimoramentos de performance compatíveis com os novos certificados. Se você não fizer essas atualizações até 20 de julho, o provisionamento de sessões para seu Linux WorkSpaces falhará e seus usuários finais não conseguirão se conectar a eles. WorkSpaces

Como atualizar o agente PCoIP para a versão mais recente

1. Abra o WorkSpaces console em https://console.aws.amazon.com/workspaces/.
2. No painel de navegação, escolha WorkSpaces.
3. Selecione seu Linux WorkSpace e reinicie-o escolhendo Ações, WorkSpacesReinicializar. Se o WorkSpace status for`STOPPED`, você deve escolher Ações, Iniciar WorkSpaces primeiro e esperar até que o status seja `AVAILABLE` antes de poder reinicializá-lo.
4. Depois de reinicializar e seu status ser`AVAILABLE`, recomendamos que você altere o status do WorkSpace para `ADMIN_MAINTENANCE` enquanto estiver executando essa atualização.

WorkSpace Ao terminar, altere o status do WorkSpace para`AVAILABLE`. Para obter mais informações sobre o modo `ADMIN_MAINTENANCE`, consulte Manutenção manual.

Para alterar o status de um WorkSpace para`ADMIN_MAINTENANCE`, faça o seguinte:

a. Selecione WorkSpace e escolha Ações, Modificar WorkSpace.
b. Selecione Modify State (Modificar estado).
c. Em Estado pretendido, escolha ADMIN_MAINTENANCE.
d. Escolha Modificar.

5. Conecte-se ao seu Linux WorkSpace por meio de SSH. Para ter mais informações, consulte Habilite conexões SSH para seu Linux WorkSpaces.
6. Para atualizar o agente PCoIP, execute o seguinte comando:

```
sudo yum --enablerepo=pcoip-stable install pcoip-agent-standard-20.10.6
```

7. Para verificar a versão do agente e confirmar que a atualização foi bem-sucedida, execute o seguinte comando:

```
rpm -q pcoip-agent-standard
```

O comando de verificação deve produzir o seguinte resultado:

```
pcoip-agent-standard-20.10.6-1.el7.x86_64
```

8. Desconecte-se do WorkSpace e reinicie-o novamente.
9. Se você definir o status do WorkSpace para `ADMIN_MAINTENANCE` inStep 4, repita Step 4 e defina o Estado pretendido como`AVAILABLE`.

Se o Linux WorkSpace ainda falhar ao iniciar após a atualização do agente PCoIP, entre em contato com o Support AWS .

O lançamento WorkSpaces no meu diretório conectado geralmente falha

Verifique se os dois servidores DNS ou controladores de domínio em seu diretório local são acessíveis a partir de cada uma das sub-redes que você especificou quando se conectou ao seu diretório. Você pode verificar essa conectividade executando uma instância Amazon EC2 em cada sub-rede e associando a instância ao seu diretório usando os endereços IP dos dois servidores DNS.

O lançamento WorkSpaces falha com um erro interno

Verifique se suas sub-redes estão configuradas para atribuir automaticamente endereços IPv6 a instâncias ativadas na sub-rede. Para verificar essa configuração, abra o console do Amazon VPC, selecione sua sub-rede e escolha Ações da sub-rede e Modificar configurações de IP de atribuição automática. Se essa configuração estiver ativada, você não poderá iniciar WorkSpaces usando os pacotes de desempenho ou gráficos. Em vez disso, desative essa configuração e especifique endereços IPv6 manualmente ao ativar suas instâncias.

Quando tento registrar um diretório, o registro falha e deixa o diretório em um estado de ERRO

Esse problema pode ocorrer se você estiver tentando registrar um diretório AWS gerenciado do Microsoft AD que tenha sido configurado para replicação multirregional. Embora o diretório na região principal possa ser registrado com sucesso para uso com a Amazon WorkSpaces, a tentativa de registrar o diretório em uma região replicada falha. A replicação multirregional com o AWS Microsoft AD gerenciado não é suportada para uso com a Amazon WorkSpaces em regiões replicadas.

Meus usuários não conseguem se conectar a um Windows WorkSpace com um banner de logon interativo

Se uma mensagem de login interativa tiver sido implementada para exibir um banner de login, isso impedirá que os usuários acessem o Windows. WorkSpaces A configuração da Política de Grupo da mensagem de logon interativa não é atualmente suportada pelo WorkSpaces PCoIP. Mova o WorkSpaces para uma unidade organizacional (OU) onde a Política de Interactive logon: Message text for users attempting to log on Grupo não seja aplicada. A mensagem de login é suportada no WSP WorkSpaces, e os usuários precisam fazer login novamente após aceitarem o banner de login.

Meus usuários não conseguem se conectar a um Windows WorkSpace

Meus usuários recebem o seguinte erro quando tentam se conectar ao Windows WorkSpaces:

```
"An error occurred while launching your WorkSpace. Please try again."
```

Esse erro geralmente ocorre quando não é WorkSpace possível carregar a área de trabalho do Windows usando o PCoIP. Verifique o seguinte:

- Esta mensagem aparece se o serviço PCoIP Standard Agent for Windows não estiver em execução. Conecte-se usando RDP para verificar se o serviço está em execução, que está definido para iniciar automaticamente e que pode se comunicar pela interface de gerenciamento (eth0).

- Se o agente PCoIP tiver sido desinstalado, reinicie-o por meio WorkSpace do WorkSpaces console da Amazon para reinstalá-lo automaticamente.

- Você também pode receber esse erro no WorkSpaces cliente da Amazon após um longo atraso se o grupo de WorkSpaces segurança for modificado para restringir o tráfego de saída. Restringir o tráfego de saída impede que o Windows se comunique com os controladores de diretório para login. Verifique se seus grupos de segurança permitem que você WorkSpaces se comunique com seus controladores de diretório em todas as portas necessárias na interface de rede primária.

Outra causa deste erro está relacionada à Política de grupo de atribuição de direitos de usuário. Se a política de grupo a seguir estiver configurada incorretamente, ela impedirá que os usuários acessem o Windows WorkSpaces:

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment (Configuração do computador\Configurações do Windows\Configurações de segurança\Políticas locais\Atribuição de direitos de usuário)

- Política incorreta:

  Política: Access this computer from the network (Acessar este computador pela rede)

  Configuração: *Nome de domínio*\Computadores de domínio

  GPO vencedor: permitir acesso a arquivos
- Política correta:

  Política: Access this computer from the network (Acessar este computador pela rede)

  Configuração: *Nome de domínio*\Usuários de domínio

  GPO vencedor: permitir acesso a arquivos

> **Note**
>
> Esta definição de política deve ser aplicada a Domain users (Usuários do domínio) em vez de Domain Computers (Computadores do domínio).

Para obter mais informações, consulte Acessar este computador pela rede – configuração de política de segurança e Definir configurações de política de segurança na documentação do Microsoft Windows.

Meus usuários estão tendo problemas quando tentam se conectar a WorkSpaces partir do WorkSpaces Web Access

A Amazon WorkSpaces depende de uma configuração específica da tela de login para permitir que os usuários façam login com sucesso a partir do seu cliente Web Access.

Para permitir que os usuários do Web Access façam login em seus WorkSpaces, você deve definir uma configuração de Política de Grupo e três configurações de Política de Segurança. Se essas configurações não estiverem definidas corretamente, os usuários poderão enfrentar longos tempos de login ou telas pretas ao tentarem fazer login no seu WorkSpaces. Para definir essas configurações, consulte Ativar e configurar o Amazon WorkSpaces Web Access.

> **Important**
>
> A partir de 1º de outubro de 2020, os clientes não poderão mais usar o cliente Amazon WorkSpaces Web Access para se conectar ao Windows 7 Custom WorkSpaces ou ao Windows 7 Bring Your Own License (BYOL) WorkSpaces.

O WorkSpaces cliente da Amazon exibe uma tela cinza “Carregando...” por um tempo antes de retornar à tela de login. Nenhuma outra mensagem de erro é exibida.

Esse comportamento geralmente indica que o WorkSpaces cliente pode se autenticar pela porta 443, mas não pode estabelecer uma conexão de streaming pela porta 4172 (PCoIP) ou pela porta 4195 (WSP). Esta situação pode ocorrer quando os pré-requisitos da rede não são atendidos. Os problemas do lado do cliente geralmente causam falha na verificação de

rede do cliente. Para ver quais verificações de integridade estão apresentando falha, clique no ícone de verificação de rede (normalmente é um triângulo vermelho com um ponto de exclamação no canto inferior direito da página de login para clientes 2.0+ ou o ícone de rede

no canto superior direito para clientes 3.0+).

> **Note**
>
> A causa mais comum desse problema é um firewall ou proxy do lado do cliente que impede o acesso pelas portas 4172 ou 4195 (TCP e UDP). Se esta verificação de integridade falhar, verifique as configurações de firewall locais.

Se a verificação de rede for aprovada, pode haver um problema com a configuração de rede do WorkSpace. Por exemplo, uma regra do Windows Firewall pode bloquear a porta UDP 4172 a 4195 na interface de gerenciamento. Conecte-se ao WorkSpace usando um cliente RDP (Remote Desktop Protocol) para verificar se WorkSpace ele atende aos requisitos de porta necessários.

Meus usuários recebem a mensagem "WorkSpace Status: Insalubre. Não foi possível conectar você ao seu WorkSpace. Tente novamente em alguns minutos”.

Esse erro geralmente indica que o SkyLightWorkSpacesConfigService serviço não está respondendo às verificações de saúde.

Se você acabou de reiniciar ou iniciar o seu WorkSpace, aguarde alguns minutos e tente novamente.

Se o estiver em execução WorkSpace há algum tempo e você ainda vê esse erro, conecte-se usando o RDP para verificar se o SkyLightWorkSpacesConfigService serviço:

- Está em execução.
- Está definido para iniciar automaticamente.
- Pode se comunicar pela interface de gerenciamento (eth0).
- Não está bloqueado por um software antivírus de terceiros.

Meus usuários recebem a mensagem “Este dispositivo não está autorizado a acessar WorkSpace o. Entre em contato com o administrador para obter ajuda”.

Esse erro indica que os grupos de controle de acesso IP estão configurados no WorkSpace diretório, mas o endereço IP do cliente não está na lista de permissões.

Verifique as configurações no diretório. Confirme se o endereço IP público do qual o usuário está se conectando permite acesso ao WorkSpace.

