



Guia do administrador

Amazon WorkSpaces Thin Client



Amazon WorkSpaces Thin Client: Guia do administrador

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

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestige a Amazon. Todas as outras marcas comerciais que não são propriedade da Amazon pertencem aos respectivos proprietários, os quais podem ou não ser afiliados, estar conectados ou ser patrocinados pela Amazon.

Table of Contents

O que é o console do administrador do Amazon WorkSpaces Thin Client?	1
Você é um usuário iniciante do ?	1
Arquitetura	1
Configurando o console de administrador do Amazon WorkSpaces Thin Client	4
Cadastre-se no AWS	4
Criar um usuário do IAM	4
Comece a usar sua VDI para o console de administrador do Amazon WorkSpaces Thin Client	6
Configuração WorkSpaces para o Amazon WorkSpaces Thin Client	6
Antes de começar	7
Etapa 1: Verifique se o sistema atende aos recursos WorkSpaces necessários	7
Etapa 2: use a configuração avançada para iniciar seu Workspace	8
Configuração AppStream 2.0 para o Amazon WorkSpaces Thin Client	9
Etapa 1: Verifique se o sistema atende aos recursos exigidos pela AppStream versão 2.0	9
Etapa 2: configurar suas AppStream pilhas 2.0	10
Configurando o Amazon WorkSpaces Secure Browser para o Amazon WorkSpaces Thin Client	11
Etapa 1: Verifique se seu sistema atende aos recursos exigidos pelo Amazon WorkSpaces Secure Browser	11
Etapa 2: configurar os portais do WorkSpaces Secure Browser	12
Iniciando o console do administrador do WorkSpaces Thin Client	13
Regiões cobertas	13
Lançamento do console do administrador do WorkSpaces Thin Client	14
Usando o console do administrador do WorkSpaces Thin Client	15
Ambientes do	16
Lista de ambientes	16
Detalhes do ambiente	17
Criar um ambiente	18
Editar um ambiente	26
Excluir um ambiente	26
Dispositivos	27
Lista de dispositivos	27
Detalhes do dispositivo	29
Editar o nome do dispositivo	30
Redefinir e cancelar o registro de um dispositivo	30

Arquivar um dispositivo	31
Excluir um dispositivo	31
Exportar os detalhes do dispositivo	32
Atualizações de software	32
Atualizar o software do ambiente	32
Atualizar o software do dispositivo	33
WorkSpaces Lançamentos do software Thin Client	34
Usando tags em recursos do WorkSpaces Thin Client	39
Segurança	42
Proteção de dados	42
Criptografia de dados	44
Criptografia inativa	45
Criptografia em trânsito	59
Gerenciamento de chaves	59
Privacidade de tráfego no trabalho na Internet	59
Gerenciamento de identidade e acesso	60
Público	60
Autenticando com identidades	61
Gerenciamento do acesso usando políticas	65
Como o Amazon WorkSpaces Thin Client funciona com o IAM	67
Exemplos de políticas baseadas em identidade	75
Solução de problemas	80
Resiliência	82
Análise e gerenciamento de vulnerabilidades	83
Monitoramento	84
CloudTrail troncos	84
WorkSpaces Informações do Thin Client em CloudTrail	84
Compreendendo as entradas do arquivo de log do WorkSpaces Thin Client	85
AWS CloudFormation recursos	88
WorkSpaces Thin Client e AWS CloudFormation modelos	88
Saiba mais sobre AWS CloudFormation	88
AWS PrivateLink	89
Considerações	89
Como criar um endpoint de interface	89
Crie uma política de endpoint	90
Histórico do documento	91

..... **xcii**

O que é o console do administrador do Amazon WorkSpaces Thin Client?

Com o console de administrador do Amazon WorkSpaces Thin Client, os administradores podem gerenciar ambientes e dispositivos WorkSpaces Thin Client por meio de um portal WorkSpaces Thin Client. A partir desse console web, os administradores podem criar ambientes, gerenciar dispositivos e definir parâmetros para usuários do WorkSpaces Thin Client em sua rede.

Os ambientes de desktop virtual que você usa para o WorkSpaces Thin Client devem ser criados ou modificados em seu próprio console.

Important

Para que o console do administrador do WorkSpaces Thin Client funcione corretamente, seu sistema deve primeiro atender aos requisitos específicos. Esses requisitos estão listados em [Pré-requisitos](#) e configurações.

Tópicos

- [Você é um usuário iniciante do ?](#)
- [Arquitetura](#)

Você é um usuário iniciante do ?

Se você é um usuário iniciante do console de administrador do WorkSpaces Thin Client, recomendamos que você comece lendo as seguintes seções:

- [Iniciando o console do administrador do WorkSpaces Thin Client](#)
- [Usando o console do administrador do WorkSpaces Thin Client](#)

Arquitetura

Cada WorkSpaces Thin Client está associado a um provedor de interface de desktop virtual (VDI). WorkSpaces Thin Client oferece suporte a três provedores de VDI:

- [Amazon WorkSpaces](#)
- [AppStream 2.0](#)
- [WorkSpaces Navegador Amazon Secure](#)

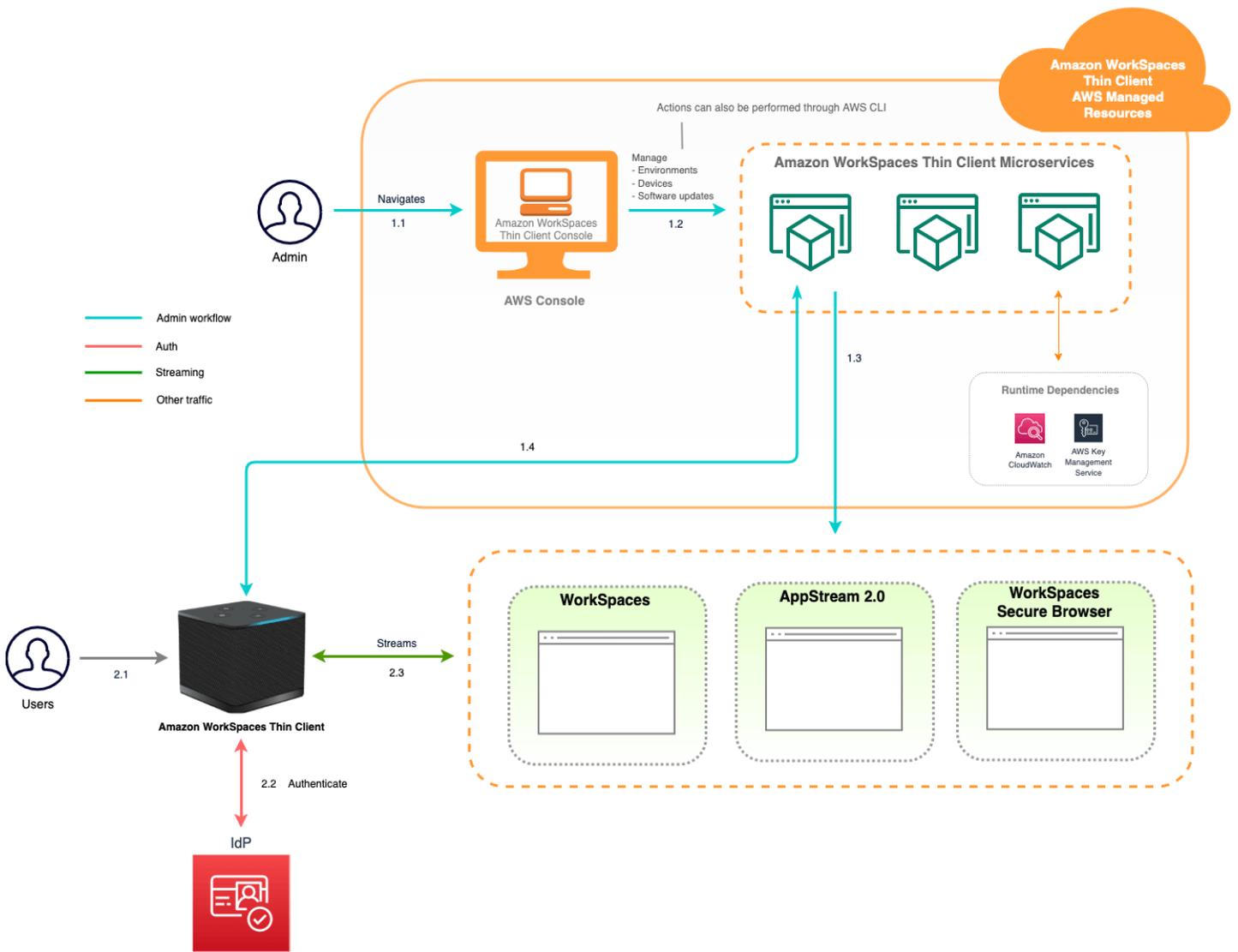
Dependendo da VDI usada, as informações do seu WorkSpaces Thin Client são acessadas e gerenciadas por meio de diretórios para WorkSpaces, pilhas para AppStream 2.0 e endpoints de portal da web para o Secure Browser. WorkSpaces

Para obter mais informações sobre a Amazon WorkSpaces, consulte [Comece com a configuração WorkSpaces rápida](#). Os diretórios são gerenciados por meio do AWS Directory Service, que oferece as seguintes opções: Simple AD, AD Connector ou AWS Directory Service for Microsoft Active Directory, também conhecido como AWS Managed Microsoft AD. Para obter mais informações, consulte o [Guia do administrador do AWS Directory Service](#).

Para obter mais informações sobre AppStream 2.0, consulte [Get Started with Amazon AppStream 2.0: configure com aplicativos de amostra](#). AppStream 2.0 gerencia AWS os recursos necessários para hospedar e executar seus aplicativos, dimensiona automaticamente e fornece acesso aos usuários sob demanda. AppStream O 2.0 fornece aos usuários acesso aos aplicativos de que precisam no dispositivo de sua escolha, com uma experiência de usuário responsiva e fluida que é indistinguível dos aplicativos instalados nativamente.

Para obter informações sobre o WorkSpaces Secure Browser, consulte [Introdução ao Amazon WorkSpaces Secure Browser](#). O Amazon WorkSpaces Secure Browser é um serviço sob demanda, totalmente gerenciado e baseado em Linux, projetado para facilitar o acesso seguro do navegador a sites internos e aplicativos (software-as-a-service SaaS). Acesse o serviço em navegadores da web existentes, sem a carga administrativa do gerenciamento da infraestrutura, do software cliente especializado ou das soluções de rede privada virtual (VPN).

O diagrama a seguir mostra a arquitetura do WorkSpaces Thin Client.



Configurando o console de administrador do Amazon WorkSpaces Thin Client

Tópicos

- [Cadastre-se no AWS](#)
- [Criar um usuário do IAM](#)

Cadastre-se no AWS

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

Para se inscrever em um Conta da AWS

1. Abra <https://portal.aws.amazon.com/billing/signup>.
2. Siga as instruções on-line.

Parte do procedimento de inscrição envolve receber uma chamada telefônica e digitar um código de verificação no teclado do telefone.

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

Criar um usuário do IAM

Para criar um usuário administrador, selecione uma das opções a seguir.

Selecionar uma forma de gerenciar o administrador	Para	Por	Você também pode
Centro de Identidade e do IAM (Recomendado)	<p>Use credenciais de curto prazo para acessar a AWS.</p> <p>Isso está de acordo com as práticas recomendadas de segurança. Para obter informações sobre as práticas recomendadas, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.</p>	Seguindo as instruções em Conceitos básicos no Guia do usuário do AWS IAM Identity Center .	Configure o acesso programático configurando o AWS CLI para uso AWS IAM Identity Center no Guia do AWS Command Line Interface usuário.
No IAM (Não recomendado)	Use credenciais de curto prazo para acessar a AWS.	Seguindo as instruções em Criar o seu primeiro usuário administrador e um grupo de usuários do IAM no Guia do usuário do IAM.	Para configurar o acesso programático, consulte Gerenciamento de chaves de acesso de usuários do IAM no Guia do usuário do IAM.

Introdução à sua VDI para o Amazon WorkSpaces Thin Client

O Amazon WorkSpaces Thin Client é um dispositivo thin client econômico criado para funcionar com serviços de computação de usuário AWS final para fornecer acesso seguro e instantâneo a aplicativos e desktops virtuais.

Escolha uma infraestrutura de desktop virtual (VDI) e configure-a para funcionar com o WorkSpaces Thin Client.

Important

Para que o console do administrador do WorkSpaces Thin Client funcione corretamente, seu sistema deve primeiro atender aos requisitos específicos. Esses requisitos estão listados no procedimento de configuração de cada provedor de desktop virtual.

WorkSpaces O Thin Client requer configurações de software específicas, dependendo do seu provedor de desktop virtual.

Tópicos

- [Configuração WorkSpaces para o Amazon WorkSpaces Thin Client](#)
- [Configuração AppStream 2.0 para o Amazon WorkSpaces Thin Client](#)
- [Configurando o Amazon WorkSpaces Secure Browser para o Amazon WorkSpaces Thin Client](#)

Configuração WorkSpaces para o Amazon WorkSpaces Thin Client

Para que o WorkSpaces Thin Client seja usado com a Amazon WorkSpaces, seu serviço precisará ser configurado para acessar os WorkSpaces diretórios. A Amazon WorkSpaces é listada com base em seus nomes de diretório na página do ambiente WorkSpaces Thin Client Create no AWS console.

Note

As configurações devem ser feitas antes de usar o console pela primeira vez. Não é recomendável modificar nenhum recurso de pré-requisito depois de começar a usar o console.

Antes de começar

Verifique se você tem uma AWS conta para criar ou administrar uma WorkSpace. Os usuários de dispositivos, no entanto, não precisam de uma AWS conta para se conectar e usar seus WorkSpaces.