Meus usuários recebem a mensagem “Sem rede. Conexão de rede perdida. Verifique a conexão de rede ou entre em contato com o administrador para obter ajuda.” ao tentar se conectar a um WSP WorkSpace

Se esse erro ocorrer e os usuários não tiverem problemas de conectividade, verifique se a porta 4195 está aberta nos firewalls da sua rede. Para WorkSpaces usar o WorkSpaces Streaming Protocol (WSP), a porta usada para transmitir a sessão do cliente foi alterada de 4172 para 4195.

O WorkSpaces cliente dá aos meus usuários um erro de rede, mas eles podem usar outros aplicativos habilitados para rede em seus dispositivos

Os aplicativos WorkSpaces cliente dependem do acesso a recursos na AWS nuvem e exigem uma conexão que forneça pelo menos 1 Mbps de largura de banda de download. Se um dispositivo tiver uma conexão intermitente com a rede, o aplicativo WorkSpaces cliente poderá relatar um problema com a rede.

WorkSpaces impõe o uso de certificados digitais emitidos pela Amazon Trust Services a partir de maio de 2018. A Amazon Trust Services já é uma CA raiz confiável nos sistemas operacionais que são suportados pela WorkSpaces. Se a lista de CA raiz do sistema operacional não estiver atualizada, o dispositivo não poderá se conectar WorkSpaces e o cliente apresentará um erro de rede.

Para reconhecer problemas de conexão devido a falhas de certificado

- Clientes zero PCoIP: a mensagem de erro a seguir é exibida.

```
Failed to connect. The server provided a certificate that is invalid. See below for
 details:
- The supplied certificate is invalid due to timestamp
- The supplied certificate is not rooted in the devices local certificate store
```

- Outros clientes: as verificações de integridade falham com um triângulo de aviso vermelho para internet.

Para resolver falhas de certificado

- Aplicação cliente para Windows
- Clientes zero PCoIP
- Outras aplicações cliente

Aplicação cliente para Windows

Use uma das seguintes soluções para falhas de certificado.

Solução 1: atualizar o aplicativo cliente

Durante a instalação, o aplicativo cliente garante que seu sistema operacional confie em certificados emitidos pelo Amazon Trust Services.

Solução 2: adicionar o Amazon Trust Services à lista local de autoridades de certificação raiz

1. Acesse https://www.amazontrust.com/repository/.
2. Faça download do certificado Starfield no formato DER (2b071c59a0a0ae76b0eadb2bad23bad4580b69c3601b630c2eaf0613afa83f92).
3. Abra o Console de Gerenciamento Microsoft. (No prompt de comando, execute mmc.)
4. Selecione File (Arquivo), Add/Remove Snap-in (Adicionar/Remover snap-in), Certificates (Certificados) e Add (Adicionar).
5. Na página Certificates snap-in (Snap-in de certificados), selecione Computer account (Conta de computador) e Next (Avançar). Mantenha o padrão, Local computer (Computador local). Escolha Terminar. Escolha OK.
6. Expanda Certificates (Local Computer) [Certificados (computador local)] e selecione Trusted Root Certification Authorities (Autoridades de certificação raiz confiáveis). Selecione Action (Ação), All Tasks (Todas as tarefas) e Import (Importar).

7. Siga o assistente para importar o certificado que você obteve por download.
8. Saia e reinicie o aplicativo WorkSpaces cliente.

Solução 3: implantar o Amazon Trust Services como uma CA confiável usando a política de grupo

Adicione o certificado Starfield às CAs raiz confiáveis do domínio usando a política de grupo. Para obter mais informações, consulte Usar política para distribuir certificados.

Clientes zero PCoIP

Para se conectar diretamente a um usuário WorkSpace usando a versão 6.0 ou posterior do firmware, baixe e instale o certificado emitido pela Amazon Trust Services.

Para adicionar o Amazon Trust Services como uma CA raiz confiável

1. Abra https://certs.secureserver.net/repository/.
2. Faça o download do certificado em Starfield Certificate Chain (Cadeia de certificado Starfield) com a impressão digital 14 65 FA 20 53 97 B8 76 FA A6 F0 A9 95 8E 55 90 E4 0F CC 7F AA 4F B7 C2 C8 67 75 21 FB 5F B6 58.
3. Carregue o certificado para o cliente zero. Para obter mais informações, consulte Upload de certificados na documentação do Teradici.

Outras aplicações cliente

Adicione o certificado Starfield (2b071c59a0a0ae76b0eadb2bad23bad4580b69c3601b630c2eaf0613afa83f92) no Amazon Trust Services. Para obter mais informações sobre como adicionar uma CA raiz, consulte a seguinte documentação:

- Android: Adicionar e remover certificados
- Chrome OS: Gerenciar certificados de cliente em dispositivos Chrome
- macOS e iOS: Instalar o certificado raiz de uma CA no dispositivo de teste

Meus WorkSpace usuários veem a seguinte mensagem de erro: “O dispositivo não consegue se conectar ao serviço de registro. Verifique suas configurações de rede."

Quando ocorre uma falha no serviço de registro, seus WorkSpace usuários podem ver a seguinte mensagem de erro na página Connection Health Check: “Seu dispositivo não consegue se conectar ao serviço de WorkSpaces registro. Você não poderá registrar seu dispositivo com WorkSpaces. Please check your network settings."

Esse erro ocorre quando o aplicativo WorkSpaces cliente não consegue acessar o serviço de registro. Normalmente, isso acontece quando o WorkSpaces diretório é excluído. Para resolver esse erro, verifique se o código de registro é válido e corresponde a um diretório em execução na AWS nuvem.

Meus usuários de cliente zero PCoIP estão recebendo o erro "The supplied certificate is invalid due to timestamp" (O certificado fornecido é inválido devido ao time stamp)

Se o Network Time Protocol (NTP) não estiver habilitado no Teradici, seus usuários de cliente zero PCoIP poderão receber erros de falha de certificado. Para configurar o NTP, consulte Configurar clientes zero PCoIP para WorkSpaces.

Impressoras USB e outros periféricos compatíveis com USB não estão funcionando para clientes zero PCoIP

A partir da versão 20.10.4 do agente PCoIP, a Amazon WorkSpaces desativa o redirecionamento USB por padrão por meio do registro do Windows. Essa configuração do registro afeta o comportamento dos periféricos USB quando seus usuários estão usando dispositivos PCoIP zero client para se conectar aos seus. WorkSpaces

Se você WorkSpaces estiver usando a versão 20.10.4 ou posterior do agente PCoIP, os dispositivos periféricos USB não funcionarão com dispositivos cliente zero PCoIP até que você habilite o redirecionamento USB.

> **Note**
>
> Se você estiver usando drivers de impressora virtual de 32 bits, também deverá atualizar esses drivers para as versões de 64 bits.

Como habilitar o redirecionamento USB para dispositivos de cliente zero PCoIP

Recomendamos que você envie essas alterações do registro para você WorkSpaces por meio da Política de Grupo. Para obter mais informações, consulte Como configurar o agente e Definições configuráveis na documentação da Teradici.

1. Defina o valor de chave de registro a seguir como 1 (ativado):

   KeyPath = HKEY_LOCAL_MACHINE\ SOFTWARE\ Políticas\ Teradici\ PCoIP\ pcoip_admin

   KeyName = pcoip.enable_usb

   KeyType = DWORD

   KeyValue = 1
2. Defina o valor de chave de registro a seguir como 1 (ativado):

   KeyPath = HKEY_LOCAL_MACHINE\ SOFTWARE\ Policies\ Teradici\ PCoIP\ pcoip_admin_defaults

   KeyName = pcoip.enable_usb

   KeyType = DWORD

   KeyValue = 1
3. Se você ainda não tiver feito isso, saia do e WorkSpace, em seguida, faça login novamente. Os dispositivos USB agora devem funcionar.

Meus usuários ignoraram a atualização dos aplicativos cliente Windows ou macOS e não foram solicitados a instalar a versão mais recente

Quando os usuários ignoram as atualizações do aplicativo cliente Amazon WorkSpaces Windows, a chave de registro da SkipThisversão é definida e eles não são mais solicitados a atualizar seus

clientes quando uma nova versão do cliente é lançada. Para atualizar para a versão mais recente, você pode editar o registro conforme descrito em Atualizar o aplicativo WorkSpaces Windows Client para uma versão mais recente no Guia do WorkSpaces usuário da Amazon. Você também pode executar o seguinte PowerShell comando:

```
Remove-ItemProperty -Path "HKCU:\Software\Amazon Web Services. LLC\Amazon WorkSpaces
\WinSparkle" -Name "SkipThisVersion"
```

Quando os usuários ignoram as atualizações do aplicativo cliente do Amazon WorkSpaces macOS, `SUSkippedVersion` a preferência é definida e eles não são mais solicitados a atualizar seus clientes quando uma nova versão do cliente é lançada. Para atualizar para a versão mais recente, você pode redefinir essa preferência conforme descrito em Atualizar o aplicativo cliente WorkSpaces macOS para uma versão mais recente no Guia do usuário da Amazon WorkSpaces .

Meus usuários não conseguem instalar o aplicativo cliente Android em seus Chromebooks

A versão 2.4.13 é a versão final do aplicativo cliente Amazon WorkSpaces Chromebook. Como o Google está eliminando gradualmente o suporte aos aplicativos Chrome, não haverá mais atualizações no aplicativo cliente do WorkSpaces Chromebook e seu uso não é suportado.

Para Chromebooks que oferecem suporte à instalação de aplicativos Android, recomendamos usar o aplicativo cliente WorkSpaces Android em vez disso.

Em alguns casos, talvez seja necessário habilitar os Chromebooks de seus usuários para instalar aplicativos Android. Para ter mais informações, consulte Configurar o Android para Chromebooks.

Meus usuários não estão recebendo e-mails de convite nem e-mails de redefinição de senha

Os usuários não recebem automaticamente e-mails de boas-vindas ou de WorkSpaces redefinição de senha criados usando o AD Connector ou um domínio confiável. Os e-mails de convite também não são enviados automaticamente se o usuário já existir no Active Directory.

Para enviar manualmente e-mails de boas-vindas a esses usuários, consulte Enviar um convite por e-mail.

Para redefinir senhas de usuário, consulte Configurar as ferramentas de administração do Active Directory para WorkSpaces.

Meus usuários não veem a opção Esqueceu sua senha? na tela de login do cliente

Se você estiver usando o AD Connector ou um domínio confiável, os usuários não poderão redefinir as próprias senhas. (O Esqueceu a senha? a opção na tela de login WorkSpaces do aplicativo cliente não estará disponível.) Para obter informações sobre como redefinir senhas de usuários, consulte Configurar as ferramentas de administração do Active Directory para WorkSpaces.

Eu recebo a mensagem “O administrador do sistema definiu políticas para impedir essa instalação” quando tento instalar aplicativos em um Windows WorkSpace

Você pode resolver esse problema modificando a configuração de política de grupo do Windows Installer. Para implantar essa política WorkSpaces em vários em seu diretório, aplique essa configuração a um objeto de Política de Grupo vinculado à unidade WorkSpaces organizacional (OU) de uma instância EC2 associada ao domínio. Se você estiver usando o AD Connector, poderá fazer essas alterações por um controlador de domínio. Para obter mais informações sobre como usar as ferramentas de administração do Active Directory para trabalhar com objetos de Política de Grupo, consulte Installing the Active Directory Administration Tools no Guia de administração do AWS Directory Service .

O procedimento a seguir mostra como definir a configuração do Windows Installer para o objeto de Política de WorkSpaces Grupo.

1. Certifique-se de que o modelo administrativo de Política de WorkSpaces Grupo mais recente esteja instalado em seu domínio.
2. Abra a ferramenta Gerenciamento de Política de Grupo em seu WorkSpace cliente Windows, navegue até o objeto de Política de WorkSpaces Grupo e selecione-o para suas contas WorkSpaces de máquina. No menu principal, escolha Action (Ação), Edit (Editar).
3. No editor de gerenciamento de política de grupo, selecione Computer Configuration (Configuração do computador), Policies (Políticas), Administrative Templates (Modelos administrativos), Classic Administrative Templates (Modelos administrativos clássicos), Windows Components (Componentes do Windows) e Windows Installer.
4. Abra a configuração Turn Off Windows Installer (Desativar o Windows Installer).

5. Na caixa de diálogo Turn Off Windows Installer (Desativar o Windows Installer), altere Not Configured (Não configurado) para Enabled (Habilitado) e defina Disable Windows Installer (Desativar o Windows Installer) como Never (Nunca).
6. Escolha OK.
7. Para aplicar as alterações de política de grupo, execute um destes procedimentos:
   - Reinicie o WorkSpace (no WorkSpaces console, selecione o e, em seguida WorkSpace, escolha Ações, Reinicializar WorkSpaces).
   - Em um prompt de comando administrativo, insira gpupdate /force.

Não WorkSpaces , no meu diretório, posso me conectar à internet

WorkSpaces não pode se comunicar com a Internet por padrão. Você deve fornecer explicitamente o acesso à internet. Para ter mais informações, consulte Forneça acesso à Internet a partir do seu WorkSpace.

Meu WorkSpace perdeu o acesso à Internet

Se você WorkSpace perdeu o acesso à Internet e não consegue se conectar WorkSpace usando o RDP, esse problema provavelmente é causado pela perda do endereço IP público do WorkSpace. Se você ativou a atribuição automática de endereços IP elásticos no nível do diretório, um endereço IP elástico (do pool fornecido pela Amazon) será atribuído ao seu WorkSpace quando for lançado. No entanto, se você associar um endereço IP elástico de sua propriedade a um WorkSpace e depois desassociar esse endereço IP elástico do WorkSpace, ele WorkSpace perderá seu endereço IP público e não obterá automaticamente um novo do pool fornecido pela Amazon.

Para associar um novo endereço IP público do pool fornecido pela Amazon ao WorkSpace, você deve reconstruir o. WorkSpace Se você não quiser reconstruir o WorkSpace, você deve associar outro endereço IP elástico de sua propriedade ao WorkSpace.

Recomendamos que você não modifique a interface de elastic network de a WorkSpace após WorkSpace o lançamento. Depois que um endereço IP elástico é atribuído a um WorkSpace, ele WorkSpace retém o mesmo endereço IP público (a menos que WorkSpace seja reconstruído; nesse caso, ele obtém um novo endereço IP público).

Eu recebo um erro de "DNS indisponível" quando tento me conectar ao meu diretório on-premises

Você recebe uma mensagem de erro semelhante à seguinte quando se conecta ao seu diretório local.

```
DNS unavailable (TCP port 53) for IP: dns-ip-address
```

O AD Connector deve ser capaz de se comunicar com seus servidores de DNS on-premises via TCP e UDP na porta 53. Verifique se seus grupos de segurança e firewalls on-premises permitem a comunicação de TCP e UDP por essa porta.

Eu recebo um erro "Problemas de conectividade detectados" quando tento me conectar ao meu diretório on-premises

Você recebe uma mensagem de erro semelhante à seguinte quando se conecta ao seu diretório local.

```
Connectivity issues detected: LDAP unavailable (TCP port 389) for IP: ip-address
Kerberos/authentication unavailable (TCP port 88) for IP: ip-address
Please ensure that the listed ports are available and retry the operation.
```

O AD Connector deve ser capaz de se comunicar com seus controladores de domínio on-premises via TCP e UDP nas portas a seguir. Verifique se seus grupos de segurança e firewalls locais permitem a comunicação de TCP e UDP por estas portas:

- 88 (Kerberos)
- 389 (LDAP)

Eu recebo um erro "Registro SRV" quando tento me conectar ao meu diretório on-premises

Você recebe uma mensagem de erro semelhante a uma ou mais das seguintes quando se conecta ao seu diretório local.

```
SRV record for LDAP does not exist for IP: dns-ip-address
```

```
SRV record for Kerberos does not exist for IP: dns-ip-address
```

O AD Connector precisa obter os registros de SRV `_ldap._tcp.`*`dns-domain-name`* e `_kerberos._tcp.`*`dns-domain-name`* ao se conectar ao seu diretório. Você receberá esse erro se o serviço não conseguir obter esses registros dos servidores DNS que você especificou ao se conectar ao seu diretório. Certifique-se de que os seus servidores DNS contenham esses registros de SRV. Para obter mais informações, consulte SRV Resource Records na Microsoft TechNet.

Meu Windows WorkSpace adormece quando fica ocioso

Para resolver esse problema, conecte-se ao WorkSpace e altere o plano de energia para Alto desempenho usando o seguinte procedimento:

1. No Painel de Controle WorkSpace, abra o Painel de Controle e escolha Hardware ou Hardware e Som (o nome pode ser diferente, dependendo da versão do Windows).
2. Em Opções de Energia, selecione Escolher um plano de energia.
3. No painel Escolher ou personalizar um plano de energia, selecione o plano de energia Alta performance e escolha Alterar configurações do plano.
   - Se a opção para escolher o plano de energia de Alta performance estiver desabilitada, escolha Alterar configurações que não estão disponíveis no momento e selecione o plano de energia de Alta performance.
   - Se o plano de Alta performance não estiver visível, escolha a seta à direita de Mostrar planos adicionais para exibi-lo. Você também pode escolher Criar um plano de energia no painel de navegação à esquerda, escolher Alta performance, dar um nome ao plano de energia e escolher Próximo.
4. Na página Alterar configurações do plano: alta performance, defina as opções Desligar a tela e (se disponível) Colocar o computador em repouso como Nunca.
5. Se você fez alguma alteração no plano de alta performance, escolha Salvar alterações (ou escolha Criar se estiver criando um plano).

Se as etapas anteriores não resolverem o problema, faça o seguinte:

1. No Painel de Controle WorkSpace, abra o Painel de Controle e escolha Hardware ou Hardware e Som (o nome pode ser diferente, dependendo da versão do Windows).
2. Em Opções de Energia, selecione Escolher um plano de energia.

3. No painel Escolher ou personalizar um plano de energia, selecione o link Alterar configurações do plano à direita do plano de energia Alto desempenho e, em seguida, selecione o link Alterar configurações de energia avançadas.
4. Na caixa de diálogo Opções de energia, na lista de configurações, escolha o sinal de mais à esquerda de Disco rígido para exibir as configurações relevantes.
5. Verifique se o valor de Desligar o disco rígido após para Na tomada é maior que o valor de Na bateria (o valor padrão é de 20 minutos).
6. Selecione o sinal de mais à esquerda de PCI Express e faça o mesmo para Gerenciamento de Energia do Estado da Conexão.
7. Verifique se as configurações de Gerenciamento de Energia do Estado da Conexão estão no modo Desligado.
8. Selecione OK (ou Aplicar se você alterou qualquer configuração) para fechar a caixa de diálogo.
9. No painel Alterar configurações do plano, se você alterou qualquer configuração, selecione Salvar alterações.

Um dos meus WorkSpaces tem um estado de **UNHEALTHY**

O WorkSpaces serviço envia periodicamente solicitações de status para um WorkSpace. A WorkSpace é marcado UNHEALTHY quando não responde a essas solicitações. As causas comuns para esse problema são:

- Um aplicativo no WorkSpace está bloqueando portas de rede, o que impede que WorkSpace eles respondam à solicitação de status.
- A alta utilização da CPU está impedindo que WorkSpace eles respondam à solicitação de status em tempo hábil.
- O nome do computador do WorkSpace foi alterado. Isso evita que um canal seguro seja estabelecido entre WorkSpaces e WorkSpace o.

Você pode tentar corrigir a situação usando os seguintes métodos:

- Reinicie o a WorkSpace partir do WorkSpaces console.
- Conecte-se ao não íntegro WorkSpace usando o procedimento a seguir, que deve ser usado somente para fins de solução de problemas:

  1. Conecte-se a um operacional WorkSpace no mesmo diretório do não WorkSpace íntegro.

2. Do operacional WorkSpace, use o Remote Desktop Protocol (RDP) para se conectar ao não íntegro WorkSpace usando o endereço IP do não íntegro. WorkSpace Dependendo da extensão do problema, talvez você não consiga se conectar ao insalubre WorkSpace.
3. Se não estiver íntegro WorkSpace, confirme se os requisitos mínimos de porta foram atendidos.

- Certifique-se de que o SkyLightWorkSpacesConfigService serviço possa responder às verificações de saúde. Para solucionar esse problema, consulte Meus usuários recebem a mensagem "WorkSpace Status: Insalubre. Não foi possível conectar você ao seu WorkSpace. Tente novamente em alguns minutos”..
- Reconstrua o a WorkSpace partir do WorkSpaces console. Como a reconstrução de um WorkSpace pode potencialmente causar perda de dados, essa opção deve ser usada somente se todas as outras tentativas de corrigir o problema não tiverem sido bem-sucedidas.