Analise e compreenda os seguintes conceitos antes de continuar com a configuração:

- Ao iniciar um WorkSpace, selecione um WorkSpace pacote. Para obter mais informações, consulte [Amazon WorkSpaces Bundles](#).
- Ao iniciar um WorkSpace, selecione qual protocolo você deseja usar com seu pacote. Para obter mais informações, consulte [Protocolos para a Amazon WorkSpaces](#).
- Ao iniciar um WorkSpace, especifique as informações do perfil de cada usuário, incluindo nome de usuário e endereço de e-mail. Os usuários completam seus perfis criando uma senha. As informações sobre usuários WorkSpaces e os usuários são armazenadas em um diretório. Para obter mais informações, consulte [Gerenciar diretórios para WorkSpaces](#).
- Ao iniciar um WorkSpace, habilite e configure o acesso à WorkSpaces web. Para obter mais informações, consulte [Habilitar e configurar o Amazon WorkSpaces Web Access](#)

Etapa 1: Verifique se o sistema atende aos recursos WorkSpaces necessários

Para que o console do administrador do WorkSpaces Thin Client funcione adequadamente com a Amazon WorkSpaces, seu sistema deve atender aos seguintes requisitos específicos. Esta tabela lista todos esses recursos suportados e seus requisitos.

Atributo	Requisito
Web access	Habilitado

Atributo	Requisito
Sistema operacional com suporte	<ul style="list-style-type: none"> • Windows 10 • Windows 10 (Traga sua própria licença) • Windows 11 • Windows 11 (Traga sua própria licença)
Pacotes compatíveis	<ul style="list-style-type: none"> • Microsoft Power com Windows 10 (baseado em Server 2016, 2019 e 2022) • Microsoft Power com Windows 10 (baseado em Server 2016, 2019 e 2022) com Office • Microsoft PowerPro com Windows 10 (baseado em Server 2016, 2019 e 2022) • Microsoft PowerPro com Windows 10 (baseado em Server 2016, 2019 e 2022) com Office • Microsoft Performance com Windows 10 (baseado em Server 2016, 2019 e 2022) • Microsoft Performance com Windows 10 (baseado em Server 2016, 2019 e 2022) com Office
Protocolos compatíveis	Somente WSP

Etapa 2: use a configuração avançada para iniciar seu WorkSpace

Para usar a configuração avançada para iniciar seu WorkSpace

1. Abra o WorkSpaces console 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.

Configuração AppStream 2.0 para o Amazon WorkSpaces Thin Client

AppStream As instâncias 2.0 serão listadas com base nos nomes das pilhas e exigirão que uma URL de login do IdP seja configurada na página de criação do ambiente. Como a autenticação SAML para AppStream 2.0 só oferece suporte à autenticação iniciada, o administrador precisará inserir a URL de login correta manualmente.

Note

As configurações devem ser feitas antes de usar o console pela primeira vez. Não é recomendável modificar nenhum recurso de pré-requisito depois de começar a usar o console.

Etapa 1: Verifique se o sistema atende aos recursos exigidos pela AppStream versão 2.0

Para que o console do administrador do WorkSpaces Thin Client funcione corretamente com o AppStream 2.0, seu sistema deve atender aos seguintes requisitos específicos. Esta tabela lista todos esses recursos suportados e seus requisitos.

Atributo	Requisito
Provedor de identidades	<p>Acesse Configurando o SAML no Guia do Administrador AppStream 2.0 para criar um provedor de identidade.</p> <p>Quando solicitado a Criar console env, insira sua URL de login do IDP.</p>
Sistema operacional	Windows

Atributo	Requisito
Tipo de plataforma	Windows Server (2012 R2, 2016 ou 2019)
Protocolo de streaming	Streaming TCP Há um mecanismo de fallback automático para TCP, se UDP não estiver disponível.
Copiar e colar local	Disable (Desabilitar) Configurado no nível de pilha AppStream 2.0
Compartilhamento de pastas local	Disable (Desabilitar) Configurado no nível de pilha AppStream 2.0
Impressão local	Disable (Desabilitar) Configurado no nível de pilha AppStream 2.0

O requisito de bloqueio de tela por meio da autenticação SAML na AppStream versão 2.0 também é suportado. O grupo de usuários e os mecanismos de autenticação programática não são suportados no WorkSpaces Thin Client.

Etapa 2: configurar suas AppStream pilhas 2.0

Para transmitir seus aplicativos, o AppStream 2.0 requer um ambiente que inclua uma frota associada a uma pilha e pelo menos uma imagem do aplicativo. Siga estas etapas para configurar uma frota e uma pilha e dar aos usuários acesso à pilha. Se você ainda não tiver feito isso, recomendamos que você experimente os procedimentos em [Introdução ao AppStream 2.0: Configurar com aplicativos de amostra](#).

Se você quiser criar uma imagem para usar, consulte [Tutorial: Criar uma imagem AppStream 2.0 personalizada usando o console AppStream 2.0](#).

Se você planeja associar uma frota a um domínio do Active Directory, configure seu domínio do Active Directory antes de concluir as etapas a seguir. Para obter mais informações, consulte [Usando o Active Directory com AppStream 2.0](#).

Tarefas

- [Criar uma frota](#)
- [Criar um stack](#)
- [Fornecer acesso aos usuários](#)
- [Limpar os recursos](#)

Configurando o Amazon WorkSpaces Secure Browser para o Amazon WorkSpaces Thin Client

O Amazon WorkSpaces Secure Browser é baseado em seus endpoints do portal web na página do ambiente WorkSpaces Thin Client Create no AWS console.

Note

As configurações devem ser feitas antes de usar o console pela primeira vez. Não é recomendável modificar nenhum recurso de pré-requisito depois de começar a usar o console.

Etapa 1: Verifique se seu sistema atende aos recursos exigidos pelo Amazon WorkSpaces Secure Browser

Para que o WorkSpaces Thin Client Administrator Console funcione adequadamente com o Amazon WorkSpaces Secure Browser, seu sistema deve atender aos seguintes requisitos específicos. Esta tabela lista todos esses recursos suportados e seus requisitos.

Atributo	Requisito
Copiar e colar local	Disable (Desabilitar)
Compartilhamento de pastas local	Disable (Desabilitar)

Note

Atualmente, a extensão WorkSpaces Secure Browser para login único não é suportada no WorkSpaces Thin Client.

Etapa 2: configurar os portais do WorkSpaces Secure Browser

WorkSpaces O Thin Client funciona com o WorkSpaces Secure Browser VPC em uma configuração específica:

1. Crie uma [VPC](#) usando o modelo do [AWS CodeBuild Cloudformation](#).
2. Configure seu [provedor de identidades](#).
3. [Crie](#) um portal do Amazon WorkSpaces Secure Browser.
4. [Teste](#) seu novo portal do Amazon WorkSpaces Secure Browser.

Iniciando o console do administrador do WorkSpaces Thin Client

WorkSpaces O Thin Client é um dispositivo thin client econômico criado para funcionar com serviços de computação de usuário AWS final para fornecer acesso seguro e instantâneo a aplicativos e desktops virtuais.

Tópicos

- [Regiões cobertas](#)
- [Lançamento do console do administrador do WorkSpaces Thin Client](#)

Regiões cobertas

WorkSpaces O Thin Client está disponível nas seguintes regiões.

Somente o console do administrador do WorkSpaces Thin Client está disponível nessas regiões. WorkSpaces Atualmente, os dispositivos Thin Client só estão disponíveis nos EUA, Alemanha, França, Itália e Espanha.

Nome da região	Região	Endpoint	Link do console
Leste dos EUA (Norte da Virgínia)	us-east-1	thinclient.us-east-1.amazonaws.com	https://us-east-1.console.aws.amazon.com/workspaces-thin-client/home
Oeste dos EUA (Oregon)	us-west-2	thinclient.us-west-2.amazonaws.com	https://us-west-2.console.aws.amazon.com/workspaces-thin-client/home
Ásia-Pacífico (Mumbai)	ap-south-1	thinclient.ap-south-1.amazonaws.com	https://ap-south-1.console.aws.amazon.com/workspaces-thin-client/home

Nome da região	Região	Endpoint	Link do console
Europa (Irlanda)	eu-west-1	thinclient.eu-west-1.amazonaws.com	https://eu-west-1.console.aws.amazon.com/workspaces-thin-client/home
Canadá (Central)	ca-central-1	thinclient.ca-central-1.amazonaws.com	https://ca-central-1.console.aws.amazon.com/workspaces-thin-client/home
Europa (Frankfurt)	eu-central-1	thinclient.eu-central-1.amazonaws.com	https://eu-central-1.console.aws.amazon.com/workspaces-thin-client/home
Europa (Londres)	eu-west-2	thinclient.eu-west-2.amazonaws.com	https://eu-west-2.console.aws.amazon.com/workspaces-thin-client/home

Lançamento do console do administrador do WorkSpaces Thin Client

Quando você tem uma AWS conta, pode iniciar o console do administrador e acessar o console do WorkSpaces Thin Client. Para iniciar o console, faça o seguinte:

1. Faça login na sua AWS conta.
2. Acesse o [console do WorkSpaces Thin Client](#).
3. Selecione Começar e você será direcionado para [Ambientes](#).

Usando o console do administrador do WorkSpaces Thin Client

The screenshot shows the Amazon WorkSpaces Thin Client administrator console landing page. At the top left, it says "End User Computing". The main heading is "Amazon WorkSpaces Thin Client" with the subtext "Affordable, easy-to-manage thin client for secure access to virtual desktops". Below this is a short paragraph: "Improve end-user productivity by going from unboxing to desktop access in just a few minutes, while improving IT staff productivity through centralized remote management of your fleet." On the right side, there are two buttons: "Get started" (orange) and "Order devices" (white with a link icon). Below these is a "Pricing" section with the text: "You pay up front for the WorkSpaces Thin Client device, plus a monthly service fee per device to manage, monitor, and maintain your thin client fleet in the WorkSpaces Thin Client management console." and a link "Learn more about WorkSpaces Thin Client pricing". At the bottom right, there is a section titled "Amazon WorkSpaces Thin Client devices" with an image of the physical device. The main content area is titled "How it works" and contains a flowchart titled "Admin management flow" with five steps: 1. Amazon WorkSpaces Thin Client (Cost-effective, secure, and easy-to-manage access to virtual desktops). 2. Administrator sets up Amazon WorkSpaces, Amazon WorkSpaces Web, or Amazon AppStream 2.0 in desired AWS Region to associate with WorkSpaces Thin Client service. 3. Administrator copies activation codes from Console and emails them to end users. 4. End users enter activation code to register the device and log into their virtual desktop environment. 5. Administrator manages, monitors, and maintains WorkSpaces Thin Client fleet and controls access through device management service.

Bem-vindo ao WorkSpaces Thin Client Administrator Console!

A partir daqui, você pode gerenciar sua frota de dispositivos e ambientes WorkSpaces Thin Client para sua equipe.

Para obter informações sobre o dispositivo WorkSpaces Thin Client, consulte o [Guia do usuário do WorkSpaces Thin Client](#).

Vamos começar.

Tópicos

- [Ambientes do](#)
- [Dispositivos](#)
- [Atualizações de software](#)

Ambientes do

Cada dispositivo WorkSpaces Thin Client usa um ambiente de desktop virtual individual para acessar seus recursos on-line. Os usuários acessam esse ambiente usando um dos seguintes provedores de desktop virtual:

- Amazon WorkSpaces
- AppStream 2.0
- WorkSpaces Navegador Amazon Secure

Lista de ambientes

Detalhes da lista de ambientes

Nome: o identificador exclusivo associado ao ambiente.

Serviço de área de trabalho virtual: o provedor de área de trabalho virtual que o ambiente usa.

ID do serviço de desktop virtual - O identificador exclusivo que o provedor de serviços de desktop virtual atribui a esse ambiente.

Código de ativação - O código usado pelos usuários finais para acessar o ambiente de desktop virtual.

Contagem de dispositivos - O número de dispositivos WorkSpaces Thin Client que estão acessando esse ambiente.

Ações da lista de ambientes

Pesquisar: pesquisa todos os ambientes que você gerencia.

Atualizar: atualiza a lista de ambientes.

Visualizar detalhes: exibe os [detalhes do ambiente](#).

Ações - Abre uma lista suspensa na qual você pode [editar](#) ou [excluir um ambiente](#).

Criar ambiente: inicia o processo de [criação de um ambiente](#)

Criar ambiente: inicia o processo de [criação de um ambiente](#).

Tópicos

- [Detalhes do ambiente](#)
- [Criar um ambiente](#)
- [Editar um ambiente](#)
- [Excluir um ambiente](#)

Detalhes do ambiente

Quando você seleciona um ambiente, o console do WorkSpaces Thin Client exibe os detalhes desse ambiente para você revisar. O console também exibe os detalhes sobre o provedor de desktop virtual que esse ambiente usa.

Tópicos

- [Resumo](#)
- [Detalhes de ambientes da área de trabalho virtual](#)

Resumo

Nome: o identificador exclusivo associado ao ambiente.

Serviço de área de trabalho virtual: o provedor de área de trabalho virtual que o ambiente usa.

ID do serviço de desktop virtual - O identificador exclusivo que o provedor de serviços de desktop virtual atribui a esse ambiente.

Código de ativação: é código usado pelos usuários finais para acessar o ambiente de área de trabalho virtual.

Sempre mantenha o software up-to-date - Essa configuração permite atualizações automáticas de software.

Horário de início da janela de manutenção - O horário semanal em que as atualizações automáticas de software começam.

Horário de término da janela de manutenção - O horário semanal em que as atualizações automáticas de software terminam.

Janela de manutenção de dias da semana: os dias para as atualizações automáticas de software.

Dispositivos associados - O número de dispositivos WorkSpaces Thin Client que estão acessando esse ambiente.

Hora de criação - A data e a hora em que esse ambiente foi criado.

Detalhes de ambientes da área de trabalho virtual

Detalhes WorkSpaces do diretório Amazon

ID do diretório - O WorkSpaces diretório da Amazon associado a esse ambiente.

Nome do diretório - O identificador exclusivo associado a esse WorkSpaces diretório da Amazon.

Nome da organização - O nome da organização que controla o WorkSpaces diretório da Amazon.