Meu WorkSpace está travando ou reiniciando inesperadamente

Se sua WorkSpace configuração para PCoIP estiver travando ou reiniciando repetidamente e seus registros de erros ou despejos de falha estiverem apontando para problemas com `spacedeskHookKmode.sys` ou`spacedeskHookUmode.dll`, ou se você estiver recebendo as seguintes mensagens de erro, talvez seja necessário desativar o acesso via Web ao: WorkSpace

```
The kernel power manager has initiated a shutdown transition.
Shutdown reason: Kernel API
```

```
The computer has rebooted from a bugcheck.
```

> **Note**
>
> - Essas etapas de solução de problemas não são aplicáveis às WorkSpaces que estão configuradas para o WorkSpaces Streaming Protocol (WSP). Eles são aplicáveis somente aos WorkSpaces que estão configurados para PCoIP.
> - Você deve desativar o Web Access somente se não estiver permitindo que os usuários utilizem o Web Access.

Para desativar o Acesso à Web ao WorkSpace, você deve desativar o Acesso à Web no WorkSpaces diretório e reinicializar o. WorkSpace

O mesmo nome de usuário tem mais de um WorkSpace, mas o usuário só pode fazer login em um dos WorkSpaces

Se você excluir um usuário no Active Directory (AD) sem primeiro excluí-lo WorkSpace e depois adicionar o usuário novamente ao Active Directory e criar um novo WorkSpace para esse usuário, o mesmo nome de usuário agora terá dois WorkSpaces no mesmo diretório. No entanto, se o usuário tentar se conectar ao original WorkSpace, ele receberá o seguinte erro:

```
"Unrecognized user. No WorkSpace found under your username. Contact your administrator
 to request one."
```

Além disso, as pesquisas pelo nome de usuário no WorkSpaces console da Amazon retornam somente o novo WorkSpace, mesmo que ambos WorkSpaces ainda existam. (Você pode encontrar o original WorkSpace pesquisando o WorkSpace ID em vez do nome de usuário.)

Esse comportamento também pode ocorrer se você renomear um usuário no Active Directory sem primeiro excluí-lo. WorkSpace Se você alterar o nome de usuário novamente para o nome de usuário original e criar um novo WorkSpace para o usuário, o mesmo nome de usuário terá dois WorkSpaces no diretório.

Esse problema ocorre porque o Active Directory usa o identificador de segurança (SID) do usuário, em vez do nome de usuário, para identificar exclusivamente o usuário. Quando um usuário é excluído e recriado no Active Directory, ele recebe um novo SID, mesmo que seu nome de usuário permaneça o mesmo. Durante as pesquisas por um nome de usuário, o WorkSpaces console da Amazon usa o SID para pesquisar correspondências no Active Directory. Os WorkSpaces clientes da Amazon também usam o SID para identificar usuários quando eles estão se conectando a. WorkSpaces

Para resolver esse problema, execute um dos seguintes procedimentos:

- Se o problema ocorreu porque o usuário foi excluído e recriado no Active Directory, talvez seja possível restaurar o objeto do usuário original excluído caso o recurso Lixeira no Active Directory esteja habilitado. Se você conseguir restaurar o objeto de usuário original, certifique-se de que o usuário possa se conectar ao original WorkSpace. Se possível, você poderá excluir o novo WorkSpace depois de fazer backup e transferir manualmente todos os dados do usuário do novo WorkSpace para o original WorkSpace (se necessário).

- Se você não conseguir restaurar o objeto de usuário original, exclua o original do usuário WorkSpace. Em WorkSpace vez disso, o usuário deve ser capaz de se conectar e usar o novo. Certifique-se de fazer backup e transferir manualmente todos os dados do usuário do original WorkSpace para o novo WorkSpace.

> **Warning**
>
> Excluir um WorkSpace é uma ação permanente e não pode ser desfeita. Os dados do WorkSpace usuário não persistem e são destruídos. Para obter ajuda para fazer backup dos dados do usuário, entre em contato com o AWS Support.

Estou tendo problemas para usar o Docker com a Amazon WorkSpaces

Janelas WorkSpaces

A virtualização aninhada (incluindo o uso do Docker) não é suportada no Windows. WorkSpaces Para obter mais informações, consulte a Documentação do Docker.

Linux WorkSpaces

Para usar o Docker no Linux WorkSpaces, certifique-se de que os blocos CIDR usados pelo Docker não se sobreponham aos blocos CIDR usados nas duas interfaces de rede elástica (ENIs) associadas ao. WorkSpace Se você encontrar problemas com o uso do Docker no Linux WorkSpaces, entre em contato com o Docker para obter ajuda.

Eu recebo ThrottlingException erros em algumas das minhas chamadas de API

A taxa padrão permitida para chamadas de WorkSpaces API é uma taxa constante de duas chamadas de API por segundo, com uma taxa máxima de “intermitência” permitida de cinco chamadas de API por segundo. A tabela a seguir mostra como o limite da taxa de intermitência funciona para solicitações de API.

Segundo	Número de solicitações enviadas	Solicitações líquidas permitidas	Detalhes
1	0	5	Durante o primeiro segundo (segundo 1), cinco solicitações são permitidas, até a taxa máxima de intermitência de cinco chamadas por segundo.
2	2	5	Como duas ou menos chamadas foram emitidas no segundo 1, a capacidade de intermitência total de cinco chamadas ainda está disponível.
3	5	5	Como apenas duas chamadas foram emitidas no segundo 2, a capacidade de intermitência total de cinco chamadas ainda está disponível.
4	2	2	Como a capacidade de intermitência total foi usada no segundo 3, apenas a taxa constante de duas chamadas por segundo está disponível.
5	3	2	Como não há capacidade de intermitência restante, apenas duas chamadas são permitidas no momento. Isso significa que uma das três chamadas de API é limitada. A chamada limitada responderá após um curto atraso.
6	0	1	Como uma das chamadas do segundo 5 está sendo repetida no segundo 6, há capacidade para apenas uma chamada adicional no segundo 6 devido ao limite de taxa constante de duas chamadas por segundo.
7	0	3	Agora que não há mais nenhuma chamada de API limitada na fila, o limite da taxa continuará a aumentar, até o limite de taxa de intermitência de cinco chamadas.

Segundo	Número de solicitações enviadas	Solicitações líquidas permitidas	Detalhes
8	0	5	Como nenhuma chamada foi emitida no segundo 7, o número máximo de solicitações é permitido.
9	0	5	Embora nenhuma chamada tenha sido emitida no segundo 8, o limite de taxa não aumenta acima de cinco.

Meu WorkSpace continua se desconectando quando eu o deixo rodar em segundo plano

Para usuários de Mac, verifique se o recurso Power Nap está ativado. Se estiver ativado, clique para desativá-lo. Para desativar o Power Nap, abra seu terminal e execute o seguinte comando:

```
defaults write com.amazon.workspaces NSAppSleepDisabled -bool YES
```

A federação SAML 2.0 não está funcionando. Meus usuários não estão autorizados a transmitir seus WorkSpaces desktops.

Isso pode ocorrer porque a política em linha incorporada para o perfil do IAM de federação SAML 2.0 não inclui permissões para transmitir do diretório do nome do recurso da Amazon (ARN). A função do IAM é assumida pelo usuário federado que está acessando um WorkSpaces diretório. Edite as permissões da função para incluir o ARN do diretório e garantir que o usuário tenha um WorkSpace no diretório. Para obter mais informações, consulte Autenticação do SAML 2.0 e Solução de problemas da federação do SAML 2.0 com. AWS

Meus usuários são desconectados da WorkSpaces sessão a cada 60 minutos.

Se você configurou a autenticação SAML 2.0 para WorkSpaces, dependendo do seu provedor de identidade (IdP), talvez seja necessário configurar as informações para as quais o IdP passa como atributos AWS do SAML como parte da resposta de autenticação. Isso inclui a configuração

do elemento Attribute (Atributo) com o atributo `SessionDuration` definido como `https://aws.amazon.com/SAML/Attributes/SessionDuration`.

`SessionDuration` especifica a quantidade máxima de tempo que uma sessão de streaming federada pode permanecer ativa para um usuário antes que a uma nova autenticação seja necessária. Embora `SessionDuration` seja um atributo opcional, recomendamos que você o inclua na resposta de autenticação SAML. Se você não especificar esse atributo, a duração da sessão será definida com o padrão de 60 minutos.

Para resolver esse problema, configure seu IdP para incluir o valor `SessionDuration` na resposta de autenticação SAML e defina o valor conforme necessário. Para obter mais informações, consulte Step 5: Create assertions for the SAML authentication response.

Meus usuários recebem um erro de redirecionamento de URI quando se federam usando o fluxo iniciado pelo provedor de identidade (IdP) SAML 2.0 ou uma instância adicional do aplicativo WorkSpaces cliente é iniciada toda vez que meus usuários tentam fazer login a partir do cliente após a federação no IdP.

Esse erro ocorre devido a um URL de estado de retransmissão inválido. Verifique se o estado de retransmissão na configuração da federação de IdP está correto e se a URL de acesso do usuário e o nome do parâmetro do estado de retransmissão estão configurados corretamente para sua federação de IdP nas propriedades do diretório. WorkSpaces Se elas forem válidas e o problema persistir, entre em contato com o AWS Support. Para obter mais informações, consulte Como configurar o SAML.

Meus usuários recebem a mensagem “Algo deu errado: ocorreu um erro ao iniciar seu WorkSpace” quando tentam entrar no aplicativo WorkSpaces cliente após a federação no IdP.

Analise as declarações SAML 2.0 da federação. O valor SAML Subject NameID deve corresponder ao nome do usuário e geralmente é WorkSpaces o mesmo que o atributo SaM para o usuário do AccountName Active Directory. Além disso, o elemento Attribute que tem o `PrincipalTag:Email` atributo definido como `https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email` deve corresponder ao endereço de e-mail do WorkSpaces usuário, conforme definido no WorkSpaces diretório. Para obter mais informações, consulte Como configurar o SAML.

Meus usuários recebem a mensagem “Não é possível validar as tags” quando tentam entrar no aplicativo WorkSpaces cliente após a federação no IdP.

Revise os valores do atributo `PrincipalTag` nas declarações SAML 2.0 para sua federação, como `https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`. Os valores da etiqueta podem incluir combinações de letras, números, espaços e os caracteres `_ . : / = + - @`. Para obter mais informações, consulte Regras para marcação no IAM e. AWS STS

Meus usuários recebem a mensagem: “O cliente e o servidor não conseguem se comunicar porque não possuem um algoritmo comum”.

Esse problema pode ocorrer se você não habilitar o TLS 1.2.

Meu microfone ou webcam não está funcionando no Windows WorkSpaces.

Abra o menu Iniciar para verificar a configuração de privacidade

- Iniciar > Configurações > Privacidade > Câmera
- Iniciar > Configurações > Privacidade > Microfone

Se estiverem desligados, ligue-os.

Como alternativa, WorkSpaces os administradores podem criar um Objeto de Política de Grupo (GPO) para habilitar o microfone e/ou a webcam conforme necessário.

Meus usuários não conseguem fazer login usando a autenticação baseada em certificado e a senha é solicitada no WorkSpaces cliente ou na tela de login do Windows quando se conectam à sessão do desktop.

A autenticação baseada em certificado não teve êxito na sessão. Se o problema persistir, a falha na autenticação baseada em certificado pode ser resultado de um dos seguintes problemas:

- O WorkSpaces ou o cliente não é suportado. A autenticação baseada em certificado é compatível com pacotes do Windows WorkSpaces on WorkSpaces Streaming Protocol (WSP) usando o aplicativo cliente Windows mais recente. WorkSpaces

- O WorkSpaces precisa ser reinicializado após habilitar a autenticação baseada em certificado no Diretório. WorkSpaces
- WorkSpaces não conseguiu se comunicar AWS Private CA ou AWS Private CA não emitiu o certificado. Verifique o AWS CloudTrail para determinar se houve emissão de certificado. Para ter mais informações, consulte Gerenciar a autenticação baseada em certificado.
- O controlador de domínio não tem nenhum certificado de controlador de domínio para login com cartão inteligente ou o certificado está expirado. Para obter mais informações, consulte a etapa 7, “Como configurar controladores de domínio com um certificado de controlador de domínio para autenticar usuários de cartões inteligentes” em Pré-requisitos.
- O certificado não é confiável. Para obter mais informações, consulte a etapa 7, “Como publicar a CA no Active Directory” em Pré-requisitos. Execute `certutil –viewstore –enterprise NTAuth` em controladores de domínio para confirmar que a CA foi publicada.
- Há um certificado no cache, mas os atributos foram alterados para o usuário que invalidou o certificado. Entre em contato AWS Support para limpar o cache antes da expiração do certificado (24 horas). Para obter mais informações, consulte o AWS Support Center.
- O userPrincipalName formato do atributo `UserPrincipalName` SAML não está formatado corretamente ou não se resolve para o domínio real do usuário. Para obter mais informações, consulte a etapa 1 em Pré-requisitos.
- O atributo `0bjectSid` (opcional) na declaração SAML não corresponde ao identificador de segurança (SID) do Active Directory do usuário especificado no `NameID` de SAML_Subject. Confirme se o mapeamento de atributos está correto em sua federação SAML e se o provedor de identidades SAML está sincronizando o atributo SID para o usuário do Active Directory.
- Há configurações da política de grupo que estão modificando as configurações padrão do Active Directory para login com cartão inteligente ou tomando medidas quando um cartão inteligente é removido de um leitor de cartões inteligentes. Essas configurações podem causar um comportamento inesperado adicional além dos erros listados acima. A autenticação baseada em certificado apresenta um cartão inteligente virtual ao sistema operacional da instância e o remove após a conclusão do login. Verifique as Configurações principais da política de grupo para cartões inteligentes e as Configurações adicionais da política de grupo para o cartão inteligente e chaves de registro, incluindo o comportamento de remoção do cartão inteligente.
- O ponto de distribuição da CRL para a CA privada não está on-line nem pode ser acessado pelo controlador de domínio WorkSpaces ou pelo controlador de domínio. Para obter mais informações, consulte a etapa 5 em Pré-requisitos.
- Para verificar se há CAs obsoletas no domínio ou na floresta, execute `PKIVIEW.msc` na CA para verificar. Se houver CAs obsoletas, use o `PKIVIEW.msc` mmc para excluí-las manualmente.

- Para verificar se a replicação do Active Directory está funcionando e se não há controladores de domínio obsoletos no domínio, execute. `repadmin /replsum`

Etapas adicionais de solução de problemas envolvem a análise dos registros de eventos do Windows da WorkSpaces instância. Um evento comum que deve ser analisado em busca de falha de login é o Evento 4625: uma conta não conseguiu realizar login no log de Segurança do Windows.

Se o problema persistir, entre em contato AWS Support. Para obter mais informações, consulte o AWS Support Center.

Estou tentando fazer algo que requer mídia de instalação do Windows, mas WorkSpaces não a fornece.

Se você estiver usando um pacote público AWS fornecido, poderá usar os snapshots do EBS da mídia de instalação do sistema operacional Windows Server fornecidos pelo Amazon EC2 quando necessário.

Crie um volume do EBS a partir desses snapshots, anexe-o ao Amazon EC2 e transfira os arquivos para onde estão os arquivos, WorkSpace conforme necessário. Se você estiver usando o Windows 10 no BYOL WorkSpaces e precisar de uma mídia de instalação, precisará preparar sua própria mídia de instalação. Para obter mais informações, consulte Como adicionar componentes do Windows usando uma mídia de instalação. Como você não pode conectar diretamente um volume do EBS a um WorkSpace, você precisará anexá-lo a uma instância do Amazon EC2 e copiar os arquivos.

Quero iniciar WorkSpaces com um diretório AWS gerenciado existente criado em uma WorkSpaces região sem suporte.

Para iniciar a Amazon WorkSpaces usando um diretório em uma região que atualmente não é suportada pelo WorkSpaces, siga as etapas abaixo.

> **Note**
>
> Se você receber erros ao executar AWS Command Line Interface comandos, verifique se está usando a AWS CLI versão mais recente. Para obter mais informações, consulte Como confirmar se você está executando uma versão recente da AWS CLI.

Etapa 1: Criar um emparelhamento entre nuvens privadas virtuais (VPCs) em sua conta

1. Crie uma conexão de emparelhamento da VPC com uma VPC em uma região diferente. Para obter mais informações, consulte Como criar com VPCs na mesma conta e em diferentes regiões.
2. Aceite a conexão de emparelhamento da VPC. Para obter mais informações, consulte Como aceitar uma conexão de emparelhamento da VPC.
3. Depois de ativar a conexão de emparelhamento de VPC, você pode visualizar suas conexões de emparelhamento de VPC usando o console Amazon VPC, o ou uma API. AWS CLI

Etapa 2: Atualizar as tabelas de rotas para emparelhamento da VPC em ambas as regiões

Atualize as tabelas de rotas para ativar a comunicação com a VPC de mesmo nível via IPv4 ou IPv6. Para obter mais informações, consulte Como atualizar as tabelas de rotas para uma conexão de emparelhamento da VPC.

Etapa 3: Crie um AD Connector e registre a Amazon WorkSpaces

1. Para analisar os pré-requisitos do AD Connector, consulte Pré-requisitos do AD Connector.
2. Conecte seu diretório existente ao AD Connector. Para obter mais informações, consulte Como criar um AD Connector.
3. Quando o status do AD Connector mudar para Ativo, abra o console do AWS Directory Service e escolha o hiperlink para o ID de diretório.
4. Para AWS aplicativos e serviços, escolha Amazon WorkSpaces para ativar o acesso WorkSpaces neste diretório.
5. Registre o diretório com WorkSpaces. Para obter mais informações, consulte Registrar um diretório com WorkSpaces.

Quero atualizar o Firefox no Amazon Linux 2.

Etapa 1: Verificar se a atualização automática está habilitada

Para verificar se a atualização automática está ativada, execute o comando `systemctl status *os-update-mgmt.timer | grep enabled` no seu. WorkSpace Na saída, deve haver duas linhas com a palavra `enabled`.

Etapa 2: Iniciar uma atualização

O Firefox geralmente é atualizado automaticamente no Amazon Linux 2 WorkSpaces junto com todos os outros pacotes de software no sistema durante a janela de manutenção. No entanto, isso depende do tipo de WorkSpaces que você está usando.

- Pois AlwaysOn WorkSpaces, a janela de manutenção semanal é no domingo, das 00h00 às 04h00, no fuso horário do. WorkSpace
- Por AutoStop WorkSpaces... a partir da terceira segunda-feira do mês e por até duas semanas, a janela de manutenção está aberta todos os dias, das 00h00 às 05h00, no fuso horário da AWS Região para o. WorkSpace

Para obter mais informações sobre janelas de manutenção, consulte WorkSpace manutenção.

Você também pode iniciar um ciclo de atualização imediato reiniciando o seu WorkSpace e reconectando-o após 15 minutos. Você também pode iniciar as atualizações inserindo `sudo yum update`. Para iniciar uma atualização somente para o Firefox, digite `sudo yum install firefox`.

Se você não conseguir configurar o acesso aos repositórios do Amazon Linux 2 e preferir instalar o Firefox usando binários criados pela Mozilla, consulte Como instalar o Firefox a partir de compilações da Mozilla no suporte da Mozilla. Recomendamos desinstalar completamente a versão empacotada com RPM do Firefox para garantir que você não execute uma versão desatualizada por engano. Execute o comando `sudo yum remove firefox` para desinstalá-la.

Você também pode baixar os pacotes RPM necessários dos repositórios Amazon Linux 2 executando o comando `yumdownloader firefox` em uma máquina diferente. Em seguida, carregue os repositórios paralelamente WorkSpaces, onde você pode instalá-los com um comando padrãoYUM, como. `sudo yum install firefox-102.11.0-2.amzn2.0.1.x86_64.rpm`

> **Note**
>
> O nome exato do arquivo mudará com base na versão do pacote.

Etapa 3: Verificar se o repositório do Firefox está em uso

O Amazon Linux Extras fornece automaticamente atualizações do Firefox para o Amazon Linux 2 WorkSpaces. O Amazon Linux 2 WorkSpaces criado após 31 de julho de 2023 já terá o repositório Firefox Extra ativado. Para verificar se você WorkSpace está usando o repositório Firefox Extra, execute o comando a seguir.

```
yum repolist | grep amzn2extra-firefox
```

A saída do comando deve ser semelhante a `amzn2extra-firefox/2/x86_64 Amazon Extras repo for firefox 10` se o repositório Firefox Extra for usado. Ele ficará vazio se o repositório Firefox Extra não for usado. Se o repositório Firefox Extra não for usado, você pode tentar habilitá-lo manualmente com o seguinte comando:

```
sudo amazon-linux-extras install firefox
```

Se a ativação do repositório Firefox Extra ainda falhar, verifique seu acesso à internet e garanta que os endpoints da VPC estejam desconfigurados. Para continuar recebendo atualizações do Firefox para o Amazon Linux 2 WorkSpaces por meio dos repositórios YUM, certifique-se de que você possa acessar WorkSpaces os repositórios do Amazon Linux 2. Para obter mais informações sobre como acessar os repositórios do Amazon Linux 2 sem ter acesso à internet, consulte este artigo da central de conhecimento.