Tipo de diretório - O formato do WorkSpaces diretório da Amazon.

Registrado - Se esse WorkSpaces diretório da Amazon está registrado.

Status - Se esse WorkSpaces diretório da Amazon está ativo.

Detalhes do portal Amazon WorkSpaces Secure Browser

Nome - O identificador exclusivo associado a este portal do Amazon WorkSpaces Secure Browser.

Hora de criação - A data e a hora em que essa pilha AppStream 2.0 foi criada.

Endpoint do portal da Web: o URL usado para acessar o ambiente de área de trabalho virtual.

AppStream 2.0 detalhes

Nome da pilha - O identificador exclusivo associado a essa pilha AppStream 2.0.

URL de login do IdP - A URL do provedor de identidade usada para entrar e sair da sua pilha AppStream 2.0.

Hora de criação - A data e a hora em que essa pilha AppStream 2.0 foi criada.

Criar um ambiente

Para começar, cada dispositivo requer um serviço de computação do usuário AWS final.

WorkSpaces O Thin Client usa os seguintes serviços:

- Amazon WorkSpaces por meio de um diretório atribuído

- AppStream 2.0 por meio de uma pilha atribuída
- Amazon WorkSpaces Secure Browser por meio de um endereço de portal da web

Você deve atribuir um serviço a um ambiente existente ou criar um novo.

 Note

WorkSpaces O Thin Client exibe somente desktops virtuais na mesma região.

Tópicos

- [Etapa 1: informar os detalhes do ambiente](#)
- [Etapa 2: selecionar seu provedor de área de trabalho virtual](#)
- [Etapa 3: enviar o código de ativação aos usuários de dispositivos](#)

Etapa 1: informar os detalhes do ambiente

1. Insira um nome para seu ambiente no campo Detalhes do ambiente.
2. Para configurar patches automáticos de software, marque a caixa Sempre mantenha o software up-to-date.

 Note

Se as atualizações automáticas de software não estiverem habilitadas, os dispositivos registrados nesse ambiente não receberão atualizações de software até que você envie manualmente a atualização ou quando o software expirar e o sistema forçar uma atualização.

Além disso, a versão do conjunto de software do dispositivo é determinada pelo sistema. Essa versão pode não ser a mais recente.

3. Selecione quando você deseja programar a janela de manutenção do seu ambiente.
 - Aplique a janela de manutenção em todo o sistema - atualiza automaticamente o software do ambiente em um determinado horário a cada semana.
 - Aplicar a janela de manutenção personalizada: defina o dia e a hora em que você deseja que o software do ambiente seja atualizado toda semana.

4. Selecione um serviço de área de trabalho virtual.

- [Amazon WorkSpaces](#)
- [WorkSpaces Navegador Amazon Secure](#)
- [AppStream 2.0](#)

Etapa 2: selecionar seu provedor de área de trabalho virtual

Você deve ter um serviço para fornecer aos usuários acesso ao desktop virtual e aos recursos compatíveis.

Important

Para que o WorkSpaces Thin Client Administrator Console funcione corretamente, seu sistema deve atender a requisitos específicos. Esses requisitos estão listados em [Pré-requisitos](#) e configurações.

Verifique se o sistema atende a esses requisitos antes de configurar o console.

Usando a Amazon WorkSpaces

WorkSpaces A Amazon é um serviço de virtualização de desktop totalmente gerenciado para Windows que permite acessar recursos de qualquer dispositivo compatível.

1. Para usar a Amazon WorkSpaces, faça o seguinte:

- Selecione o diretório que você deseja usar para o ambiente. Você pode navegar pela lista suspensa ou pesquisar os diretórios usando o campo de pesquisa.

Note

Se você não encontrar seus diretórios existentes na lista, verifique no WorkSpaces Management Console se eles atendem aos [requisitos](#) do WorkSpaces Thin Client.

- Crie um diretório selecionando o botão Criar WorkSpaces diretório. Para obter mais informações sobre a criação de WorkSpaces diretórios, consulte [Gerenciar diretórios](#) para WorkSpaces

2. Selecione o botão Criar ambiente.

Virtual desktop services

Choose the virtual desktop service to provision your environment, then select the resource to use or create a new one. The time to provision depends on your chosen configuration.

WorkSpaces

Amazon WorkSpaces is a fully managed desktop virtualization service for Windows that enables you to access resources from any supported device.

AppStream 2.0

Amazon AppStream 2.0 is a fully managed, secure application streaming service that allows you to stream desktop applications from AWS to a web browser.

WorkSpaces Web

Amazon WorkSpaces Web is a low-cost, fully managed Workspace built to deliver secure web-based workloads and software-as-a-service (SaaS) application access to users within existing web browsers.

Note: When creating a new Workspace directory for your environment, you will be taken to the WorkSpaces console. Amazon Thin Client requires certain Workspace configuration to be compatible. For more information and help with setup, please refer to the [Create a Workspace](#) for Amazon Thin Client tutorial.

WorkSpaces directories (5) [Info](#)

Amazon WorkSpaces is a fully managed desktop virtualization service for Windows and Linux that enables you to access resources from any supported device.

↻
Create Workspace directory [↗](#)

< 1 > ⚙

	Directory ID	Directory name	Organization name	Directory type
<input type="radio"/>	abc	xyz.com	Name 1	Simple AD
<input type="radio"/>	abc	xyz.com	Name 2	Simple AD
<input checked="" type="radio"/>	abc	xyz.com	Name 3	Simple AD
<input type="radio"/>	abc	xyz.com	Name 4	Simple AD
<input type="radio"/>	abc	xyz.com	Name 5	Simple AD

Cancel
Create environment

Ao criar seu ambiente, você ainda pode editar os detalhes posteriormente. Para obter mais informações, consulte [Editar um ambiente](#).

Usando AppStream 2.0

AppStream 2.0 é um serviço de streaming de aplicativos totalmente gerenciado e seguro que você pode usar para transmitir aplicativos de desktop AWS para um navegador da web.

⚠ Warning

Para criar um ambiente AppStream 2.0, você deve ter `cli_follow_urlparam` definido como `false`. Para conseguir isso, faça o seguinte:

- Para um perfil padrão, execute `aws configure set cli_follow_urlparam false`.
- Para um perfil com o nome `ProfileName`, execute `aws configure set cli_follow_urlparam false --profile ProfileName`.

1. Para configurar o AppStream 2.0, faça o seguinte:

- Selecione a pilha que você deseja usar no ambiente. Você pode navegar pela lista suspensa ou pesquisar as pilhas usando o campo de pesquisa.

ℹ Note

Se você não encontrar suas pilhas existentes na lista, verifique no console de gerenciamento AppStream 2.0 se elas atendem aos [requisitos](#) do WorkSpaces Thin Client.

- Crie uma pilha selecionando o botão Criar pilha. Para obter mais informações sobre a criação de pilhas AppStream 2.0, consulte [Criar uma pilha](#).
2. Insira o URL de login e logout do provedor de identidade no campo URL de login do IdP. Isso fornece aos usuários um local para entrar e sair do WorkSpaces Thin Client.
 3. Selecione o botão Criar ambiente.

Virtual desktop services

Choose the virtual desktop service to provision your environment, then select the resource to use or create a new one.

WorkSpaces

Amazon WorkSpaces is a fully managed desktop virtualization service for Windows that enables you to access resources from any supported device.

AppStream 2.0

Amazon AppStream 2.0 is a fully managed, secure application streaming service that allows you to stream desktop applications from AWS to a web browser.

WorkSpaces Web

Amazon WorkSpaces Web is a low-cost, fully managed Workspace built to deliver secure web-based workloads and software-as-a-service (SaaS) application access to users within existing web browsers.

Note: When creating a new AppStream 2.0 Stack for your environment, you will be taken to the AppStream 2.0 Stack console. Amazon Thin Client requires certain AppStream 2.0 Stack configuration to be compatible. For more information and help with setup, please refer to the [Create a AppStream 2.0 Stack](#) for Amazon Thin Client tutorial.

Stacks (1) [Info](#)

You can set up an AppStream 2.0 Stack to start streaming apps to your users' browsers. An AppStream 2.0 Stack consists of a fleet of streaming instances, user access policies, and storage configurations.

< 1 >
⚙️

	Name	Time created
<input type="radio"/>	Name 1	January 31, 2010, 14:32 (UTC+3:30)
<input type="radio"/>	Name 2	January 31, 2010, 14:32 (UTC+3:30)
<input checked="" type="radio"/>	Name 3	January 31, 2010, 14:32 (UTC+3:30)
<input type="radio"/>	Name 4	January 31, 2010, 14:32 (UTC+3:30)
<input type="radio"/>	Name 5	January 31, 2010, 14:32 (UTC+3:30)

AppStream 2.0 Stack details [Info](#)

With your AppStream Stack selected, enter your Identity provider (IdP) login and logout URL. This provides users the place to login and out of the Amazon Thin Client.

IdP login URL

Specify the details from your IdP.

Cancel
Create environment

Depois de criar seu ambiente, você ainda pode editar os detalhes posteriormente. Para obter mais informações, consulte [Editar um ambiente](#).

Usando o Amazon WorkSpaces Secure Browser

O Amazon WorkSpaces Secure Browser é um WorkSpaces console de baixo custo e totalmente gerenciado, criado para fornecer cargas de trabalho seguras baseadas na web e acesso a aplicativos de software como serviço (SaaS) aos usuários nos navegadores da web existentes.

1. Para configurar o Amazon WorkSpaces Secure Browser, faça o seguinte:
 - Selecione o portal da web que você deseja usar para seu ambiente. Você pode navegar pela lista suspensa ou pesquisar nos portais da web usando o campo de pesquisa.

Note

Se você não encontrar seus portais da Web existentes na lista, verifique no console de gerenciamento do WorkSpaces Secure Browser se eles atendem aos [requisitos](#) do WorkSpaces Thin Client.

- Crie um portal da web selecionando o botão Criar navegador WorkSpaces seguro. Para obter mais informações sobre a criação de portais web do WorkSpaces Secure Browser, consulte [Configurando o Amazon WorkSpaces Secure Browser](#).
2. Selecione o botão Criar ambiente.

Virtual desktop services

Choose the virtual desktop service to provision your environment, then select the resource to use or create a new one.

WorkSpaces

Amazon WorkSpaces is a fully managed desktop virtualization service for Windows that enables you to access resources from any supported device.

AppStream 2.0

Amazon AppStream 2.0 is a fully managed, secure application streaming service that allows you to stream desktop applications from AWS to a web browser.

[External link](#)

WorkSpaces Web

Amazon WorkSpaces Web is a low-cost, fully managed WorkSpace built to deliver secure web-based workloads and software-as-a-service (SaaS) application access to users within existing web browsers.

Note: When creating a new WorkSpaces Web portal for your environment, you will be taken to the WorkSpaces Web console. Amazon Thin Client requires certain WorkSpaces Web configuration to be compatible. For more information and help with setup, please refer to the [Create a WorkSpace](#) for Amazon Thin Client tutorial.

WorkSpaces Web (0) [Info](#)

Amazon WorkSpaces Web is a low-cost, fully managed WorkSpace built to deliver secure web-based workloads and software-as-a-service (SaaS) application access to users within existing web browsers.

[Create WorkSpace Web](#)

< 1 >

	Display name ▼	Status ▼	Web portal endpoint ▼	VPC ▼	Created at ▼
<input type="radio"/>	Name 1	✔ Active	amazon.awsapp.com	vpc-name	January 31, 2010, 14:32 (UTC+3:30)
<input type="radio"/>	Name 2	✔ Active	amazon.awsapp.com	vpc-name	January 31, 2010, 14:32 (UTC+3:30)
<input checked="" type="radio"/>	Name 3	✔ Active	amazon.awsapp.com	vpc-name	January 31, 2010, 14:32 (UTC+3:30)
<input type="radio"/>	Name 4	✔ Active	amazon.awsapp.com	vpc-name	January 31, 2010, 14:32 (UTC+3:30)
<input type="radio"/>	Name 5	✔ Active	amazon.awsapp.com	vpc-name	January 31, 2010, 14:32 (UTC+3:30)

Cancel

Create environment

Depois de criar seu ambiente, você ainda pode editar os detalhes posteriormente. Para obter mais informações, consulte [Editar um ambiente](#).

Etapa 3: enviar o código de ativação aos usuários de dispositivos

Depois de configurar seu ambiente e serviço de desktop virtual, você receberá um código de ativação exclusivo para sua configuração no AWS Management Console.

Forneça esse código de ativação a qualquer usuário do dispositivo WorkSpaces Thin Client e ele poderá usá-lo para acessar seu desktop virtual.

Consulte o [Guia do usuário do WorkSpaces Thin Client](#) para obter informações adicionais sobre como ajudar o usuário do seu dispositivo a configurar seu Amazon WorkSpaces Thin Client.

Editar um ambiente

O console de administração do WorkSpaces Thin Client gerencia ambientes de desktop virtual para usuários individuais. Nesse console, você pode editar ou excluir ambientes de desktop virtual.

1. Selecione o ambiente que você deseja editar.

Note

Você pode navegar pela lista suspensa ou pesquisar os ambientes usando o campo de pesquisa.

2. Selecione o botão Ações.
3. Selecione Editar na lista suspensa. Você será direcionado para a janela Editar ambiente.
4. Edite qualquer um dos seguintes elementos:
 - Altere o nome do seu ambiente no campo Nome do ambiente.
 - Altere a caixa de seleção dos detalhes das atualizações de software para atualizações automáticas de patches de software.
 - Altere o período agendado para a janela de manutenção do seu ambiente.
5. Selecione o botão Editar ambiente.

Excluir um ambiente

Note

Você não poderá excluir um ambiente se não houver dispositivos registrados nele. Primeiro, você precisa [cancelar o registro](#) e [excluir](#) todos os dispositivos de um ambiente.

1. Selecione o ambiente que você deseja excluir. Você pode navegar pela lista suspensa ou pesquisar os ambientes usando o campo de pesquisa.