Meu usuário consegue redefinir sua senha usando o WorkSpaces cliente, ignorando a configuração Fine Grained Password Policy (FFGP) que está configurada. AWS Managed Microsoft AD

Se o WorkSpaces cliente do seu usuário estiver associado AWS Managed Microsoft AD, ele precisará redefinir a senha usando a configuração de complexidade padrão.

A senha de complexidade padrão diferencia maiúsculas de minúsculas e deve ter entre 8 e 64 caracteres, inclusive. Ele deve conter pelo menos um caractere de cada uma das seguintes categorias:

- Caracteres minúsculos (a-z)
- Caracteres maiúsculos (A-Z)
- Números (0-9)
- Caracteres não alfanuméricos (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Certifique-se de que a senha não inclua caracteres Unicode não imprimíveis, como espaços em branco, guias de retenção de carro, quebras de linha e caracteres nulos.

Se sua organização exigir que você aplique o FFGP para WorkSpaces, entre em contato com o administrador do Active Directory para redefinir a senha do usuário diretamente do Active Directory em vez do cliente. WorkSpaces

Meus usuários recebem a mensagem de erro “Este sistema operacional não está autorizado a acessar seu WorkSpace” ao tentar acessar o WorkSpace Windows/Linux usando o Web Access

A versão do sistema operacional que seu usuário está tentando usar não é compatível com o WorkSpaces Web Access. Certifique-se de habilitar o Web Access na configuração Outra plataforma do WorkSpace diretório. Para obter mais informações sobre como habilitar seu WorkSpace acesso à Web, consulteAtivar e configurar o Amazon WorkSpaces Web Access.

Política de fim de vida útil da aplicação cliente Amazon WorkSpaces

A política de fim de vida útil (EOL) do Amazon WorkSpaces é aplicável a versões principais específicas (e todas as suas versões secundárias) do WorkSpaces que não recebem mais suporte e não são mais testadas quanto à compatibilidade com versões mais recentes.

O ciclo de vida de uma versão do cliente do WorkSpaces tem três fases: suporte geral, orientação técnica e fim de vida útil (EOL). A fase de suporte geral começa na data do lançamento público inicial de um cliente do WorkSpaces e possui uma duração fixa. Durante a fase de suporte geral, a equipe de suporte do WorkSpaces fornece suporte completo para problemas de configuração. As resoluções de defeitos e as solicitações de recursos são implementadas para essa versão principal e para as versões secundárias associadas do cliente do WorkSpaces.

A orientação técnica é fornecida desde o final da fase de suporte geral até a data de fim de vida útil. Durante a fase de orientação técnica, você recebe suporte e orientação somente para configurações compatíveis. As resoluções de defeitos e as solicitações de recursos são implementadas apenas para as versões mais recentes do cliente do WorkSpaces. Elas não são implementadas para versões mais antigas. Durante a fase de orientação técnica, se uma correção for necessária, a AWS agendará essa correção para o próximo lançamento da versão disponível ao público, e você terá a opção de atualizar para a versão mais recente do WorkSpaces para receber suporte relacionado à correção.

O fim de vida útil de uma versão principal ocorre quando o suporte geral e a orientação técnica terminam. Após a data de fim de vida útil, nenhum suporte ou manutenção adicional é fornecido. A AWS interrompe os testes de problemas de compatibilidade. Para obter suporte contínuo, você deve atualizar para a versão mais recente do cliente do WorkSpaces.

Consulte esta tabela para obter mais informações sobre o suporte para versões específicas.

Cliente Windows	Suporte geral	Orientação técnica	Fim de vida útil
2.x	2018	31 de março de 2023	31 de agosto de 2023

Cliente do Linux	Suporte geral	Orientação técnica	Fim de vida útil
4.x para Ubuntu 18.04	12 de agosto de 2021	31 de março de 2023	31 de agosto de 2023
3.x para Ubuntu 18.04	25 de novembro de 2019	31 de março de 2023	31 de agosto de 2023

Cliente para macOS	Suporte geral	Orientação técnica	Fim de vida útil
2.x	2019	31 de março de 2023	31 de agosto de 2023
1.x	2018	31 de março de 2023	31 de agosto de 2023

Cliente iPad	Suporte geral	Orientação técnica	Fim de vida útil
1.x	2018	31 de março de 2023	31 de agosto de 2023

Cliente Android	Suporte geral	Orientação técnica	Fim de vida útil
2.x	2019	31 de março de 2023	31 de agosto de 2023
1.x	2018	31 de março de 2023	31 de agosto de 2023

Web access	Suporte geral		
Google Chrome	Versão atual, além das duas versões principais mais recentes		
Firefox	Versão atual, além das duas versões		

Web access	Suporte geral		
	principais mais recentes		
Microsoft Edge	Versão atual, além das duas versões principais mais recentes		

Clientes sem suporte

Não há suporte para os clientes do WorkSpaces a seguir.

Sistema operacional	Versão do cliente	Suporte geral	Orientação técnica	Fim de vida útil	Observações
Windows	5.11	3 de julho de 2023	1.º de outubro de 2023	1.º de outubro de 2023	Não compatível devido a problemas de qualidade
Windows	5.10	19 de junho de 2023	1.º de outubro de 2023	1.º de outubro de 2023	Não compatível devido a problemas de qualidade
Windows	5.9	9 de maio de 2023	1.º de outubro de 2023	1.º de outubro de 2023	Não compatível devido a problemas de qualidade

Perguntas frequentes sobre o fim de vida útil

Estou usando uma versão de um cliente do WorkSpaces que atingiu seu fim de vida útil. O que devo fazer para atualizar para uma versão compatível?

Acesse a página de download do cliente do WorkSpaces para baixar e instalar uma versão totalmente compatível do WorkSpaces.

Posso usar uma versão do cliente do WorkSpaces que atingiu seu fim de vida útil com um WorkSpace compatível?

É altamente recomendável atualizar seus clientes para a versão mais recente, pois as resoluções e os recursos anteriores não são mais aplicados às versões de clientes que atingiram seu fim de vida útil. Se estiver usando uma versão do cliente que atingiu seu fim de vida útil, entre em contato com a equipe de suporte da AWS para obter mais informações.

Estou usando uma versão de um cliente do WorkSpaces que atingiu seu fim de vida útil. Ainda posso relatar problemas para ela?

Primeiro, você deve atualizar para uma versão compatível e tentar reproduzir o problema. Se o problema persistir na versão compatível, abra um caso de suporte com a equipe de suporte da AWS.

Estou usando uma versão compatível do cliente do WorkSpaces em um sistema operacional que atingiu seu fim de vida útil. Ainda posso relatar problemas para ela?

A assistência técnica e as atualizações de software não estão mais disponíveis para sistemas operacionais que atingiram o fim de vida útil e a AWS não oferece suporte aos clientes do WorkSpaces que usam sistemas operacionais que atingiram o fim de vida útil. Use um sistema operacional compatível para garantir que você tenha suporte para seus clientes do WorkSpaces.

WorkSpaces Cotas da Amazon

WorkSpaces A Amazon fornece diferentes recursos que você pode usar em sua conta em uma determinada região, incluindo imagens WorkSpaces, pacotes, diretórios, aliases de conexão e grupos de controle de IP. Ao criar uma conta da Amazon Web Services, definimos cotas padrão (também conhecidas como limites) para o número de recursos que você pode criar.

A seguir estão as cotas padrão WorkSpaces para sua AWS conta. É possível usar o console do Service Quotas para visualizar cotas padrão e cotas aplicadas, ou para solicitar aumentos de cota para cotas ajustáveis.

Em algumas regiões, onde o Service Quotas não está disponíveis, você deve enviar um caso de suporte para solicitar o aumento do limite. Para obter mais informações, consulte Viewing service quotas e Requesting a quota increase no Guia do usuário do Service Quotas.

Recurso	Padrão	Descrição	Ajustável
WorkSpaces	1	O número máximo de WorkSpaces nesta conta na região atual.	Sim
Gráficos WorkSpaces	0	O número máximo de gráficos WorkSpaces nessa conta na região atual. **Note** O pacote Graphics deixará de receber suporte a partir de 30 de novembro de 2023. Recomenda	Sim

Recurso	Padrão	Descrição	Ajustável
		mos migrar seu pacote para o WorkSpaces Graphics.g4dn. Para ter mais informações, consulte Migre um WorkSpace.	
Gráficos.G4DN WorkSpaces	0	O número máximo de Graphics.G4DN nessa conta WorkSpaces na região atual.	Sim
GraphicsPro WorkSpaces	0	O número máximo de GraphicsPro WorkSpaces nesta conta na região atual.	Sim
GraphicsPro.g4dn WorkSpaces	0	O número máximo de GraphicsPro .g4dn nessa conta WorkSpaces na região atual.	Sim
Em espera WorkSpaces	0	O número máximo de WorkSpaces nesta conta na região atual.	Sim

Recurso	Padrão	Descrição	Ajustável
Pacotes	50	O número máximo de pacotes para esta conta na região atual. Essa cota se aplica somente a pacotes personalizados, não a pacotes públicos.	Não
Aliases de conexão	20	O número máximo de aliases de conexão para esta conta na região atual.	Não
Diretórios	50	O número máximo de diretórios que podem ser registrados para uso com a Amazon WorkSpaces nessa conta na região atual.	Não
Imagens	40	O número máximo de imagens para esta conta na região atual.	Sim
Grupos de controle de acesso de IP	100	O número máximo de grupos de controle de acesso de IP para esta conta na região atual.	Não
Grupos de controle de acesso de IP por diretório	25	O número máximo de grupos de controle de acesso de IP por diretório para esta conta na região atual.	Não

Recurso	Padrão	Descrição	Ajustável
Regras por grupo de controle de acesso de IP	10	O número máximo de regras por grupo de controle de acesso de IP para esta conta na região atual.	Não

Controle de utilização de API

A tarifa permitida é de duas chamadas por segundo. Para obter mais informações, consulte Exceções de controle de utilização.

WorkSpaces Versões do agente host do Streaming Protocol (WSP)

O agente host do WorkSpaces Streaming Protocol (WSP) é um agente host executado dentro do seu WorkSpace. Ele transmite os pixels do seu WorkSpace para um aplicativo cliente e inclui recursos em sessão, como áudio e vídeo bidirecionais e impressão. Para obter mais informações sobre o WorkSpaces Streaming Protocol (WSP), consulte Protocolos para Amazon WorkSpaces.