2. Selecione o botão Ações.
3. Selecione Excluir na lista suspensa. A janela de confirmação de exclusão do ambiente é exibida.
4. Digite “excluir” no campo de confirmação.
5. Selecione o botão Excluir.

Dispositivos

Cada usuário final do WorkSpaces Thin Client tem um dispositivo dedicado que o conecta a seus ambientes de desktop virtual e recursos on-line. Esses dispositivos são gerenciados por meio do console do administrador do WorkSpaces Thin Client no [AWS site](#).

Nesse console, você pode solicitar dispositivos para sua equipe.

Lista de dispositivos

Detalhes da lista de dispositivos

ID do dispositivo: o número de identificação atribuído a um dispositivo individual.

Nome do dispositivo - (opcional) O nome exclusivo que você atribui a um dispositivo.

Status da atividade - O status atual de um dispositivo. Há dois estados de status:

- Ativo: conectado a uma rede pelo menos uma vez nos últimos sete dias.
- Inativo: não conectado a uma rede nos últimos sete dias.

Status da inscrição - Confirmação de que um dispositivo foi configurado, está associado a essa AWS conta e faz parte de um ambiente específico. Ele pode estar em um dos seguintes estados:

- Registrado - Esse é o status padrão.
- Cancelamento do registro - O dispositivo está no processo de redefinição e cancelamento do registro.

Note

Você pode excluir um dispositivo se ele estiver em um estado de cancelamento de registro.

- Registro cancelado: o registro do dispositivo foi cancelado com êxito.

 Note

Você só pode excluir um dispositivo se ele estiver com o status Cancelado ou Cancelado.

- Arquivado: o dispositivo está arquivado.

ID do ambiente: o identificador do ambiente ao qual esse dispositivo está conectado.

Conformidade de software: o status de conformidade do software do dispositivo. Há dois estados de status:

- Compatível
- Não compatível

Ações da lista de dispositivos

Pesquisar: pesquisa todos os dispositivos que você gerencia.

Atualizar: atualiza a lista de dispositivos.

Visualizar detalhes: exibe os detalhes do dispositivo.

Ações - Abre uma lista suspensa na qual você pode fazer o seguinte:

- Editar o nome do dispositivo
- Cancelar registro
- Arquivo
- Delete
- Exportar os detalhes do dispositivo

Solicitar dispositivos: inicia o processo de solicitação de dispositivos.

Tópicos

- [Detalhes do dispositivo](#)
- [Editar o nome do dispositivo](#)

- [Redefinir e cancelar o registro de um dispositivo](#)
- [Arquivar um dispositivo](#)
- [Excluir um dispositivo](#)
- [Exportar os detalhes do dispositivo](#)

Detalhes do dispositivo

Resumo

Número de série do dispositivo - O número de identificação atribuído a um dispositivo individual.

ARN - O identificador exclusivo do dispositivo no formato Amazon Resource Name (ARN).

Nome do dispositivo - O nome que você dá a um dispositivo. Se você não criou um nome, pode nomeá-lo ou ele receberá um nome padrão.

Tipo de dispositivo - O tipo de dispositivo do usuário final vinculado à conta.

Status da atividade: o status atual do dispositivo. Os dois estados de status são:

- Ativo
- Inativa

ID do ambiente - O número de identificação do ambiente que o dispositivo usa.

Status da inscrição - Confirmação de que um dispositivo foi configurado, está associado a essa AWS conta e faz parte de um ambiente específico. Ele pode estar em um dos quatro estados a seguir:

- Registrado - Esse é o status padrão.
- Cancelamento do registro - O dispositivo está no processo de redefinição e cancelamento do registro.
- Registro cancelado: o registro do dispositivo foi cancelado com êxito.

Note

Você só pode excluir o dispositivo se ele estiver com o status Cancelado ou Arquivado.

- Arquivado - Este dispositivo foi marcado pelo administrador como não em serviço no momento.

Inscrito desde: a data em que o dispositivo foi ativado.

Último login em: a data e a hora do login mais recente.

Última postura verificada em - A data e a hora do check-in mais recente do dispositivo.

Versão atual do software: a versão do software usada no dispositivo.

Programada para atualização de software - A versão programada do software no dispositivo.

Conformidade de software: confirmação de que o conjunto de software é válido. Há dois estados de status:

- Compatível
- Não compatível

Log do usuário

Último acesso ao dispositivo - A data e a hora em que esse dispositivo foi usado pela última vez.

Editar o nome do dispositivo

1. Selecione o dispositivo a ser editado. Você pode navegar pela lista suspensa ou pesquisar o dispositivo usando o campo de pesquisa.
2. Selecione o botão Ações.
3. Selecione Editar nome do dispositivo na lista suspensa. A janela Editar nome do dispositivo é exibida.
4. Insira o novo nome do dispositivo no campo de confirmação Nome do dispositivo.
5. Selecione o botão Salvar.

Redefinir e cancelar o registro de um dispositivo

1. Selecione o dispositivo para o qual deseja cancelar o registro. Você pode navegar pela lista suspensa ou pesquisar o dispositivo usando o campo de pesquisa.
2. Selecione o botão Ações.
3. Selecione Cancelar registro na lista suspensa. A janela Cancelar registro é exibida.
4. Insira "cancelar registro" no campo de confirmação.
5. Selecione o botão Cancelar registro.

Note

O cancelamento do registro desconecta o usuário à força e exige a reinicialização do dispositivo WorkSpaces Thin Client no meio de uma sessão.

Arquivar um dispositivo

1. Selecione o dispositivo que você deseja arquivar. Você pode navegar pela lista suspensa ou pesquisar o dispositivo usando o campo de pesquisa.
2. Selecione o botão Ações.
3. Selecione Arquivar na lista suspensa. A janela Arquivamento é exibida.
4. Insira “redefinir e arquivar” no campo de confirmação.
5. Selecione o botão Redefinir e arquivar.

Note

O arquivamento forçado de um dispositivo desconecta o usuário e exige a reinicialização do dispositivo WorkSpaces Thin Client no meio de uma sessão.

Excluir um dispositivo

1. Selecione o dispositivo que deseja excluir. Você pode navegar pela lista suspensa ou pesquisar o dispositivo usando o campo de pesquisa.
2. Selecione o botão Ações.
3. Selecione Excluir na lista suspensa. A janela Excluir é exibida.
4. Insira “excluir” no campo de confirmação.
5. Selecione o botão Excluir.

Note

Quando o dispositivo for excluído com sucesso, o usuário deverá devolver o dispositivo WorkSpaces Thin Client à Amazon.

Exportar os detalhes do dispositivo

1. Selecione o dispositivo do qual você deseja exportar os detalhes. Você pode navegar pela lista suspensa ou pesquisar o dispositivo usando o campo de pesquisa.
2. Selecione o botão Ações.
3. Selecione Exportar detalhes do dispositivo na lista suspensa. Os detalhes do download do dispositivo selecionado em formato de planilha.

Atualizações de software

WorkSpaces Às vezes, o Thin Client exige atualizações de software que introduzam novas funcionalidades e apliquem patches de segurança. Essas atualizações são representadas por um conjunto de software versionado.

Um conjunto de software pode conter atualizações dos aplicativos de software ou do sistema operacional do dispositivo WorkSpaces Thin Client. Nesse console, você pode optar por atualizar o software imediatamente ou agendar uma atualização automática durante a janela de manutenção dos ambientes.

Consulte os [conjuntos de software do ambiente WorkSpaces Thin Client](#) para obter a lista dos conjuntos de software lançados.

Tópicos

- [Atualizar o software do ambiente](#)
- [Atualizar o software do dispositivo](#)
- [WorkSpaces Lançamentos do software Thin Client](#)

Atualizar o software do ambiente

WorkSpaces O Thin Client é um serviço de computação de usuário AWS final que fornece aos usuários acesso a desktops virtuais. Esses desktops virtuais são atualizados periodicamente com novos conjuntos de software. Para atualizar o software do ambiente, faça o seguinte:

1. Selecione o conjunto de software na lista em Atualizações de software disponíveis. Para obter uma lista de conjuntos de software, consulte Conjuntos de [software do ambiente WorkSpaces Thin Client](#).

2. Selecione o botão Instalar.
3. Selecione Ambientes na parte superior da página.
4. Selecione o ambiente a ser atualizado na lista na seção Ambientes.
5. Selecione quando atualizar o ambiente em Agendar a atualização escolhendo uma das seguintes opções:
 - Atualizar o software agora: inicia a atualização do software do ambiente em todos os dispositivos registrados.

 Note

A atualização do software agora pode interromper qualquer sessão ativa do usuário.

- Atualize o software durante a janela de manutenção de cada ambiente - Atualiza o software do ambiente durante a janela de manutenção programada do ambiente.
6. Marque a caixa para autorizar a atualização. Essa caixa deve ser marcada para que o software seja atualizado.
 7. Selecione o botão Instalar.

Atualizar o software do dispositivo

WorkSpaces O Thin Client é um serviço de computação de usuário AWS final que fornece um dispositivo thin client que conecta usuários a desktops virtuais dedicados. Esses dispositivos são atualizados periodicamente com novos softwares. Para atualizar o software do dispositivo, faça o seguinte:

1. Selecione o conjunto de software na lista em Atualizações de software disponíveis.
2. Selecione o botão Instalar.
3. Selecione Dispositivo na parte superior da página.
4. Selecione o dispositivo ou dispositivos a serem atualizados na lista na seção Dispositivos. Para obter uma lista de conjuntos de software, consulte Conjuntos de [software do ambiente WorkSpaces Thin Client](#).
5. Selecione quando atualizar o ambiente em Agendar a atualização escolhendo uma das seguintes opções:
 - Atualizar o software agora: atualiza imediatamente o software do dispositivo.

Note

A atualização do software agora pode interromper qualquer sessão ativa do usuário.

- Atualize o software durante a janela de manutenção de cada dispositivo - Atualiza o software do ambiente durante a janela de manutenção programada do dispositivo.
6. Marque a caixa para autorizar a atualização. Essa caixa deve ser marcada para que o software seja atualizado.
 7. Selecione o botão Instalar.

WorkSpaces Lançamentos do software Thin Client

WorkSpaces O Thin Client é um serviço de computação de usuário AWS final que fornece aos usuários acesso a desktops virtuais em um dispositivo. Esses dispositivos são atualizados periodicamente com novos conjuntos de software. A tabela a seguir descreve todos os conjuntos de software lançados. Os administradores podem usar o [console AWS de gerenciamento](#) para visualizar os conjuntos de software disponíveis.

Conjunto de software	Data de lançamento	Alterações
2.5.0	13/06/2024	<ul style="list-style-type: none">• Corrigido o problema em que o dispositivo mostrava brevemente a tela de configuração do teclado e do mouse ao acordar do sono antes de iniciar a sessão.• O botão Início na barra de ferramentas do dispositivo foi renomeado para Entrar.• Melhorias no desempenho das chamadas de áudio/vídeo na sessão.

Conjunto de software	Data de lançamento	Alterações
2.4.3	29/05/2024	<ul style="list-style-type: none">• Correção de dia zero para o problema crítico de segurança CVE-2024-5274 do Chromium.
2.4.2	17/05/2024	<ul style="list-style-type: none">• Correção de dia zero para o problema crítico de segurança CVE-2024-4947 do Chromium.
2.4.1	15/05/2024	<ul style="list-style-type: none">• Correções de dia zero para problemas críticos de segurança do CVE-2024-4671 e CVE-2024-4761 do Chromium.• Corrigido o problema que permitia clicar com o botão direito do mouse nos links da AWS e da Privacidade WorkSpaces na página de login para abrir o navegador em um modo independente.
2.4.0	05-09-2024	<ul style="list-style-type: none">• Foi corrigido um problema que bloqueava “accounts.google.com” e impedia o uso do Google Workspace como IDP para a sessão 2.0. AppStream• A barra de ferramentas de configurações do dispositivo se contrai automaticamente com um clique em qualquer área da tela.

Conjunto de software	Data de lançamento	Alterações
2.3.0	04-05-2024	<ul style="list-style-type: none">• As configurações do dispositivo aparecem em uma barra de ferramentas reduzida, permitindo uma melhor utilização da tela visível.• Agora, os usuários finais podem configurar a duração da espera antes que o dispositivo fique inativo.• Corrigido o problema em que o URL “about:blank” aparecia na segunda tela.• Corrigido o problema que resultava em uma tela branca quando a tela estendida era fechada.• Os níveis de volume definidos pelos usuários finais agora persistem nas reinicializações do dispositivo.
2.2.1	16/02/2024	<ul style="list-style-type: none">• Foi corrigido um problema que ocorria durante o processo de login e impedia que os usuários fizessem login WorkSpaces configurado com a autenticação SAML 2.0.

Conjunto de software	Data de lançamento	Alterações
2.2.0	02-08-2024	<ul style="list-style-type: none">Foi adicionado suporte para teclados ISO com localidades em inglês (Reino Unido), francês, alemão, italiano e espanhol.
2.1.2	26/01/2024	<ul style="list-style-type: none">Correção de dia zero para o problema crítico de segurança CVE-2024-0519 do Chromium.Melhoria na latência do usuário final associada à funcionalidade de bloqueio.Os endpoints internos voltados para o dispositivo são transferidos para o domínio 'thinclient*'.
2.1.1	21-12-2023	<ul style="list-style-type: none">Correção de dia zero para o problema crítico de segurança CVE-2023-7024 do Chromium.
2.1.0	12-20-2023	<ul style="list-style-type: none">Adiciona um botão Início às configurações do dispositivo e ativa o suporte para teclas Meta. Isso permite que os usuários finais invoquem a tela de bloqueio pressionando Meta+L.
2.0.1	12-06-2023	<ul style="list-style-type: none">Correção de dia zero para o problema crítico de segurança CVE-2024-6345 do Chromium.

Conjunto de software	Data de lançamento	Alterações
2.0.0	15-11-2023	<ul style="list-style-type: none">• Lançamento inicial

Usando tags em recursos do WorkSpaces Thin Client

Você pode organizar e gerenciar os recursos do seu WorkSpaces Thin Client atribuindo seus próprios metadados a cada recurso como 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. Você pode usar tags como uma forma simples, mas poderosa, de gerenciar recursos da AWS e organizar 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 dispositivo WorkSpaces Thin Client existente em 15 de julho, as tags não aparecerão em seu relatório de alocação de custos até 1º de agosto. Para obter mais informações, consulte Como [usar tags de alocação de custos](#) no Guia do usuário do AWS Billing.

Note

Para visualizar suas tags de recursos do WorkSpaces Thin Client no Cost Explorer, você deve ativar as tags que você aplicou aos seus recursos do WorkSpaces Thin Client seguindo as instruções em [Ativando Tags de Alocação de Custos Definidas pelo Usuário no Guia do AWS Billing Usuário](#).

As tags aparecem 24 horas após a ativação, mas pode levar de 4 a 5 dias para que os valores associados a essas tags apareçam no Cost Explorer. Além disso, para aparecer e fornecer dados de custo no Cost Explorer, WorkSpaces os recursos do Thin Client que foram marcados devem ser cobrados durante esse período. O Cost Explorer mostra apenas os dados de custo do momento em que as tags foram ativadas. Não há dados de histórico disponíveis no momento.

Recursos que você pode marcar:

- Você pode adicionar tags aos seguintes recursos ao criá-los: ambientes WorkSpaces Thin Client.
- Você pode adicionar tags aos recursos existentes dos seguintes tipos: ambientes, dispositivos e conjuntos de software WorkSpaces Thin Client.

Restrições de tags

- Número máximo de tags por recurso: 50

- Tamanho máximo da chave — 128 caracteres Unicode
- Tamanho máximo do valor — 256 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 o aws : prefixo nos nomes ou valores das tags porque ele está reservado para AWS uso. Você não pode editar nem excluir nomes ou valores de tag com esse prefixo.

Para atualizar as tags de um ambiente existente usando o console

1. Abra o [console do WorkSpaces Thin Client](#).
2. Selecione o Ambiente para abrir sua página de detalhes
3. Selecione a opção Editar.
4. Na seção Tags, faça um ou mais dos seguintes:
 - Para adicionar uma tag, escolha Adicionar nova tag e, em seguida, edite os valores de Chave e Valor.
 - Para atualizar uma tag, edite o valor de Value.
 - Para excluir uma tag, escolha Remover ao lado da tag.
5. Quando terminar de atualizar as tags, escolha Salvar.

Para atualizar as tags de um dispositivo existente usando o console

1. Abra o [console do WorkSpaces Thin Client](#).
2. Selecione o dispositivo para abrir sua página de detalhes.
3. Escolha Tags.
4. Selecione Gerenciar tags.
5. Faça uma ou mais das coisas a seguir:
 - Para adicionar uma tag, escolha Adicionar nova tag e, em seguida, edite os valores de Chave e Valor.
 - Para atualizar uma tag, edite o valor de Value.
 - Para excluir uma tag, escolha Remover ao lado da tag.
6. Quando terminar de atualizar as tags, escolha Salvar.

Para atualizar as tags para uma atualização de software usando o console

1. Abra o [console do WorkSpaces Thin Client](#).
2. Selecione a atualização de software para abrir sua página de detalhes.
3. Na seção Tags, escolha Gerenciar tags.
4. Faça uma ou mais das coisas a seguir:
 - Para adicionar uma tag, escolha Adicionar nova tag e, em seguida, edite os valores de Chave e Valor.
 - Para atualizar uma tag, edite o valor de Value.
 - Para excluir uma tag, escolha Remover ao lado da tag.
5. Quando terminar de atualizar as tags, escolha Salvar.

Segurança no Amazon WorkSpaces Thin Client

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

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de [responsabilidade compartilhada](#) descreve isso como a segurança da nuvem e segurança na nuvem:

- **Segurança da nuvem** — AWS é responsável por proteger a infraestrutura que executa AWS os serviços no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de [AWS](#) de . Para saber mais sobre os programas de conformidade que se aplicam ao Amazon WorkSpaces Thin Client, consulte [AWS Serviços no escopo do programa de conformidade AWS](#) .
- **Segurança na nuvem** — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Essa documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o WorkSpaces Thin Client. Os tópicos a seguir mostram como configurar o WorkSpaces Thin Client para atender aos seus objetivos de segurança e conformidade. Você também pode aprender a usar outros AWS serviços que ajudam você a monitorar e proteger seus recursos do WorkSpaces Thin Client.

Tópicos

- [Proteção de dados no Amazon WorkSpaces Thin Client](#)
- [Gerenciamento de identidade e acesso para Amazon WorkSpaces Thin Client](#)
- [Resiliência no Amazon WorkSpaces Thin Client](#)
- [Análise e gerenciamento de vulnerabilidades no Amazon WorkSpaces Thin Client](#)

Proteção de dados no Amazon WorkSpaces Thin Client

O [modelo de responsabilidade AWS compartilhada](#) se aplica à proteção de dados no Amazon WorkSpaces Thin Client. 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 ter mais informações sobre a privacidade de dados, consulte as [Perguntas frequentes sobre privacidade de dados](#). Para ter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog [AWS Shared Responsibility Model and GDPR](#) no Blog de segurança da AWS .

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, 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 o WorkSpaces Thin Client ou outro Serviços da AWS usando 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, recomendamos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

O Amazon WorkSpaces Thin Client coleta e fornece informações sobre o uso de dispositivos WorkSpaces Thin Client pelo usuário e sua interação com os serviços de desktop virtual. Por

exemplo, memória disponível, diagnósticos de rede, informações de rede, conectividade do dispositivo, credenciais SAML, informações de identificação do dispositivo e relatórios de falhas. Essas informações são usadas para fornecer o serviço e podem ser usadas para melhorar a experiência do usuário com o serviço. Além disso, somente para fornecer o serviço a você, as informações podem ser transferidas para fora da AWS região em que os usuários estão usando o serviço. Processamos essas informações de acordo com o [Aviso AWS de Privacidade](#).

Tópicos

- [Criptografia de dados](#)
- [Criptografia de dados em repouso para Amazon WorkSpaces Thin Client](#)
- [Criptografia em trânsito](#)
- [Gerenciamento de chaves](#)
- [Privacidade de tráfego no trabalho na Internet](#)

Criptografia de dados

WorkSpaces O Thin Client coleta dados de personalização do ambiente e do dispositivo, como configurações do usuário, identificadores de dispositivos, informações do provedor de identidade e identificadores de desktop de streaming. WorkSpaces O Thin Client também coleta registros de data e hora da sessão. Os dados coletados são armazenados no Amazon DynamoDB e no Amazon S3. WorkSpaces O Thin Client usa o AWS Key Management Service (KMS) para criptografia.

Para proteger seu conteúdo, siga estas diretrizes:

- Implemente o acesso com privilégios mínimos e crie funções específicas para serem usadas nas ações do WorkSpaces Thin Client.
- Proteja os dados end-to-end fornecendo uma chave gerenciada pelo cliente, para que o WorkSpaces Thin Client possa criptografar seus dados em repouso com as chaves que você fornece.
- Tenha cuidado ao compartilhar códigos de ativação de ambientes e credenciais de usuários:
 - Os administradores devem fazer login no console do WorkSpaces Thin Client, e os usuários devem fornecer códigos de ativação para a configuração do WorkSpaces Thin Client e usar as credenciais para fazer login na área de trabalho de streaming.
 - Qualquer pessoa com acesso físico pode configurar um WorkSpaces Thin Client, mas não pode iniciar uma sessão a menos que tenha um código de ativação válido e credenciais de usuário para fazer login.

- Os usuários podem encerrar explicitamente suas sessões optando por bloquear a tela, reinicializar ou desligar o dispositivo usando a barra de ferramentas do dispositivo. Isso descarta a sessão do dispositivo e limpa as credenciais da sessão.

WorkSpaces O Thin Client protege conteúdo e metadados por padrão, criptografando todos os dados confidenciais com o KMS. AWS Se houver um erro ao aplicar as configurações existentes, o usuário não poderá acessar novas sessões e os dispositivos não poderão aplicar atualizações de software.

Criptografia de dados em repouso para Amazon WorkSpaces Thin Client

O Amazon WorkSpaces Thin Client fornece criptografia por padrão para proteger dados confidenciais de clientes em repouso usando chaves de criptografia AWS próprias.

- AWS chaves próprias — O Amazon WorkSpaces Thin Client usa essas chaves por padrão para criptografar automaticamente dados de identificação pessoal. Você não pode visualizar, gerenciar ou usar chaves AWS próprias nem auditar seu uso. No entanto, não é necessário tomar nenhuma medida nem alterar qualquer programa para proteger as chaves que criptografam seus dados. Para obter mais informações, consulte [Chaves de propriedade da AWS](#) no Guia do desenvolvedor do AWS Key Management Service.

A criptografia de dados em repouso por padrão ajuda a reduzir a sobrecarga operacional e a complexidade envolvidas na proteção de dados confidenciais. Ao mesmo tempo, ela permite que você crie aplicações seguras que atendam aos rigorosos requisitos regulatórios e de conformidade de criptografia.

Embora você não possa desativar essa camada de criptografia nem selecionar um tipo de criptografia alternativo, você pode adicionar uma segunda camada de criptografia sobre as chaves de criptografia existentes de propriedade da AWS, escolhendo uma chave gerenciada pelo cliente ao criar seu ambiente do Thin Client:

- Chaves gerenciadas pelo cliente — O Amazon WorkSpaces Thin Client oferece suporte ao uso de uma chave simétrica gerenciada pelo cliente que você cria, possui e gerencia para adicionar uma segunda camada de criptografia à criptografia existente AWS . Como você tem controle total dessa camada de criptografia, você pode realizar tarefas como as seguintes:
 - Estabelecer e manter as políticas de chave
 - Estabelecer e manter subsídios e políticas do IAM
 - Habilitar e desabilitar políticas de chaves

- Alternar os materiais de criptografia de chaves
- Adicionar etiquetas
- Criar aliases de chaves
- Chaves de agendamento para exclusão

Para obter mais informações, consulte [chave gerenciada pelo cliente](#) no Guia do desenvolvedor do AWS Key Management Service.

A tabela a seguir resume como o Amazon WorkSpaces Thin Client criptografa dados de identificação pessoal.

Tipo de dados	Criptografia de chave própria da AWS	Criptografia de chave gerenciada pelo cliente (opcional)
Nome do ambiente WorkSpaces Nome do ambiente Thin Client	Habilitado	Habilitado
Nome do dispositivo WorkSpaces Nome do dispositivo Thin Client	Habilitado	Habilitado

Note

O Amazon WorkSpaces Thin Client habilita automaticamente a criptografia em repouso usando chaves AWS próprias para proteger dados de identificação pessoal sem nenhum custo.

No entanto, as cobranças do AWS KMS se aplicam ao uso de uma chave gerenciada pelo cliente. Para obter informações sobre a definição de preço, consulte [Definição de preço do serviço de gerenciamento de chaves da AWS](#).

Como o Amazon WorkSpaces Thin Client usa subsídios no AWS KMS

O Amazon WorkSpaces Thin Client exige uma [concessão](#) para você usar sua chave gerenciada pelo cliente.

Quando você cria um [ambiente WorkSpaces](#) Thin Client criptografado com uma chave gerenciada pelo cliente, o Amazon WorkSpaces Thin Client cria uma concessão em seu nome enviando uma CreateGrant solicitação ao AWS KMS. Os subsídios no AWS KMS são usados para dar ao Amazon WorkSpaces Thin Client acesso a uma chave KMS em uma conta de cliente.

Quando um novo [dispositivo](#) Thin Client é registrado em um [ambiente](#) criptografado WorkSpaces Thin Client com uma chave gerenciada pelo cliente e o nome desse dispositivo é alterado, o Amazon WorkSpaces Thin Client cria uma concessão em seu nome enviando uma CreateGrant solicitação ao AWS KMS. Os subsídios no AWS KMS são usados para dar ao Amazon WorkSpaces Thin Client acesso a uma chave KMS em uma conta de cliente.

O Amazon WorkSpaces Thin Client exige a concessão para usar sua chave gerenciada pelo cliente para as seguintes operações internas:

- Envie solicitações de [descriptografia ao AWS KMS para descriptografar](#) os dados criptografados

Você pode revogar o acesso à concessão ou remover o acesso do serviço à chave gerenciada pelo cliente a qualquer momento. Se você fizer isso, o Amazon WorkSpaces Thin Client não poderá acessar nenhum dos dados criptografados pela chave gerenciada pelo cliente, o que afeta as operações que dependem desses dados. Por exemplo, se você tentar [obter detalhes do ambiente](#) que o Amazon WorkSpaces Thin Client não pode acessar, a operação retornará um AccessDeniedException erro. Além disso, o dispositivo WorkSpaces Thin Client não poderá usar um ambiente WorkSpaces Thin Client.

Crie uma chave gerenciada pelo cliente

Você pode criar uma chave simétrica gerenciada pelo cliente usando o AWS Management Console ou as operações de API do AWS KMS.

Para criar uma chave simétrica gerenciada pelo cliente

Siga as etapas em [Criar chaves do KMS de criptografia simétrica](#) no [Guia do desenvolvedor do AWS Key Management Service](#).

Política de chave

As políticas de chaves controlam o acesso à chave gerenciada pelo seu cliente. Cada chave gerenciada pelo cliente deve ter exatamente uma política de chaves, que contém declarações que determinam quem pode usar a chave e como pode usá-la. Ao criar a chave gerenciada pelo cliente, você pode especificar uma política de chaves. Para obter mais informações, consulte [Controlar o acesso a chaves gerenciadas pelo cliente](#) no [Guia do desenvolvedor do AWS Key Management Service](#).