Recomendamos manter o software do agente do host atualizado com a versão mais recente. Você pode reinicializar manualmente o seu WorkSpaces para atualizar o WSP Host Agent. O agente host do WSP também é atualizado automaticamente durante a janela normal de manutenção WorkSpaces padrão. Para obter mais informações sobre janelas de manutenção, consulte WorkSpace manutenção. Alguns desses recursos exigem a versão mais recente WorkSpaces do cliente. Para obter mais informações sobre as versões mais recentes do cliente, consulte WorkSpaces Clientes.

A tabela a seguir descreve as alterações em cada versão do agente do host do WSP.

Versão	Data	Alterações
• Windows WorkSpaces - 2.1.0.1554	15 de maio de 2024	• Foi adicionado suporte para Idle Disconnect Timeout. • Foi adicionada uma nova configuração de Política de Grupo para configurar o Tempo Limite de Desconexão Ociosa. • Corrigido um problema em WorkSpaces que era desconectado e exibia uma tela branca quando os usuários modificavam as configurações de exibição. • Correções de erros e melhorias na performance.

Versão	Data	Alterações
• Ubuntu WorkSpaces - 2.1.0.1342	29 de fevereiro de 2024	• A resolução preferencial da webcam foi alterada para entre 480x360 e 640x480. • Correções de erros e melhorias na performance.
• Windows WorkSpaces - 2.0.0.1425	22 de fevereiro de 2024	• Foi adicionado suporte para solicitações de WebAuthn redirecionamento em sessão de aplicativos da Web executados em navegadores remotos Google Chrome ou Microsoft Edge. Esse recurso adiciona um aviso único do navegador que solicita que o usuário habilite a extensão de WebAuthn redirecionamento DCV. Ele só é compatível com Windows WorkSpaces e clientes WorkSpaces nativos. • Corrigido um problema em que uma tela branca ou congelada às vezes aparecia ao fazer login. • Correções de erros e melhorias na performance.
• Windows WorkSpaces - 2.0.0.1304	11 de janeiro de 2024	• Corrigido um bug relacionado a possíveis congelamentos de streaming durante o login. • Corrigido um bug relacionado ao registro.

Versão	Data	Alterações
• Windows WorkSpaces - 2.0.0.1288	16 de novembro de 2023	• Foi adicionado suporte para o Indirect Display Driver (IDD) no Windows 10+, o que reduz o consumo da CPU e melhora o desempenho de streaming. • Foi adicionada uma nova configuração de Política de Grupo para ativar ou desativar o driver IDD. • Erros corrigidos relacionados à transparência da imagem da prancheta. • Erros corrigidos que preservavam os fatores de escala do Windows. • Correções de erros e melhorias na performance.
• Windows WorkSpaces - 2.0.0.1164	13 de outubro de 2023	• Adicionado suporte para o VSync no driver de exibição virtual. • Adicionada nova configuração de política de grupo para habilitar ou desabilitar o VSync. • Melhorias em problemas de reconexão e confiabilidade. • Correções de erros e melhorias na performance.

Versão	Data	Alterações
• Amazon Linux WorkSpaces - 2.0.0.1086 • Ubuntu WorkSpaces - 2.1.0.1086	18 de agosto de 2023	• Adicionada nova configuração para habilitar ou desabilitar o redirecio namento de fuso horário. • Estendido o tempo limite de login e adicionada uma opção de configuração. • Melhoria no gateway para permitir reconexões mais rápidas após interrupção. • Correções de erros e melhorias na performance.
• Amazon Linux WorkSpaces - 2.0.0.907	30 de junho de 2023	• Adição de suporte ao SDK da extensão DCV para habilitar integrações específicas de ISV. • Alterado o comportamento de desconexão para que o logout encerre a sessão do usuário. • Adicionado suporte para redirecio namento de fuso horário. • Estendido o tempo limite de login e adicionada uma opção de configuração. • Corrigidos problemas de atualizaç ão. • Correções de erros e melhorias na performance.

Versão	Data	Alterações
• Windows WorkSpaces - 2.0.0.829	8 de junho de 2023	• Alterado o comportamento de desconexão para que o logout encerre a sessão do usuário. • Corrigidos erros relacionados à sincronização A/V e teclados japoneses. • Aprimorada a confiabilidade do instalador do WSP.
• Ubuntu WorkSpaces - 2.1.0.829	16 de maio de 2023	• Alterado o comportamento de desconexão para que o logout encerre a sessão do usuário. • Adição de suporte ao SDK da extensão DCV para habilitar integrações específicas de ISV. • Adicionado suporte para redirecio namento de fuso horário. • Corrigidos problemas de atualizaç ão.

Versão	Data	Alterações
• Windows WorkSpaces - 2.0.0.799	8 de maio de 2023	• Aprimoramento do transporte QUIC baseado em UDP com várias otimizações de performance e qualidade de imagem. • Adição de suporte ao SDK da extensão DCV para habilitar integrações específicas de ISV. • Adicionadas novas configurações de política de grupo para habilitar ou desabilitar o SDK de extensão. • Melhoria nos layouts de teclado coreano, japonês e alemão. • Correção de erros relacionados a problemas de congelamento de sessão, aceleração de hardware, redirecionamento de impressora, detalhamento de log e configura ções de Política de Grupo de target-fps.

Note

- Para obter informações sobre como verificar a versão do agente do host, consulte Quais sistemas operacionais de host e cliente são compatíveis com a versão mais recente do WSP?.
- Para obter informações sobre como atualizar sua versão do Host Agent, consulte Se eu já tiver um WSP WorkSpace, como faço para atualizá-lo? .
- Para obter as notas de lançamento da versão do cliente macOS do WSP, consulte Notas de versão na seção do aplicativo cliente WorkSpaces macOS do Guia do usuário. WorkSpaces

- Para obter as notas de lançamento da versão do cliente Windows do WSP, consulte Notas de versão na seção do aplicativo cliente WorkSpaces Windows do Guia do WorkSpaces Usuário.

Extensão SDK compatível com o WSP

O Amazon WorkSpaces Streaming Protocol (WSP) foi criado usando a tecnologia NICE DCV, permitindo acesso remoto de alta performance às instâncias do WorkSpaces para uma ampla variedade de workloads e casos de uso. Com o SDK da extensão NICE DCV, os desenvolvedores podem personalizar a experiência em WorkSpaces com WSP para os usuários finais, incluindo:

- Facilitar o suporte a hardware personalizado.
- Melhorar a usabilidade de aplicações de terceiros em sessões remotas. Por exemplo, adicionando terminação de áudio local para aplicações de VoIP ou reprodução de vídeo local para aplicações de conferência.
- Fornecer software de acessibilidade, como leitores de tela, com informações sobre a sessão remota e as aplicações executadas remotamente.
- Permitir que o software de segurança analise a postura de segurança do endpoint local para permitir políticas de acesso condicional.
- Executar transferências de dados arbitrárias em uma sessão remota estabelecida.

Para começar a usar o SDK da extensão NICE DCV, consulte a documentação NICE DCV Extension SDK. É possível encontrar o SDK no repositório “NICE DCV Extension SDK” do Github. Além disso, também é possível encontrar exemplos de integração do SDK no repositório “NICE DCV Extension SDK Samples” do Github.

Os itens a seguir são compatíveis com WorkSpaces.

- Protocolo de streaming: WorkSpaces Streaming Protocol (WSP).
- Cliente do WorkSpaces para Windows: Windows: 5.9.0.4110 e posterior.

> **Note**
>
> O Acesso via Web e os clientes do WorkSpaces para Android e iOS não são compatíveis com o SDK da extensão NICE DCV.

- Compatível com WorkSpaces: servidores Windows, Linux e Ubuntu.

Histórico do documento do WorkSpaces

A tabela a seguir descreve as mudanças importantes no serviço do WorkSpaces e no Guia de administração do Amazon WorkSpaces de 1.º de janeiro de 2018 em diante. Também atualizamos a documentação com frequência para abordar os comentários enviados por você.

Para receber notificações sobre essas atualizações, você pode se inscrever no feed RSS do WorkSpaces.

Alteração	Descrição	Data
Atualização da política gerenciada AmazonWorkSpacesAdmin	O WorkSpaces adicionou a ação workspaces:RestoreWorkspace à política gerenciada AmazonWorkSpacesAdmin, concedendo aos administradores acesso para restaurar WorkSpaces.	17 de julho de 2023
Extensão SDK compatível com o WSP	Com o SDK da extensão NICE DCV, os desenvolvedores podem personalizar a experiência em WorkSpaces com WSP para os usuários finais:	25 de maio de 2023
Versões do agente do host do WorkSpaces Streaming Protocol (WSP)	Informações sobre a versão do WorkSpaces Streaming Protocol (WSP).	8 de maio de 2023
Lançamento do Amazon WorkSpaces na AWS GovCloud (Leste dos EUA)	O Amazon WorkSpaces está disponível na AWS GovCloud (Leste dos EUA).	3 de maio de 2023
Suporte a webcam do Amazon WorkSpaces	O Amazon WorkSpaces agora oferece suporte a áudio e vídeo (AV) em tempo real, redirecionando perfeitamente	5 de abril de 2021

	a entrada de vídeo da webcam local para as áreas de trabalho WorkSpaces para Windows usando o WorkSpaces Streaming Protocol (WSP).	
Suporte a cartões inteligentes do Amazon WorkSpaces com a aplicação cliente do WorkSpaces para macOS	Agora você pode usar a aplicação cliente do Amazon WorkSpaces para macOS com cartões inteligentes Common Access Card (CAC) e Personal Identity Verification (PIV). O suporte a cartões inteligentes está disponível no WorkSpaces usando o WorkSpaces Streaming Protocol (WSP).	5 de abril de 2021
APIs de gerenciamento de pacotes do Amazon WorkSpaces	Agora, as APIs de gerenciamento de pacotes do Amazon WorkSpaces estão disponíveis. Essas ações de API oferecem suporte a operações de criação, exclusão e associação de imagem para pacotes do WorkSpaces.	15 de março de 2021
Lançamento do Amazon WorkSpaces na região Ásia-Pacífico (Mumbai)	O Amazon WorkSpaces está disponível na região da Ásia-Pacífico (Mumbai).	8 de março de 2021