Para usar sua chave gerenciada pelo cliente com seus recursos do Amazon WorkSpaces Thin Client, as seguintes operações de API devem ser permitidas na política de chaves:

- [kms:DescribeKey](#)— Fornece detalhes da chave gerenciada pelo cliente para que o Amazon WorkSpaces Thin Client possa validar a chave.
- [kms:GenerateDataKey](#): permite usar a chave gerenciada pelo cliente para criptografar os dados.
- [kms:Decrypt](#): permite usar a chave gerenciada pelo cliente para descriptografar os dados.
- [kms:CreateGrant](#): adiciona uma concessão a uma chave gerenciada pelo cliente. Concede acesso de controle a uma chave KMS especificada, que permite acesso às [operações de concessão](#) exigidas pelo Amazon WorkSpaces Thin Client. Para obter mais informações, consulte [Usar concessões](#) no [Guia do desenvolvedor do AWS Key Management Service](#).

Isso permite que o Amazon WorkSpaces Thin Client faça o seguinte:

- Chamar Decrypt para o descriptografar os dados criptografados.

A seguir estão exemplos de declarações de política que você pode adicionar para o Amazon WorkSpaces Thin Client:

```
{
  "Statement": [
    {
      "Sid": "Allow access to principals authorized to use Amazon WorkSpaces Thin Client",
      "Effect": "Allow",
      "Principal": {"AWS": "*"},
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:Decrypt",
```

```

        "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:ViaService": "thinclient.region.amazonaws.com",
            "kms:CallerAccount": "111122223333"
        }
    }
},
{
    "Sid": "Allow access for key administrators",
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
    "Action": ["kms:*"],
    "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
},
{
    "Sid": "Allow read-only access to key metadata to the account",
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
    "Action": [
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "kms:RevokeGrant"
    ],
    "Resource": "*"
}
]
}

```

Para obter mais informações sobre [como especificar permissões em uma política](#), consulte o [Guia do desenvolvedor do AWS Key Management Service](#).

Para obter mais informações sobre [como solucionar problemas de acesso à chave](#), consulte o [Guia do desenvolvedor do AWS Key Management Service](#).

Especificação de uma chave gerenciada pelo cliente para o WorkSpaces Thin Client

Você pode especificar uma chave gerenciada pelo cliente para fornecer uma segunda camada de criptografia para os seguintes recursos:

- WorkSpaces [Ambiente](#) Thin Client

Ao criar um ambiente, você pode especificar a chave de dados fornecendo um `kmsKeyArn`, que o Amazon WorkSpaces Thin Client usa para criptografar os dados pessoais identificáveis.

- `kmsKeyArn`— Um identificador de chave para uma chave gerenciada pelo cliente do AWS KMS. Fornece um ARN da chave.

Quando um novo dispositivo WorkSpaces Thin Client é adicionado ao [Ambiente WorkSpaces](#) Thin Client criptografado com uma chave gerenciada pelo cliente, o Dispositivo WorkSpaces Thin Client herda a configuração da chave gerenciada pelo cliente do Ambiente WorkSpaces Thin Client.

Um [contexto de criptografia](#) é um conjunto opcional de pares de valores-chave que contém informações contextuais adicionais sobre os dados.

AWS O KMS usa o contexto de criptografia como [dados autenticados adicionais](#) para oferecer suporte à criptografia autenticada. Quando você inclui um contexto de criptografia em uma solicitação para criptografar dados, o AWS KMS vincula o contexto de criptografia aos dados criptografados. Para descriptografar dados, inclua o mesmo contexto de criptografia na solicitação.

Contexto de criptografia do Amazon WorkSpaces Thin Client

O Amazon WorkSpaces Thin Client usa o mesmo contexto de criptografia em todas as operações criptográficas do AWS KMS, onde a chave está `aws:thinclient:arn` e o valor é o Amazon Resource Name (ARN).

A seguir está o contexto de criptografia do ambiente:

```
"encryptionContext": {
  "aws:thinclient:arn": "arn:aws:thinclient:region:111122223333:environment/
environment_ID"
}
```

A seguir está o contexto de criptografia do dispositivo:

```
"encryptionContext": {
  "aws:thinclient:arn": "arn:aws:thinclient:region:111122223333:device/device_ID"
}
```

Usar o contexto de criptografia para monitoramento

Ao usar uma chave simétrica gerenciada pelo cliente para criptografar os dados do ambiente e do dispositivo WorkSpaces Thin Client, você também pode usar o contexto de criptografia nos registros e registros de auditoria para identificar como a chave gerenciada pelo cliente está sendo usada. O contexto de criptografia também aparece nos [registros gerados pela AWS CloudTrail ou Amazon CloudWatch Logs](#).

Usar o contexto de criptografia para controlar o acesso à chave gerenciada pelo cliente

Você pode usar o contexto de criptografia nas políticas de chave e políticas do IAM como condições para controlar o acesso à sua chave simétrica gerenciada pelo cliente. Você também pode usar restrições no contexto de criptografia em uma concessão.

O Amazon WorkSpaces Thin Client usa uma restrição de contexto de criptografia nas concessões para controlar o acesso à chave gerenciada pelo cliente em sua conta ou região. A restrição da concessão exige que as operações permitidas pela concessão usem o contexto de criptografia especificado.

Veja a seguir exemplos de declarações de políticas de chave para conceder acesso a uma chave gerenciada pelo cliente para um contexto de criptografia específico. A condição nessa declaração de política exige que a chamada `kms:Decrypt` tenha uma restrição ao contexto de criptografia que especifique o contexto da criptografia.

```
{
  "Sid": "Enable Decrypt to access Thin Client Environment",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"},
  "Action": "kms:Decrypt",
  "Resource": "*",
  "Condition": {
    "StringEquals": {"kms:EncryptionContext:aws:thinclient:arn":
"arn:aws:thinclient:region:111122223333:environment/environment_ID"}
  }
}
```

Monitorando suas chaves de criptografia para o Amazon WorkSpaces Thin Client

Ao usar uma chave gerenciada pelo cliente do AWS KMS com seus recursos do Amazon WorkSpaces Thin Client, você pode usar AWS CloudTrail o Amazon CloudWatch Logs para rastrear solicitações que o Amazon WorkSpaces Thin Client envia para o AWS KMS.

Os exemplos a seguir são AWS CloudTrail eventos para `DescribeKey`, `CreateGrant`, `GenerateDataKeyDecrypt`, `Decrypt` (usando `Grant`) monitorar operações KMS chamadas pelo Amazon WorkSpaces Thin Client para acessar dados criptografados pela chave gerenciada pelo cliente:

Nos exemplos a seguir, você pode ver `encryptionContext` o ambiente WorkSpaces Thin Client. CloudTrail Eventos semelhantes são registrados para o WorkSpaces Thin Client Device.

DescribeKey

O Amazon WorkSpaces Thin Client usa a `DescribeKey` operação para verificar a chave gerenciada pelo cliente AWS KMS.

O evento de exemplo a seguir registra a operação `DescribeKey`:

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2023-11-21T13:43:33Z",
        "mfaAuthenticated": "false"
      }
    },
    "invokedBy": "thinclient.amazonaws.com"
  },
  "eventTime": "2023-11-21T13:44:22Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "DescribeKey",
  "awsRegion": "eu-west-1",
```

```

    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {"keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"},
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
      {
        "accountId": "111122223333",
        "type": "AWS::KMS::Key",
        "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
      }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
  }

```

CreateGrant

O Amazon WorkSpaces Thin Client usa a CreateGrant operação para criar uma concessão KMS, que permite descriptografar dados quando o dispositivo os está acessando.

O evento de exemplo a seguir registra a operação CreateGrant:

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "userName": "Admin"
      }
    }
  }
}

```

```
    },
    "webIdFederationData": {},
    "attributes": {
      "creationDate": "2023-11-21T13:43:33Z",
      "mfaAuthenticated": "false"
    }
  },
  "invokedBy": "thinclient.amazonaws.com"
},
"eventTime": "2023-11-21T13:44:23Z",
"eventSource": "kms.amazonaws.com",
"eventName": "CreateGrant",
"awsRegion": "eu-west-1",
"sourceIPAddress": "thinclient.amazonaws.com",
"userAgent": "thinclient.amazonaws.com",
"requestParameters": {
  "granteePrincipal": "thinclient.eu-west-1.amazonaws.com",
  "operations": ["Decrypt"],
  "retiringPrincipal": "thinclient.eu-west-1.amazonaws.com",
  "constraints": {
    "encryptionContextSubset": {"aws:thinclient:arn":
"arn:aws:thinclient:eu-west-1:111122223333:environment/abcSAMPLE"}
  },
  "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
},
"responseElements": {
  "grantId":
"0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
  "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
},
"requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
"eventID": "ffa00af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
"readOnly": false,
"resources": [
  {
    "accountId": "111122223333",
    "type": "AWS::KMS::Key",
    "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
  }
],
"eventType": "AwsApiCall",
```

```

"managementEvent": true,
"recipientAccountId": "111122223333",
"eventCategory": "Management"
}

```

GenerateDataKey

O Amazon WorkSpaces Thin Client usa a GenerateDataKey operação para criptografar dados.

O evento de exemplo a seguir registra a operação GenerateDataKey:

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2024-03-12T12:21:03Z",
        "mfaAuthenticated": "false"
      }
    },
    "invokedBy": "thinclient.amazonaws.com"
  },
  "eventTime": "2024-03-12T13:03:56Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "GenerateDataKey",
  "awsRegion": "eu-west-1",
  "sourceIPAddress": "thinclient.amazonaws.com",
  "userAgent": "thinclient.amazonaws.com",
  "requestParameters": {
    "keyId": "arn:aws:kms:eu-west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",

```

```

    "encryptionContext": {
      "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
      "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
    },
    "numberOfBytes": 32
  },
  "responseElements": null,
  "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
  "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
  "readOnly": true,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "eventCategory": "Management"
}

```

Decrypt

O Amazon WorkSpaces Thin Client usa a Decrypt operação para descriptografar dados.

O evento de exemplo a seguir registra a operação Decrypt:

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",

```

```
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "userName": "Admin"
    },
    "webIdFederationData": {},
    "attributes": {
        "creationDate": "2023-11-21T13:43:33Z",
        "mfaAuthenticated": "false"
    }
},
"invokedBy": "thinclient.amazonaws.com"
},
"eventTime": "2023-11-21T13:44:25Z",
"eventSource": "kms.amazonaws.com",
"eventName": "Decrypt",
"awsRegion": "eu-west-1",
"sourceIPAddress": "thinclient.amazonaws.com",
"userAgent": "thinclient.amazonaws.com",
"requestParameters": {
    "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "encryptionContext": {
        "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
        "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
    },
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
},
"responseElements": null,
"requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
"eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
"readOnly": true,
"resources": [
    {
        "accountId": "111122223333",
        "type": "AWS::KMS::Key",
        "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111122223333",
```

```

    "eventCategory": "Management"
  }

```

Decrypt (using Grant)

Quando o WorkSpaces Thin Client Device acessa as informações do ambiente ou do dispositivo, a Decrypt operação é usada, o que é permitido por meio de uma chave KMS. Grant

O exemplo de evento a seguir registra a Decrypt operação, autorizada por meio deGrant:

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AWSService",
    "invokedBy": "thinclient.amazonaws.com"
  },
  "eventTime": "2023-11-21T13:44:23Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "Decrypt",
  "awsRegion": "eu-west-1",
  "sourceIPAddress": "thinclient.amazonaws.com",
  "userAgent": "thinclient.amazonaws.com",
  "requestParameters": {
    "encryptionContext": {
      "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
      "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
    },
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
    "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
  },
  "responseElements": null,
  "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
  "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
  "readOnly": true,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    }
  ]
}

```

```
  ],  
  "eventType": "AwsApiCall",  
  "managementEvent": true,  
  "recipientAccountId": "111122223333",  
  "sharedEventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",  
  "eventCategory": "Management"  
}
```

Saiba mais

Os recursos a seguir fornecem mais informações sobre a criptografia de dados em pausa:

- Para obter mais informações sobre os [conceitos básicos do AWS Key Management Service](#), consulte o [Guia do desenvolvedor do AWS Key Management Service](#).
- Para obter mais informações sobre [as melhores práticas de segurança do AWS Key Management Service](#), consulte o [AWS Key Management Service Developer Guide](#).

Criptografia em trânsito

WorkSpaces O Thin Client criptografa dados em trânsito por HTTPS e TLS 1.2. Você pode enviar uma solicitação para o WorkSpaces Thin Client usando o console ou chamadas diretas de API. Os dados da solicitação transferidos são criptografados enviando-os por meio de uma conexão HTTPS ou TLS. Os dados da solicitação podem ser transferidos do AWS console, da interface de linha de comando ou do AWS SDK para o WorkSpaces Thin Client. Isso também inclui todas as atualizações de software no dispositivo.

A criptografia em trânsito é configurada por padrão, e as conexões seguras (HTTPS, TLS) são configuradas por padrão.

Gerenciamento de chaves

Você pode fornecer sua própria chave AWS KMS gerenciada pelo cliente para criptografar as informações do cliente. Se você não fornecer uma chave, o WorkSpaces Thin Client usa uma AWS chave própria. Você pode definir sua chave usando o AWS SDK.

Privacidade de tráfego no trabalho na Internet

Os administradores podem visualizar os eventos da sessão do WorkSpaces Thin Client, incluindo horários de início e informações de atualização de software pendentes. Esses registros são

criptografados e entregues com segurança aos clientes no console do WorkSpaces Thin Client. As informações do usuário e mais detalhes sobre sessões individuais de streaming para desktop são registradas pelos serviços de desktop. Para obter mais informações, consulte [Monitore seu WorkSpaces](#), [Monitoring and Reporting for AppStream 2.0](#) ou [Registro de acesso do usuário](#) para a WorkSpaces Web.

Gerenciamento de identidade e acesso para Amazon WorkSpaces Thin Client

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

Tópicos

- [Público](#)
- [Autenticando com identidades](#)
- [Gerenciamento do acesso usando políticas](#)
- [Como o Amazon WorkSpaces Thin Client funciona com o IAM](#)
- [Exemplos de políticas baseadas em identidade para o Amazon Thin Client WorkSpaces](#)
- [Solução de problemas de identidade e acesso ao Amazon WorkSpaces Thin Client](#)

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no WorkSpaces Thin Client.

Usuário do serviço — Se você usa o serviço WorkSpaces Thin Client para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais recursos do WorkSpaces Thin Client para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudá-lo a solicitar as permissões corretas ao seu administrador. Se você não conseguir acessar um recurso no WorkSpaces Thin Client, consulte [Solução de problemas de identidade e acesso ao Amazon WorkSpaces Thin Client](#).

Administrador de serviços — Se você é responsável pelos recursos do WorkSpaces Thin Client em sua empresa, provavelmente tem acesso total ao WorkSpaces Thin Client. É seu trabalho determinar quais recursos e recursos do WorkSpaces Thin Client seus usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como sua empresa pode usar o IAM com o WorkSpaces Thin Client, consulte [Como o Amazon WorkSpaces Thin Client funciona com o IAM](#).

Administrador do IAM — Se você for administrador do IAM, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso ao WorkSpaces Thin Client. Para ver exemplos de políticas baseadas em identidade do WorkSpaces Thin Client que você pode usar no IAM, consulte [Exemplos de políticas baseadas em identidade para o Amazon Thin Client WorkSpaces](#)

Autenticando com identidades

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

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

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

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

Independentemente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação

multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte [Autenticação multifator](#) no Guia do usuário do AWS IAM Identity Center e [Usar a autenticação multifator \(MFA\) na AWS](#) no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele pode executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte [Tarefas que exigem credenciais de usuário raiz](#) no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas acessam Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte [O que é o Centro de Identidade do IAM?](#) no Guia do usuário do AWS IAM Identity Center .

Grupos e usuários do IAM

Um [usuário do IAM](#) é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos depender de credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais

informações, consulte [Altere as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo](#) no Guia do usuário do IAM.

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

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte [Quando criar um usuário do IAM \(em vez de uma função\)](#) no Guia do usuário do IAM.

Perfis do IAM

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

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

- **Acesso de usuário federado:** para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte [Criar uma função para um provedor de identidade de terceiros](#) no Guia do usuário do IAM. Se você usar o IAM Identity Center, deverá configurar um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte [Conjuntos de permissões](#) no Guia do usuário do AWS IAM Identity Center .
- **Permissões temporárias para usuários do IAM:** um usuário ou um perfil do IAM pode assumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- **Acesso entre contas:** é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma

de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte [Como os perfis do IAM diferem das políticas baseadas em recurso](#) no Guia do usuário do IAM.

- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões da entidade principal da chamada por meio de um perfil de serviço ou um perfil vinculado ao serviço.
- Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte [Encaminhar sessões de acesso](#).
- Perfil de serviço: é um [perfil do IAM](#) que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte [Criar uma função para delegar permissões a um AWS service \(Serviço da AWS\)](#) no Guia do usuário do IAM.
- Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um AWS service (Serviço da AWS). O serviço pode assumir o perfil para executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode exibir, mas não pode editar as permissões para perfis vinculados ao serviço.
- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. É preferível fazer isso e armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte [Uso de uma função do IAM](#)

[para conceder permissões a aplicações em execução em instâncias do Amazon EC2](#) no Guia do usuário do IAM.

Para saber se deseja usar perfis do IAM ou usuários do IAM, consulte [Quando criar uma função do IAM \(em vez de um usuário\)](#) no Guia do usuário do IAM.

Gerenciamento do acesso usando políticas

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

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

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

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

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte [Criação de política do IAM](#) no Guia do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda mais como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário,

grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte [Escolher entre políticas gerenciadas e políticas em linha](#) no Guia do usuário do IAM.

Políticas baseadas em recurso

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

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

Listas de controle de acesso (ACLs)

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

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

Outros tipos de política

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

- **Limites de permissões:** um limite de permissões é um atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade e dos seus limites de permissões. As políticas baseadas em recurso que especificam o

usuário ou perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte [Limites de permissões para identidades do IAM](#) no Guia do usuário do IAM.

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

Vários tipos de política

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

Como o Amazon WorkSpaces Thin Client funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao WorkSpaces Thin Client, saiba quais recursos do IAM estão disponíveis para uso com o WorkSpaces Thin Client.

Recursos do IAM que você pode usar com o Amazon WorkSpaces Thin Client

Recurso do IAM	WorkSpaces Suporte ao Thin Client
Políticas baseadas em identidade	Sim

Recurso do IAM	WorkSpaces Suporte ao Thin Client
Políticas baseadas em recurso	Não
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de políticas	Sim
ACLs	Não
ABAC (tags em políticas)	Sim
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Não
Perfis vinculados ao serviço	Não

Para ter uma visão de alto nível de como o WorkSpaces Thin Client e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte [AWS os serviços que funcionam com o IAM](#) no Guia do usuário do IAM.

Políticas baseadas em identidade para WorkSpaces Thin Client

É compatível com políticas baseadas em identidade	Sim
---	-----

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

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou função à qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte [Referência de elementos da política JSON do IAM](#) no Guia do Usuário do IAM.

Exemplos de políticas baseadas em identidade para WorkSpaces Thin Client

Para ver exemplos de políticas baseadas em identidade do WorkSpaces Thin Client, consulte. [Exemplos de políticas baseadas em identidade para o Amazon Thin Client WorkSpaces](#)

Políticas baseadas em recursos no Thin Client WorkSpaces

Oferece suporte a políticas baseadas em recurso	Não
---	-----

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

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recurso. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma outra política baseada em identidade será necessária. Para obter mais informações, consulte [Como os perfis do IAM diferem de políticas baseadas em recursos](#) no Guia do usuário do IAM.

Ações políticas para WorkSpaces Thin Client

Oferece suporte a ações de políticas	Sim
--------------------------------------	-----

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

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

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

Para ver uma lista de ações do WorkSpaces Thin Client, consulte [Ações definidas pelo Amazon WorkSpaces Thin Client](#) na Referência de autorização de serviço.

As ações de política no WorkSpaces Thin Client usam o seguinte prefixo antes da ação:

```
workspaces-thin-client
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas, conforme mostrado no exemplo a seguir:

```
"Action": [  
  "workspaces-thin-client:action1",  
  "workspaces-thin-client:action2"  
]
```

Para ver exemplos de políticas baseadas em identidade do WorkSpaces Thin Client, consulte [Exemplos de políticas baseadas em identidade para o Amazon Thin Client WorkSpaces](#)

Recursos de política para WorkSpaces Thin Client

Oferece suporte a recursos de políticas	Sim
---	-----

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

O elemento de política `Resource` JSON especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou um elemento `NotResource`. Como prática recomendada, especifique um recurso usando seu [nome do recurso da Amazon \(ARN\)](#). Isso pode ser feito para ações que oferecem suporte a um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem suporte a permissões em nível de recurso, como operações de listagem, use um caractere curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Para ver uma lista dos tipos de recursos do WorkSpaces Thin Client e seus ARNs, consulte [Recursos definidos pelo Amazon WorkSpaces Thin Client](#) na Referência de autorização de serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte [Ações definidas pelo Amazon WorkSpaces Thin Client](#).

Para ver exemplos de políticas baseadas em identidade do WorkSpaces Thin Client, consulte [Exemplos de políticas baseadas em identidade para o Amazon Thin Client WorkSpaces](#)

Chaves de condição de política para WorkSpaces Thin Client

Compatível com chaves de condição de política específicas do serviço	Sim
--	-----

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

O elemento `Condition` (ou bloco de `Condition`) permite que você especifique condições nas quais uma instrução está em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usam [atendentes de condição](#), como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único elemento `Condition`, a AWS os avaliará usando uma operação lógica AND. Se você especificar

vários valores para uma única chave de condição, AWS avalia a condição usando uma OR operação lógica. Todas as condições devem ser atendidas para que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar as condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte [Elementos de política do IAM: variáveis e tags](#) no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as [chaves de contexto de condição AWS global](#) no Guia do usuário do IAM.

Para ver uma lista das chaves de condição do WorkSpaces Thin Client, consulte [Chaves de condição do Amazon WorkSpaces Thin Client](#) na Referência de autorização de serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte [Ações definidas pelo Amazon WorkSpaces Thin Client](#).

Para ver exemplos de políticas baseadas em identidade do WorkSpaces Thin Client, consulte [Exemplos de políticas baseadas em identidade para o Amazon Thin Client WorkSpaces](#)

ACLs no WorkSpaces Thin Client

Oferece suporte a ACLs	Não
------------------------	-----

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

ABAC com WorkSpaces Thin Client

Oferece suporte a ABAC (tags em políticas)	Sim
--	-----

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. A marcação de entidades

e recursos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela está tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no [elemento de condição](#) de uma política usando as `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys` chaves de condição.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial.

Para obter mais informações sobre o ABAC, consulte [O que é ABAC?](#) no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte [Usar controle de acesso baseado em atributos \(ABAC\)](#) no Guia do usuário do IAM.

Usando credenciais temporárias com o WorkSpaces Thin Client

Oferece suporte a credenciais temporárias	Sim
---	-----

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS [“Trabalhe com o IAM”](#) no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar perfis, consulte [Alternar para uma função \(console\)](#) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte [Credenciais de segurança temporárias no IAM](#).

Permissões principais entre serviços para WorkSpaces Thin Client

Suporte para o recurso Encaminhamento de sessões de acesso (FAS) Sim

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte [Encaminhar sessões de acesso](#).

Funções de serviço para WorkSpaces Thin Client

Oferece suporte a perfis de serviço Não

O perfil de serviço é um [perfil do IAM](#) que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte [Criar uma função para delegar permissões a um AWS service \(Serviço da AWS\)](#) no Guia do usuário do IAM.

Warning

Alterar as permissões de uma função de serviço pode interromper a funcionalidade do WorkSpaces Thin Client. Edite as funções de serviço somente quando o WorkSpaces Thin Client fornecer orientação para fazer isso.

Funções vinculadas a serviços para Thin Client WorkSpaces

Oferece suporte a perfis vinculados ao serviço Não

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um AWS service (Serviço da AWS). O serviço pode assumir o perfil para executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode exibir, mas não pode editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre como criar ou gerenciar funções vinculadas a serviços, consulte Serviços do [AWS que funcionam com o IAM](#). Encontre um serviço na tabela que inclua um Yes na coluna Perfil vinculado ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a esse serviço.

Exemplos de políticas baseadas em identidade para o Amazon Thin Client WorkSpaces

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do WorkSpaces Thin Client. Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder aos usuários permissões para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis, e os usuários podem assumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte [Criação de políticas do IAM](#) no Guia do Usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pelo WorkSpaces Thin Client, incluindo o formato dos ARNs para cada um dos tipos de recursos, consulte [Ações, recursos e chaves de condição para o Amazon WorkSpaces Thin Client](#) na Referência de autorização de serviço.

Tópicos

- [Práticas recomendadas de políticas](#)
- [Usando o console WorkSpaces Thin Client](#)
- [Conceda acesso somente de leitura ao Thin Client WorkSpaces](#)
- [Permitir que os usuários visualizem suas próprias permissões](#)
- [Conceda acesso total ao WorkSpaces Thin Client](#)

Práticas recomendadas de políticas

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

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

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

Usando o console WorkSpaces Thin Client

Para acessar o console do Amazon WorkSpaces Thin Client, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do WorkSpaces Thin Client em seu Conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva do que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente a ações que correspondam a operação de API que estiverem tentando executar.

Conceda acesso somente de leitura ao Thin Client WorkSpaces

Este exemplo mostra como você pode criar uma política que permite que os usuários do IAM visualizem uma configuração do WorkSpaces Thin Client, mas não façam alterações. Essa política inclui permissões para concluir essa ação no console ou no programa usando a AWS CLI ou a API da AWS.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "thinclient:GetEnvironment",
        "thinclient:ListEnvironments",
        "thinclient:GetDevice",
        "thinclient:ListDevices",
        "thinclient:ListDeviceSessions",
        "thinclient:GetSoftwareSet",
        "thinclient:ListSoftwareSets",
        "thinclient:ListTagsForResource"
      ],
      "Resource": "arn:aws:thinclient:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": ["workspaces:DescribeWorkspaceDirectories"],
```

```

    "Resource": "arn:aws:workspaces:*:*:directory/*"
  },
  {
    "Effect": "Allow",
    "Action": ["workspaces-web:GetPortal"],
    "Resource": ["arn:aws:workspaces-web:*:*:portal/*"]
  },
  {
    "Effect": "Allow",
    "Action": ["workspaces-web:GetUserSettings"],
    "Resource": ["arn:aws:workspaces-web:*:*:userSettings/*"]
  },
  {
    "Effect": "Allow",
    "Action": ["appstream:DescribeStacks"],
    "Resource": ["arn:aws:appstream:*:*:stack/*"]
  }
]
}

```

Permitir que os usuários visualizem suas próprias permissões

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

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam:*:*:user/${aws:username}"]
    },
    {

```

```

    "Sid": "NavigateInConsole",
    "Effect": "Allow",
    "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
}

```

Conceda acesso total ao WorkSpaces Thin Client

Este exemplo mostra como você pode criar uma política que conceda acesso total aos usuários do WorkSpaces Thin Client IAM. Essa política inclui permissões para concluir todas as ações do WorkSpaces Thin Client no console ou no programa usando a AWS CLI ou a API da AWS.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["thinclient:*"],
      "Resource": "arn:aws:thinclient:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": ["workspaces:DescribeWorkspaceDirectories"],
      "Resource": "arn:aws:workspaces:*:*:directory/*"
    },
    {
      "Effect": "Allow",
      "Action": ["workspaces-web:GetPortal"],
      "Resource": ["arn:aws:workspaces-web:*:*:portal/*"]
    },
    {
      "Effect": "Allow",

```

```
    "Action": ["workspaces-web:GetUserSettings"],
    "Resource": ["arn:aws:workspaces-web:*:*:userSettings/*"]
  },
  {
    "Effect": "Allow",
    "Action": ["appstream:DescribeStacks"],
    "Resource": ["arn:aws:appstream:*:*:stack/*"]
  }
]
```

Solução de problemas de identidade e acesso ao Amazon WorkSpaces Thin Client

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o WorkSpaces Thin Client e o IAM.

Tópicos

- [Não estou autorizado a realizar uma ação no WorkSpaces Thin Client](#)
- [Quero visualizar minhas chaves de acesso](#)
- [Sou administrador e quero permitir que outras pessoas acessem o WorkSpaces Thin Client](#)
- [Quero permitir que pessoas fora da minha acessem meus Conta da AWS recursos do WorkSpaces Thin Client](#)

Não estou autorizado a realizar uma ação no WorkSpaces Thin Client

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

O erro do exemplo a seguir ocorre quando o usuário do IAM mateojackson tenta usar o console para visualizar detalhes sobre um recurso do *my-thin-client-device* fictício, mas não tem as permissões fictícias do `workspaces-thin-client:ListDevices`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
workspaces-thin-client:ListDevices on resource: my-thin-client-device
```

Nesse caso, Mateo pede ao administrador que atualize suas políticas para permitir que ele acesse o *my-thin-client-device* recurso usando a `workspaces-thin-client:ListDevices` ação.