WorkSpaces Streaming Protocol (WSP)	O WorkSpaces Streaming Protocol (WSP) agora está disponível tanto para WorkSpaces incluídos na licença (Windows Server 2016) quanto para WorkSpaces BYOL baseados em Windows 10 em todos os tipos de pacotes, exceto Graphics e GraphicsPro. O WSP também está disponível para Linux WorkSpaces na região AWS GovCloud (Oeste dos EUA).	1º de dezembro de 2020
Cartões inteligentes	O Amazon WorkSpaces agora oferece suporte à autenticação por cartão inteligente pré-sessão (login) e em sessão nos Windows e Linux WorkSpaces na região AWS GovCloud (Oeste dos EUA).	1º de dezembro de 2020
Compartilhe imagens personalizadas	Agora, é possível compartilhar imagens personalizadas do WorkSpaces entre contas AWS. Após compartilhar uma imagem, a conta do destinatário poderá copiar a imagem e usá-la para criar pacotes para lançar novos WorkSpaces.	1º de outubro de 2020

Redirecionamento entre regiões	Agora, você pode usar o redirecionamento entre regiões, um recurso que trabalha com as políticas de roteamento do Sistema de Nomes de Domínio (DNS) para redirecionar os usuários para WorkSpaces alternativos quando os WorkSpaces primários não estão disponíveis.	10 de setembro de 2020
Assine o Microsoft Office 2016 ou 2019 para o BYOL WorkSpaces	Agora, você pode assinar o Microsoft Office Professional 2016 ou 2019 fornecido pela AWS no Bring Your Own Windows License (BYOL) WorkSpaces.	3 de setembro de 2020
Automação do BYOL na China (Ningxia)	É possível usar a automação do tipo traga a sua própria licença (BYOL) para simplificar o processo de uso de licenças de área de trabalho do Windows 10 para WorkSpaces na China (Ningxia).	2 de abril de 2020

Verificador de imagens	A ferramenta Verificador de Imagens ajuda a determina r se o Windows WorkSpace atende aos requisitos de criação de imagem. O Verificador de Imagens executa uma série de testes no WorkSpace que você deseja usar para criar a imagem e fornece orientações sobre como resolver quaisquer problemas encontrados.	30 de março de 2020
Migrar WorkSpaces	O recurso de migração do Amazon WorkSpaces permite migrar um WorkSpace de um pacote para outro, mantendo os dados no volume do usuário. É possível usar esse recurso para migrar os WorkSpaces da experiênc ia de desktop do Windows 7 para a experiência de desktop do Windows 10. Também é possível usar esse recurso para migrar os WorkSpace s de um pacote público ou personalizado para outro.	9 de janeiro de 2020

Integração do PrivateLink para APIs do Amazon WorkSpaces	É possível se conectar diretamente a endpoints de API do Amazon WorkSpaces por meio de um endpoint de interface em sua nuvem privada virtual (VPC) em vez de se conectar pela internet. Quando você usa um endpoint de interface da VPC, a comunicação entre a VPC e o endpoint de API do Amazon WorkSpaces é realizada inteiramente e com segurança na rede da AWS.	25 de novembro de 2019
Cliente do Linux para Amazon WorkSpaces	Os usuários agora podem usar o cliente Linux para acessar seus WorkSpaces.	25 de novembro de 2019
Lançamento do Amazon WorkSpaces na China (Ningxia)	Agora o Amazon WorkSpaces está disponível na região da China (Ningxia).	13 de novembro de 2019
Restaurar WorkSpaces para o último estado íntegro conhecido	É possível usar o recurso de restauração para reverter um WorkSpace para seu último estado íntegro conhecido.	18 de setembro de 2019

Criptografia de endpoints FIPS	Para estar em conformidade com o Programa federal de gerenciamento de riscos e autorizações (FedRAMP) ou com o Guia de requisitos de segurança de computaçã o em nuvem (SRG) do Departamento de Defesa (DoD), é possível configurar o Amazon WorkSpaces para usar a criptografia de endpoint dos Padrões federais de processamento de informaçõ es (FIPS) no nível do diretório.	12 de setembro de 2019
Copiar imagens do WorkSpace	Você pode copiar suas imagens na mesma região ou entre regiões.	27 de junho de 2019
Recursos de gerenciamento de autoatendimento para os usuários do WorkSpace	Você pode habilitar os recursos de gerenciamento de autoatendimento para os seus usuários do WorkSpace para fornecer mais controle sobre sua experiência.	19 de novembro de 2018
Automação do BYOL	É possível usar a automação do Bring Your Own License (BYOL – Traga sua própria licença) para simplificar o processo de uso de licenças de desktop do Windows 7 e Windows 10 para o WorkSpaces.	16 de novembro de 2018

Pacotes PowerPro e GraphicsPro	Os pacotes PowerPro e GraphicsPro agora estão disponíveis para WorkSpaces.	18 de outubro de 2018
Monitorar logins bem-sucedidos no WorkSpace	Você pode usar eventos de eventos do Amazon CloudWatch Events para monitorar e responder a logins bem-sucedidos no WorkSpace .	17 de setembro de 2018
Acesso via Web para WorkSpaces do Windows 10	Os usuários agora podem usar o cliente Web Access para acessar um WorkSpace executando a experiência de desktop do Windows 10.	24 de agosto de 2018
Login de URI	Você pode usar identificadores de recursos uniforme (URIs) para fornecer aos usuários acesso a seus WorkSpaces.	31 de julho de 2018
WorkSpaces do Amazon Linux	Você pode provisionar WorkSpaces do Amazon Linux para os usuários.	26 de junho de 2018
Grupos de controle de acesso de IP	Você pode controlar os endereços IP de onde os usuários podem acessar seus WorkSpaces.	30 de abril de 2018
Atualizações no local	Você pode atualizar o Windows 10 BYOL WorkSpaces para uma versão mais recente do Windows 10.	9 de março de 2018

Atualizações anteriores

A tabela a seguir descreve adições importantes feitas ao serviço do Amazon WorkSpaces e em seu conjunto de documentação definidas antes de 1.º de janeiro de 2018.

Alteração	Descrição	Data
Opções flexíveis de computação	Você pode alternar seus WorkSpaces entre os pacotes Value, Standard, Performance e Power	22 de dezembro de 2017
Armazenamento configurável	Você pode configurar o tamanho da raiz e volumes de usuário para seus WorkSpaces quando eles forem iniciados, e aumentar o tamanho desses volumes posteriormente.	22 de dezembro de 2017
Controlar o acesso de dispositivos	Você pode especificar os tipos de dispositivos que têm acesso aos WorkSpaces. Além disso, você pode restringir o acesso aos WorkSpaces a dispositivos confiáveis (também conhecidos como dispositivos gerenciados).	19 de junho de 2017
Confiança entre florestas	É possível estabelecer uma relação de confiança entre o Microsoft AD gerenciado pela AWS e o domínio local do Microsoft Active Directory e, assim, provisionar WorkSpaces para usuários no domínio no local.	9 de fevereiro de 2017
Pacotes do Windows Server 2016	O WorkSpaces oferece pacotes que incluem uma experiência de área de trabalho do Windows 10, promovida pelo Windows Server 2016.	29 de novembro de 2016
Web Access	Você pode acessar os WorkSpaces do Windows em um navegador da web usando o Acesso via Web do WorkSpaces.	18 de novembro de 2016

Alteração	Descrição	Data
WorkSpaces por hora	Você pode configurar os WorkSpaces para que os usuários sejam cobradas por hora.	18 de agosto de 2016
Windows 10 BYOL	Você pode trazer sua licença de área de trabalho do Windows 10 para o WorkSpaces (BYOL).	21 de julho de 2016
Compatibilidade com marcação	Você pode usar tags para gerenciar e monitorar seus WorkSpaces.	17 de maio de 2016
Registros salvos	Sempre que você insere um novo código de registro, o cliente de WorkSpaces o armazena. Isso facilita a alternância entre WorkSpaces em diferentes diretórios ou regiões.	28 de janeiro de 2016
Windows 7 (BYOL), cliente do Chromebook, criptografia do WorkSpace	Você pode trazer sua licença de área de trabalho do Windows 7 para o WorkSpaces (BYOL), usar o cliente para Chromebook e usar a criptografia do WorkSpace.	1 de outubro de 2015
Monitoramento do CloudWatch	Adição de informações sobre o monitoramento do CloudWatch.	28 de abril de 2015
Reconexão automática da sessão	Adição de informações sobre o recurso de reconexão automática de sessão nas aplicações cliente de desktop de WorkSpaces.	31 de março de 2015
Endereços IP públicos	É possível atribuir automaticamente um endereço IP público aos WorkSpaces.	23 de janeiro de 2015
Lançamento do WorkSpaces na Ásia-Pacífico (Singapura)	Agora, o WorkSpaces está disponível na região Ásia-Pacífico (Singapura).	15 de janeiro de 2015
Adição do pacote Value, atualizações do pacote Standard, adição do Office 2013	O pacote Value está disponível, o hardware do pacote Standard foi atualizado e o Microsoft Office 2013 está disponível em pacotes Plus.	6 de novembro de 2014

Alteração	Descrição	Data
Suporte a imagens e pacotes	É possível criar uma imagem a partir do WorkSpace que você personalizou e um pacote do WorkSpace personalizado a partir da imagem.	28 de outubro de 2014
Suporte ao cliente PCoIP zero	É possível acessar dispositivos cliente zero PCoIP do WorkSpaces.	15 de outubro de 2014
Lançamento do WorkSpaces na Ásia-Pacífico (Tóquio)	Agora, o WorkSpaces está disponível na região Ásia-Pacífico (Tóquio).	26 de agosto de 2014
Suporte a impressora local	É possível habilitar o suporte a impressora local para os WorkSpaces.	26 de agosto de 2014
Autenticação multifator	É possível usar a autenticação multifator em diretórios conectados.	11 de agosto de 2014
Suporte à UO padrão e suporte a domínio de destino	É possível selecionar uma unidade organizacional (UO) padrão na qual as contas de máquina do WorkSpace são colocadas, e um domínio separado no qual as contas de máquina do WorkSpace são criadas.	7 de julho de 2014
Adição de grupos de segurança	É possível adicionar um security group aos WorkSpaces.	7 de julho de 2014
Lançamento do WorkSpaces na Ásia-Pacífico (Sydney)	Agora, o WorkSpaces está disponível na região Ásia-Pacífico (Sydney).	15 de maio de 2014
Lançamento do WorkSpaces na Europa (Irlanda)	O WorkSpaces já está disponível na região Europa (Irlanda).	5 de maio de 2014
Beta público	O WorkSpaces está disponível como beta público.	25 de março de 2014

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.