Quero visualizar minhas chaves de acesso

Depois de criar suas chaves de acesso de usuário do IAM, é possível visualizar seu ID da chave de acesso a qualquer momento. No entanto, você não pode visualizar sua chave de acesso secreta novamente. Se você perder sua chave secreta, crie um novo par de chaves de acesso.

As chaves de acesso consistem em duas partes: um ID de chave de acesso (por exemplo, AKIAIOSFODNN7EXAMPLE) e uma chave de acesso secreta (por exemplo, wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY). Como um nome de usuário e uma senha, você deve usar o ID da chave de acesso e a chave de acesso secreta em conjunto para autenticar suas solicitações. Gerencie suas chaves de acesso de forma tão segura quanto você gerencia seu nome de usuário e sua senha.

Important

Não forneça as chaves de acesso a terceiros, mesmo que seja para ajudar a [encontrar o ID de usuário canônico](#). Ao fazer isso, você pode dar a alguém acesso permanente ao seu Conta da AWS.

Ao criar um par de chaves de acesso, você é solicitado a guardar o ID da chave de acesso e a chave de acesso secreta em um local seguro. A chave de acesso secreta só está disponível no momento em que é criada. Se você perder sua chave de acesso secreta, será necessário adicionar novas chaves de acesso para seu usuário do IAM. Você pode ter no máximo duas chaves de acesso. Se você já tiver duas, você deverá excluir um par de chaves para poder criar um novo. Para visualizar as instruções, consulte [Gerenciar chaves de acesso](#) no Guia do usuário do IAM.

Sou administrador e quero permitir que outras pessoas acessem o WorkSpaces Thin Client

Para permitir que outras pessoas acessem o WorkSpaces Thin Client, você deve criar uma entidade do IAM (usuário ou função) para a pessoa ou o aplicativo que precisa de acesso. Elas usarão as credenciais dessa entidade para acessar a AWS. Em seguida, você deve anexar uma política à entidade que conceda a ela as permissões corretas no WorkSpaces Thin Client.

Para começar a usar imediatamente, consulte [Criar os primeiros usuário e grupo delegados pelo IAM](#) no Guia do usuário do IAM.

Para ter mais informações, consulte [Conceda acesso total ao WorkSpaces Thin Client](#).

Quero permitir que pessoas fora da minha acessem meus Conta da AWS recursos do WorkSpaces Thin Client

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

Para saber mais, consulte:

- Para saber se o WorkSpaces Thin Client oferece suporte a esses recursos, consulte [Como o Amazon WorkSpaces Thin Client funciona com o IAM](#).
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como [fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui](#) no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como [fornecer acesso Contas da AWS a terceiros](#) no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte [Conceder acesso a usuários autenticados externamente \(federação de identidades\)](#) no Guia do usuário do IAM.
- Para saber a diferença entre usar perfis e políticas baseadas em recursos para acesso entre contas, consulte [Como os perfis do IAM diferem de políticas baseadas em recursos](#) no Guia do usuário do IAM.

Resiliência no Amazon WorkSpaces Thin Client

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que executam o failover automaticamente entre as zonas de disponibilidade sem interrupção. As Zonas de

Disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

Para obter mais informações sobre zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte [Infraestrutura AWS global](#).

Além da infraestrutura AWS global, o WorkSpaces Thin Client oferece vários recursos para ajudar a suportar suas necessidades de resiliência e backup de dados.

Análise e gerenciamento de vulnerabilidades no Amazon WorkSpaces Thin Client

A configuração e os controles de TI são uma responsabilidade compartilhada entre você AWS e você. Para obter mais informações, consulte o [modelo de responsabilidade AWS compartilhada](#).

O Amazon WorkSpaces Thin Client tem integração cruzada com WorkSpaces Amazon, Amazon AppStream 2.0 e WorkSpaces Web. Consulte os links a seguir para obter mais informações sobre o gerenciamento de atualizações para cada um desses serviços:

- [Gerenciamento de atualizações na Amazon AppStream 2.0](#)
- [Gerenciamento de atualizações na Amazon WorkSpaces](#)
- [Análise de configuração e vulnerabilidade na Amazon WorkSpaces Web](#)

Monitoramento do Amazon WorkSpaces Thin Client

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho do Amazon WorkSpaces Thin Client e de suas outras AWS soluções. AWS fornece as seguintes ferramentas de monitoramento para monitorar o WorkSpaces Thin Client, relatar quando algo está errado e realizar ações automáticas quando apropriado:

- AWS CloudTrail captura chamadas de API e eventos relacionados feitos por ou em nome de sua AWS conta e entrega os arquivos de log para o bucket do Amazon S3 que você especificar. Você pode identificar usuários e contas que ligaram AWS, o endereço IP de origem a partir do qual as chamadas foram feitas e quando as chamadas ocorreram. Para obter mais informações, consulte o [Guia do usuário da AWS CloudTrail](#).

Registro de chamadas de API do Amazon WorkSpaces Thin Client usando AWS CloudTrail

O Amazon WorkSpaces Thin Client é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no WorkSpaces Thin Client. CloudTrail captura todas as chamadas de API para o WorkSpaces Thin Client como eventos. As chamadas capturadas incluem chamadas do console do WorkSpaces Thin Client e chamadas de código para as operações da API do WorkSpaces Thin Client. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o WorkSpaces Thin Client. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita ao WorkSpaces Thin Client, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais sobre isso CloudTrail, consulte o [Guia AWS CloudTrail do usuário](#).

WorkSpaces Informações do Thin Client em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre no WorkSpaces Thin Client, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode exibir, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte [Visualização de eventos com histórico de CloudTrail eventos](#).

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

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

Todas as ações do WorkSpaces Thin Client são registradas CloudTrail e documentadas na [Amazon WorkSpaces Thin Client API Reference](#). Por exemplo, chamadas para as `GetSoftwareSet` ações `CreateEnvironmentListDevices`, e geram entradas nos arquivos de CloudTrail log.

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

- Se a solicitação foi feita com credenciais de usuário root ou AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte [Elemento userIdentity do CloudTrail](#).

Compreendendo as entradas do arquivo de log do WorkSpaces Thin Client

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

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a GetDevice ação.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "<principal-id>",
    "arn": "<arn>",
    "accountId": "<account-id>",
    "accessKeyId": "<access-key-id>",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "<principal-id>",
        "arn": "arn:aws:iam::<arn>",
        "accountId": "<accpimt-id>",
        "userName": "<user-name>"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2023-11-18T23:07:01Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-11-18T23:11:57Z",
  "eventSource": "thinclient.amazonaws.com",
  "eventName": "GetDevice",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "<source-ip-address>",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0)
  Gecko/20100101 Firefox/115.0",
  "requestParameters": {
    "id": "<ip>"
  },
  "responseElements": null,
  "requestID": "<request-id>",
  "eventID": "<event-id>",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "<recipient-account-id>",
  "eventCategory": "Management"
}
```

```
}
```

Criação de recursos do Amazon WorkSpaces Thin Client com AWS CloudFormation

O Amazon WorkSpaces Thin Client está integrado com AWS CloudFormation, um serviço que ajuda você a modelar e configurar seus AWS recursos. Dessa forma, você pode passar menos tempo criando e gerenciando recursos e infraestrutura. Você cria um modelo que descreve todos os AWS recursos que você deseja (como Ambientes) e AWS CloudFormation provisiona e configura esses recursos para você.

Ao usar AWS CloudFormation, você pode reutilizar seu modelo para configurar seus recursos do WorkSpaces Thin Client de forma consistente e repetida. Descreva seus recursos uma vez e, em seguida, provisione os mesmos recursos repetidamente em várias Contas da AWS regiões.

WorkSpaces Thin Client e AWS CloudFormation modelos

Para provisionar e configurar recursos para o WorkSpaces Thin Client e serviços relacionados, você deve entender [AWS CloudFormation os modelos](#). Os modelos são arquivos de texto formatados no formato JSON ou YAML. Esses modelos descrevem os recursos que você deseja provisionar em suas AWS CloudFormation pilhas. Se você não estiver familiarizado com os formatos JSON ou YAML, você pode usar o AWS CloudFormation Designer para ajudá-lo a começar a usar modelos. AWS CloudFormation Para obter mais informações, consulte [O que é o AWS CloudFormation Designer?](#) no Manual do usuário da AWS CloudFormation .

WorkSpaces O Thin Client suporta a criação de ambientes em AWS CloudFormation. Para obter mais informações, incluindo exemplos de modelos JSON e YAML para ambientes, consulte a [referência do tipo de recurso Amazon WorkSpaces Thin Client](#) no Guia do AWS CloudFormation usuário.

Saiba mais sobre AWS CloudFormation

Para saber mais sobre isso AWS CloudFormation, consulte os seguintes recursos:

- [AWS CloudFormation](#)
- [AWS CloudFormation Guia do usuário](#)
- [Referência de API do AWS CloudFormation](#)
- [AWS CloudFormation Guia do usuário da interface de linha de comando](#)

Acesse o Amazon WorkSpaces Thin Client usando um endpoint de interface ()AWS PrivateLink

Você pode usar AWS PrivateLink para criar uma conexão privada entre sua VPC e o Amazon WorkSpaces Thin Client. Você pode acessar o WorkSpaces Thin Client como uma VPC, sem o uso de um gateway de internet, dispositivo NAT, conexão VPN ou conexão. AWS Direct Connect As instâncias em sua VPC não exigem endereços IP públicos para acessar o WorkSpaces Thin Client.

Você estabelece essa conexão privada criando um endpoint de interface que é alimentado por AWS PrivateLink. Criaremos um endpoint de interface de rede em cada sub-rede que você habilitar para o endpoint de interface. Essas são interfaces de rede gerenciadas pelo solicitante que servem como ponto de entrada para o tráfego destinado ao Thin Client. WorkSpaces

Para obter mais informações, consulte [Acessar os Serviços da AWS pelo AWS PrivateLink](#) no Guia do AWS PrivateLink .

Considerações sobre o WorkSpaces Thin Client

Antes de configurar um endpoint de interface para o WorkSpaces Thin Client, consulte [as Considerações](#) no AWS PrivateLink Guia.

WorkSpaces O Thin Client oferece suporte para fazer chamadas para todas as suas ações de API por meio do endpoint da interface.

Crie um endpoint de interface para o WorkSpaces Thin Client

Você pode criar um endpoint de interface para o WorkSpaces Thin Client usando o console Amazon VPC ou AWS Command Line Interface o AWS CLI(). Para obter mais informações, consulte [Criar um endpoint de interface](#) no Guia do usuário do AWS PrivateLink .

Crie um endpoint de interface para o WorkSpaces Thin Client usando o seguinte nome de serviço:

```
com.amazonaws.region.thinclient.api
```

Se você habilitar o DNS privado para o endpoint da interface, poderá fazer solicitações de API ao WorkSpaces Thin Client usando seu nome DNS regional padrão. Por exemplo, `api.thinclient.us-east-1.amazonaws.com`.

Criar uma política de endpoint para o endpoint da interface

Política de endpoint é um recurso do IAM que você pode anexar ao endpoint de interface. A política de endpoint padrão oferece acesso total ao WorkSpaces Thin Client por meio do endpoint da interface. Para controlar o acesso concedido ao WorkSpaces Thin Client a partir de sua VPC, anexe uma política de endpoint personalizada ao endpoint da interface.

Uma política de endpoint especifica as seguintes informações:

- Os diretores que podem realizar ações (Contas da AWS usuários do IAM e funções do IAM).
- As ações que podem ser executadas.
- Os recursos nos quais as ações podem ser executadas.

Para obter mais informações, consulte [Controlar o Acesso a Serviços Usando Políticas de Endpoint](#) no AWS PrivateLink Guia.

Exemplo: política de VPC endpoint para ações de Thin Client WorkSpaces

O exemplo a seguir refere-se a uma política de endpoint personalizada. Quando você anexa essa política ao seu endpoint de interface, ela concede acesso às ações do WorkSpaces Thin Client listadas para todos os principais em todos os recursos.

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "thinclient:ListEnvironments",
        "thinclient:ListDevices",
        "thinclient:ListSoftwareSets"
      ],
      "Resource": "*"
    }
  ]
}
```

Histórico de documentos do Guia do Administrador do WorkSpaces Thin Client

A tabela a seguir descreve o histórico da documentação das versões do Guia do Administrador do WorkSpaces Thin Client.

Alteração	Descrição	Data
<ul style="list-style-type: none">• Configuração WorkSpaces para o Amazon WorkSpaces Thin Client• Configuração AppStream 2.0 para o Amazon WorkSpaces Thin Client	<ul style="list-style-type: none">• Atualizou a lista de sistemas operacionais.• Atualizado o procedimento do provedor de identidade.	12 de fevereiro de 2024
Lançamento inicial	Lançamento inicial	26 de novembro de 2023

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.